РЕПУБЛИКА МАКЕДОНИЈА

УНИВЕРЗИТЕТ „Св. КИРИЛ И МЕТОДИЈ“во СКОПЈЕ

ФАКУЛТЕТ ЗА ЕЛЕКТРОТЕХНИКА И ИНФОРМАЦИСКИ ТЕХНОЛОГИИ

Горјан Наџински

РАЗВОЈ НА НОВ ПРОТОКОЛ ЗА БЕЗБЕДНА КОМУНИКАЦИЈА ОТПОРНА НА ШУМ КАЈ ИНДУСТРИСКИ ВМРЕЖЕНИ СИСТЕМИ НА АВТОМАТСКО УПРАВУВАЊЕ

- ДОКТОРСКА ДИСЕРТАЦИЈА–

Скопје, 2018 година

Ментор: **Проф. д-р Миле Станковски**
Универзитет "Св. Кирил и Методиј" – Скопје
Факултет за електротехника и информациски технологии
Институт за автоматика и системско инженерство

Членови на комисијата: **Претседател: Проф. д-р Георги М. Димировски**
Dogus University, Istanbul, Republic of Turkey
Faculty of Engineering
Department of Computer Engineering
Универзитет "Св. Кирил и Методиј" – Скопје
Факултет за електротехника и информациски технологии
Институт за автоматика и системско инженерство

Проф. д-р Драган Антиќ
Универзитет во Ниш - Република Србија
Електронски факултет
Катедра за автоматика

Проф. д-р Елизабета Лазаревска
Универзитет "Св. Кирил и Методиј" – Скопје
Факултет за електротехника и информациски технологии
Институт за автоматика и системско инженерство

Проф. д-р Александар Ристески
Универзитет "Св. Кирил и Методиј" – Скопје
Факултет за електротехника и информациски технологии
Институт за телекомуникации

Дата на одбрана: _____

Дата на промоција: _____

Научна област: Автоматика и системско инженерство

ГОРЈАН НАЦИНСКИ

РАЗВОЈ НА НОВ ПРОТОКОЛ ЗА БЕЗБЕДНА КОМУНИКАЦИЈА ОТПОРНА НА ШУМ КАЈ ИНДУСТРИСКИ ВМРЕЖЕНИ СИСТЕМИ НА АВТОМАТСКО УПРАВУВАЊЕ

АПСТРАКТ: Главната цел на оваа докторска дисертација е зголемувањето на нивото на безбедност на индустриските комуникациски протоколи. Ова е постигнато со развој на алгоритам кој користи функции на спрега помеѓу два динамички системи за енкрипција, и динамичка Баесова инференција за декрипција на податоците. Алгоритамот е искористен за имплементација на комуникациски протокол чија работа е тестирана и верифицирана во присуство на бел и на обоен шум, и во реални експериментални услови. Ваквиот пристап резултира во комуникација која е криптографски безбедна и отпорна на електромагнетен шум, способна да функционира во индустриски услови, и која се одликува со намалени моќности на емитување и енергетска ефикасност.

КЛУЧНИ ЗБОРОВИ: Вмрежени системи на автоматско управување, комуникација во индустриски услови, шум, функции на спрега, динамичка Баесова инференција.

GORJAN NADZINSKI

DEVELOPMENT OF A NOVEL PROTOCOL FOR NOISE-ROBUST AND SECURE COMMUNICATION IN INDUSTRIAL NETWORKED CONTROL SYSTEMS

ABSTRACT: The main goal of this dissertation is to increase the level of safety of industrial communication protocols. Thus, it shows the development of an algorithm which uses coupling functions for encryption and dynamical Bayesian inference for decryption of data. This algorithm is used to implement a communication protocol whose work is tested and verified in the presence of both white Gaussian and colored low frequency noise, and in practical experimental conditions. This results in data transfer which is both cryptographically secure and noise resistant, and thus capable of functioning in real life industrial environments with reduced transmission power levels and increased energy efficiency.

KEY WORDS: Networked control systems, industrial communication, noise, coupling functions, dynamical Bayesian inference.

БЛАГОДАРНОСТ

Изработката на овој докторски труд претставуваше долг и макотрпен процес, но и интересен и неповторлив предизвик. Неговото успешно завршување немаше да биде можно без помошта, поддршката и разбирањето од голем број на луѓе на кои сум им неизмерно благодарен.

Би сакал да ја изразам мојата искрена благодарност на мојот ментор проф. д-р Миле Станковски за неговата безрезервна помош, мотивација, разбирање, и водење кон успешното завршување на оваа докторска дисертација.

Посебна благодарност сакам да му изразам на доц. д-р Томислав Станковски за сесрдната помош, стрпливост и одвоеното време додека ја надгледуваше мојата работа и ме водеше во вистинска насока. Значаен дел од оваа дисертација се заснова на неговата работа, во соработка со колегите од Институтот за физика на Универзитетот во Ланкастер, Велика Британија, и со м-р Матеј Добревски, на кои поради тоа исто така сум им благодарен.

Исто така искрено се заблагодарувам и на колегите од Институтот за автоматика и системско инженерство на Факултетот за електротехника и информациски технологии во Скопје за нивната помош, совети и поддршка во текот на моите докторски студии.

Конечно, најмногу им благодарам и на мојата сестра и на моите родители, за нивното неисцрпно охрабрување што ми го даваа во минативе години.

СОДРЖИНА

ЛИСТА НА СЛИКИ

ЛИСТА НА ТАБЕЛИ

ЛИСТА НА КОРИСТЕНИ КРАТЕНКИ

Кратенка на анг. јазик	Значење на анг. јазик	Кратенка на мак. јазик	Значење на мак. јазик
NCS	Networked control system	ВСАУ	Вмрежен систем на автоматско управување
SNR	Signal-to-noise ratio	/	Однос сигнал-шум
OU	Ornstein-Uhlenbeck noise	/	/
BER	Bit error rate	/	Стапка на грешка во битовите
LMI	Linear matrix inequalities	/	Линеарни матрични неравенства
LQR	Linear quadratic regulator	/	Линеарен квадратен управувач
LQG	Linear quadratic Gaussian control	/	Линеарен квадратен Гаусов управувач
QoS	Quality of service	/	Квалитет на (мрежна) услуга
FTC	Fault tolerant control	/	Управување отпорно на дефекти
IDS	Intrusion detection system	/	Систем за детекција на упад (провала)
TCP	Transmission control protocol	/	/
PID	Proportional-integral-derivative control	ПИД	Пропорционално-интегрирачко-диференцирачки управувач
QIQM	Quantized input from quantized measurements	/	Квантизиран влез кој произлегува од квантизирани мерења
SCADA	Supervisory control and data	/	Систем за надзорно управување и

	acquisition system		собирање на податоци
ELF	Extremely low frequency	/	Екстремно ниска фреквенција
VLF	Very low frequency	/	Многу ниска фреквенција
HF	High frequency	/	Висока фреквенција
SHF	Super high frequency	/	Супер висока фреквенција
EHF	Extremely high frequency	/	Екстремно висока фреквенција
ESD	Electrostatic discharge	/	Електростатско празнење
PLC	Programmable logic controller	ПЛУ	Програмабилен логички управувач
HMI	Human-machine interface	/	Интерфејс помеѓу човек и машина
RTU	Remote terminal unit	/	Оддалечен терминал
IED	Intelligent electronic device	/	Интелигентен електронски уред
DoS	Denial of service attack	/	/
PKI	Public key infrastructure	/	Инфраструктура со јавен (криптографски) клуч

1. ВОВЕД

1.1. Мотивација за изработка на докторската дисертација

Дури и во недостаток на перспективите кои вообичаено ги нуди историската дистанца, рапидниот прогрес на науката и технологијата и неговото влијание во подобрувањето на секојдневниот живот на човекот е очигледен. Присуството на интелигентни уреди (сензори, актуатори, управувачи, интерфејси) во фабриките и во домовите веќе одамна не е преседан туку станува секојдневие и неопходност; додека во човековите живеалишта присуството и вмрежувањето на ваквите уреди нуди безбедност, удобност и други погодности и предности во усовршувањето на квалитетот на секојдневниот живот, во индустријата игра уште поголема и позначајна улога, бидејќи дава огромен и клучен придонес кон подобрувањето на индустриските процеси и на нивната економичност и ефикасност, оптимизацијата на искористените ресурси, и осигурувањето на безбедноста при работа на луѓето инволвирани во процесите.

Индустриските постројки веќе извесно време не се само изолирани комплекси на сложени механички, хемиски, или термодинамички процеси, управувани и погонувани од стандардизирана опрема, која не е способна да го задржи, анализира, протолкува и искористи најголемиот дел од богатството на релевантни сигнали и информации од околината. Напротив, замавот на четвртата индустриска револуција и светските и локалните трендови велат дека денес индустриските постројки се (или забрзано се претвораат во) "живи" ентитети кои комуницираат и соработуваат помеѓу себе, а интелигентните уреди во нив се способни методично да ги прибираат и обработуваат сите процесни податоци од интерес, и со тоа да отворат можности за подобрување на квалитетот на производите и оптимизација на целокупната работа на процесите и постројките, како и на потрошените ресурси.

Без да се обезвреднат улогите на интелигентните уреди, усовршеното производство на управувачка и мерна опрема, микро и нано електромеханичките системи, машинското учење, и методите за работа со огромни количества на податоци (Big Data), сепак може да се каже дека еден од најважните аспекти на оваа нова генерација на системи на управување е комуникацијата. Сензорите, актуаторите и управувачите се дигитални, што значи дека наместо аналогни сигнали во истиот момент, сега разменуваат податочни пакети во конечно ненулево време. Тие податочни пакети можат да се испратат преку кабел или безжично, во локална мрежа или преку Интернет, и освен корисната

информација содржат и останати придружни податоци неопходни од безбедносен или дијагностички аспект.

Сето ова наложува дека веќе има логика да се говори само за *вмрежени* системи на автоматско управување, со сите бенефиции кои тие ги носат од аспект на брзина и ефикасност, но и со проблемите кои се јавуваат како резултат. Нагласениот акцент на комуникацијата како клучен сегмент во овие системи отвора нови ранливости кои претходно не биле присутни. Комуникациските канали сега треба да функционираат во индустриски средини исполнети со шум и интерференција, и да пренесуваат податоци од исклучителна важност, некогаш и преку јавни или недоволно безбедни мрежи. Според тоа, од клучно значење е обезбедувањето на заштита на комуникацијата кај овие системи, и од спонтани изобличувања на податоците предизвикани од околниот шум, но и од намерни и малициозни менувања и/или пресретнувања на нивните вредности.

1.2. Придобивки од докторската дисертација

Предмет на истражувањето во рамките на оваа дисертација е развој и тестирање на нов протокол за безбедна комуникација кај вмрежените системи на автоматско управување. Главната цел на протоколот е овозможување на сигурна и безбедна комуникација, но и нејзина отпорност на влијанието на електромагнетен шум, која би значела можност за примена на протоколот во индустриски средини и апликации.

Безбедноста на овој комуникациски протокол се однесува на криптографскиот аспект и отпорноста на напади, и таа се обезбедува со користење на функции на спрега помеѓу два или повеќе динамички системи кај испраќачкиот дел, при што протоколот суштински дозволува мултиплексирање на информации. Кај приемниот дел се користи динамичка Баесова инференција за добивање на информациите од испратениот сигнал. Притоа, користењето на Баесовото заклучување овозможува ефективно разделување на детерминистичките сигнали кои носат корисна информација од динамичките пертурбации во каналот, правејќи го протоколот исклучително отпорен на шум.

Основната цел на истражувањето е да придонесе за подобрување на безбедноста на комуникациите кај индустриските вмрежени системи на автоматско управување преку развој на алгоритам за безбедна размена на информации.

Задачи на истражувањето се:

- да се истакне потребата од посигурна и побезбедна комуникација кај индустриските системи;

- да се развие алгоритмот за безбедна комуникација базиран на функции на спрега помеѓу два динамички системи и на динамичка Баесова инференција;

- алгоритамот да се примени на симулациски сценарија за различни услови и во присуство на различни видови на шум и интерференција;

- да се развие практичен експеримент каде ќе може да се испитаат и анализираат реалните можности на комуникацискиот протокол кој би го користел овој алгоритам.

1.3. Структура на докторската дисертација

Структурата на докторската дисертација е изложена во продолжение на овој дел. По дадениот вовед, теоретскиот дел содржи детален преглед на вмрежените системи на автоматско управување, презентира краток историски преглед на нивниот концепциски и практичен развој, и ги изложува најчестите проблеми кои се јавуваат кај нив и со тоа и главните области на истражувања. Понатаму, овој дел детално се задржува на два од овие проблеми - на влијанието на електромагнетниот шум врз комуникацијата и со тоа и стабилноста и перформансите кај индустриските ВСАУ, како и на безбедноста на овие системи, давајќи преглед на досегашните проблеми и решенија од оваа област. На тој начин е истакната потребата од индустриска комуникација отпорна на шум и на надворешни малициозни напади.

Истражувачкиот дел го презентира развиениот протокол за безбедна индустриска комуникација. Тој ги изложува основите на концептите за функции на спрега и динамичка Баесова инференција на кои се базира протоколот, го покажува неговото добивање, и ја презентира неговата имплементација. Дополнително, истражувачкиот дел е поткрепен и со практична реализација на алгоритмот, при што се прави обид експериментално да се потврдат безбедносните карактеристики и отпорноста на индустриски шум на протоколот. Аналитичко - синтетичкиот дел, пак, претставува анализа на добиените резултати и во овој дел, во зависност од добиените резултати, се испитува и енергетската ефикасност на развиениот комуникациски протокол.

Конечно, на крајот се дадени заклучокот и можностите за понатамошна работа, пред да се заврши со преглед на користената литература.

1.4. Објавени трудови поврзани со докторската дисертација

1.4.1. Трудови објавени во списанија

Gorjan Nadzinski, Matej Dobrevski, Christopher Anderson, Peter V. E. McClintock, Aneta Stefanovska, Mile Stankovski, and Tomislav Stankovski "Experimental Realization of the Coupling Function Secure Communication Protocol and Analysis of its Noise Robustness," *IEEE Transactions on Information Forensics and Security*, 2018 (трудот е прифатен и е во процес на објавување).

- Овој труд ја изложува практичната имплементација на протоколот за безбедна комуникација со функции на спрега помеѓу два динамички системи и динамичка Баесова инференција, и ги анализира добиените резултати. Трудот покажува дека протоколот функционира и во реални услови и е отпорен на шум од различна природа, и на бел Гаусов шум и на нискофреквентен Ornstein-Uhlenbeck шум, и ги поставува границите на толеранција на интерференцијата, споредувајќи ги и со границите на толеранција на друг често користен протокол за безбедна комуникација базиран на функции на спрега (signal masking protocol).

Gorjan Nadzinski, Mile Stankovski, and Ivan Gochev, "Dealing with the Effects of Random Time Delay and Data Dropouts in Networked Control Systems Through Robust Control," *Journal of Electrical Engineering and Information Technologies*, vol. 1, no. 1-2, January 2017.

- Трудот се осврнува на ефектите на случајните временски доцнења и губења на податочни пакети кај вмрежените системи на автоматско управување, и предложува алгоритам за робусно H_∞ управување кој овие случајни доцнења и загуби ги моделира како неизвесности во системот и соодветно се справува со нив. Управувачот се тестира на вмрежен систем на автоматско управување кој комуницира преку ZigBee мрежа во услови на шум и загуба на податоци.

1.4.2. Трудови објавени на меѓународни конференции

Gorjan Nadzinski, Mile Stankovski, Vesna Ojleska Latkoska, and Ivan Gochev, "Experimental Test of the Effects of Electrostatic Discharge on an Industrial Networked Control System," Proceedings of the 13th IEEE International Conference on Control and Automation, July 3-6, 2017, Ohrid, Macedonia.

- Овој труд дава основен преглед на проблемите кои се јавуваат кај индустриските вмрежени системи на автоматско управување со нагласен акцент на интерференциите предизвикани од околниот шум. Сепак, главниот придонес е во практичното и

експериментално испитување на влијанијата на електромагнетен и електростатски шум врз комуникацискатa мрежа во еден реален индустриски вмрежен систем на автоматско управување. Анализата на резултатите ги утврдува праговите на функционирање и толеранција на модерните индустриски системи во присуство на шум.

Ivan Gochev, **Gorjan Nadzinski**, and Mile Stankovski, "Path Planning and Collision Avoidance Regime for a Multi-agent System in Industrial Robotics," International Scientific Conference on Industry 4.0, December 13-16, 2017, Borovec, Bulgaria.

- Овој труд предложува алгоритам за планирање на пат и избегнување на препреки во повеќеагентен систем составен од мобилни роботи чија заедничка задача е транспорт на материјали во индустриска околина. Меѓусебната координација на роботите прави овде да стане збор за еден вмрежен систем на автоматско управување кој со предложениот алгоритам има за цел ефикасно и оптимално да функционира во индустриска средина.

Ivan Gochev, **Gorjan Nadzinski**, and Mile Stankovski, "Effects of Time Delay and Loss Probability on Performance and Stability in a Networked Control System," Proceedings of the 13th International Conference on Systems, Automatic Control, and Measurements (SAUM), November 9-11, 2016, Nis, Serbia.

- Овој труд ги испитува ефектите на случајните временски доцнења и на загубата на податочни пакети врз стабилноста и перформансите на реален вмрежен систем на автоматско управување на DC мотор.

Ivan Gochev, **Gorjan Nadzinski**, and Mile Stankovski, "Effects of Time Delay and Loss Probability on the Power Consumption in a Networked Control System," Proceedings of the 13th International Conference on Electronics, Telecommunication, Automation, and Informatics (ETAI), September 22-24, 2016, Struga, Macedonia.

- Трудот го анализира влијанието на случајните временски доцнења и на загубата на податочни пакети врз оптималноста и потрошувачката на енергија кај реален вмрежен систем на автоматско ПИД управување на сервомотор.

2. ВМРЕЖЕНИ СИСТЕМИ НА АВТОМАТСКО УПРАВУВАЊЕ (ВСАУ)

2.1. Основи

Кога сите компоненти на еден конвенционален систем на автоматско управување со повратна врска (анг. feedback control system) меѓусебно ќе се поврзат преку соодветен комуникациски канал или медиум, кој пак може да е споделен со други јазли надвор од системот, истиот се класифицира како вмрежен систем на автоматско управување (анг. networked control system). Еден ваков систем е прикажан на Слика 1.

Слика 1 Конфигурација на вмрежен систем на автоматско управување

Иако во реалноста сите врски помеѓу било кои елементи на еден систем се остварени преку некаков комуникациски канал (без разлика дали станува збор за жична или за безжична комуникација), сепак до неодамна модерната теорија на автоматско управување во голема мера се базираше на претпоставката дека сигналите и информациите кои тие ги содржат се пренесуваат низ идеални канали без временски доцнења, како и дека сите пресметки во управувачот се одвиваат моментално. Ваквата

асумпција со децении била прифатлива во автоматиката, но ненадејното зголемување на сложеноста на системите и содржајноста на информациите во нив, предизвикало потреба од веродостојно моделирање на комуникацискиот медиум и на целиот процес на примање и праќање на сигналите и пресметување на управувачките величини. Ова подразбира дека основните влезно/излезни сигнали во системите се податочни пакети кои пристигнуваат во различни (неретко случајни) моменти, често по недетерминиран редослед, а алгоритмите на управување мораат да прават компромис помеѓу квалитетното управување и брзото време на пресметување (Murray R. M., 2006). Од тие причини, на изучувањето на вмрежените системи на автоматско управување мора да се гледа како на спој помеѓу теоријата на автоматско управување и теоријата на телекомуникациите.

Предностите од употребата на вмрежените системи на автоматско управување се многубројни и се евидентни: нивната улога во индустријата е незаменлива поради потребата од поврзување на голем број на физички дистрибуирани сензори, актуатори и управувачи. Понатаму, поврзувањето на различните компоненти на системите во заедничка мрежа нуди модуларност, флексибилност, и можности за полесно одржување, а овозможува и поедноставно евентуално модифицирање на управувачките стратегии, и поголема редундантност на системите преку едноставно превклучување на резервни (анг. backup) компоненти. Сепак, можеби највпечатливо од се, системите дизајнирани на овој начин овозможуваат едноставна и брза имплементација на набљудувачко управување над целата управувана постројка, и дозволуваат лесно прибирање на податоци и информации за работата на целокупниот систем.

Постојат многу ситуации каде имплементацијата на заедничка комуникациска мрежа за меѓусебно поврзување на управувачките апликации е корисна. Една од нив е при управувањето на воздухопловите, каде има огромен број на меѓусебно поврзани и подеднакво важни сензори и подсистеми задолжени за секој сегмент на летањето и безбедноста на леталата. Понатаму, производните процеси не можат да се замислат без соодветни системи за собирање на податоци (анг. data acquisition systems), кои ги обединуваат информациите од сензорите поставени на клучни точки долж производната линија: информациите се собираат во централна точка преку индустриска комуникациска мрежа, истата онаа која веќе се користи за пренос на сигнали помеѓу управувачите, актуаторите и сензорите во постројката.

Главните недостатоци на вмрежените системи на автоматско управување произлегуваат од нивната сложена природа. Имено, мора да се смета дека во општ случај не може да се гарантираат синхронизацијата помеѓу компонентите на вмрежените системи на автоматско управување и нулевото или константното доцнење на сигналите помеѓу нив. Ова е така поради тоа што како комуникациски медиум неретко се користи некоја споделена мрежа, поради што често доаѓа до застој на сообраќајот и до губење на податочни пакети. Додека овие појави кај добро дизајнираните комуникациски мрежи резултираат со опаѓање на квалитетот и брзината на преносот, тие можат да придонесат за

појава на системска нестабилност кога низ таквите мрежи се споделуваат податоци и информации клучни за реално временски управувачки апликации (Azimi-Sadjadi, 2003).

2.2. Преглед на историјата на вмрежените системи на автоматско управување

Главните напори во областа на вмрежените системи на автоматско управување се движат во насоката на анализа на системите и синтеза на управувачи кои ќе можат да се справат со гореспоменатите проблеми и повторно да гарантираат стабилност и коректна работа на системот. Но методите и алатките развиени во рамките на теоријата на конвенционалното автоматско управување самите по себе не се доволни за тоа и мораат да бидат модифицирани за да можат да се носат со значително зголемената комплексност.

Во продолжение следува осврт на историскиот развој на вмрежените системи на автоматско управување како област од особено значење во рамките на теоријата на автоматско управување.

Почетоците на вмрежените системи на автоматско управување можат да се најдат во средината на педесеттите години на минатиот век, со развојот на првиот воздухоплов со електронски команди Авро Вулкан (анг. Avro Vulcan) (The Vulcan Story, 1958). Овој авион бил производ на обидите за заменување на комплексното и тешко хидрауличното управување со лесни и флексибилни електрични кола (анг fly-by-wire) и претставува првото големо достигнување во областа на аналогните вмрежени системи на автоматско управување. По пронаоѓањето на микропроцесорите и нивната имплементација во автоматиката, првото летало со дигитален fly-by-wire управувачки систем, наречено F-8C Crusader, било конструирано во 1972 година.

Следниот чекор во еволуцијата на вмрежените системи на автоматско управување претставувале системите на дистрибуирано управување (анг. distributed control systems). По наглото опаѓање на цената на компјутерите во 70-те години на минатиот век, тие станале сеприсутни во светската индустрија; на пример, вкупниот број на глобално употребувани компјутери во процесната автоматика се зголемил од околу 5,000 во 1970 година, на околу 50,000 во 1975 година. Со тоа се променила и улогата на компјутерите при управувањето на процесите – од гломазни и инертни машини задолжени за собирање и печатење на податоци, и за менување на референтни вредности во управуваните системи, тие се претвориле во интегрален и незаменлив дел од процесите, целосно заменувајќи ги аналогните уреди и значително придонесувајќи за доверливоста и флексибилноста на производните системи. Од тие причини, откако се увидело дека компјутерите можат да ги извршуваат сите улоги во рамките на еден процес на автоматско

управување, од централни управувачки единици па сé до собирачи на податоци и подредени и локализирани управувачи, наредната етапа се состоела од нивно целосно интегрирање во индустријата. Се смета дека Универзитетот во Мелбурн, со развој на прототип за напредна автоматизација на домови чиј главен микропроцесор преку сериска врска ги споделувал својата меморија и своите задачи со останати физички дистрибуирани, но меѓусебно координирани управувачи, всушност ја направил првата успешна имплементација на систем на дистрибуирано управување во овој период. Во играта набрзо се приклучиле и светските гиганти како Honeywell, Johnson Controls, и Yokogawa.

Во текот на овој почетен период, мрежната конфигурација кај сите системи на дистрибуирано управување била имплементирана со таканаречената Token Bus Network, според IEEE 802.4 стандардот. Кај оваа конфигурација, еден податочен пакет од три бајти наречен жетон (анг. token), секвенцијално се препраќа од еден до друг член (јазол) на мрежата. Членот кој кај себе го има жетонот е единствениот на кој му е дозволено користење на заедничката мрежа, т.е. праќање на податоци до другите јазли. Очигледно е дека ваквата конфигурација има многу свои недостатоци, а пред сé недостатокот на флексибилност и редундантност.

Понатамошниот развој на системите за дистрибуирано управување подразбирал и потреба од усовршени мрежни конфигурации и мрежни топологии, кои овозможувале зголемена редундантност на системите и поквалитетно и доверливо реалновременско управување. Брзиот развој на индустријата и драстично зголемените побарувања од индустриските апликации за многу кратко време на виделина ги изнеле сите недостатоци на едноставните комуникациски архитектури од типот јазел-до-јазел (анг. point-to-point), во кои спаѓала и Token Bus Network.

Најголемите исчекори кај вмрежените системи на автоматско управување се поклопуваат со појавата на безжичните комуникации и на Интернетот. Развојот на нови комуникациски стандарди отворил и нови можности за подобрување на системите за дистрибуирано управување; на пазарот брзо се појавиле нови стандарди и протоколи специјализирани за работа во индустрија (меѓу нив и Profibus, DeviceNet, ControlNet, ModBus), како резултат на желбата да се надминат импровизираните кабелски инсталации и да се стандардизираат и развијат нови дигитални методи на комуникација базирани на Ethernet технологијата.

Откако се поставени темелите на индустриските системи на дистрибуирано управување, се доаѓа до моменталната денешна состојба. Најновите стремежи во последните децении се однесуваат на искористување на постоечките мрежи (со особен акцент на безжичните), за преку нив да се одвива комуникацијата помеѓу сензорите, актуаторите, управувачите и воопшто сите географски и физички дистрибуирани компоненти на системите на автоматско управување, без разлика дали станува збор за

индустриски погони и процеси, интелигентни домови или други апликации (Zampieri, 2008).

Но, како што веќе беше споменато претходно, тука настануваат проблеми базирани на природата на мрежите и на стандардите кои треба да се користат како комуникациски медиум во вмрежените системи на автоматско управување. Поради тоа што сега станува збор за комуникациски канали кои секој системски компонент ги дели со уште десетици, стотици, или илјадници останати јазли, неопходно е на исто ниво во предвид да се земат и управувачкиот и телекомуникацискиот аспект, и со тоа да се понудат решенија кои ќе овозможат правилно функционирање на вмрежените системи на автоматско управување при распределбата на комуникациските ресурси.

Главните дискусии во врска со вмрежените системи на автоматско управување се однесуваат на **доцнењата во мрежите**, **губењето на податочни пакети**, конфликтите при **распоредот на пристап на мрежата** и **квантизацијата на сигналите** (Zhang, Gao, & Kaynak, 2013). Општо гледано, постојат три главни пристапи при решавањето на ваквите проблеми: првиот е базиран на управувањето затоа што експлицитно ги зема предвид постоечките карактеристики на мрежата како фиксни, и потоа ги проучува управувачките методологии за соодветната ситуација; вториот пристап е мрежно базиран, бидејќи системот на управување се синтетизира независно од мрежата, а дури отпосле се дефинираат перформансните барања за комуникацискиот систем; третиот пристап претставува комбинација од претходните два, бидејќи ги проучува и мрежните карактеристики и управувачките методологии со цел да го оптимизира системот (Sun, Li, & Wang, 2007).

- **Доцнењата предизвикани од мрежата (анг. network induced delays)** го претставуваат едно од најважните прашања поврзани со вмрежените системи на автоматско управување, бидејќи се неизбежни без разлика на тоа каков тип на мрежа се користи (Tipsuwan & Chow, 2003). Самата природа на комуникациските мрежи кај вмрежените системи на автоматско управување (и фактот дека системите се принудени да ги делат овие мрежи со други ентитети) е таа која предизвикува недоверливи и недетерминистички појави во вид на доцнења, губење на податоци и т.н. треперење (анг. jitter, или високоамплитудни осцилации на вредностите на стандардното време на доцнење во мрежата) во најлош случај. Надминувањето на прифатливите граници од страна на овие појави предизвикува значително влошување на поведението на системите, што може да биде од голема штета при критични реално-временски апликации. Од тие причини, правилното моделирање на временските доцнења и наоѓањето на методи за нивна компензација е од клучна важност.

Доцнењата можат да се моделираат како константни доцнења со временски бафери, или како случајни доцнења - независни или со своја функција на случајна распределба. На пример, (Wu, Deng, & Gao, 2005) ја моделираат и анализираат стабилноста на системи со долги случајни доцнења. Понатаму, (Kamrani & Mehraban, 2006) ја моделираат динамиката на доцнењата кај Интернет мрежите со помош на конвенционални методи за идентификација, додека пак пософистициран пристап се користи од страна на (Shakkottai, Kumar, Karnik, & Anvekar, 2001), кои користат Маркови вериги, како и од страна на (Li & Mills, 2001), кои користат ARMA модел.

За компензација на доцнењата се користат различни математички, евристички и статистички методи (Montestruque & Antsaklis, 2004); оптималниот стохастички метод на (Nilsson, Bernhardsson, & Wittenmark, 1998) го решава проблемот како проблем на линеарен квадратен Гаусов управувач, каде вредностите на LQG матрицата се бираат според статистички податоци врзани за мрежните доцнења; методите на робусно управување се доста застапени во последните дваесетина години: (Goktas, Smith, & Bajcsy, 1996) ги моделираат доцнењата како пертурбации во системот и на тој начин ги компензираат без притоа да има потреба од претходна информација за нивната распределба на веројатноста, додека (Yue, Han, & Lam, 2005) даваат решение во вид на робустен H_∞ управувач; треба да се споменат и компензационите методи со редици на чекање, дадени во (Luck & Ray, 1994) и (Chan & Ozguner, 1995), кои вмрежениот систем на автоматско управување го претставуваат како стационарен систем (Gupta & Chow, 2010). Понатаму, (Soucek, Sauter, & Koller, 2003) го класифицираат феноменот на треперење (jitter) во две различни групи според неговите причинители, при што може да биде предизвикан од сообраќајот во мрежата, или пак предизвикан од комуникацискиот протокол. Авторите (Li, Yi, Wang, Wu, & Ma, 2006) развиле системи на линеарни матрични неравенства (анг. linear matrix inequalities - LMI) како услов за стабилноста на вмрежените системи на автоматско управување; (Xia, Liu, & Rees, 2006) понудиле решение кое се состои од генератор на предвидувања за управувачкото поведение и компензатор на доцнења, но кое бара многу прецизно моделирање на временските доцнења во мрежата; пофлексибилно решение кое содржи набљудувач и затоа не бара толку прецизен модел дале (Natori & Ohnishi, 2008); (Liu G. , Xia, Chen, Rees, & Hu, 2007) предложиле употреба на предвидувачки управувач и во главната но и во повратната врска; решението на (Zhang, Yang, & Su, 2007) се состои од моделирање на нелинеарните вмрежени системи на автоматско управување со помош на T-S

фази модел, и потоа од компензирање на доцнењата преку робусно H_∞ управување на таквиот модел.

- Секој од системските компоненти и подсистеми кои го делат заедничкиот комуникациски медиум имаат свој сопствен пропусен опсег. Големите фреквенции на семплирање и брзата динамика на системите подразбираат широки пропусни опсези, што пак од друга страна предизвикува **колизии при комуникациите и губење на податочните пакети низ мрежата (анг. packet dropout).** Додека кај секојдневните комуникациски апликации ова може да предизвика забавена работа и слични непријатности за корисниците, кај вмрежените системи на автоматско управување директно придонесува за некоректна работа и нестабилности кои можат да бидат и потенцијално опасни, во зависност од природата на управуваниот процес. Општо земено, губењата на податочните пакети во литературата се опишуваат на детерминистички начин при што губењето на пакетите се дава усреднето по време или преку горната граница на максималниот број на дозволени последователни губења, или на стохастички начин, при што се смета дека губењето на податоците во мрежите задоволува некаков познат модел на случајна распределба. Од моделирањето на детерминистички начин, можат да се издвојат користењето на едноставен независен Бернулиев процес и проектирањето на оптимален управувач за линеарни вмрежени системи на автоматско управување (Imer, Yuksel, & Basar, 2006), и користењето на произволен конечен превклучувачки сигнал, при што вмрежените системи на автоматско управување се стабилизираат со помош на алатки и пристапи од теоријата на превклучувачки динамички системи (Xiong & Lam, 2007). Од стохастичките методи, може да се издвојат моделирањето на губењето на податочни пакети со користење на дискретен линеарен систем со Марков параметар на прескокнување (Seiler & Sengupta, 2005), и со дискретна Маркова верига (Xiong & Lam, 2007).

  Други значајни трудови кои се баваат со проблемот на колизии и губење на податочните пакети се оној на (Marti, Yez, Velasco, Villa, & Fuertes, 2004), кој предложува адаптивни онлајн управувачи раководени според динамиката на колизиите во мрежата; оној на (Li & Chow, 2007), кој предложува динамичка адаптација на периодата на семплирање и динамичка прераспределба на комуникациските ресурси (Слика 2); понатаму (Al-Hammouri, Branicky, Liberatore, & Phillips, 2006) предложуваат сведување на проблемот на барање на оптималниот пропусен опсег на проблем на конвексна оптимизација; (Pereira, Andersson, & Tovar, 2007) развиле нов MAC (анг. Medium Access Control Protocol) протокол кој успешно се

справува со колизиите кај безжичните индустриски мрежи. Многу од трудовите за справување со ефектите на губењето на податочните пакети предложуваат и најразлични алатки базирани на Петри мрежи, на динамичко програмирање, на генетски алгоритми (Gupta & Chow, 2010), на естимација на дистрибуирани параметри (Li & Al-Regib, 2007), како и решенија базирани на оптички мрежи (McGarry, Maier, & Reisslein, 2004).

Слика 2 Модел на вмрежен систем на автоматско управување кој ги дава фазите на алокација на комуникациските ресурси, според (Li & Chow, 2007)

- **Делегирањето на ефикасен распоред (анг. scheduling) за пристап кон заедничката мрежа** претставува значаен обид за подобрување на поведението на вмрежените системи на автоматско управување. Од оваа област можат да се издвојат трудовите за распоред на матрицата на управувачко засилување (анг. gain scheduling) на вмрежените управувачки системи преку реалновременско прилагодување на управувачките параметри во зависност од квалитетот на услугата (анг. Quality of Service - QoS) на мрежата (Tipsuwan & Chow, 2001), (Tipsuwan & Chow, 2004), како и обидот за прилагодување на периодата на земање на примероци и на пропусниот опсег на мрежата за постигнување на ефикасно делегирање на пристапот (Park, Kim, Kim, & Kwon, 2002).

- Еден од начините на кој може да се изврши редуцирање на потребниот пропусен опсег на вмрежениот систем и со тоа да се намали веројатноста за

колизии и губење на податочни пакети, претставува редукцијата на бројот на битови од кои се состои секој пакет преку **квантизација на соодветниот сигнал**. Вакви пристапи се опишани од (Montestruque & Antsaklis, 2005), и се однесуваат на статичка квантизација со фиксен број на децимални места (анг. fixes-point data), и на динамичка квантизација со променлив број на децимални места (анг. floating-point data).

Треба да се истакнат и трудовите кои систематски и детално ги сумираат и анализираат сите досегашни достигнувања на полето на вмрежени системи на автоматско управување и на тој начин претставуваат цврст темел за понатамошна работа. Најчесто цитираните вакви трудови се прегледот на историскиот развој и теоријата на вмрежените системи на (Xia, Gao, Yan, & Fu, 2015) и на (Gupta & Chow, 2010), сличните такви трудови на (Hespanha, Haghshtabrizi, & Xu, 2007) и на (Sun, Li, & Wang, 2007), како и прегледот на најчестите управувачки методологии кај овие системи на (Tipsuwan & Chow, 2003).

Кога се во прашање идните истражувања од оваа област, во преден план се управувањето со толеранција на грешки (анг. fault tolerant control - FTC) и безбедноста на мрежите.

Управувањето со толеранција на грешки дава различни методи за спречување на пропагацијата на евентуалните дефекти и грешки во системите. Од трудовите од оваа област може да се издвои моделот на (Patankar, 2004) за толеранција на грешки преку временски побудувани комуникациски протоколи; понатаму, трудот на (Wang, Ye, & Wang, 2006) нуди можност за детекција на грешките кај вмрежените системи на автоматско управување како мултипликативни грешки предизвикани од случајните доцнења генерирани од самата мрежа; во трудот на (Mendes, Santos, & da Costa, 2007) е предложена повеќеагентна платформа за децентрализирана синтеза и дистрибуирани пресметка за сложени вмрежени системи на автоматско управување; (Zhu & Zhou, 2007) предлагаат користење на состојбен набљудувач со цел детекција и идентификација на потенцијално опасни грешки предизвикани од доцнењата; конечно, (Klinkhieo, Kambhampati, & Patton, 2007) предложуваат управување толерантно кон грешки преку модификација на големината на пакетите во мрежата.

Што се однесува пак до безбедноста на мрежите, таа се проучува веќе долго време, и тоа од самиот почеток на користењето на комуникациските мрежи за поврзување на системските компоненти, особено кај критични системи какви што се нуклеарните централи, вселенските проекти, воените апликации и ним слични. Во сите вакви случаи безбедноста на комуникацискатa мрежа има највисок приоритет, особено во денешните услови на зачестеност на електронските напади и појавата на сајбертероризам (анг. cyber-terrorism), па затоа изразена е зголемената побарувачката за соодветно скалабилни системи за детекција на натрапници (анг. intrusion detection systems - IDS). Освен

постоечките мерки за заштита, можат да се споменат и трудовите на (Tsang & Kwong, 2005), кои предлагаат ефикасен повеќеагентен систем за заштита на мрежите во индустриските постројки мотивиран од кластерирање на мравји колонии; начини за намалување на ранливоста на вмрежените системи на автоматско управување кај индустриски постројки презентираат и (Creery & Byres, 2005), додека пак (Gupta & Chow, 2008) даваат целосна и детална анализа на моменталната состојба на полето на безбедноста на комуникациските мрежи и на перспективите и понатамошните предизвици во таа област.

И покрај тоа, останува да важи заклучокот дека управувањето со толеранција кон грешки и безбедноста на мрежите сеуште претставуваат значајни предизвици кај вмрежените системи на автоматско управување, особено кога станува збор за нивна коректна и правилна имплементација при комплексни системи со голем број на елементи и при чувствителни или критични апликации (Gupta & Chow, 2010). Посебен акцент на безбедноста на вмрежените системи на автоматско управување во индустријата ќе биде даден во една од подоцнежните глави од оваа дисертација.

Како заклучок на сé што досега беше изложено, во продолжение во Табела 1 дадени се насловите на дваесетте најцитирани трудови во последните 7 години во списанието IEEE Transactions on Automatic Control, кое претставува едно од најрелевантните списанија од областа на автоматиката и системското инженерство (импакт фактор од 4.35). Очигледно е зачестеното присуство на трудовите кои се бават со проблеми од областа на вмрежените системи на автоматско управување; доколку оваа дефиниција се прошири и на проблеми од областа на дистрибуирано и децентрализирано управување и управување на повеќеагентни, тогаш може да се смета дека дури 15 од најцитираните 20 трудови (или 75 %) се на тие теми. Може да се заклучи дека моделирањето, стабилизацијата и управувањето на вмрежени системи претставува растечки тренд во светот на автоматиката. Еден од најактуелните трудови кој дава детален преглед на работата на сите релевантни теми од областа на вмреженото управување е оној на (Xia, Gao, Yan, & Fu, 2015).

р.б.	***Наслов***	***Автор(и)***	***Год.***	***Бр. цит.***
1.	Constrained Consensus and Optimization in Multi-agent Networks	A. Nedic, A Ozdaglar, P.A. Parilo	2010	706
2.	Event-triggering in Distributed Networked Control Systems	X. Wang, M. D. Lemmon	2011	603
3.	Distributed Event-triggered Control for Multi-Agent Systems	D. V. Dimarogonas, E. Frazzoli	2012	532
4.	To Sample or Not to Sample: Self-triggered	A. Anta, P.	2010	506

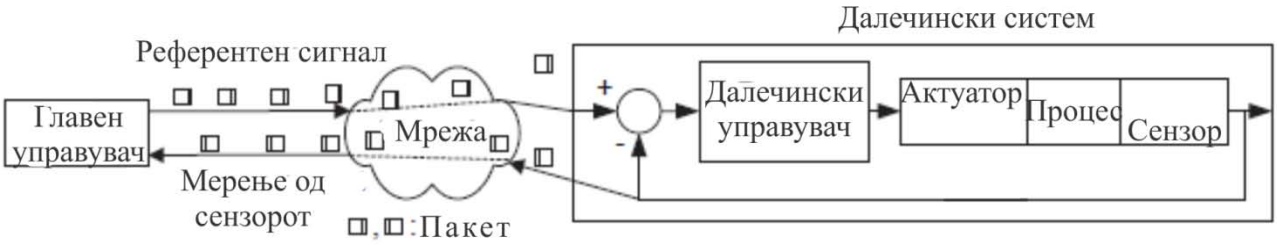
	Control for Non-linear Systems	Tabuada		
5.	Finite-time Consensus Problems for Networks of Dynamic Agents	L. Wang, F. Xiao	2010	480
6.	Networked Control Systems With Communication Constraints: Tradeoffs Between Transmission Intervals, Delays and Performance	W. P. M. H. Heemels, A. R. Teel	2010	460
7.	Optimal Design for Synchronization of Cooperative Systems: State Feedback, Observer and Output Feedback	H. Zhang, F. L. Lewis, A. Das	2011	428
8.	State Estimation and Sliding-mode Control of Markovian jump Singular Systems	L. Wu, P. Shi, H. Gao	2010	422
9.	Dual Averaging for Distributed Optimization: Convergence Analysis and Network Scaling	J. C. Duchi, A. Agarwal	2012	412
10.	Necessary and Sufficient Conditions for Consensusability of Linear Multi-agent Systems	C. Q. Ma, J. F. Zhang	2010	402
11.	Output Consensus of Heterogeneous Uncertain Linear Multi-agent Systems	H. Kim, H. Shim, J. H. Seo	2011	382
12.	Output-based Event Triggered Control With Guaranteed L_∞-Gain and Improved and Decentralized Event-triggering	M. C. F. Donkers, W. Heemels	2012	355
13.	Decentralized Event-triggered Control Over Wireless Sensor/Actuator Networks	M. Mazo, P. Tabuada	2011	354
14.	Diffusion Strategies for Distributed Kalman Filtering and Smoothing	F. S. Cattivelli, A. H. Sayed	2010	345
15.	Necessary and Sufficient Conditions for Analysis and Synthesis of Markov Jump Linear Systems with Incomplete Transition Descriptions	L. Zhang, J. Lam	2010	338
16.	Consensus Conditions of Multi-agent Systems with Time-varying Topologies and Stochastic Communication Noises	T. Li, J. F. Zhang	2010	337
17.	A Linear Representation of Dynamics of Boolean Networks	D. Cheng, H. Qi	2010	336
18.	Distributed Coordinated Tracking With Reduced Interaction via a Variable Structure Approach	Y. Cao, W. Ren	2012	326
19.	A Delay System Method for Designing Event-triggered Controllers of Networked Control Systems	D. Yue, E. Tian, Q. L. Han	2013	326
20.	Attack Detection and Identification in Cyber-Physical Systems	F. Pasqualetti, F. Doerfler, F. Bullo	2013	322

Табела 1 Преглед на најцитираните трудови во списанието IEEE Transactions on Automatic Control

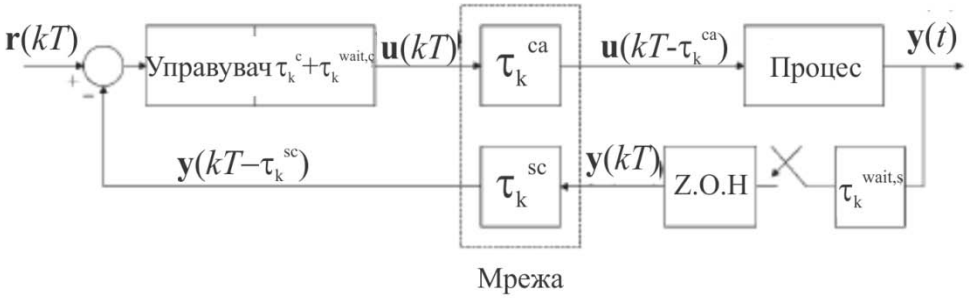
2.3. Проблем на доцнењата предизвикани од мрежата кај вмрежените системи на автоматско управување

Во овој дел ќе биде даден фокус на доцнењата предизвикани од мрежата и на губењата на податочните пакети, како и на најчестите управувачки методологии кои се користат при справувањето со ваквите појави кај вмрежените системи на автоматско управување.

Првни, на Слика 3 е дадена општата структура со која се прикажуваат вмрежените системи на автоматско управување, додека на Слика 4 (Tipsuwan & Chow, 2003) е прикажана основна претстава за доцнењата во нивните комуникациски мрежи. Тука, со **r** е означен референтниот сигнал, со **u** е означен управувачкиот сигнал, **y** е управуваната величина, а **T** е периодата на дискретизација во системот.



Слика 3 Општа блок структура на вмрежен систем на автоматско управување



Слика 4 Временски дијаграм на доцнењата кај вмрежените системи на автоматско управување (Tipsuwan & Chow, 2003)

Според текот на сигналите во системот, доцнењата кај овие системи можат да се поделат на доцнења од сензорот до управувачот τ^{sc}, и на доцнења од управувачот до

актуаторот τ^{ca}. Доколку со τ^{se} се означи моментот во кој од управуваниот систем започнува праќањето на соодветниот пакет информации, со τ^{cs} се означи моментот во кој управувачот започнува со нова итерација на пресметки на управувачкиот сигнал врз основа на сигналот на грешката, со τ^{ce} се означи моментот во кој управувачот започнува со праќање на информациските патеки кои го содржат управувачкиот сигнал, а со τ^{rs} се означи моментот кога управуваниот систем започнува да го процесира применият управувачки сигнал, тогаш гореспоменатите доцнења можат да се пресметаат со:

$$\tau^{sc} = \tau^{cs} - \tau^{se} \quad (1)$$
$$\tau^{ca} = \tau^{rs} - \tau^{ce} \quad (2)$$

Како што може да се види на слика 4, вкупното време на доцнење τ всушност претставува сума од овие две доцнења τ^{sc} и τ^{sa}, и од времето на пресметување на вредноста на управувачкиот сигнал во управувачот означено со τ^{c} (ова време во голем дел од случаите е занемарливо во однос на транспортните доцнења во самата мрежа).

Ако работите се разгледуваат на физичко ниво, тогаш може да се каже дека τ^{sc} и τ^{ca} се состојат од следните компоненти на доцнење: времето на чекање (анг. waiting time delay) τ^{W}, кое го претставува периодот кој испраќачот треба да го помине чекајќи да се ослободи канал за испраќање на податочните пакети, времето на врамување (анг. frame time delay) τ^{F}, кое го претставува временскиот период потребен за подготвување на податоците за праќање во самата мрежа, и времето на пропагација (анг. propagation delay) τ^{P}, кое го претставува времето на патување на податочните пакети низ физичкиот медиум и во голема мера зависи од брзината на пренос на сигналите и од физичкото растојание помеѓу изворот и помеѓу дестинацијата на сигналот.

Се разбира, постојат и останати доцнења на физичко ниво кои се придодаваат на вкупното освен овие три основни, а до нив најчесто доаѓа во редовите на чекање или пак при преминувањето на податочните пакети од еден уред (рутер, превклучувач) на друг. На доцнењата често знаат да влијаат и пропусниот опсег на медиумот и големината на рамките на податочните пакети, а тоа се параметри кои се под директно влијание на спецификациите на соодветниот комуникациски протокол.

Доцнењата со најдолго траење најчесто настануваат во ситуации кога доаѓа до грешки при транспортот и до загуба на податоците, па потребно е препраќање на соодветниот податочен пакет. Оваа акција на пример е доста карактеристична за мрежните протоколи на повисоките нивоа, како што е на пример TCP. Сепак, во најголемиот дел од случаите кај вмрежените системи на автоматско управување препраќањето воопшто не се препорачува и не се имплементира, бидејќи во споредба со големите доцнења кое тоа би ги предизвикало, загубата на информациите е прифатлива.

Од аспект на влијанието на изборот на комуникациска мрежа врз доцнењето во системот, мрежите можат да се поделат на два вида:

- Мрежи со циклично сервисирање (анг. cyclic service networks), каде сигналите се пренесуваат по предетерминиран цикличен распоред, па од таа причина доцнењата се детерминистички и периодични, а со тоа и едноставни за моделирање. Протоколи со циклично сервисирање се PROFIBUS, IEEE 802.4, IEEE 802.5, MIL-STD-1553B, FIB и др.

- Мрежи со случаен пристап (анг. random access networks), каде компонентите пристапуваат до комуникациските ресурси по случаен редослед, па затоа доаѓа до голем број на стохастички доцнења, кои се предизвикани од неуспешните обиди за пристап на ентитетите до мрежата и од колизиите на податочните пакети. Најпознати примери за протоколи кои се базираат на случаен пристап до мрежата се CAN и Ethernet.

Во трудот на (Yuan, Qigong, Ming, & Yiqing, 2013) се наведуваат четири основни модели на доцнењата кај вмрежените системи:

- Моделот на константни доцнења е наједноставниот и најдиректниот пристап кој воведува бафер за примање на податоците кај управувачот или актуаторот, на тој начин овозможувајќи целиот систем да се третира како детерминистички, и за негово управување да можат да се користат методи соодветни за детерминистичките системи. Пристапот е добар за ситуации каде случајните доцнења се релативно кратки и не се менуваат многу (на пример switched Ethernet), но во суштина вештачки го зголемува доцнењето и ја намалува стабилноста на системот земајќи ја горната граница на можните вредности на случајните доцнења за константна (Yorke, 1970), (Hirai & Satoh, 1980).

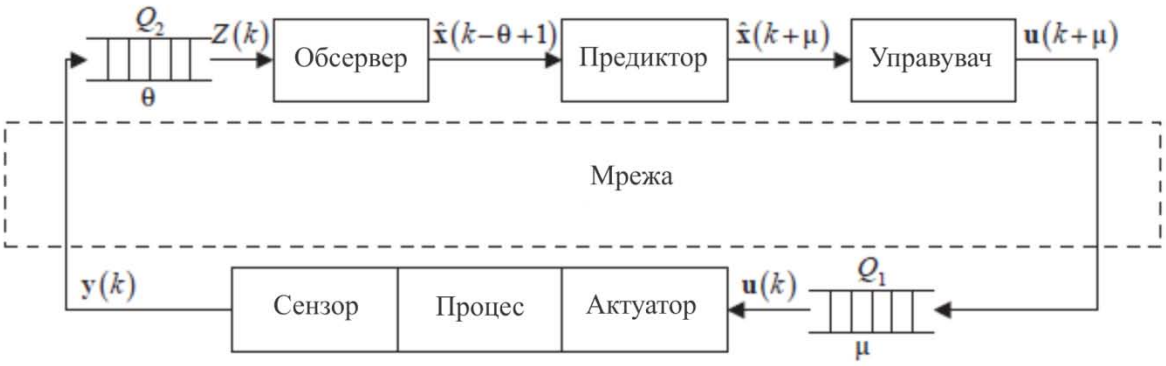
- Моделот со стохастички доцнења се употребува кога доцнењата се меѓусебно независни. Главните управувачки стратегии за ваквиот модел се стохастичкото управување (кое директно ги цели доцнењата), робусното управување (кое доцнењата ги моделира како неизвесности во системот), и предиктивното управување (кое се користи за комплексни динамички системи со неизвесности во моделот).

- Моделот со Маркови вериги, кој се користи во случаи кога доцнењата се меѓусебно зависни, при што Марковите вериги ја моделираат таа зависност и го олеснуваат процесот на дизајнирање на управувачки алгоритам.

- Скриен Марков модел, кој се користи за моделирање на најлошите сценарија во случаи кога состојбата на мрежата во ВСАУ не е директно набљудлива па мора да се естимира преку мерењето на доцнењата. Овој пристап е најопшт за моделирање на случајните доцнења кај вмрежените системи, но за жал управувачките методи базирани на него сеуште се одликуваат со незадоволителни и бавни перформанси при реални апликации.

Имајќи ги предвид сите претходно споменати карактеристики на доцнењата кај вмрежените системи и начините за нивно моделирање, може да се разгледаат неколку основни пристапи за справување нивните негативни ефекти и за обезбедување на стабилност и задоволителни перформанси на управуваните системи во нивно присуство.

- Во (Luck & Ray, 1990) и (Luck & Ray, 1994) се предлага воведување на редици на чекање (анг. queuing) со што случајните доцнења се моделираат како детерминистички. Како што се гледа на Слика 5, тука управувачот се состои од набљудувач (обсервер) на чиј влез се наоѓа FIFO бафер во кој се чуваат претходните измерени вредности на управуваната величина, предвидувач (предиктор) кој врз основа на состојбата естимирана од набљудувачот ги предвидува следните состојби, и од управувачки дел кој го генерира управувачкиот сигнал, чии квантизирани вредности се чуваат во баферот на влезот од управуваниот систем. Ваквото решение се покажува како доста успешно и се користи често, но исклучиво во ситуации во кои постои прецизен модел на управуваниот процес.



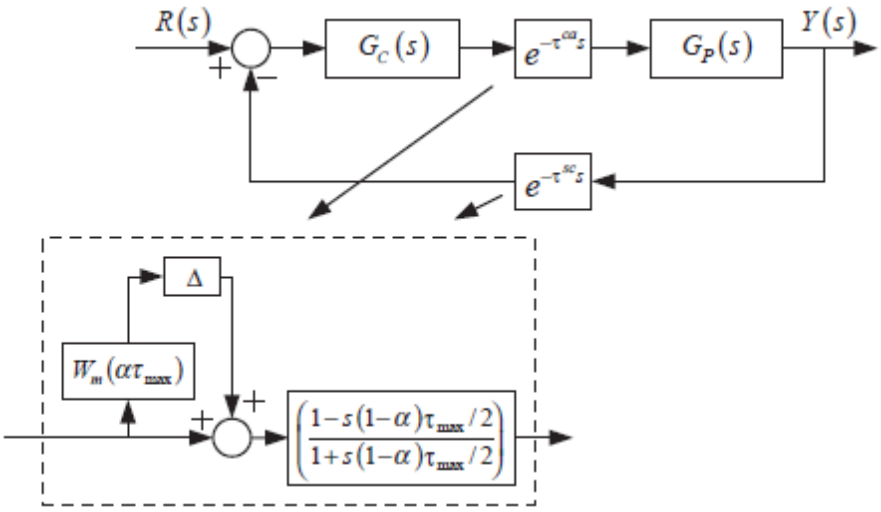
Слика 5 Конфигурација на детерминистичкиот компензатор на доцнења со естимација и предвидување (Luck & Ray, 1990), (Luck & Ray, 1994)

- Во трудовите на (Walsh, Beldiman, & Bushnell, 1999a) и (Walsh, Ye, & Bushnell, 1999c) се изложува метод за моделирање на ефектите од периодичните доцнења како придушени пертурбации (нарушувања) кај континуален реално-временски систем. Ваквиот метод е применлив само кај системи со мали вредности на периодата за дискретизација. Стабилизацијата овде се состои од бирање на вредности на управувачката матрица кои гарантираат пригушување на пертурбациите во рамките на еден период на доцнење.

- Во (Hong, 1995) се предлага метод на избор на периодата на семплирање, кој може да се применува во случаи кога повеќе различни вмрежени системи се поврзани на иста мрежа. Станува збор за управувач чија задача се состои од одредување на вредност

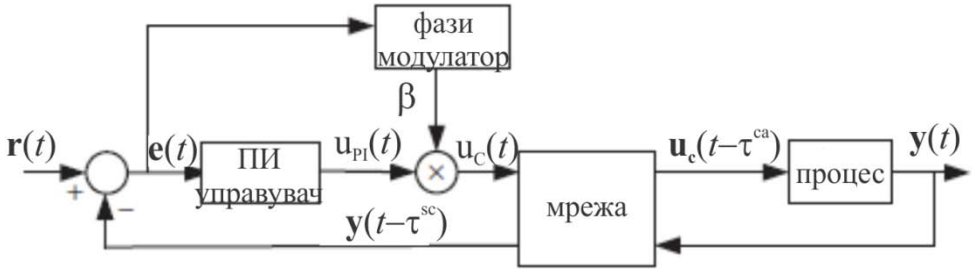
на периодата на семплирање која ќе осигура дека доцнењата во мрежата не би имале посериозен ефект врз системското поведение. Ова се прави со подредување на сите поврзани системи според нивната чувствителност на доцнењата и со одредување на периодата на семплирање за најчувствителниот од нив (таа се одредува како една третина од сумата на горната прифатлива граница на доцнење и времето на пренос на еден податочен пакет), а периодите на семплирање за останатите системи претставуваат функции од оваа вредност.

- Во (Goktas, 2000) е даден дизајн на робустен управувач за справување со доцнења, како што е покажано на Слика 6. Доцнењата τ^{sc} и τ^{ca} се моделирани како мултипликативни нарушувања во системот, а при тоа важи претпоставката дека тие имаат горна граница (максимум). После тоа се врши проектирање на континуален H_∞ управувач кој се дискретизира преку билинеарна трансформација.



Слика 6 Конфигурација на робустниот управувач за вмрежени системи на автоматско управување од (Goktas, 2000)

- Во (Almutairi, Chow, & Tipsuwan, 2001), авторите предлагаат компензирање на ефектите на доцнењата во мрежата со помош на фази логички управувач. Како што се гледа на Слика 7, главниот управувач во управувачката јамката е PI регулатор чии коефициенти се ажурирани од страна на фази логичкиот управувач врз основа на тоа колкава е системската грешка. Оваа грешка, пак, е под влијание на доцнењата во целокупниот систем. Функциите на припадност на грешката (како на влезен сигнал во фази логичкиот управувач) се добиваат со алгоритми за оптимизација кои за функции на цел земаат различни перформансни критериуми за поведението на системот базирани на системската грешка и динамиката на нејзина промена.



Слика 7 Конфигурација на фази логичкиот управувач за вмрежени системи на автоматско управување од (Almutairi, Chow, & Tipsuwan, 2001)

- Во (Tarn & Xi, 1998), авторите даваат интересно решение за справување со доцнењата. Имено, тие предлагаат управувач базиран на настани (анг. event-based control methodology) за управување на роботски манипулатор преку Интернет. Од причина што управувачот не е временски-базиран, доцнењата во мрежата всушност немаат никакво влијание врз него.

- Во (Tipsuwan & Chow, 2001) е дадена методологија на управување преку адаптација од страна на крајниот корисник (анг. end-user control methodology), во ситуација во која управувач на повисоко хиерархиско ниво го набљудува и естимира сообраќајот во мрежата, и врз основа на овие мерења како и на проектните барања, ги прилагодува коефициентите на управувачот во јамката (кој самиот најчесто е PI управувач), а сé со цел максимизирање на критериумите за квалитетот на услугата на мрежата (анг. Quality of Service – QoS). Пример за вакви критериуми се пропустноста на мрежата и горната граница на траењето на доцнењата при преносот на најголемите можни пакети. Ваквиот пристап се покажува прилично успешен во ситуации на случајни доцнења во комплексни мрежи.

- Во (Zhang, Shi, Chen, & Huang, 2005), авторите ја разгледуваат можноста за моделирање на доцнењата дадени кај дискретен вмрежен систем на автоматско управување како две независни Маркови вериги. На овој начин, вредноста на управувачкиот сигнал која се пресметува во секој семплирачки момент зависи исклучиво од моменталната состојба на системот и од последните вредности на доцнењата помеѓу сензорот и управувачот и доцнењата помеѓу управувачот и актуаторот. Управувачкиот закон за стабилизирање на целокупниот систем се добива со решавање на систем од линеарни матрични неравенства.

- Во (Peng & Tian, 2009) се дава предлог за дизајнирање на робустен H_∞ управувач кој е функција од доцнењето во системот преку проверка на границите на асимптотска

стабилност на системот со помош на функција на Љапунов-Красовскији. Ваквиот пристап се покажува успешен за системи со неизвесни параметри и со променливо но ограничено временско доцнење, и истиот подоцна се применува и на вмрежени системи на автоматско управување со слични карактеристики, за што примери можат да се најдат кај (Yue, Han, & Lam, 2005), (Yue, Han, & Lam, 2008).

- Во (Zhu & GH, 2009) е даден и уште еден нов вид на функција на Љапунов за проектирање на робустен H_∞ управувач за вмрежен систем на автоматско управување; оваа функција гарантира помалку конзервативни и помалку строги услови за стабилност. Истовремено се предлага и метод за елиминирање на неколку од редундантните променливи во линеарните матрични неравенства, со што значително се намалува комплексноста при пресметувањето на управувачкиот закон.

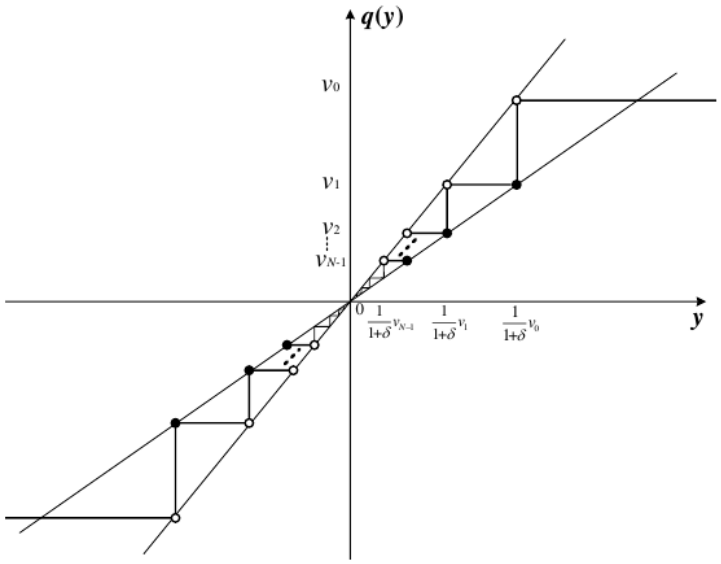
2.4. Ефектите на квантизацијата кај вмрежените системи на автоматско управување

Квантизацијата е значаен проблем кај вмрежените системи на автоматско управување. Таа претставува процес на претворање на континуалната вредност на некој сигнал во дискретна вредност од некое предетерминирано конечно множество. Ова се прави со цел сигналот да се дигитализира и да може да се испрати преку комуникациската мрежа (која во реалност има ограничен капацитет и не е способна да пренесува вредности од неограничено множество). Едноставно кажано, квантизацијата е пресликување на реалната вредност на амплитудата на сигналот **y** во дигитален број **q(y)** составен од n цифри, при што вкупниот број на вредности од кои може да се избира е 2^n. Очигледно е дека при квантизацијата се губи дел од информацијата која ја носел сигналот, па ефектите од квантизацијата мора да се земат предвид при работата со вмрежените системи на автоматско управување.

Фундаменталниот проблем кај ВСАУ е тоа како грешката при квантизацијата (т.е. загубата на информација) ќе влијае на целокупното поведение на системот. Јасно е дека мрежата ќе е помалку оптоварена доколку се користат помалку бити за квантизација, но во тој случај грешката може да биде преголема за управувачот воопшто да може да го стабилизира системот. Затоа, насоката на проучување на ефектите на квантизацијата е во поглед на дизајнирање на соодветен квантизатор кој ќе овозможи стабилно поведение при минимално оптоварување на комуникацискиот медиум. Притоа, се воочуваат два основни проблеми: проблемот на заситување, кој се јавува кога вредноста на сигналот го надминува опсегот на квантизаторот и истата може да се претстави само со максималната

вредност од 2^n множеството при што грешката постојано се зголемува, и проблемот на мали вредности, кој се јавува кога амплитудата на сигналот има толку мали вредности што квантизаторот не може прецизно да разликува помеѓу нив.

Во случаите на мали вредности, подобри резултати покажува логаритамскиот квантизатор (Elia & Mitter, 2001), (Fu & Xie, 2005). Овој квантизатор ги пресликува вредностите на сигналот погусто околу нултата точка (Слика 8), постигнувајќи поголема прецизност за помали амплитуди (кои се јавуваат почесто).

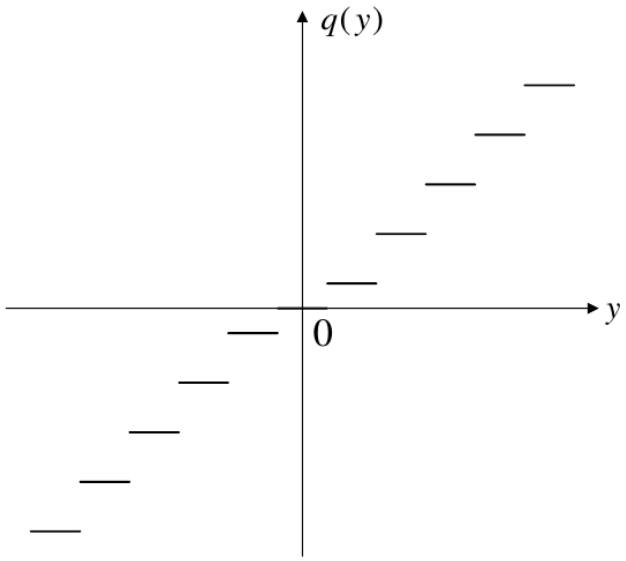


Слика 8 Пресликувачка функција кај логаритамскиот квантизатор

Многу трудови се занимаваат со улогата на логаритамскиот квантизатор кај ВСАУ. Во (Ishii & Basar, 2005) се проучува ваквата квантизација кај далечински управуван систем. Во (Hayakawa, Ishii, & Tsumura, Adaptive Quantized Control for Linear Uncertain Discrete-time Systems, 2009) и (Hayakawa, Ishii, & Tsumura, Adaptive Quantized Control for Nonlinear Uncertain Systems, 2009) се проучува адаптивно логаритамско квантизирање кај линеарни и нелинеарни дискретни системи со неизвесности соодветно. Понатаму, (You, Su, Fu, & Xie, 2011) се бави со наоѓање на минимален просечен проток на податоци за стабилизација на линеарни ВСАУ со логаритамска квантизација, а (Yue, Peng, & Tang, 2006) го прави истото за ВСАУ со неизвесности во моделот. Во (Zhang, Feng, & Qiu, 2011) се дискутира имплементација на H_2 и H_∞ филтри соодветно за нелинеарни ВСАУ со логаритамски квантизатори и при загуба на податочни пакети. Во (Li, Xia, Qiu, & Yang, 2012) се разгледува проблемот на робусно H_∞ управување за дискретни Такаги-Сугено фази логички ВСАУ со неизвесности, во услови на логаритамска квантизација, при што е

развиен нов модел на управување базирано на мрежа, кое истовремено предвид ги зема и доцнењата во мрежата и загубите на податочни пакети. Трудот на (Yan & Xia, 2012) изведува услов за стабилност на линеарен ВСАУ во присуство на податочни загуби кој зависи од карактеристиките на логаритамскиот квантизатор. Трудот на (Xia, Yan, Shi, & Fu, 2013) се занимава со случај на систем со логаритамски квантизиран влез кој произлегува од квантизирани мерења (анг. quantized input from quantized measurements - QIQM) и со глобалната асимптотска стабилност на такви системи кај кои всушност се јавува двослојна квантизација.

За разлика од логаритамскиот квантизатор, униформниот квантизатор (Слика 9) врши рамномерно мапирање на реалните вредности во дискретни и го третира целокупниот универзум на дискурс подеднакво, но затоа е поедноставен за употреба.



Слика 9 Пресликувачка функција кај униформниот квантизатор

Со ваквиот поедноставен квантизатор се постигнати интересни резултати кај различни класи на ВСАУ. На пример, (You & Xie, 2010) и (You & Xie, 2011) предложуваат неопходен и доволен услов за стабилност на линеарен дискретен ВСАУ со униформна квантизација и губење на пакети и преку управување во повратната врска. Со користење на униформен пристап, (Tian, Yue, & Zhao, 2007) ги истражува стабилноста и H_∞ управувањето на ВСАУ, при што се истражуваат ефектите и на доцнењата во мрежата и на изборот на квантизациони нивоа. Понатаму, во (Persis, 2009) се студира проблемот на стабилизација на нелинеарни ВСАУ со користење на мерењата на излезот но и на опсервер вграден во управувачот, при што карактеристиките на квантизаторот играат

важна улога во условите за стабилност. Слични резултати кои ја потврдуваат улогата на униформниот квантизатор во условите за стабилност на целокупниот ВСАУ се добиени и во случаи каде губењето на податочните пакети се моделира како Марков процес (Yan, Xia, & Li, 2014), каде е присутно значително количество на шум и се користи Калманов филтер (Xia, Yan, Shang, Fu, & Liu, 2012), и каде ВСАУ е подложен на нарушувања од непозната природа и магнитуда (Sharon & Liberzon, 2012).

Еден од главните недостатоци на униформниот квантизатор е неговата неможност соодветно да се справи (т.е. да придонесе за квалитетно управување и стабилизација) со ситуации каде се имплементира гореспоменатиот QIQM метод (Xia, Gao, Yan, & Fu, 2015).

2.5. Фузија на податоци кај вмрежените системи на автоматско управување

Во последно време состојбената естимација станува клучно поле на истражување кај вмрежените системи на управување, пред сé заради зголемената комплексност на мрежите и на системите (Xia, Gao, Yan, & Fu, 2015). Притоа, фузијата на податоци (анг. data fusion) е најчесто користената техника, која подразбира комбинирање на податоци од повеќе различни сензори за да даде попрецизни, поконзистентни и покорисни информации отколку било кој единечен извор на податоци. Според структурата, фузијата на податоци може да се подели на:

- централизирана фузија, кога сите мерења од различни сензори се испраќаат за процесирање во централна точка. Ова е најоптималниот метод за фузија бидејќи централната точка ги има сите податоци, меѓутоа недостатоците се тоа што бара големи компјутациони ресурси и капацитет на мрежата.

- дистрибуирана фузија, кога секој од сензорите локално ги обработува податоците и праќа само естимации до централниот јазол, што придонесува за отстапување од оптималноста но и ги намалува барањата за ресурси на мрежата и компјутациона моќ на центарот. Со други зборови, дистрибуираната податочна фузија ја жртвува оптималноста за цена на флексибилноста на системот и намалената комуникациска цена.

- хибридна фузија, која претставува комбинација од централизираната и дистрибуираната фузија.

Проучувањето на фузијата на податоци е тема која е актуелна веќе извесно време (пр. (Castanon & Tenekzis, 1985), (Grime, Durrant-Whyte, & Ho, 1992), (Mahmoud & Xia, 2014)), но кај ВСАУ неопходен е нов пристап во однос на традиционалните, заради карактеристичните променливи доцнења и губења на податочни пакети. Така, (Besada-

Portas, Lopez-Orozco, Besada, & de la Cruz, 2011) предлага множество на нови централизирани алгоритми за состојбена естимација кај линеарни динамички повеќевеличински системи со несинхронизирани и изобличени мерења добиени од повеќе сензори. Понатаму, (Chen, Zhang, & Yu, 2014) работи на алгоритам за децентрализирана фузија за ВСАУ со случајни доцнења, изгубени информации и загуба на податочни пакети, а (Xia, Shang, Chen, & Liu, 2009) и (Zhu, Xia, Yan, & Fu, 2010) предлагаат пристап со централизирана фузија на податоците кај сличен тип на ВСАУ. Во (Zhu, Xia, Yan, & Fu, 2012), предложен е алгоритам за централизирана фузија за ВСАУ каде локалните сензори ги означуваат временски податочните пакети пред да ги пратат (анг. time stamp), а посебен бафер во централниот јазол ги анализира временските ознаки и времињата на пристигање и на тој начин се справува со доцнењата и/или податочните загуби.

Во (Zhang, Feng, & Yu, 2012) е претставена дистрибуирана фузија каде сензорите во вмрежениот систем семплираат и естимираат податоци со една фреквенција, а естимациите ги праќаат до централниот јазол со друга, помала фреквенција која е променлива во зависност од состојбата во која се наоѓа целокупниот систем. На тој начин значително се растоварува комуникациската мрежа. Сличен пристап за исклучиво нелинеарни ВСАУ е даден во (Yan, Xiao, Xia, & Fu, 2012).

Исто така, трудовите како што се (Renzo, Imbriglio, Graziosi, & Santucci, 2009), (Yan, Li, Xia, & Fu, 2013), (Bian, Xia, Deng, & Fu, 2014), (Bian & Xia, 2014), се бават со комуникациските ограничувања во системот и со потрошувачката на енергија на тој начин што се трудат да ја најдат корелацијата помеѓу веројатноста за загуба на податочни пакети и/или погрешни естимации, и тековните услови во мрежата на системот, како што се на пример доцнењата, големината на пакетите, моќноста на емитување на податоците, итн.

Проучувањето на податочната фузија кај ВСАУ со неизвесности во моделот и во комуникациското медиум останува една од најпредизвикувачките теми за работа од ова поле за во иднина (Xia, Gao, Yan, & Fu, 2015).

2.6. Детекција и дијагноза на дефекти кај вмрежените системи на автоматско управување

Овој дел ќе го сумира прогресот на полето на дијагноза на дефекти кај ВСАУ. Во суштина, дијагнозата на дефекти е процес при кој информациите кои му се достапни на системот за дијагноза се процесираат за да се добијат моделот на правилно функционирање на процесот и условите кои значат дека е детектиран дефект. Детектирањето и дијагнозата кај ВСАУ во неколку работи се разликува од генералната дијагноза на дефекти:

- Моделот на целиот систем е во дискретен домен, бидејќи податоците кои минуваат низ мрежата се дигитални;

- Моделот на процесот е нелинеарен (Xia, Gao, Yan, & Fu, 2015);

- Доцнењата во системот не се занемарливи;

- Губењето на податочни пакети е реална појава која има значителни негативни ефекти врз процесот на дијагноза.

Оваа тематика е популарна при проучувањето на ВСАУ. На пример, трудовите (Huo & Fang, 2005), (Huo & Fang, 2006), ги проучуваат подсистемите за дијагноза на грешки кај ВСАУ во присуство на случајни доцнења и ограничувања на мрежата. Понатаму, трудовите (Fang, Zhang, Fang, & Yang, 2006), (Fang, Yang, & Zheng, 2006), и (Zheng, Fang, & Wang, 2006) истражуваат користење на квази Такаги-Сугено фази модел за дизајнирање на дијагностичкиот подсистем кај ВСАУ со големи доцнења и загуба на податоци, а (Mao, Jiang, & Shi, 2009) го прави сличното за класа на нелинеарни ВСАУ. Во (Ye & Ding, 2004) се истражува влијанието на доцнењата во мрежата врз успешноста на процесот на детекција на дефекти кога тој процес е базиран на класична состојбена естимација. На овој труд се надоврзува (Zhang, Branicky, & Phillips, 2001), каде се докажува дека доколку доцнењето во мрежата е помало од периодата на семплирање, истото може да се третира како непознат влез во случај на дефект. Во (Huang & Nguang, 2010) се истражува ситуација кога доцнењата може да се поголеми од периодата на семплирање, но мораат да се ограничени. Притоа трудот предлага користење на робусна естимација на дефекти базирана на методот на Љапунов - Разумикин, а естиматорот се добива со решавање на систем на билинеарни матрични неравенства кои зависат од моделот на системот и типот на комуникациска мрежа.

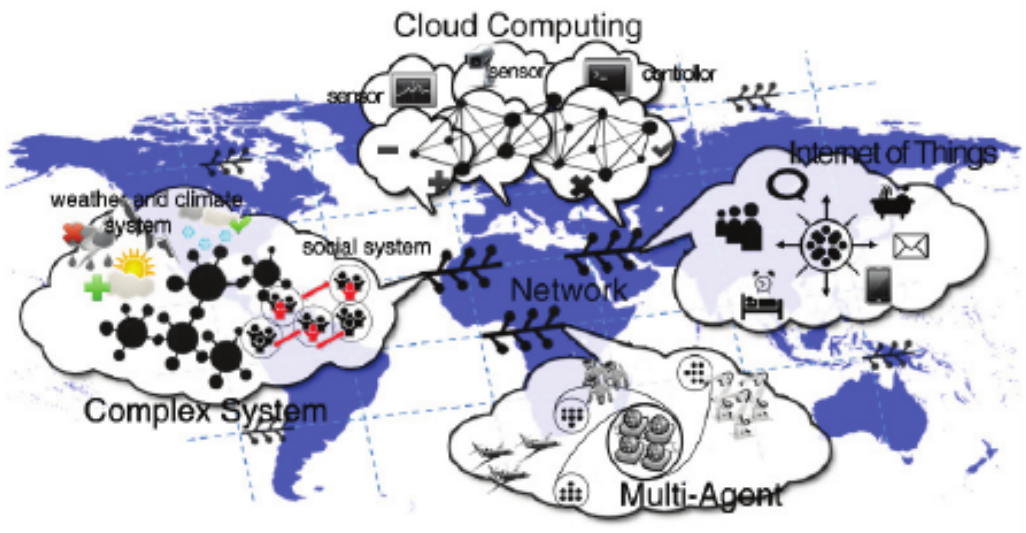
Со цел рационално да се користат ресурсите на мрежата и да се намалат застоите и доцнењата во неа, (Xie, Fang, & Zheng, 2004) конструира едноставна шема за проток и приоритет на информациите од дијагностичкиот систем. Оваа шема овозможува периодична распределба на мрежните ресурси помеѓу компонентите на ВСАУ. Понатаму, (Yang, Xia, & Liu, 2011) ја студира детекцијата и дијагнозата на дефекти кај фази дискретни ВСАУ од Такаги-Сугено тип, (Liu & Xia, 2011) предлага статистички базиран метод за детекција на дефекти кај вмрежени системи со предиктивно управување, мрежни доцнења и несинхронизирани часовници кај поединечните компоненти. Во (Xia & Liu, 2013) е предложена детекција на дефекти и ненадејни промени во повеќевеличински систем преку анализа на податоците (влезовите и излезите на системот) во фреквентен домен, а во (Xia, Amann, & Liu, 2010) е даден пример за реална имплементација на таков пристап кај електрокардиограм.

Она што привлекува внимание од прегледот на трудови кои се баваат со детекција и дијагноза на дефекти кај вмрежените системи е тоа што мал е бројот на трудови кои ги

испитуваат нелинеарните ВСАУ, како и бројот на трудови кои во процесот на детекција и дијагноза го вклучуваат влијанието на мрежниот протокол. Затоа овие теми се наметнуваат како особено погодни за истражување во иднина.

2.7. Иднината на вмрежените системи за автоматско управување

Техниките за управување преку облак (анг. cloud control techniques) (Xia Y. Q., 2012) (Слика 10) добиваат зголемена популарност во науката и индустријата како резултат на огромните компјутациони и мемориски ресурси и потенцијали со кои располагаат денешните компјутери. Генерално гледано, cloud техниките се нуспроизвод на успехот на Интернет сајтовите за управување од далечина и нивното усовршување се должи на сеприсутноста на Интернет протоколите како проверени и доверливи комуникациски протоколи кај вмрежените системи на автоматско управување. Техниките за управување преку облак ги спојуваат предностите на cloud пристапот и напреднатата теорија за ВСАУ.



Слика 10 Приказ на систем на управување вмрежен во облак

Понатаму, кај големите и комплексни системи, информациите од интерес се распространети насекаде, од различни мобилни и дистрибуирани сетилни уреди, преку камери, микрофони, радио - фреквентни идентификациски читачи, сé до софтверски записи и дневници и безжични сензорски мрежи (Segaran & Hammerbacher, 2009). Ваквата

поставеност ги означува почетоците на т.н. Big Data, колекција од податочни множества толку голема и комплексна, што било која конвенционална метода за менаџирање и обработка на овие податоци не е доволна, па постојано се работи на развој на нови вакви методи (White, 2012). Но огромно количество на достапни податоци може да е од клучно значење за соодветниот систем, бидејќи со нивно правилно процесирање и толкување може да се донесат детерминистички заклучоци за системот и да се дизајнираат попрецизни и поквалитетни управувачки закони.

Иднината на вмрежените системи на автоматско управување е во cloud системи каде елементите на системот ги собираат потребните податоци кои потоа се праќаат и процесираат во големи центри во облакот за обработка на Big Data. Таму на тој начин се генерираат и управувачките сигнали кои потоа се враќаат до системот. Системите на автоматско управување вмрежени во облак и со пристап до специјализирани сметачки центри за работа со големи податочни датотеки ќе овозможат моќни алатки за работа со комплексни системи и процеси, кои до скоро беа незамисливи (Xia Y. Q., 2014).

3. ВЛИЈАНИЕТО НА ЕЛЕКТРОСТАТИЧКИ ПРАЗНЕЊА ВРЗ ПЕРФОРМАНСИТЕ НА ИНДУСТРИСКИ ВМРЕЖЕН СИСТЕМ НА АВТОМАТСКО УПРАВУВАЊЕ: ЕКСПЕРИМЕНТАЛЕН ПРИМЕР

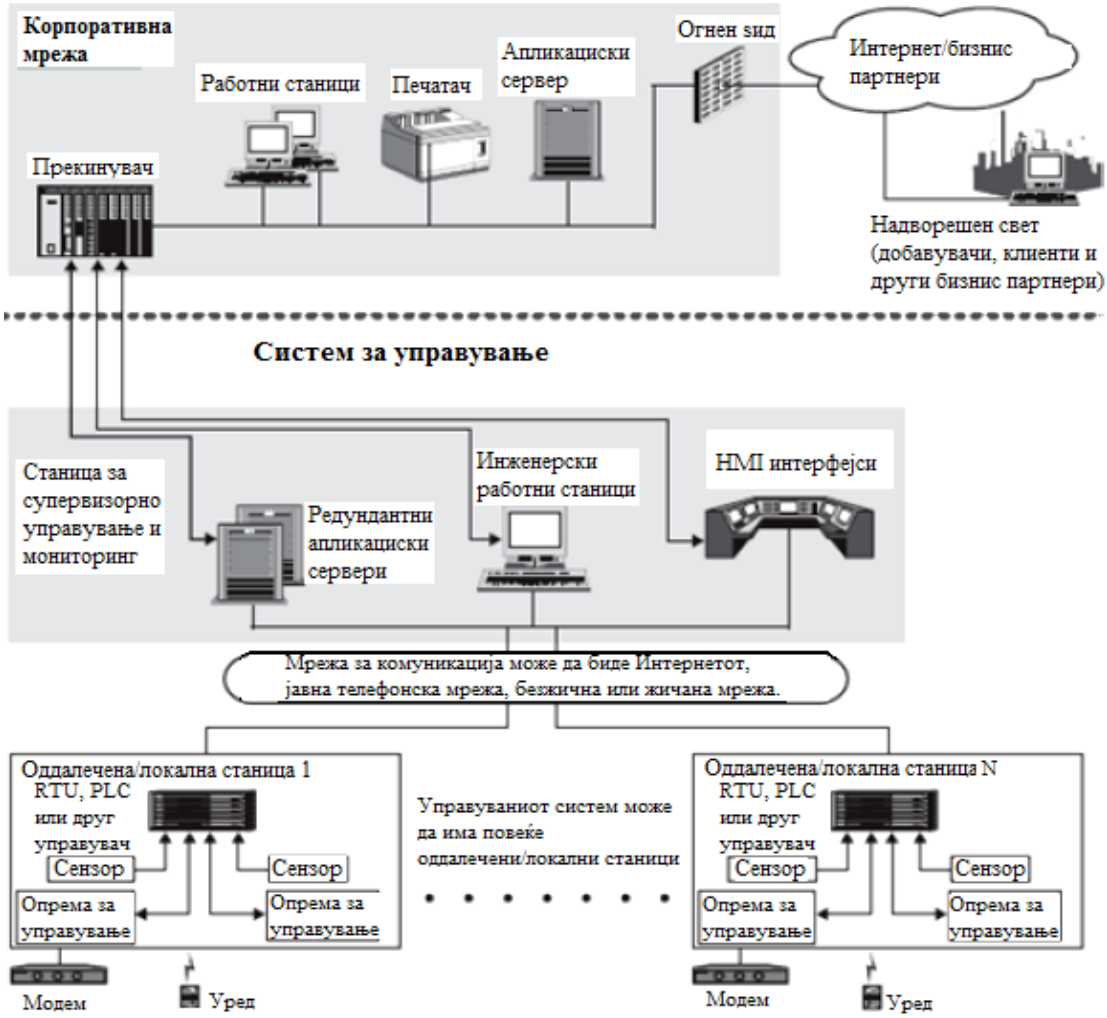
3.1. Шумот кај индустриските вмрежени системи на автоматско управување

Генерално, најголемиот дел од вмрежените системи за управување се користат во индустријата, за набљудување и управување на чувствителни процеси. Обично, системите за управување ги прибираат мерењата од сензорите и оперативните податоци од другите уреди, потоа ги процесираат и прикажуваат информациите и на крај, испраќаат управувачки команди до локалната или оддалечената опрема. Во електроенергетската индустрија тие може да служат за менаџирање и за управување со преносот и испораката на електричната енергија, така што ќе ги отвораат и затвораат прекинувачите и ќе поставуваат прагови за превенција на прекин во работата. Со користење на интегрирани системи за управување, индустриите за нафта и гас можат да управуваат со операциите на рафинериите и далечински да го набљудуваат притисокот и протокот во цевководите или да управуваат со протокот и преносот на нафта и гас. Кај водоводите пак, овие системи може далечински да го набљудуваат нивото во бунарите, протокот на вода, нивото или притисокот во резервоарите и да управуваат со пумпите. Исто така, може да ги набљудуваат карактеристиките за квалитет на водата, како што се pH факторот, заматеноста и присуството на хлор и да управуваат со додавањето на хемикалии. Функциите на системите за управување варираат од едноставни до комплексни. Тие може да се користат за едноставно набљудување на процесите, на пример, условите на средината во некоја канцелариска зграда (наједноставна форма на набљудување), па сé до менаџирање на повеќето (или сите) активности за некој општински систем за вода, па дури и нуклеарна централа.

Предностите на вмрежените системи на автоматско управување кои беа споменати во претходната глава доаѓаат до полн израз кога ваквите системи се имплементираат во индустријата. Потребата од далечинско управување на комплексни процеси во опасни средини и на тешко достапни локации, и од набљудување на голем број на физички величини, сигнали и информации во процесите, ги прави вмрежените системи логично и природно решение во таквите ситуации. Типичен пример за тоа се SCADA (анг. supervisory control and data acquisition - супервизорско управување и собирање на податоци) системите, кои претставуваат комплексна управувачка архитектура која се состои од теренски уреди (сензори и актуатори), подредени локални управувачи (најчесто ПЛУ-а), комуникациска мрежа, терминали за интерфејс, и централна компјутерска

станица која служи за прибирање, фузија и обработка на сите податоци, и за супервизорско управување на највисоко ниво. Денес индустриската автоматика е незамислива без SCADA системите. Но токму клучните концепти на вмрежените системи на автоматско управување кои придонесуваат за нивните предности и за нивното користење во индустријата, се истовремено и причините за ранливост на ваквите системи при нивното функционирање во индустриски услови.

Општ изглед на еден SCADA систем е прикажан на Слика 11.



Слика 11 Општ изглед на SCADA систем (од (US Government Accountability Office, 2004))

Како што беше изложено претходно, шумот има значаен негативен ефект врз поведението и перформансите на вмрежените системи на автоматско управување. Заедничката мрежа или комуникациски медиум која ја користат компонентите на системот всушност додава цело едно ново ниво на ранливост на ВСАУ, бидејќи подложноста на мрежата на шум предизвикува изобличување на сигналите, губење на податочни пакети, или во некои случаи дури и целосен прекин на комуникацијата, секако во зависност од природата и моќноста на шумот.

Шумот во кој влијае на вмрежените системи е од електромагнетна природа, и во поголема мера има природно потекло, па од тие причини е сеприсутен во индустриските средини. Затоа, денес може да се смета дека речиси секоја опрема наменета за работа во индустрија е дизајнирана да биде отпорна на шум и да функционира коректно во негово присуство.

Сепак, дел од шумот во природата е и од вештачко потекло, т.е. е предизвикан од човечките технологии (Bianchi & Meloni, 2007), при што причинители на ваквиот шум можат да бидат радио и телевизиските сигнали, далноводите и системите за транспорт на електрична енергија, итн. Големо влијание на тоа кои се ефектите на шумот има и околината во која тој се јавува, како и карактеристиките на шумот и на сигналот кој тој го попречува, како што се модулацијата, поларизацијата и континуалната или дискретна (импулсна) природа.

Во последните неколку декади нивото на електромагнетна радијација е зголемено заради зачестената употреба на системи за сателитска комуникација и на системи за пренос на електрична енергија. Овој шум обично се наоѓа во ELF (анг. extremely low frequency - екстремно ниски фреквенции) делот од спектарот. Понатаму, во опсегот VLF-HF (анг. very low frequency to high frequency - од многу ниски фреквенции до високи фреквенции), често се наоѓа шум предизвикан од електрични уреди за внатрешна/домашна употреба, како и од системи за индустриска и радио комуникација. Надвор од овие претходно споменати појаси, шум може да се најде и во опсегот SHF-EHF (анг. super high frequency to extremely high frequency - од супер високи фреквенции до екстремно високи фреквенции), но во овој појас оперира само специфична опрема (радарски системи, сателитски комуникациски системи, научна и медицинска опрема) на специфични фреквенции со насочени модели на пропагација, па влијанието на шумот од вештачко потекло овде е доста ограничено.

Една од најчестите и најопасни појави во индустриските средини е електростатското празнење (анг. electrostatic discharge - ESD), кое се случува кога набој на статички електрицитет предизвикува пробив на диелектрикот помеѓу два објекти со различна наелектризираност. Високите напони кои се јавуваат при празнењето се со многу кратко траење, но можат да предизвикаат значителна штета врз секаква електронска опрема. Од тие причини, производителите на таква опрема задолжително вградуваат

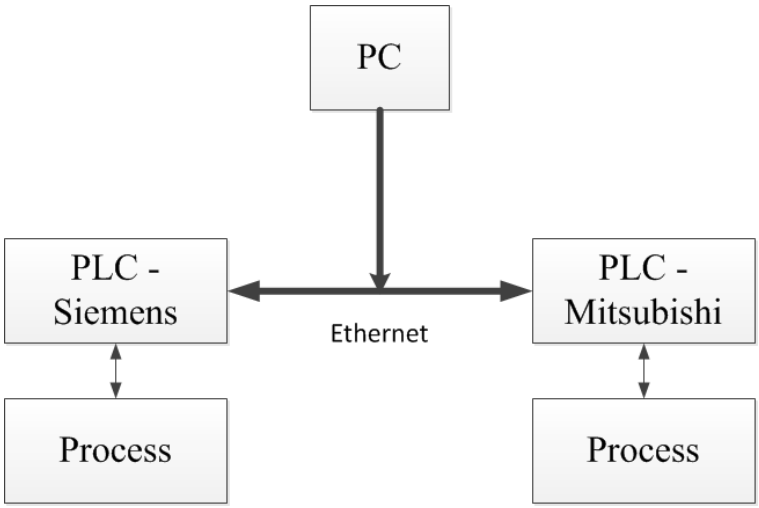
заштита од електростатско празнење и вршат екстензивни тестирања на издржливост при процесот на производство на опремата.

Но кај индустриските системи, електростатското празнење може да има значителен ефект и врз комуникацискиот медиум и да предизвика проблеми како компромитирани податоци, податочни колизии и загуба на пакети, променливи доцнења и слично, пред сé во зависност од пристапот за справување со грешки во податоците кој го користи соодветниот мрежен протокол во системот. Уште посериозен проблем е што електростатските празнења можат да предизвикаат искрење и се особено опасни кога се јавуваат во средини со запаливи материјали, како на пример во хемиската индустрија. Како комуникациски протокол често користен во индустријата, Ethernet се соочувал со доста проблеми предизвикани од електростатското празнење (Greason, 2009). Од тие причини, заштитата и тестирањето на Ethernet опремата за работа во индустриски средини е актуелна и интересна тема (Huang, Tichenor, & et al, 2014).

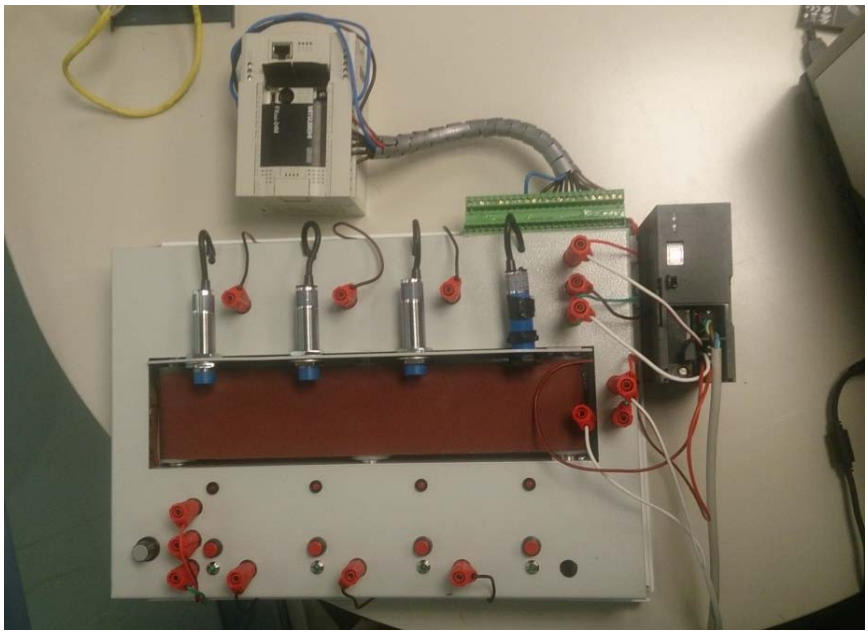
3.2. Експеримент за испитување на влијанието на електростатското празнење врз работата на индустриски вмрежен систем на автоматско управување

Во оваа глава, ќе биде презентиран експеримент во кој е симулирана работата на индустриски вмрежен систем на автоматско управување во околина оптоварена со електромагнетен шум во форма на често електростатско празнење. Целта на експериментот да се испита перформансот на индустриски ВСАУ во такви услови, и да се одредат границите на функционирање и праговите на толеранција.

На Слика 12 е прикажана структурата на испитуваниот систем, а на Слика 13 може да се види и фотографија од неговата поставеност за опишаниот експеримент. Влијанието на електростатското празнење, како честа појава во индустриските услови, се испитува врз два различни видови на програмабилни логички управувачи (ПЛУ) од различни производители - ПЛУ-то од Siemens е S7-1200 (Siemens, 2012), а ПЛУ-то од Mitsubishi е FX3GE (Mitsubishi, 2013).



Слика 12 Блок дијаграм на индустрискиот ВСАУ од експериментот за влијание на електростатско празнење

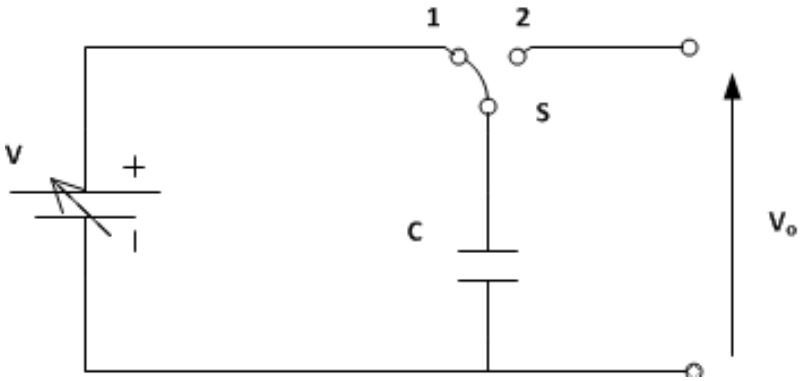


Слика 13 Фотографија од системот за експериментално испитување на електростатски шум врз работата на индустриски ВСАУ

И двата ПЛУ се користат за управување на макети од индустриски процеси кои се состојат од DC мотор кој движи подвижна лента како дигитален излез, од неколку индуктивни и фотоелектрични близински сензори како дигитални влезови, и од еден потенциометар како аналоген влез во управувачот. Преку Ethernet врска, управувачите се поврзани со централен компјутер на кој се извршува SCADA апликација за надгледување,

контрола и супервизорско управување на процесите. Управувачките алгоритми во секое од ПЛУ-ата се едноставни и базирани на бинарна логика, какви што најчесто можат да се сретнат во реални услови, и се состојат само од проверка на состојбата на влезовите и соодветна реакција, без притоа да се однесуваат на било кој друг аспект во мрежата.

Шумот се симулира со помош на систем за генерирање на електростатско празнење (Слика 14). Всушност станува збор за едноставно коло кое се состои од батериски извор на напон, чија вредност е променлива и може да варира од 0 до 8 kV, и од кондензатор со капацитет од 150 pF.



Слика 14 Коло за генерирање на електростатско празнење

Превклучувачот S го поставува системот во една од две можни состојби: кога е во состојба 1 батеријата го полни кондензаторот C, а кога е во позиција 2 кондензаторот е подготвен да ја испразни акумулираната енергија во околината на системот. Празнењето може да е и контактно и бесконтактно, во зависност од тоа дали излезните електроди на системот се во физички допир со некој објект или само во негова непосредна близина.

Во конкретниот случај, објектот во прашање може да е самиот програмабилен управувач, или пак каблите преку кој се поврзани и комуницираат управувачите и компјутерот. Како и да се одвива празнењето, се генерираат кратки напонски импулси со големи амплитуди кои ја попречуваат нормалната работа на опремата, а пред сé влијаат на податочните пакети во комуникациската мрежа.

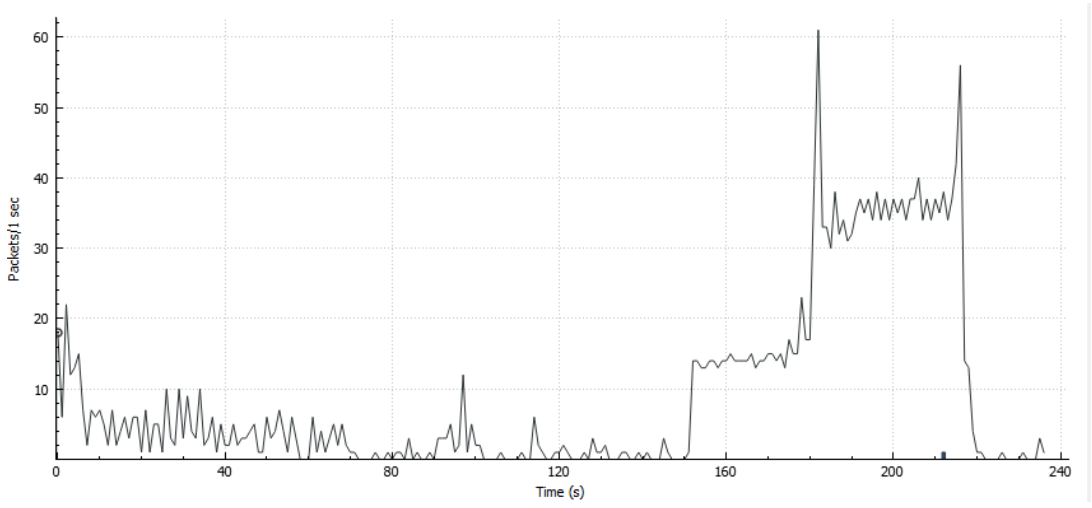
Слични уреди за генерирање на електростатско празнење се користат за испитување на доверливоста на индустриската опрема по нејзиното производство и за тестирање на границите на нејзината издржливост и функционалност во условите за кои е наменета да функционира (Pommerenke, Fan, & Drewinak, 2016). Во овој случај, ваквиот принцип го тестираше прагот на толеранција кон електростатски шум на комуникациската

мрежа од индустрискиот ВСАУ, а со тоа и границите на функционалност на целокупниот систем во такви услови.

3.3. Анализа на резултатите

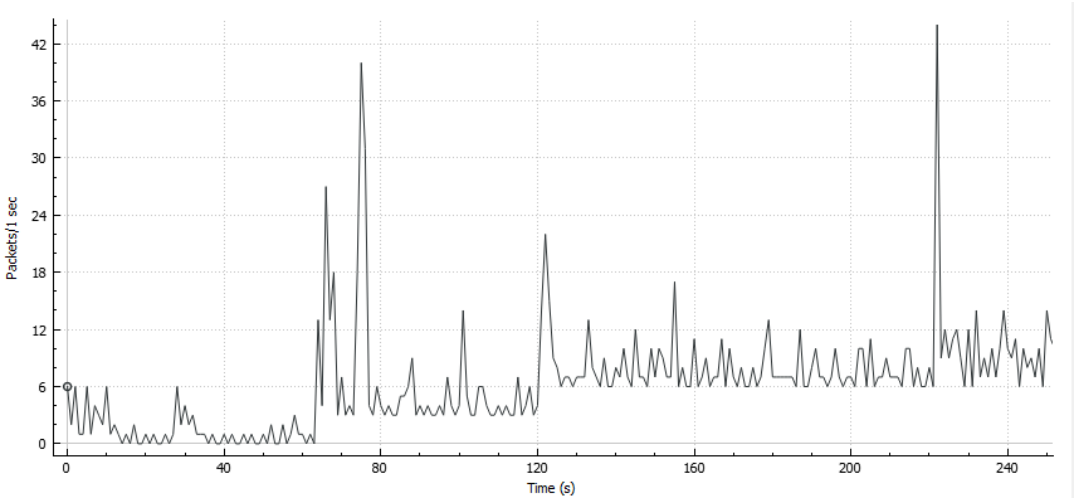
Целокупниот сообраќај на податоци во системот е испитуван со помош на специјализираниот софтвер WireShark, кој служи за евиденција на бројот на податочни пакети кои минуваат низ мрежата која е набљудувана. Преку комбинација на мониторирање на сообраќајот и набљудување на функционирањето на управуваниот процес, се доби реална претстава за ефектот на шумот во форма на електростатско празнење врз системот.

Најпрво е испитана функционалноста на целиот систем во отсуство на шум, т.е. во нормални околности. На Слика 15 може да се види протокот на податоци помеѓу програмабилниот логички управувач FX3GE и надредената SCADA апликација, претставен како график на бројот на успешно доставени податочни пакети во единица време, во одреден временски период.



Слика 15 График на протокот на податоци во ВСАУ со FX3GE ПЛУ во нормални околности

Истиот график, но овој пат за програмабилниот логички управувач од типот S7-1200, е прикажан на Слика 16.



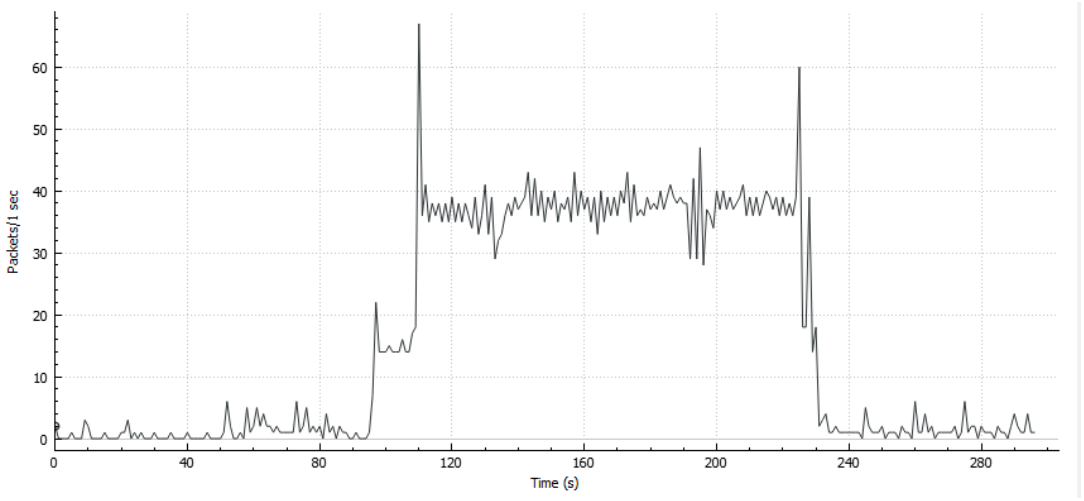
Слика 16 График на протокот на податоци во ВСАУ со S7-1200 ПЛУ во нормални околности

Од графиците може да се заклучи дека сообраќајот помеѓу ПЛУ и надзорниот компјутер се одвива нормално и непречено. Прекини на комуникацијата нема, а периодот на интензивиран проток на пакети кој се гледа на Слика 15 (во периодот помеѓу 150 секунди и 220 секунди) се должи на зголемената корисничка активност во SCADA апликацијата, т.е. на внесување на нови надредени команди и нови референтни вредности кои требаше да се проследат до ПЛУ-то. Ова е направено со цел да се види очекуваниот ефект на ваквата активност врз сообраќајот во мрежата и на тој начин да се валидира веродостојноста на експериментот.

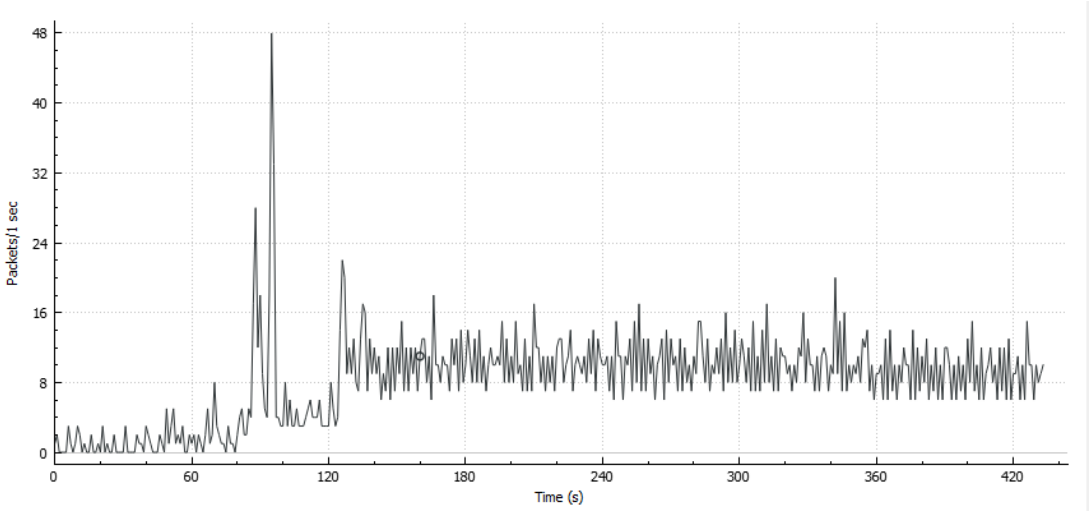
Може да се забележи дека просечниот број на пакети кај FX3GE е поголем отколку оној кај S7-1200, но големината на пакетите кај ПЛУ-то на Siemens е поголема од онаа кај Mitsubishi, па и во двата случаи просечниот број на успешно пренесени податоци низ мрежата во единица време е околу 690 бајти во секунда.

Понатаму, истото испитување е направено во услови на појава и зголемено присуство на електростатско празнење во околината на системот. Уредот за генерирање на празнењето е вклучен и напонот на изворот постепено се зголемува, набљудувајќи ги последиците врз системот. Празнењето се врши и преку директен контакт на електродите на уредот со терминалите на ПЛУ-та и со Ethernet кабелот, како и преку индиректно бесконтактно празнење во опкружувачката околина на системот.

Со зголемување на амплитудата на пулсовите до 7 kV не се забележани значителни ефекти врз работата на системот. Како пример може да се прикаже ситуацијата при генерирање на електростатско празнење од 6 kV, при што на Слика 17 е прикажан протокот на податоци низ мрежата при комуникацијата помеѓу централниот компјутер и FX3GE, а на Слика 18 се прикажани истите податоци при комуникацијата со S7-1200.



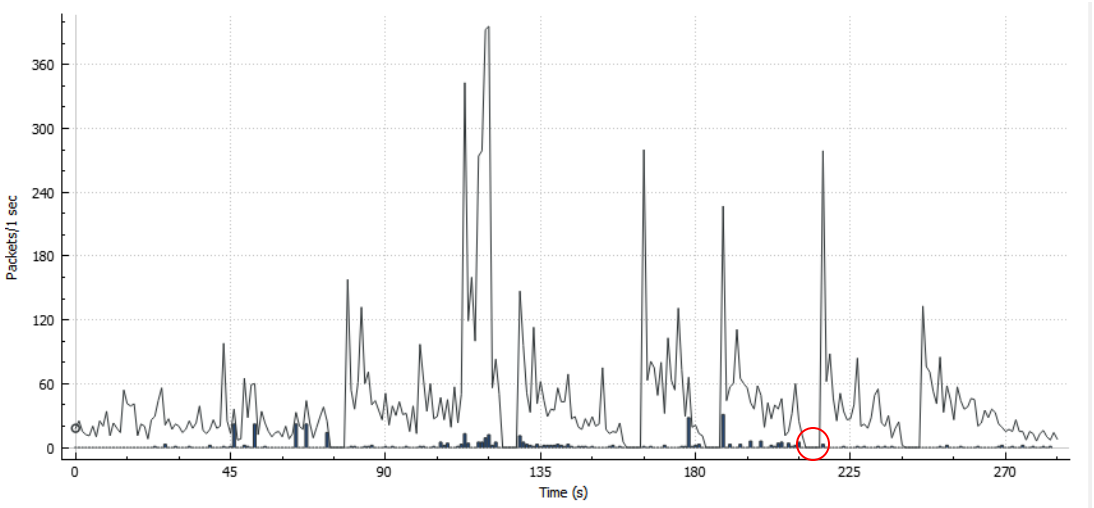
Слика 17 График на протокот на податоци во ВСАУ со FX3GE ПЛУ во услови на електростатско празнење со амплитуда од 6 kV



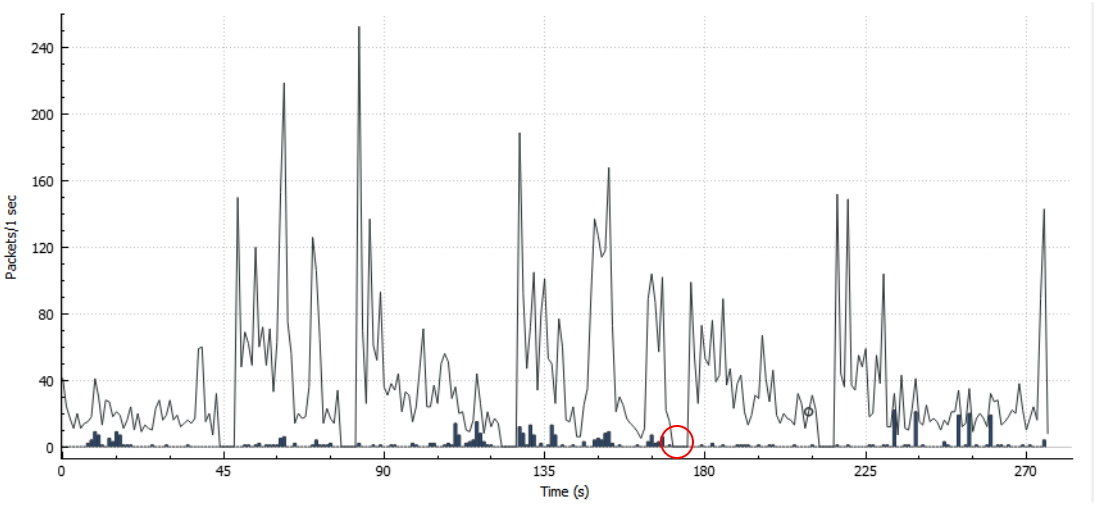
Слика 18 График на протокот на податоци во ВСАУ со S7-1200 ПЛУ во услови на електростатско празнење со амплитуда од 6 kV

Очигледно е дека електростатскиот шум нема никаков позначителен ефект врз коректната работа на системот без разлика на тоа за кој ПЛУ станува збор. Вредно е уште да се одбележи и дека кај FX3GE повторно се јавува сообраќај со зголемен интензитет во ситуација кога се зголемува корисничката активност на страната на SCADA апликацијата.

Значителни промени во перформансите на системот конечно се забележуваат по надминување на вредноста од околу 7 kV на напонот на променливиот извор во уредот. На Слика 19 и Слика 20 се прикажани графиците на проток на сообраќај во ситуација кога напонот на пулсовите на електростатското празнење е 8 kV - на горната граница која беше можна во конкретниот експеримент. Притоа, електростатски пулсови се генерирани на секои 30 секунди.



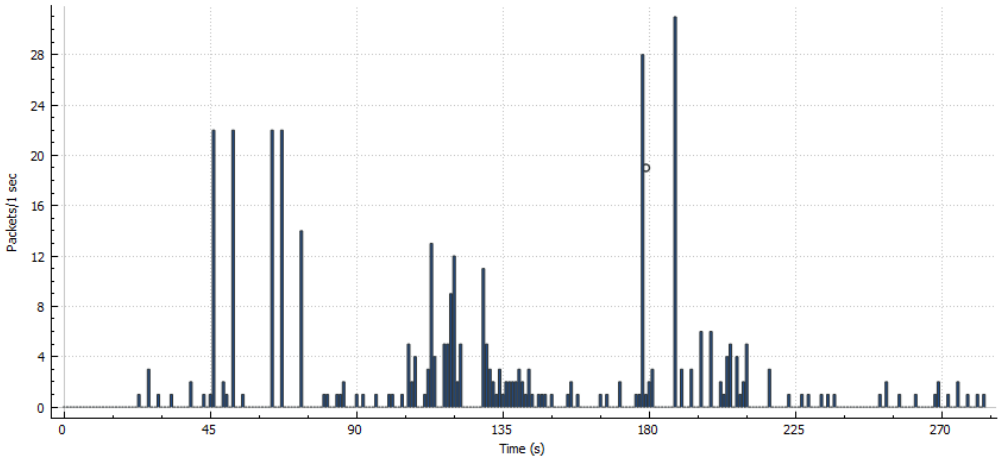
Слика 19 График на протокот на податоци во ВСАУ со FX3GE ПЛУ во услови на електростатско празнење со амплитуда од 8 kV



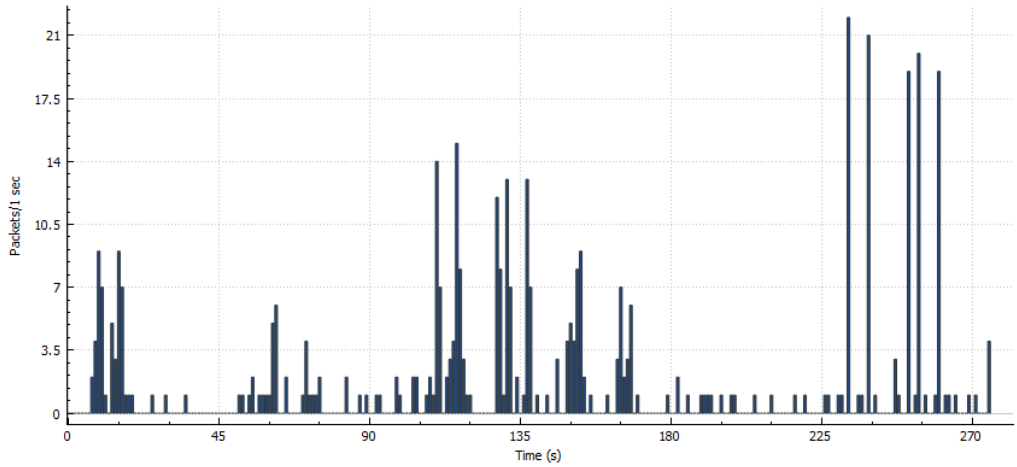
Слика 20 График на протокот на податоци во ВСАУ со S7-1200 ПЛУ во услови на електростатско празнење со амплитуда од 8 kV

Во двата случаи може да се забележи дека доаѓа до целосен прекин на комуникацијата, видлив во моментите кога протокот на пакети низ мрежата паѓа на нула (на двете слики по еден ваков пример е обележан со црвени кругови). Овие моменти се логично проследени со значително зголемување на протокот како резултат од обидите комуникациската врска да се воспостави одново. Понатаму, дури и во остатокот од времето кога нема прекини на врската, осцилациите на сообраќајот се интензивни. Се случуваат и грешки во податочните пакети, т.е. корупција и изобличување на податоците; овие грешки се детектираат со помош на соодветен алгоритам на детекција на приемната страна (вакви алгоритми се дел од комуникацискиот протокол и егзистираат и кај централниот компјутер и кај секој од управувачите), и при појава на истите се бара препраќање на засегнатион пакет. Овие корумпирани пакети се прикажани со сини вертикални графови на Слика 21 и Слика 22, но можат да се видат и на Слика 19 и Слика 20 на истите графици со протокот на пакетите во соодветните случаи. На овие слики лесно се забележува зголемувањето на сообраќајот по појавата на згрешени пакети, што се должи на нивното препраќање.

Неправилната работа на системот во овој случај е евидентна и од увиденото непредвидливо однесување на управуваните процеси, до кое доаѓа заради непостојаноста на информациите и командите кои доаѓаат од централната SCADA апликација.



Слика 21 График на корумпирани (згрешени) податочни пакети во ВСАУ со FX3GE ПЛУ во услови на електростатско празнење со амплитуда од 8 kV



Слика 22 График на корумпирани (згрешени) податочни пакети во ВСАУ со S7-1200 ПЛУ во услови на електростатско празнење со амплитуда од 8 kV

Заради ограниченост на достапната опрема, понатамошни експерименти за напон поголем од 8 kV не се направени. Сепак, утврдено е дека и на оваа амплитуда, генерираното електростатско празнење веќе има видлив ефект врз системот. Како заклучок, може да се каже дека и покрај тоа што програмабилните логички управувачи се сметаат за робусна индустриска опрема и како такви се дизајнирани да работат во тешки и сурови услови кои владеат во средините на индустриската автоматика, сепак во конкретниов случај електростатскиот шум целосно ја попречи нивната коректна работа. Причината за ова е ранливоста на мрежата од индустриски Ethernet која беше искористена за комуникација помеѓу управувачите и централниот компјутер.

Како Ethernet, така и останатите најчесто користени индустриски протоколи за комуникација (Fieldbus, Profibus, HART) се подложни на ефектите од електростатско празнење, а индустриските вмрежени системи на автоматско управување мора да се гледаат како целина од сите составни компоненти. Ова значи дека ранливоста на комуникациската мрежа подразбира и ранливост на целиот ВСАУ, без разлика на фактот дека самите управувачи се отпорни. Тоа подразбира дека е неопходен развој на методи и начини за справување со негативните ефекти на шумот врз сите елементи и аспекти од вмрежените системи, за да се осигура нивна отпорност, доверливост, и правилно функционирање во такви услови.

4. БЕЗБЕДНОСТ НА ВМРЕЖЕНИТЕ СИСТЕМИ НА АВТОМАТСКО УПРАВУВАЊЕ

4.1. Основи на индустриските ВСАУ

Индустриските вмрежени системи за управување, кои всушност целосно ги опфаќаат и се идентични на SCADA системите (накратко дискутирани во претходната глава), обично вклучуваат голем број на сензори, актуатори и софтвер за управување кои се користат на различни, меѓусебно оддалечени локации. Денес, тие се длабоко навлезени во основата на сите критични инфраструктурни сектори. На почетокот, SCADA системите користеле релативно примитивни сериски протоколи и комуникациски инфраструктури за поврзување на нивните компоненти и за пренос на податоците и управувачките команди. Исто така, оперативните барања биле поважни од безбедноста, бидејќи SCADA опремата била физички и логички изолирана од другите мрежи. Овие компјутеризирани системи за управување на процеси во реално време сé повеќе се мета на сајбер (анг. cyber) напади кои можат да предизвикаат сериозна штета поради стандардизацијата на системите и нивната поврзаност со други мрежи. Генерално, може да се смета дека SCADA системите имаат слаба заштита од сé пософистицираните сајбер закани.

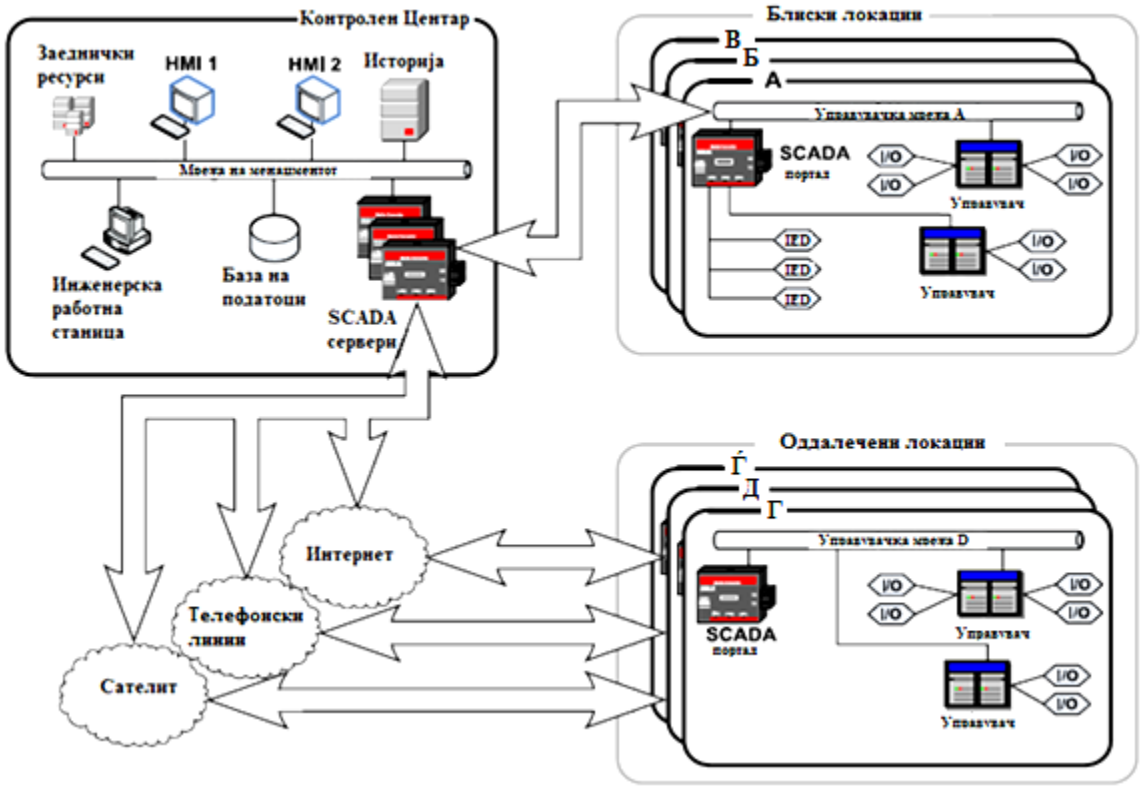
Модерните индустриски објекти, како што се нафтените рафинерии, хемиските фабрики, електричните централи и производствените објекти се големи дистрибуирани комплекси. Операторите мораат континуирано да набљудуваат и управуваат многу различни оддели во ваквите објекти за да обезбедат нивно правилно функционирање. Развојот на мрежните технологии овозможил далечинско управување на ваквите дистрибуирани комплекси. Првите типови на мрежи за управување биле едноставни мрежи од типот точка-до-точка (анг.point-to-point), кои поврзувале набљудувачки или команден уред со оддалечен сензор или актуатор. Овие мрежи еволуирале во комплексни мрежи кои поддржуваат комуникација помеѓу централна управувачка единица и повеќе далечински единици на иста комуникациска магистрала. Јазлите на овие мрежи обично се уреди со специјални задачи, како што се сензорите, актуаторите, управувачите (најчесто програмабилните логички управувачи), уреди за набљудување и дијагностика, итн.

Во денешните конкурентски пазари од есенцијална важност за индустриите е модернизацијата на нивните дигитални SCADA мрежи, со цел намалување на трошоците и зголемување на нивната ефикасност. Голем дел од денешните SCADA мрежи се поврзани на корпоративните мрежи и на Интернет. Ваквата поврзаност може да помогне во оптимизација на процесите на производство и дистрибуција, но во исто време овие безбедносно- критични индустриски мрежи ги изложува на огромен број на безбедносни

проблеми кои одат во пакет со Интернетот. Доколку процесите се набљудувани и управувани од уреди кои се поврзани преку SCADA мрежа, тогаш еден напад на SCADA мрежата има потенцијал да предизвика значителна штета на постројката. Покрај физичките и економски загуби на кои е изложена компанијата, нападот на SCADA мрежата може негативно да влијае на околината и да ја загрози јавната безбедност. Поради тоа, безбедноста на мрежите кај овие индустриски ВСАУ е од примарно значење.

4.1.3. Архитектура на SCADA мрежа

SCADA мрежата овозможува меѓусебна поврзаност на повеќе теренски уреди во рамките на фабриката. Овие уреди, во кои спаѓаат сензорите и актуаторите, се набљудувани и управувани преку SCADA мрежи од PC или од програмабилни логички управувачи (ПЛУ). Во многу случаи, фабриките имаат и контролни центри преку кои се води грижа за целата фабрика. На Слика 23 е претставена референтната мрежна архитектура на SCADA системите, која се користи за претставување на функционалниот дизајн и на аспектите на меѓуповрзаност на елементите во SCADA мрежите. Може да се каже дека SCADA мрежата, всушност, се состои од две основни компоненти, а тоа се контролниот центар и процесот што се управува (локации од А до Ѓ на Слика 23).



Слика 23 Архитектура на генеричка SCADA мрежа

Контролниот центар обично се наоѓа во физички одделен дел од процесот и е составен од напредни компјутерски и комуникациски уреди. Модерните контролни центри имаат податочни сервери, станици со PC/PLC интерфејси (Human-Machine Interfaces - HMIs) наменети за операторите, работни станици, бази на податоци, сервери за чување на историјата на процесот и други ресурси кои им помагаат на операторите во целосното управување и оптимизирање на процесите и постројките во фабриките. Неговите компоненти комуницираат преку користење на мрежата на менаџментот, додека контролниот центар и деловите од процесот што се блиску до него (Локации А, Б, В) се поврзани преку SCADA сервер. Во зависност од нивните протоколи на пониско ниво, SCADA серверите обично се имплементирани со специјален софтвер добиен од производителот и нивните услуги се често базирани на OPC стандардот (Byres & Nguyen, 2000). Контролниот центар и оддалечените локации (Локации Г, Д, Ѓ) најчесто се поврзани преку радио или сателитски врски, телефонски линии или Интернет.

Една мрежа за управување (пример: А) има три видови на компоненти: управувачки уреди, I/O уреди и SCADA портал (анг. gateway). Управувачките уреди, во кои спаѓаат:

- Програмабилни логички управувачи (PLC),
- Далечински терминални единици (RTU) ,
- Влезно/излезни управувачи (IOC),
- Интелигентни електронски уреди (IED),

ја имплементираат управувачката логика. Овие уреди манипулираат со I/O уредите (сензори и актуатори). Сензорите мерат специфични процесни параметри (пример: температура или притисок), а актуаторите извршуваат управувачки акции (пример: отвораат или затвораат вентил), ќе со цел генерирање на посакуваните промени врз процесните параметри.

Операторите во контролниот центар користат PC/PLC интерфејси (HMI) за да комуницираат со системите одговорни за индустриските процеси. Од друга страна, операторите на инженерските работни станици мора да имаат авторитет врз целата SCADA мрежа. Тие мораат да можат да ги реконфигурираат HMI и управувачките уреди и да ги модифицираат управувачките алгоритми (пример: скалестиот дијаграм).

Базата на податоци, сместена во контролниот центар, ги чува сите податоци за процесните параметри и управувачките акции. Операторите на инженерските работни станици ја користат базата на податоци за да добијат пристап и да ги модифицираат процесните податоци и управувачките променливи. Уредите за чување на историјата ги архивираат податоците за активностите на SCADA мрежата, вклучувајќи ги:

- Податоците од сензорите,
- Управувачките акции иницирани од операторите на инженерските работни станици и на HMI,
- Најавите на вработените во мрежата на менаџментот.

Мрежата на менаџментот содржи различни заеднички ресурси (принтери, факс-машини и податочни сервери), меѓутоа овие ресурси обично не се сметаат за дел од SCADA мрежата. Сепак, сé позачестена појава е корпоративните мрежи да се поврзуваат со SCADA мрежите.

SCADA порталот ги поврзува компонентите на управувачката мрежа кои не можат директно да комуницираат со SCADA серверот. Во зависност од функционалноста, секој управувачки уред може да служи како SCADA портал. Најчесто се користат специјални единици наречени front-end процесори (FEP) како SCADA портали во индустриските управувачки средини. Исто така, преку овие специјализирани портали, SCADA мрежата е поврзана со надворешната корпоративна мрежа и/или со Интернет (Sauter & Schwaiger, 2002), (Schwaiger & Treytl, 2003). Овие портали нудат интерфејс помеѓу IP-базираните мрежи од надворешна страна и SCADA мрежите базирани на Fieldbus протоколите од внатрешна страна. Порталот обезбедува механизми за конверзија на протоколите, за да овозможи комуникација помеѓу двете различни мрежи. Исто така, порталот нуди и cache механизми за податочните објекти кои се разменуваат помеѓу мрежите, со цел подобрување на неговата функционалност (Sauter & Schwaiger, 2002).

Барањата за функционалноста и дизајнот на SCADA мрежите зависат и од работните услови на мрежата (Decotignie, 1996). Овие услови влијаат на топологијата на мрежата и на мрежните протоколи, па така SCADA мрежите имаат одредени уникатни карактеристики. На пример, најголемиот дел од терминалните уреди во Fieldbus мрежите се вградливи компјутерски системи за извршување на специјални задачи, со ограничени пресметувачки можности и функционалности. За разлика од корпоративните мрежи кои имаат премногу елементи, многу од индустриските апликации на SCADA мрежите како што се мрежите за дистрибуција на електрична енергија се обично поедноставни, но сепак се географски широко распространети.

Слично, физичките услови во фабриката значително се разликуваат од условите на корпоративната, канцелариска средина. Двете мрежи, корпоративната и фабричката се често подложени на промени во температурата, електромагнетни влијанија и акумулација на одредена количина на прашина. Сите овие услови го зголемуваат шумот во мрежата и го намалуваат работниот век на проводниците. Во спецификациите за физичкото ниво на

мрежата мора да бидат земени во предвид начинот за справување со шумот во мрежата и способноста на опремата да издржи вакви услови.

Во типичните комуникациски архитектури на SCADA мрежите спаѓаат и управувачките пораки кои се разменуваат помеѓу господар и роб (анг. master and slave) уредите. Master-от е уред кој може да управува со операциите на другите уреди, како на пример PC или PLC. Slave-от обично е некој уред како едноставен сензор или актуатор кој може да испраќа пораки на командниот уред и да извршува акции зададени од истиот. Мрежниот протокол е тој што треба да обезбеди услови за комуникација, на пример, помеѓу Fieldbus уредите кои сакаат да комуницираат рамноправно. За да се задоволат овие барања, протоколите како што е PROFIBUS имаат хибриден комуникациски модел кој вклучува peer-to-peer комуникација помеѓу master уредите, а клиент-сервер комуникација помеѓу master-от и slave-овите. Комуникацијата помеѓу уредите може да биде асиметрична (Risley, Roberts, & LaDow, 2003) (на пример, пораките пратени од slave-от до master-рот обично се многу поголеми од пораките пратени во обратната насока). Некои уреди пак, можат да комуницираат само преку аларми и статусни пораки.

Бидејќи многу уреди користат заедничка магистрала, протоколот мора да има процедури за доделување на приоритет на пораките. Ова помага во разликување на критичните и некритичните пораки. На пример, една алармна порака за можно нарушување на безбедноста треба да има предност во однос на регуларните пораки за ажурирање на податоците. Протоколите во SCADA мрежите, исто така, мора да обезбедат одреден степен на стабилност и сигурност во пристигнувањето на пораките до саканата дестинација. Многу фабрички процеси имаат потреба од реалновременска комуникација помеѓу теренските уреди. Затоа, мрежниот протокол треба да има одредени карактеристики кои не само што ќе обезбедат пристигнување на критичните пораки на саканата дестинација, туку и ќе го обезбедат истото пристигнување во рамките на зададените временски ограничувања.

4.2. Аспекти на безбедност кај SCADA системите

4.2.1. Разлики помеѓу SCADA и информатичките (IT) системи од аспект на безбедноста

Во SCADA системите или системите за управување генерално, фактот што секоја логичка акција во системот има директно влијание во физичкиот свет, диктира безбедноста да биде поважна од сé. Бидејќи се применуваат во подрачја каде што можат да бидат загрозени човечки животи и индустриски и еколошки средини, теренските уреди во SCADA системите имаат иста важност како и централните компјутери (Byres, Carter,

Elramly, & Hoffman, 2002). Исто така, одредени оперативни системи и апликации што се користат во SCADA системите и кои се неконвенционални за типичниот ИТ (информатички) персонал, може да не ги поддржуваат комерцијалните ИТ решенија за сајбер безбедност. Понатаму, факторите како што се барањата за постојана достапност, временската ограниченост, ограничените пресметувачки ресурси на уредите, големите физички бази, постојаната комуникација помеѓу дигиталните и аналогните уреди, социјалното прифаќање, вклучувајќи го и отпорот на промени од страна на корисниците и др., се причина SCADA системите да се прилично комплексна цел за безбедносното инженерство.

Како што беше изложено во претходните глави, SCADA системите како претставници на вмрежените системи на автоматско управување, преставуваат строги системи на реално време, бидејќи завршувањето на некоја операција надвор од одредена временска рамка се смета во најмала рака за бескорисно, а во посериозен случај и за потенцијална опасност од причина што може да има каскаден ефект во физичкиот свет (Silberschatz, Baer Galvin, & Gagne, 2005). Временските рамки за извршување на операциите, почнувајќи од некој настан па сé до одговор од системот, поставуваат строги ограничувања; пропуштање на временската рамка или ненавремено извршување на соодветната операција може да предизвика комплетна нефункционалност на системот. Исто така, латентноста е многу деструктивна во работата на SCADA системите. Ако системот не реагира во дадената временска рамка може да настанат безбедносни пропусти како што се оштетувања на околината и опасност по човечки животи. Разликата помеѓу строгите и софт-системите на реално време е повеќе во исполнувањето на временскиот рок, отколку во должината на временската рамка. За споредба, софт-системите на реално време, какви што се аудио-видео системите во живо можат да толерираат одредена латентност и да одговорат со намален квалитет (пример: отфрлање на рамки при прикажување на видео). Малото отстапување од временските ограничувања кај овие системи повеќе води кон намален квалитет отколку кон нефункционалност на системот. Поради физичката природа на задачите во рамки на процесите кои ги извршуваат SCADA системите, често се јавува потреба тие да бидат прекинати и рестартирани. Временскиот аспект и прекините на задачите можат да ги отфрлат од употреба конвенционалните алгоритми за блоковска енкрипција.

Уште една исклучително значајна разлика е тоа што, како системи за работа во реално време (RTOS), ранливоста на SCADA системите се зголемува поради фактот што алоцирањето на меморија во ваквите системи е покритично во однос на другите оперативни системи. Многу теренски уреди во SCADA системите се вградливи системи што може да работат и неколку години без да се рестартираат со што само ја акумулираат фрагментацијата. Поради тоа, преполнувањето на баферите е попроблематично кај SCADA системите, отколку кај традиционалните ИТ системи.

4.2.2. Безбедносни цели кај SCADA системите

Поради погоре изложените разлики помеѓу SCADA и ИТ системите, оперативните системи и апликациите кои ги користат SCADA системите мора да исполнуваат специјални барања во однос на нивната функционалност и доверливост. Дури и на места каде безбедноста е добро дефинирана, примарната цел во Интернетот е да се заштити централниот сервер, а не крајниот корисник. Кај процесното управување пак, дури и еден периферен уред како што е ПЛУ или некој паметен управувач, не е ништо помалку важен од централниот сервер, бидејќи и двата уреди може да предизвикаат несакани последици од типот на загрозени човечки животи или промени во еколошките средини (Byres, Carter, Elramly, & Hoffman, 2002).

Овие разлики помеѓу SCADA системите и ИТ системите бараат дефинирање на прилагодливо множество на безбедносни цели, а со тоа и безбедносни и оперативни стратегии. Кај ИТ системите, најважни се доверливоста и интегритетот, додека во системите за управување тоа се достапноста на системот и интегритетот на податоците.

Најголем дел од истражувањата во областа на компјутерска безбедност се фокусирани на доверливоста. Безбедносните особини на SCADA системите се подредени според важноста и потребите во индустријата, посебно во секторот на управување. Ова е важно поради специјалните потреби на SCADA системите, како што се на пример временската критичност, дисперзираноста, и континуалната достапност. Постојат различни верзии на дефинирање и примена на безбедносните особини со мали меѓусебни разлики (Anderson, 2001). Меѓутоа, со цел да се направи разлика меѓу системите на управување и стандардните ИТ системи, потребно е да се објаснат уште неколку својства. Притоа, овие својства во одредени аспекти се заеднички и за двата системи.

- Навременоста, која експлицитно ја изразува временската критичност на системите за управување во реално време, во кои се вбројуваат и SCADA системите.

  Тука спаѓаат способноста за навремен одговор на системот (пример: команда од управувач до актуатор треба да биде извршена во реално време), и временската точност на испораката на било кои податоци во дадениот временски период, односно со други зборови свежината на податоците (пример: податоците се валидни само во одредениот временски период)

  Генерално, ова својство кажува дека било која барана, процесирана и испратена информација не треба да биде застарена, туку да одговара на реалниот временски момент и дека системот е доволно способен и чувствителен за навремено процесирање на барања кои потекнуваат од нормална или оправдана човечка интервенција. Во реалноста, доколку пораката не стигне навреме или пристигне повеќе пати до одреден јазол ќе се смета дека истата не е добра, иако нејзината содржина е неизменета, било да е тоа команда за актуатор или некакво мерење од

сензор. Фактички, секое препраќање на податоци лесно ја прекршува оваа безбедносна цел. Понатаму, редот на пристигнување на податоците во централата за надзор може да има големо влијание врз динамиката на процесот и врз носењето на точни одлуки на алгоритмите за управување или на човечките оператори.

- Достапноста, која означува дека секоја компонента од SCADA системот, без разлика дали е тоа сензорски или сервомеханички уред, комуникациска или мрежна опрема, радио канал, компјутерски уред, информација од сензор или управувачка команда, треба да биде подготвена за употреба, кога тоа е потребно. Најголем дел од процесите управувани од SCADA системите се континуални по природа. Неочекувани прекини на системите што ги управуваат индустриските процеси се неприфатливи. За ова посакувано својство на SCADA системите како и на безбедносните цели, потребно е користениот безбедносен механизам, вклучувајќи го и криптографскиот систем, да не ја деградира одржливоста, оперативноста и пристапноста на системот во итни случаи.

- Интегритетот, кој подразбира да генерирањето, пренесувањето, прикажувањето и чувањето на податоците во SCADA системите биде оригинално и без влијание од неовластени интервенции, вклучувајќи ја тука и нивната содржина, која пак може да ги содржи заглавието на испраќачот, дестинацијата и временската информација. Сличен термин за ова својство е автентичноста, која кај SCADA системите подразбира дека идентитетот на испраќачот и примачот на секоја информација треба да биде вистински. Според оваа дефиниција, интегритетот и автентичноста спаѓаат во иста категорија. Може да се замисли колку катастрофални би биле последиците, доколку некаква управувачка команда се пренасочи до некој актуатор наместо до саканата дестинација или пак, доколку се испрати лажна или грешна информација за адресата на испраќачот, од некој сензор до централниот управувач. Таканаречениот внатрешен интегритет на пораките подразбира содржината на пораката да биде оригинална, додека пак интегритетот помеѓу пораките се однесува на обезбедување на интегритет на податоците, така што протоколот не смее да дозволи напаѓачот да конструира неовластени пораки, да изменува пораки кои што во моментот се испраќаат, да го менува редоследот на пораките, да препраќа стари пораки или пак, да уништува пораки без да биде откриен.

- Доверливоста, која се однесува на тоа дека неовластена личност не треба да има никаков пристап до информации поврзани со SCADA системот. SCADA системите со помош на команди ги мерат и управуваат физичките процеси кои генерално се од континуална природа и одзивите обично се едноставни и повторливи, така што е релативно лесно да се предвидат пораките во овие системи. Оттука доверливоста е помалку важна во однос на интегритетот на податоците. Меѓутоа, доверливоста на критичните информации како што се лозинките, енкрипциските клучеви, деталните

мапи на системот итн., треба да се рангира високо кога станува збор за безбедноста во индустријата. Во овој аспект треба да се примени и дополнителна заштита. Исто така, информацијата која е вклучена во физичката содржина која се испраќа до управувачкиот алгоритам може да биде предмет на напади, со цел да се открие некоја критична порака. Драстичната разлика во подредувањето на посакуваните безбедносни својства настанува најмногу поради тоа што се очекува SCADA системите да бидат оперативни во реално време и да функционираат континуално.

- Милосливата деградација (анг. graceful degradation), која подразбира системот да биде способен да го задржи нападот на локално ниво и да го одржи текот на податоците во одреден регион, без да дозволи понатамошна ескалација во целосен системски, каскаден настан.

Сите овие посакувани безбедносни својства не се исклучуваат меѓусебно, туку се блиско поврзани. На пример, со пробивање на интегритетот, напаѓачот може да ги промени управувачките сигнали за да предизвика нефункционалност на некој уред, што пак може да влијае на достапноста на мрежата.

4.2.3. Ранливости кај SCADA системите

Сегашната пракса во SCADA системите остава отворени врати за различни видови на ранливости. Тука спаѓаат мрежната инфраструктура на компанијата која го користи соодветниот SCADA систем, несигурната мрежна архитектура, ранливостите на оперативниот систем кои овозможуваат пристап на неовластени корисници, како и примената на безжични уреди. Во главно, непостоењето на реално - временски надзор и добра енкрипција влијаат за намалена безбедност на SCADA системите.

Сајбер нападите на SCADA системите можат да дојдат преку различни патишта како што се Интернет поврзувањата, корпоративните мрежни поврзувања и поврзувањата со други мрежи, до ниво на управувачките мрежи или пак, до ниво на теренските уреди. Најчестите стратегии користени од напаѓачите се:

- Користење на пропусти во мрежниот периметар,
- Користење на ранливостите на протоколите,
- Сајбер напади на теренските уреди,
- Напади на базите на податоци,
- Напади на временските рамки и синхронизацијата.

Од инженерска гледна точка, нападите можат да се групираат во следните категории:

- Лажни влезни податоци на управувачот, добиени од компромитирачки сензори и/или пробиена мрежна врска помеѓу управувачот и сензорите,

- Манипулирани или погрешни излезни податоци од управувачот до актуаторите или компромитирана мрежна врска помеѓу управувачот и актуаторите,
- Историја на управувачот,
- Недостапност на услуга (анг. Denial of Service)- пропуштање на роковите за извршување на потребните задачи.

Се уште не постојат многу информации за извршените SCADA напади во индустријата и покрај растот на свеста за безбедносните пропусти во индустриските мрежи. Меѓутоа, за подобрување на постоечките решенија и разбирање на конвенционалниот ИТ систем, SCADA хиерархијата се користи како референтна точка. Тогаш, сајбер нападите може да се класифицираат во неколку категории.

1) Сајбер напади на хардвер

Еден напаѓач може да добие неовластен, далечински пристап до уредите и да ги промени нивните однапред зададени податоци. Тоа на пример може да предизвика прекин во работата на некои уреди при многу мали вредности на дефинираните прагови или пак да спречи активирање на аларм кога е потребно. Друга можност е напаѓачот, откако ќе добие неовластен пристап, да ги смени вредностите на екранот на операторот, па кога ќе се вклучи аларм, операторот да не биде известен за тоа. Ова може да го одложи човечкиот одговор на вонредна ситуација, што може да влијае на безбедноста на луѓето во близина. Главниот проблем во превенцијата на сајбер нападите на хардверот е во контролата на пристап. Имајќи го тоа на ум, треба да се спомне еден од поголемите напади во оваа категорија, наречен проба-грешка (анг. doorknob-rattling) напад. Напаѓачот изведува неколку обиди за најава во системот со чести комбинации на кориснички имиња и лозинки на повеќе компјутери што многу често резултира со успешна најава. Овој напад може да остане неоткриен доколку податоците поврзани со погрешните обиди за влез од сите хостови не се чуваат и не се проверуваат.

2) Сајбер напади на софтвер

Како што е познато, SCADA системите користат различни софтверски пакети за извршување на зададените функции. Исто така, постојат големи бази на податоци во серверите за чување на податоци, покрај другите апликации кои се користат во корпоративните сесии. Со хостирањето на централизирана база на податоци, серверите за чување податоци содржат витални и потенцијално доверливи информации за процесите. Овие податоци се неопходни не само од техничка гледна точка, бидејќи на многу алгоритми за управување им се потребни минатите податоци за процесот за да донесат правилни одлуки, туку и поради бизнис цели, како што е цената на електричната енергија и сл. Иако е претпоставено дека алгоритмите од овие софтвери се безбедни, сепак постојат ранливости поврзани со нивната имплементација.

- *Buffer Overflow (преполнување на баферите)*

Голем дел од нападите имаат за цел да предизвикаат преполнување на баферите (анг. buffer overflow), бидејќи нивна намера е да ја корумпираат програмата и да предизвикаат таа да се однесува неконтролирано. Ефектот од ваквите напади може да биде во форма на ресетирање на лозинките, модификација на содржината, извршување на штетен код итн. Проблемот со buffer overflow кај SCADA системите е во две подрачја. Едно подрачје се работните станици и серверите кои што се слични со стандардните ИТ системи. На пример, WellinTeck KingView 6.53 HistorySvr, индустриски софтвер за автоматизација, на кој работат серверите за историја и кој нашироко се користи во Кина има т.н. анг. heap buffer overflow ранливост (heap-претставува дел од меморијата кој се користи за алокација од страна на апликациите), која што претставува потенцијален ризик за Stuxnet напад (Beresford, 2001). Другото подрачје се теренските уреди и другите компоненти кои што работат на RTOS и поради тоа го наследуваат проблемот со меморијата. Нападите можат да ја искористат предноста од фиксното време за мемориска алокација кое во RTOS системите се користи за поуспешни стартувања. Исто така, многу теренски уреди работат со години без да се ресетираат. Поради тоа, овие SCADA компоненти се предмет на акумулирана мемориска фрагментација што води до застои во извршувањето на програмата.

- *SQL инјекција*

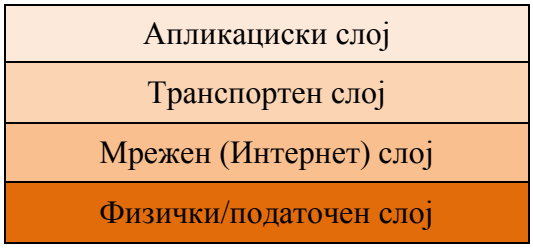
Во најголем дел од малите индустриски апликации за бази на податоци, може да се пристапи со користење на Structured Query Language - SQL, за структурна модификација и промена на содржината. Во врска со серверите за чување податоци и веб пристапноста во сегашните SCADA системи, SQL инјекциите, кои се едни од најчестите Web напади, имаат многу големо влијание врз безбедноста на SCADA системите.

Типична единица за извршување на SQL инјекцијата, која доаѓа во многу различни видови, кои се базирани на SQL-92 ANSI стандардот, е барање (анг. query) што претставува колекција од изрази кои најчесто враќаат едно множество на резултати. SQL инјекцијата настанува кога напаѓачот е во можност да манипулира со влезните податоци од некоја Web апликација, која не може добро да го прочисти влезот за податоците од вистинскиот корисник и тогаш напаѓачот внесува серија од неочекувани SQL изрази во барањето. Како последица на ова, можно е да се манипулира со базите на податоци на различни начини. Уште повеќе, доколку процедурата за зачувување (од командниот прозорец) е овозможена, напаѓачот може да добие пристап и до други функции. Процесот ќе се води со истите дозволи како и компонентата што ја извршила наредбата. Овој вид на напад може да им дозволи на напаѓачите да добијат тотална контрола врз базите на податоци, дури и можност за

извршување на команди во системот. Намерните, штетни промени во базите на податоци можат да предизвикаат катастрофални последици.

3) Напади на комуникацискиот стек

Можните напади можат да се разгледуваат и поделени по слоевите на TCP/IP комуникацискиот стек (даден на Слика 24) кои специфично ги таргетираат. Притоа, ќе бидат нагласени некои кои имаат поголем потенцијал за наштетување на SCADA системите:



Слика 24 TCP/IP комуникациски модел (стек)

- *Мрежно ниво*

1) Напади на дијагностичките сервери преку UDP порта, при кои напаѓачите имаат пристап до истите алатки како и сите RTOS програмери (тие можат да ги читаат табелите на симболи, да го разгледуваат составот итн). На пример, слаб хеширачки (анг. hashing) алгоритам би му овозможил на напаѓачот да изврши едноставен погодувачки (анг. Brute force) напад на лозинките со нагаѓање на низата која го продуцира истиот хеш (анг. hash) код како и легитимната лозинка. Конкретно, преку сервисот за дебагирање (анг. debug service) на оперативниот систем за работа во реално време VxWorks, доколку се изврши напад преку UDP порта 17185, која што е автоматски овозможена, напаѓачот може да изврши различни напади без никакво барање за автентикација, а притоа да задржи одредено ниво на прикриеност: далечинско бришење на меморија (анг. memory dump), далечинско повикување на функции и далечинско менаџирање со задачите.

2) Idlescan претставува метод за скенирање на TCP портите кој се состои од праќање на лажни пакети до саканиот компјутер со користење на т.н. „зомби“хост. MODBUS и DNP3 се подложни на вакви проблеми во случаи кога комуникацијата треба да се оствари преку TCP/IP.

3) Штрумф претставува вид на адресна имитација која функционира преку испраќање на континуално множество од модифицирани Internet Control Message Protocol (ICMP) пакети до мрежата која е цел на напад, при што адресата на испраќачот е идентична со адресата на некој од компјутерите од истата мрежа. Во контекст на SCADA системите, ако некој ПЛУ одговори на модифицираната порака, истиот може да прекине со работа или уште поопасно, да испрати погрешна наредба до актуаторите.

4) Лажирање (анг. spoofing) со Address Resolution Protocol (ARP), чија примарна употреба е преведување на IP адресите во Ethernet Medium Access Control - MAC адреси и откривање на другите поврзани уреди на LAN. Со испраќање на лажни ARP пораки што содржат лажни MAC адреси, напаѓачот може да ги збуни мрежните уреди во SCADA системите, како што се мрежните прекинувачи. Кога овие лажни рамки се испратени до друг јазол, пакетите можат да се пресретнат. Доколку пак се испратат до хост кој не е во опсегот, може да се стартува DoS, а ако намерно се испратат до хост кој е поврзан на различни актуатори, тогаш може да настане и физичка штета.

5) Ланец/Јамка напади, каде постои ланец од поврзувања преку многу јазли, при што напаѓачот се движи низ јазлите за да го скрие неговото потекло и идентитет. Во случај на јамка напад, ланецот од поврзувања е во јамка, така што е уште потешко да се следи потеклото на напаѓачот во големите SCADA системи.

- *Транспортно ниво*

Таканаречената SYN поплава е еден вид на DoS напад и има за цел да ги засити изворите, така што испраќа TCP барања за поврзување побрзо отколку што машината може да процесира.

SCADA протоколите, посебно оние кои што се извршуваат над транспортните протоколи како што е TCP/IP, имаат ранливости што можат да бидат искористени од напаѓачите преку едноставни методологии, како што е едноставно инјектирање на изменети пакети за да предизвикаат дестинациониот уред да одговори или да комуницира на несвојствени начини. Овие напади можат да предизвикаат операторот потполно да ја изгуби контролата врз некој уред во SCADA системот.

- *Апликациско ниво*

Моментално, не постои силна безбедносна контрола на протоколите кои се користат во SCADA системите, како што се: DNP3, Modbus, OLE/OPC, и ICCP. Практично, не постои можност за автентикација на изворот и податоците на оние кои што имаат пристап до уред преку SCADA протокол, иако тие можат да читаат и запишуваат. Пристапот за запишување и дијагностичките функции на овие протоколи се посебно ранливи во случај на сајбер напади. Еден од можните напади на SCADA и конвенционалните ИТ системи е DNS измамата. Во ваквиот напад се испраќа лажен

DNS одговор со соодветна IP адреса на изворот, дестинациска порта и ID на барање, меѓутоа со изменети информации од страна на напаѓачот, така што лажниот одговор може да биде процесиран од клиентот пред вистинскиот одговор да биде примен од вистинскиот DNS сервер. Повеќе детали за вакви напади има во (Hansman & Hunt, 2004).

Што се однесува конкретно до напади и ранливости врзани за самите SCADA протоколи, најранливи се сосем отворените (а со тоа и најчесто користените) протоколи, како што се на пример Modbus и DNP3.

1) MODBUS: Modbus претставува де факто стандард за протоколите на апликациско ниво користени во индустриските мрежи (Modbus IDA, 2004). Постојат повеќе верзии, од основен Modbus до Modbus+ и Modbus/TCP. Еден Modbus клиент (или master) може да испрати барање до Modbus сервер (или slave) со функциски код, што ја одредува акцијата што треба да се преземе, и податочно поле, кое содржи дополнителни информации.

Поради малиот број на објавени случаи на напади на Modbus, Digital Bond има спроведено истражување за детекција на напади, со цел да ги проучи неговите потенцијални ранливости (Digital Bond), (Byres, Hoffman, & Kube, 2006), (Byres, Carter, Elramly, & Hoffman, 2002). Нивните правила за детекција вклучуваат DoS (пример: превклучување на Modbus серверите и нивно конфигурирање за да не можат да ги извршат барањата, т.н. пасивен режим (анг. listen-only mode) и прекин на работата на серверите со голем број на барања), извидување (пример: неовластено читање на податоците и собирање на информации за уредите) и неовластени барања за запишување.

Знаејќи дека Modbus нема енкрипција или било какви други безбедносни мерки, постојат многу начини за директно истражување на слабостите на ниво на функциските кодови. Функциските кодови 0x05 и 0x0F се користат за нагодување на еден или повеќе излези на некој оддалечен уред на ON или OFF, соодветно. Ова значи дека напаѓачот може далечински да исклучи или попречи одредени излези, а со тоа да креира лажна ситуација на HMI страната. Неовластени запишувања можат да се направат со користење на функциските кодови 0x06 и 0x10. Според тоа, фалсификуваните податоци може да се запишат во еден или повеќе регистри на некој уред. Ако Modbus е имплементиран преку сериска линија, функцискиот код 0x11 може да се користи за да се добијат информации од некој далечински уред. Функцискиот код 0x08 се користи за дијагностика на сериска линија, но во комбинација со функцискиот код 0x01 може да ја иницијализира и рестартира портата од slave-от (серверот) и да го избрише бројачот за комуникациски настани, што претставува идеален начин за напад. Во комбинација пак со функцискиот код 0x04, дијагностичкиот функциски код може да го стави далечинскиот уред во

пасивен режим (Listen Only Mode). Слично, Modbus+ има функциски код (08) за бришење на настаните што може да му овозможи на напаѓачот да ги избрише записите за историјата на манипулација со податоците и DoS настаните, со што ќе си ги скрие трагите.

2) DNP3: DNP3 се користи во комуникацијата помеѓу главните управувачки станици и оддалечените компјутери или управувачи наречени надворешни станици. DNP3 е имплементиран во многу компании (претежно од енергетскиот сектор), поради неговата мала мемориска потрошувачка. Неговиот функциски код 0x0D може да ги ресетира и реконфигурира DNP3 надворешните станици, така што ќе ги натера да извршат комплетен т.н. power циклус. За времетраењето на ре-иницијализацијата на автоматски нагодените вредности, многу уреди ги бришат нивните листи со записи. Така, напаѓачот може да ја искористи предноста на ова својство за да предизвика доцнење кај надворешните станици пред тие повторно да ги прифатат барањата. Уште повеќе, функцискиот код 0x13 овозможува нови конфигурации на надворешните станици. Со неовластен пристап, напаѓачот може да ги манипулира уредите, така што ќе ги менува нагодувањата, ќе го попречува излезот и ќе создава лажни аларми.

Што се однесува до конкретни закани кон индустриските SCADA системи, историјата бележи повеќе конкретни инциденти со најразлични последици. За сите овие настани, податоци како што се вид на нападот, тип на нападнатата мрежа, последици и начин на справување со нив, можат да се најдат во (BCIT Industrial Security Database), (Kuypers, Maillart, & Pate-Cornell, 2015). Притоа, може да се нагласи дека убедливо најсофистицираниот штетен софтвер за SCADA системите е Stuxnet (Falliere, Murchuand, & Chien, 2010).

4.3. Безбедносни стратегии за SCADA системите

Во последните години, големо внимание се обрнува на анализа на ранливостите на индустриските системи од надворешни напади, при што општиот пристап подразбира анализа на ефектот на специфични напади врз одредени системи. На пример, дефинирани се лажни напади и напади на недостапност на услуга во вмрежен управувачки систем и за вторите, е одредена соодветна противмерка за справување со нападот базирана на полу-дефинитно програмирање (Amin, Cardenas, & Sastry, 2009). Лажните напади се однесуваат на можноста на компромитирање на интегритетот на управувачките пакети или мерења, кои доведуваат до менување на однесувањето на сензорите и актуаторите. Од друга страна, нападите на недостапност на услуга ја компромитираат достапноста на извори (на

пример поместување на комуникацискиот канал). Во (Liu, Reiter, & Ning, 2009) се дефинирани напади на инјектирање на лажни податоци во статичките естиматори на состојба. Нападите на инјектирање на лажни податоци се специфични напади на мамење во контекст на статички естиматори. Покажано е дека може да се дизајнираат недетектирачки напади на инјектирање на лажни податоци дури и кога напаѓачот има ограничен број на извори. На сличен начин, во (Teixeira, Amin, Sandberg, Johansson, & Sastry, 2010) се разработени тајните напади на измама против SCADA системите. Во (Mo & Sinopoli, 2010) е дискутиран ефектот на повторувачки напади врз еден управувачки систем. Повторувачките напади се дефинирани преку пресретнување на сензорите, снимање на отчитани податоци во одреден временски интервал, и повторување на вакви отчитувања во момент на инјектирање на егзогени сигнали во системот. Покажано е дека овие напади може да бидат детектирани преку инјектирање на сигнал кој е непознат за напаѓачот на системот. Во (Smith R. , 2011) е истражуван ефектот на тајните напади врз управувачките системи, при што параметризирана структура дозволува тајниот агент да го набљудува однесувањето на физичката постројка додека не е детектиран од оригиналниот управувач. Понатаму, проучен е и проблемот на естимација на состојбата на линеарен систем со неправилни мерења (Hamza, Tabuada, & Diggavi, 2011). Поточно, карактеризиран е максималниот број на толерирани погрешни сензори, и предложен е декодирачки алгоритам за детекција на ваквите мерења. За крај, особено внимание е обрнато на проблемите со сигурноста на специфични сајбер физички системи, како што се енергетските мрежи (DeMarco, Sariashkar, & Alvarado, 1996), (Dan & Sandberg, 2010), (Pasqualetti, D'Orfler, & Bullo, 2011), (Mohsenian-Rad & Leon-Garcia, 2011), (Sridhar, Hahn, & Govindarasu, 2012), и мрежните системи за дистрибуција на вода (Amin, Litrico, Sastry, & Bayen, 2010), (Eliades & Polycarpou, 2010).

Во продолжение ќе биде даден преглед на основните безбедносни приоди и механизми, подредени по растечка комплексност.

4.3.1. Надгледување на пораките

Способноста за интерпретација и филтрирање на пораките кај SCADA протоколите може да ја подобри безбедноста, сé додека е во согласност со безбедносните стандарди. Дизајнот вклучува анализа на пораките и граматика, која дефинира правила за филтрирање и акции кои треба да се преземат кога SCADA пораката ќе се совпадне со едно или повеќе правила во профилот за детекција.

Надгледувањето на пораките, кое може да биде имплементирано и во поевтините теренски уреди, има за цел да го контролира сообраќајот насочен кон специфични мрежни компоненти и сегменти. Надгледувачката функционалност може да биде вградена и во далечинските терминални единици за да се имплементира хост-базирано филтрирање. Меѓутоа, важно е да се внимава тоа да нема големо влијание на функционалноста на системот.

4.3.2. Решенија базирани на протоколи

Безбедносните решенија за застарените SCADA системи мора да се во согласност со протоколните спецификации и стандарди. Решенијата базирани на протоколи го решаваат овој проблем со примена на стандардни протоколни пораки со специјални кодови во неискористените функциски полиња, како механизам за овозможување.

Во имплементацијата на овој прототип, за Modbus се користат функциски кодови креирани од корисникот, а за DNP3 специјални податочни објекти, со цел да се пренесат пораките поврзани со безбедноста. Тоа е постигнато со:

а) имплементација на безбедносна функционалност, преку кодови дефинирани од корисникот (Modbus (Modbus IDA, 2004)) и податочни објекти резервирани за идни надградби (DNP3 (Smith & Copps, 1993)), или

б) користење на подмножество од функции, моментално имплементирани во теренските уреди.

Најголемиот дел од протоколите за индустриско управување се потпираат на механизмот на барање/одговор за комуникација и операции во рамките на фабриката. Пораките базирани на протоколи го прошируваат овој режим на работа и служат како блокови за градење на пософистицирани безбедносни услуги.

Услугите за интегритет и доверливост можат да се имплементираат со користење на протоколни рамки со специјални полиња. Овие полиња содржат потписи, а во случај на доверливи информации содржат и заглавја со обичен текст за декрипција на податоците.

Влијанието врз функционалноста на системот мора да биде земено во предвид и за двете опции. За системи каде безбедносниот модул се наоѓа во апликациското ниво, може да се случи некомпатибилност на ниво на пораките, доколку производителите не користат иста семантика за кодовите дефинирани од корисниците. Од друга страна, сместувањето на безбедносниот модул во апликациското ниво бара само репрограмирање на теренските уреди.

4.3.3. Сервиси за тунелирање

Ова решение користи едноставни комуникациски тунели, како дополнителни слоеви околу SCADA протоколите, за да додаде безбедносна функционалност на транспарентен начин (American Gas Association, 2005). Пакувањето на пораките е примарниот механизам за конструирање на заштитени тунели за комуникациските ентитети. Овие тунели може да нудат различни услуги, вклучувајќи интегритет на пораките и доверливост. Тунелирањето овозможува овие услуги да бидат транспарентно вметнати, како самостојно ниво во теренските уреди или во специјализираните вградливи уреди.

4.3.4. Middleware компоненти

Middleware компонентите (тоа е општ термин за компатибилен софтвер што овозможува различните софтверски компоненти да работат заедно) нудат софистицирани безбедносни услуги во хетерогени средини. Примената на овие компоненти кои се имплементирани како протоколни поднивоа, се разликува од решенијата базирани на протоколи и тунелирањето во тоа што ја поддржува интеграцијата на системските компоненти преку различни мрежи.

Овој приод бара развивање на решенија интегрирани на различни нивоа во постоечките инфраструктури на SCADA мрежите, со цел да понудат различни безбедносни услуги, вклучувајќи автентикација, интегритет и доверливост.

4.3.5. Менаџирање со криптографски клучеви

Безбедносните услуги кои вклучуваат криптографија бараат ефикасни решенија за менаџирање со клучеви. Многу од SCADA безбедносните стандарди ја препознаваат важноста на менаџирањето со клучеви, меѓутоа, потребно е повеќе истражување за да се развијат практични решенија (American Gas Association, 2005), (Instrumentation Systems and Automation Society, 2004).

Креирањето, распределбата, чувањето и уништувањето на клучевите без притоа да се загрози безбедноста сеуште претставуваат предизвици. За да се намали ризикот од загрозување на безбедноста на клучот, потребно е клучевите да се менуваат периодично и да се отповикаат привилегиите за пристап поврзани со старите клучеви, што исто така, претставува тешка задача.

Нека се земе во предвид целосно поврзана мрежа составена од n јазли, каде се чува таен клуч за секој линк. Како што бројот на јазли во мрежата се зголемува, бројот на линкови (и тајни клучеви) се зголемува како n^2. Предложените решенија за овој проблем вклучуваат криптографија со јавен клуч, доверливи кругови базирани на сертификат и специјални криптографски протоколи, кои комплексноста ја поврзуваат со бројот на јазли наместо со бројот на линкови. За среќа, SCADA мрежите не се целосно поврзани и во најголем дел од случаите, само комуникациите помеѓу контролниот центар и теренските уреди мора да бидат обезбедени (теренските уреди многу ретко, ако и воопшто комуницираат меѓу себе). Поради ова, топологиите на SCADA мрежите имаат потреба од многу помал број на клучеви и како последица на тоа, вклучуваат поедноставни решенија за менаџирање со клучеви.

Три позначајни решенија за менаџирање со клучеви за SCADA мрежите се:

- Менаџирањето со клучеви базирано на хеш (анг. hash) е решение кое користи хеширачки операции за генерирање на клучеви, нивно сертифицирање и

верификирање. На пример, генерирањето на клучеви се извршува со хеширање на спецификациите од главниот клуч на некој уред, заедно со други информации, како што е неговиот ID или временскиот печат. Во случаи каде доверливоста не е потребна, хеш вредностите нудат гаранции за интегритет со помалку процесирачки барања, отколку некои други криптографски алгоритми.

- Менаџирањето со клучеви базирано на PKI користи стандардни PKI (Public Key Infrastructure) кои ги земаат во предвид уникатните особини на SCADA системите за времетраењето на клучевите, како и процедурите за верификација и распределба на листата за отповикување на сертифицирањето (CRL - Certification Revocation List). Во некои од овие модификации времетраењето на сертификацијата се совпаѓа со физичките циклуси за одржување, спорадичното извршување на CRL верификацијата кога постои поврзаност со контролниот центар и користењето на нормални операции за одржување, како можности за инсталирање на нови приватни клучеви и сертификати.
- Распределбата на симетрични клучеви, која обезбедува услуги слични на PKI, освен што овде се користи симетричен криптографски клуч. Имплементацијата на прототипот користи Davis-Swick протокол, кој користи симетрична енкрипција и симетрични сертификати за клучеви (Davis & Swick, 1990).

4.4. Форензика на SCADA мрежа

Форензиката станува релевантна откако ќе се открие безбедносен инцидент (Mandia, Prosise, & Pepe, 2003), при што целта е да се открие причината за инцидентот. Ако инцидентот е напад, форензичката анализа треба да ги открие т.н. *modus operands* и идентитетите на напаѓачите, како и пропустот во системот, со цел истиот да биде отстранет за да системот се заштити од слични инциденти во иднина. Овде е опишана форензичката архитектура за прибирање и анализа на SCADA мрежниот сообраќај (Kilpatrick, Gonzalez, Chandia, & Shenoi, 2005).

Еден мрежен форензички систем го следи и чува мрежниот сообраќај и нуди пребарување и анализа на податоците, со цел да служи како поддршка за пост-инцидентните истраги, вклучувајќи ги тука и реконструкциите на инцидентите (Shanmugasundaram, Bronnimann, & Memon, 2005), (Shanmugasundaram, Memon, Savant, & Bronnimann, 2003). Исто така, форензичкиот систем за SCADA мрежите може да ги подобри индустриските операции (Kilpatrick, Gonzalez, Chandia, & Shenoi, 2005). Во контекст на SCADA мрежите, прибирањето и анализата на сензорските податоци и

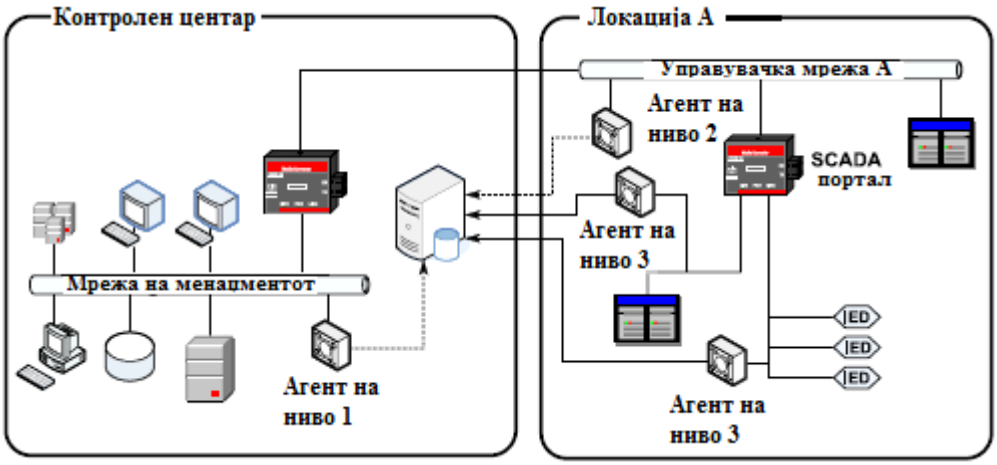
управувачките акции помага во надгледувањето на однесувањето на процесот, со цел оптимизација на функционалноста на постројката.

Форензиката во големите ИТ мрежи е екстремно комплицирана и скапа (Shanmugasundaram, Bronnimann, & Memon, 2005). Од друга страна, форензиката во SCADA мрежите може да биде релативно едноставна. SCADA сообраќајот е рутински и е предвидлив за разлика од сообраќајот во ИТ мрежите, кој пренесува сообраќај генериран од корисникот со комплексни комуникациски шаблони. Малиот волумен и униформноста на сообраќајот во SCADA мрежите овозможуваат запишување на релевантните процесни/управувачки податоци поврзани со секоја порака и постепена анализа на податоците од евалуациите за форензичките истраги и функционалноста на постројката. Поточно, оваа архитектура ја користи регуларноста на сообраќајот во SCADA мрежите за да ја минимизира количината на податоците прибрани за форензичка анализа и одговор при инциденти.

4.4.1. Форензичка архитектура

На Слика 25 е претставена форензичка архитектура што поддржува прибирање, чување и анализа на сообраќај во SCADA мрежа. Архитектурата користи „форензички агенти“ на стратегиски локации во SCADA мрежата за систематско прибирање на информации за состојбата и мрежниот сообраќај (Kilpatrick, Gonzalez, Chandia, & Shenoi, 2005). Овие агенти препраќаат релевантни порции од мрежни пакети (анг. synopses) до централна локација за чување и повикување по потреба. Комплетна историја за работата на SCADA системот може да се добие од анализа на состојбите и реконструкција на настаните во мрежата од зачуваните синопси.

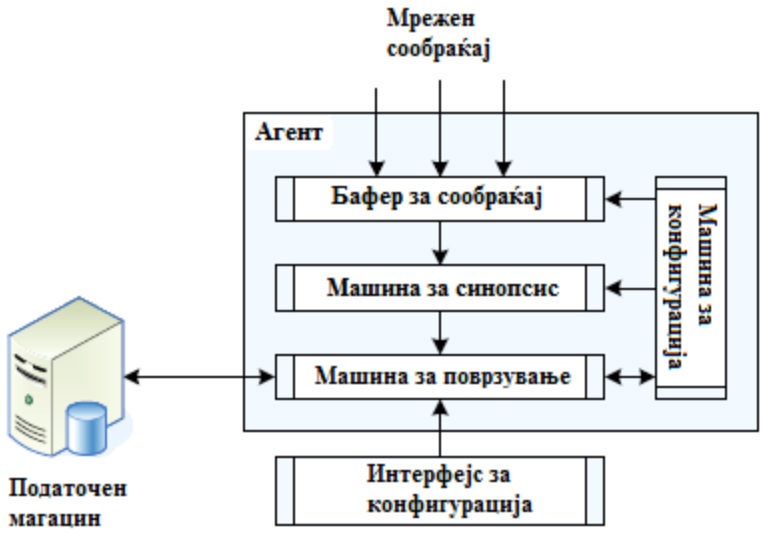
Форензичката архитектура вклучува повеќе агенти и податочен магацин. Секој агент го чува SCADA сообраќајот во неговиот локален мрежен сегмент и препраќа синопси од секој пакет до податочниот магацин. Податочниот магацин ги анализира синопсите од секој пакет и креира податочен печат, кој го чува заедно со синопсите во делот за чување, наменет за агентот кој ги испраќа. Тој, исто така, поддржува пребарувања во зачуваните податоци. Се препорачува секоја изолирана мрежа да се користи за целата комуникација помеѓу агентите и податочниот магацин.



Слика 25 SCADA мрежа со форензички способности

Една SCADA мрежа обично има неколку видови на агенти. Агент на Ниво 1 е поврзан директно до мрежата на менаџментот. Агентите на Ниво 2 се лоцирани во управувачките мрежи, а агентите на Ниво 3 се позиционирани после SCADA порталите.

Индустриските операции често вклучуваат повеќе меѓусебно поврзани SCADA мрежи, што создава потреба од набљудување на сообраќајот преку нив. Тоа се постигнува со позиционирање на агенти на Ниво 0 помеѓу SCADA мрежите и користење на податочни магацини на Ниво 0 (не се прикажани на Слика 25). За да се олесни робусното пребарување, податочниот магацин на Ниво 0 мора да биде поврзан со податочните магацини од индивидуалните SCADA мрежи преку изолирана мрежа.



Слика 26: Генерирање на синопси

4.4.2. Форензички агенти

Форензичките агенти го прибираат SCADA сообраќајот и креираат порции од мрежни пакети, кои содржат информација потребна за форензичка анализа. Еден агент вклучува бафер за мрежен сообраќај, машина за синопси, машина за поврзување и машина за конфигурација (Слика 26).

Баферот за мрежен сообраќај го чува непроцесираниот мрежен сообраќај. Тој користи имплементација со повеќе нишки (анг. threads) на стандардниот произведувач/потрошувач алгоритам и ограничен бафер.

Машината за синопси е јадрото на форензичкиот агент. Таа ги испитува пакетите во сообраќајниот бафер и генерира синопси за пакетите според нејзините конфигурациски правила. Парцијални синопси се креираат за секој енкапсулирачки протокол (на пример, агентите конфигурирани за OSI моделот може да креираат синопси за Ниво 3 (Мрежно ниво) и Ниво 4 (Транспортно ниво)). Овие парцијални синопси се комбинирани со информацијата за локацијата и временскиот печат, за да се создадат објекти од синопси што се препраќаат на податочниот магацин.

Машината за поврзување ја олеснува комуникацијата помеѓу агентите и податочниот магацин. Притоа, се користат листи за контрола на пристап (анг. Access Control List - ACLs) за да се имплементира заедничка автентикација. Машината за конфигурација обезбедува механизми за регулирање на работата на агентите. Теренските уреди кои сакаат да конфигурираат агент мораат да користат заеднички конфигурациски интерфејс. Некои безбедносни нагодувања се слични на оние кои се користат во ИТ мрежите, а други, како што се нагодувањата за синопси, се уникатни за оваа архитектура.

Правилната конфигурација на пребарувачот на синопси на еден агент е важна поради нејзината улога во архитектурата. Може да се користат две методи, конфигурација базирана на ниво и рачна конфигурација. Првата ги конфигурира агентите според нивната локација, дозволувајќи тие да бидат конфигурирани со предефинираните алгоритми за синопси. Агентите се конфигурирани како Ниво 0 (помеѓу SCADA мрежи), Ниво 1 (мрежа на менаџментот), Ниво 2 (управувачка мрежа) и Ниво 3 (зад SCADA порталот). Предефинираните алгоритми за синопси ја минимизираат големината на синопсите генерирани од појдовните барања и дојдовните одговори до агентите, а ја зголемуваат големината на синопсите како што нивото се намалува (пример: агент од Ниво 2 има поголеми пакети, додека агент од Ниво 1 има помали). Рачната конфигурација на агентите може да се изврши за фино нагодување на однесувањето на агентот и анализата на пакетите. Исто така, синопсите содржат информација за времето, но е претпоставено дека временската синхронизација на агентите и податочните магацини се врши со примена на

методи кои се надвор од форензичката архитектура (пример: мрежен временски протокол NTP).

Треба да се земе во предвид и дека во индустриските средини често се користат повеќе различни SCADA протоколи. Уште повеќе, како дополнување на стандардните протоколи како Modbus и DNP3, некои средини користат и нивни варијации или комерцијални протоколи. Барањето за справување со различни SCADA протоколи го поттикнало дизајнирањето на модуларни агенти со можност за нагодување на пребарувачите на синопси.

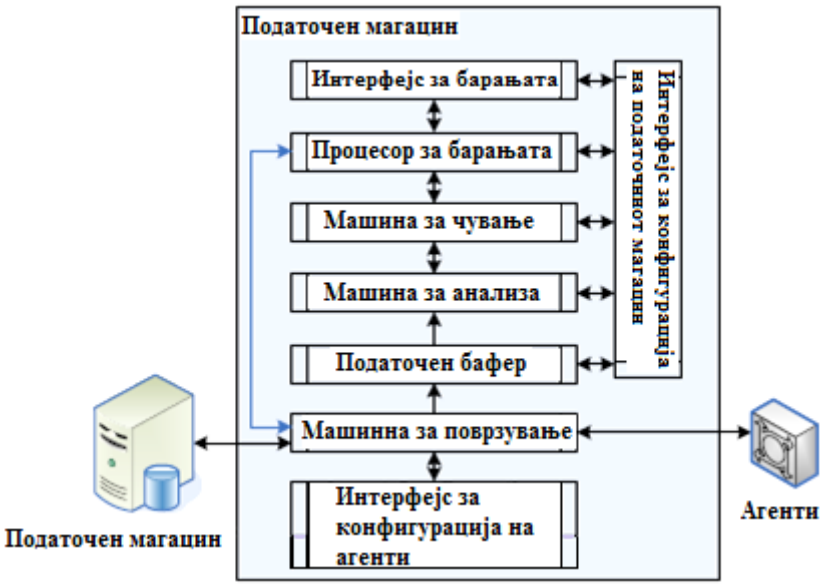
4.4.3. Чување на сообраќајот и пребарување

Форензичките агенти ги предаваат нивните синопси од SCADA сообраќајот до определено место наменето за чување на податоци. Дизајнот користи механизми за база на податоци и пребарување за поддршка на форензичките истраги. Одделот за чување на сообраќајот и пребарување користи машина за поврзување, податочен бафер, машина за анализа, машина за чување, интерфејс за пребарување, процесор за пребарување и интерфејс за конфигурација на агенти (Слика 27).

Машината за поврзување поддржува комуникација помеѓу податочниот магацин и регистрираните агенти. Врските помеѓу машината и агентите се користат за прием на синопси и конфигурација на агентите. Врските пак со други податочни магацини го олеснуваат процесирањето на пребарувањата што се распространети на повеќе SCADA мрежи.

Доставените синопси за чување се сместуваат во податочен бафер и се предаваат на машината за анализа, со користење на произведувач/потрошувач алгоритам. Оваа машина креира ознаки поврзани со синопсите кои се користат за реконструкција на настани и за анализа и поврзување на шаблоните на SCADA сообраќајот. Ознаките ги намалуваат барањата за мемориски простор и се корисни поради нивните форензички способности. На пример, ако едно PLC комуницира со одредени теренски уреди, потребно е само да се чуваат нивните адреси и да се поврзат со PLC-то. Соодветната ознака базирана на уредот е генерирана со поврзување на синопсите од сите агенти кои го набљудуваат сообраќајот поврзан со тоа PLC.

Способности за анализа на шаблоните може да се развијат за потребите на форензичката архитектура. На пример, ПЛУ-ата често извршуваат повторливи управувачки јамки со добро дефинирани комуникациски шаблони. Овие шаблони може да се анализираат за да се добијат мрежно - базирани ознаки за форензички истраги и детекција на аномалии.



Слика 27: Чување на сообраќајот и пребарување

Машината за чување користи хеш (анг. hash) табели и база на податоци. Секој регистриран агент има множество од хеш табели кои се користат за индексирање на повторливите податоци за ознаките асоцирани со агентот. На пример, парцијални синопси генерирани за време на комуникациите помеѓу два уреди со статични адреси кои разменile голема количина на податоци не треба да се чуваат повеќе од еднаш. Наместо тоа, се користи покажувач кон влезот како ознака (зачуван во базата на податоци) за идентификација на комуникацијата. Бројот на табели асоциран со еден агент зависи од видот и количината на синопси генерирани од агентот.

Интерфејсот за пребарување поддржува реконструкција на инциденти, проверка на системот и анализа на трендовите во процесот. Интерфејсот нуди два SQL базирани механизми за пребарување. Едниот користи GUI и предефинирани опции за анализа на рутини. Другиот нуди конзола што им дава повеќе слобода на аналитичарите за специфични пребарувања. Резултатите се презентирани во извештаи надополнети со графички информации за SCADA мрежата, вклучувајќи ги компонентите на системот, уредите и агентите.

Процесорот за пребарување работи со пребарувањата добиени од локалниот интерфејс за пребарувања или од некоја друга SCADA мрежа, преку машината за поврзување. Процесорот одлучува дали пребарувањето вклучува информација од некоја друга SCADA мрежа. Доколку тоа е случај, се испраќа барање до соодветниот податочен магацин кој пак динамички генерира и процесира барања и неговиот одговор се враќа до испраќачот.

Конечно, како заклучок може да се каже дека сајбер–физичката безбедност во континуалните системи на реално време побарува сеопфатен преглед и холистичко разбирање на безбедноста на мрежите, теоријата на управување и самиот физички систем. Секое остварливо техничко решение и истражување во насока на обезбедување на SCADA системите мора да биде во спој со компјутерската безбедност, комуникациската мрежа и управувањето.

Сепак, факт е дека огромната глобална база на инсталирани индустриски вмрежени системи значи дека во многу случаи во иднина ќе мора да се користат застарени безбедносни механизми, наместо да се искористи опцијата за нивно дизајнирање од почеток, што пак води до зголемување на притисокот за создавање на робусни системи за детекција на упад.

Безбедносните стратегии разгледани во ова поглавје имаат голем потенцијал, бидејќи тие балансираат помеѓу сигурноста и функционалноста на системите, додека се придржуваат до SCADA протоколите и стандардите. Решението за безбедносни услуги може систематски да се интегрира во мрежите за процесно управување, како дел од процесите за менаџирање на ризици, без да има негативно влијание врз операциите на постројката. Форензичкото решение пак поддржува истраги на безбедносните инциденти во SCADA системите, како и анализа на процесните трендови и оптимизација. Решенијата се флексибилни и скалабилни и се способни да се справат со повеќе протоколи и меѓусебно поврзани SCADA мрежи.

Поврзаноста на SCADA мрежите со надворешните мрежи ќе продолжи да расте, што ќе води кон зголемен ризик од сајбер напади и круцијална потреба да се подобри безбедноста на овие мрежи. Постојат многу професионални организации вклучени во обидот да се стандардизира и подобри безбедноста на SCADA мрежите, но се разбира дека остануваат и многу технички предизвици кои не смеат да се занемарат.

5. АЛГОРИТАМ ЗА БЕЗБЕДНА КОМУНИКАЦИЈА ВО ВСАУ ПРЕКУ ФУНКЦИИ НА СПРЕГА И ДИНАМИЧКА БАЕСОВА ИНФЕРЕНЦИЈА

Зголемената употреба на комуникациите само ја подвлекува и истакнува потребата од постојан развој на методи за сигурен и доверлив пренос на информации, (Shannon, 1949). Процесот на комуникација мора да биде способен да поднесе не само човечки напади, туку и прекини и проблеми кои произлегуваат од техничката инфраструктура и имплементацијата на самите комуникациски врски. Овие проблеми се одликуваат со зголемен шум и интерференција, што пак го намалува квалитетот на комуникацијата и ја менува содржината на информациите кои се пренесуваат.

Дизајнирани се многу различни видови на комуникациски протоколи, кои вклучуваат употреба на: логички и математички процедури, процесирање на сигналите, динамички хаотични системи, и теорија на квантни информации (Shannon, 1948), (Kish, 2006), (Cuomo & Oppenheim, 1993), (Kocarev & Parlitz, 1995), (Bennett, 2000), (Haroun & Gulliver, 2015), (Chou, Chuang, Wang, & Lin, 2013), (Irakiza, Karim, & Phoha, 2014).

5.1. Алгоритмот за безбедна комуникација

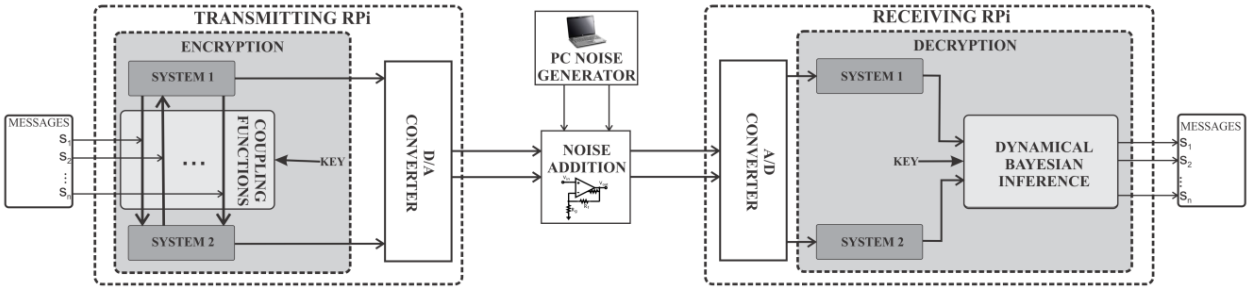
Во оваа глава, фокусот е на протокол за безбедна комуникација базиран на функциите на спрега (анг. coupling functions - CF) помеѓу два динамички системи. Овој протокол е веќе предложен и развиен во трудовите од (Stankovski, McClintock, & Stefanovska, 2014) и (Stankovski, Stefanovska, Young, & McClintock, 2016), каде се изложени неговите теоретски основи и се прикажани симулации и анализирани нивните резултати кои ги потврдуваат теоретските наоѓања. Овој докторски труд има за цел да се надоврзе на протоколот за безбедна комуникација со функции на спрега преку извршување на негова практична и експериментална верификација, и преку испитување и анализа на неговата работа во услови на појава на реален шум и интерференција.

Безбедноста на овој комуникациски протокол се однесува на криптографскиот аспект и отпорноста на напади, и таа се обезбедува со користење на функции на спрега помеѓу два или повеќе динамички системи кај испраќачкиот дел, при што протоколот суштински дозволува мултиплексирање на информации. Кај приемниот дел се користи динамичка Баесова инференција за добивање на информациите од испратениот сигнал. Притоа користењето на Баесовото заклучување овозможува ефективно разделување на

детерминистичките сигнали кои носат корисна информација од динамичките пертурбации во каналот, правејќи го протоколот исклучително отпорен на шум.

Како што беше кажано претходно, теоретските основи на овој протокол во овој докторски труд се надградени со експериментална имплементација и со практично тестирање на робустноста на протоколот во услови на присуство на реален шум. При експериментите состојбите на динамичките системи се континуални, а шумот при мерењето и другите несовршености на електронската опрема се неизбежни, па според тоа условите се доста блиски до многу реални апликации (Luchinsky, McClintock, & Dykman, 1998), (Parlitz, Junge, Lauterborn, & Kocarev, 1996), (Stankovski, McClintock, & Stefanovska, 2014), (Millerioux, Amigo, & Daafouz, 2008), (Cuomo, Oppenheim, & Strogatz, 1993). Друга цел на експериментот е да ја прикаже можноста за употреба на овој протокол на комерцијално достапни уреди (споредливи на пример со паметни телефони) (Chou, Chuang, Wang, & Lin, 2013), (Irakiza, Karim, & Phoha, 2014), па затоа испраќачот и примачот се имплементирани на два миникомпјутери Raspberry PI 2. Шумот се генерира со помош на Matlab и соодветна електроника и на тој начин се симулираат реалните околности при комуникацијата, по што конечно се тестира робустноста на целиот протокол при различни нивоа на пертурбациониот шум.

Дијаграмот на целиот комуникациски систем е илустриран на Слика 28. Целта е преку одреден комуникациски медиум да се пренесе некој број на сигнали s_i кои носат информации од интерес. Овие сигнали во општ случај доаѓаат од различни извори и уреди, и треба да се испратат истовремено.



Слика 28 Шема на комуникацискиот протокол

Комуникацискиот протокол наложува секој од овие сигнали всушност да биде скалирачки параметар (множител) во нелинеарните функции на спрега помеѓу два самоодржливи системи. Она што се испраќа низ јавниот комуникациски канал е всушност по еден сигнал од секој од овие системи, а не самите сигнали s_i кои ги содржат информациите. Овие два сигнали служат за на приемната страна да се впрегнат и целосно

да се синхронизираат два взаемно спрегнати системи слични на оние кај испраќачот. Потоа се користи динамичка Баесова инференција за да се добијат нивните параметри и со самото тоа да се декриптираат s_i.

Една од главните одлики на овој комуникациски протокол е во природата на приватниот клуч за енкрипција/декрипција. Имено, тој всушност ја содржи информацијата за тоа кои функции на спрега се користат за енкрипција на податоците, а овој избор претставува неограничен континуум на можни комбинации. Бројот на можни функции на спрега е секогаш конечен и зависи од конкретниот број на потребни комуникациски канали, но изборот на формите на функциите на спрега (што всушност е приватниот клуч) е неограничен.

Во продолжение, пред да се изложат останатите детали за комуникацискиот протокол преку соодветен експеримент, ќе биде даден и краток осврт на неговите најважни составни делови/алатки.

5.2. Атрактори и функции на спрега

Заедничка карактеристика на динамичките системи во природата е нивната способност за взаемна интеракција, меѓусебно влијание, и размена на енергија и/или материја. По дефиниција, една функција на спрега опширно ги опишува физичките правила и закони по кои се води интеракцијата помеѓу системите, и тоа од аспект на силата и обликот на спрегата (впарувањето). Функциите на спрега ги прецизираат правилата и процесите преку кои влезните вредности кај системите се пресликуваат во излезни, и тоа во општ случај како влезот кај едниот систем влијае на излезот кај другиот. На овој начин функциите на спрега ја одредуваат веројатноста на случување на квалитативни премини помеѓу состојбите на системите, како на пример патиштата со кои се влегува во и излегува од синхронизација. Декомпозицијата на една функција на спрега истовремено може да го олесни описот на функционалните придонеси на секој од подсистемите кои се спрегнати.

Постојат повеќе методи за реконструкција на функции на спрега од дадени податоци. Такви се пристапот базиран на најмали квадрати (Rosenblum & Pikovsky, 2001), на максимизација на веројатност (Tokuda, Jain, Kiss, & Hudson, 2007), динамичка Баесова инференција (Stankovski, A., McClintok, & Stefanovska, 2012), стохастичко моделирање (Schwabedal & Pikovsky, 2010), и фазно ресетирање (Levanjic & Pikovsky, 2011). Овие методи наоѓаат широка употреба во различни области, како на пример во хемијата (Tokuda, Jain, Kiss, & Hudson, 2007), (Kiss, Rusin, Kori, & Hudson, 2007), (Miyazaki & Kinoshita, 2006), (Kiss, Y., & Hudson, 2005), во невронауката (Stankovski, Ticcinelli,

McClintock, & Stefanovska, 2015), (Stankovski, Petkoski, Raeder, Smith, McClintock, & Stefanovska, 2016), (Stankovski, Ticcinelli, McClintock, & Stefanovska, 2017), во кардиореспираторната физиологија (Kralemann, et al., 2013), (Stankovski, A., McClintok, & Stefanovska, 2012), (Iatsenko, et al., 2013), во општествените науки (Ragnathan, Spaiser, Mann, & Sumpter, 2014), како и во заштитата на комуникациите (Stankovski, McClintock, & Stefanovska, 2014). Проучувањето на функциите на спрега има голема универзална важност за динамичките системи во интеракција, и станува многу важно и активно поле на проучување (Stankovski, Pereira, McClintock, & Stefanovska, 2017).

Кога два N - димензионални самоодржливи осцилатори со слаба интеракција и во услови на шум ќе се синхронизираат (Pikovsky, Rosenblum, & Kurths, 2001), нивното движење се опишува со нивната фазна динамика, дадена со:

$$\dot{\phi}_i = \omega_i + f_i(\phi_i) + g_i(\phi_i, \phi_j) + \xi_i(t)\,, \tag{3}$$

при што останатите координати се изразуваат како функции од фазата: $r_i \equiv r_i(\phi_i)$. Понатаму, ξ е дводимензионален вектор на шумот, кој вообичаено се смета за Гаусов и бел по природа, $\langle \xi_i(t)\xi_j(\tau)\rangle = \delta(t-\tau)E_{ij}$, и кој може да е, но и не мора да биде просторно корелиран. Шумот може да предизвика фазни поместувања во системите, па неопходно е прецизно познавање на f_i, g_i, и на матрицата на шум E_{ij}.

Периодичната состојба на системите подразбира дека нивните основни функции се исто така периодични, од каде и произлегуваат Фуриевите изрази за нив:

$$\begin{aligned} f_i(\phi_i) &= \sum_{k=-\infty}^{\infty} \tilde{c}_{i,2k} \sin k\phi_i + \tilde{c}_{i,2k+1} \cos k\phi_i\,, \\ g_i(\phi_i, \phi_j) &= \sum_{s=-\infty}^{\infty} \sum_{r=-\infty}^{\infty} \tilde{c}_{i;r,s} e^{i2\pi r \phi_i} e^{i2\pi s \phi_j}\,. \end{aligned} \tag{4}$$

Претпоставувајќи дека динамиката на системите е соодветно опишана од конечен број K на Фуриеови членови, фазната динамика од (3) може да се запише како конечна сума од основни функции:

$$\dot{\phi}_i = \sum_{k=-K}^{K} {c_k}^{(l)} \Phi_{l,k}(\phi_1, \phi_2) + \xi_l(t)\,, \tag{5}$$

каде што $l = 1, 2,\ \Phi_{1,0} = \Phi_{2,0} = 1, {c_0}^{(l)} = \omega_l$, а другите $\Phi_{l,k}$ и ${c_k}^{(l)}$ се K-те најважни Фуриеови компоненти.

Динамиката на системите може да се опише општо и со стохастичка диференцијална равенка:

$$\dot{x}_i = f(x_i, x_j|c) + \sqrt{D}\xi_i = g(x_i|c_1) + q(x_i, x_j|c_2) + \sqrt{D}\xi_i \ . \quad (6)$$

Тука, c е векторот на параметрите на системот, $f(x_i, x_j|c)$ се основните функции кои ја опишуваат автономната динамика $g(x_i)$ и функциите на спрега $q(x_i, x_j)$, а D е матрицата на дифузија на шумот за бел Гаусов шум, при што $i \neq j = 1, 2$.

Динамичките системи кои се користат за енкрипција на податоци во овој алгоритам, а кои во општ случај се опишани со (3), (5), и/или (6), треба да бидат самоодржливи но не мора да бидат хаотични. Сепак, хаотичните системи додаваат дополнително ниво на комплексност, а со тоа и на безбедност, доколку се гледа од криптографски аспект. Причината за ова е фактот што хаотичните системи делуваат случајни и непредвидливи, иако нивната природа во суштина е детерминистичка (Crutchfield, 2012). Исто така, атракторите на впрегнати хаотични динамички системи, како што ќе се види подоцна, типично покриваат голема површина во просторот на состојби, што е од голема предност при користењето на Баесова инференција на приемната страна за декрипција на податоците.

Уште од моментот кога Lorenz ги открил и објавил необичните карактеристики на хаосот (Lorenz, 1963), во смисла дека хаотичните системи се детерминистички по природа но делуваат како да се раководат по случајности, таквите системи во голема мерка се користат во инженерството, особено за обезбедување на безбедна комуникација (Cuomo & Oppenheim, 1993), (Kocarev & Parlitz, 1995), (Pecora & Carroll, 1990). Покрај претходно споменатите аспекти, причина повеќе за тоа е и стабилноста на ваквите системи и нивната голема отпорност дури и кон силни пертурбации.

5.3. Баесов метод за инференција (заклучување)

Предложениот алгоритам наложува на приемната страна податоците да се декриптираат со користење на динамичко Баесово заклучување (инференција), и то а во просторот на состојби. Моделот кој треба да се добие на приемната страна е всушност системот од испраќачот, даден со (6). Притоа, функцијата на спрега $q(x_i, x_j)$ всушност ја игра улогата на енкрипцискиот клуч.

Имајќи го сето тоа предвид, ако е дадена временската низа со димензии ($2 \times M$) како влез $\mathcal{X} = \{x_n \equiv x(t_n)\}$ $(t_n = nh)$, тогаш главната задача на динамичката Баесова инференција е да ги открие непознатите параметри на моделот и матрицата на дифузија на шумот, дадени како $\mathcal{M} = \{c, D\}$. Тоа всушност се сведува на максимизација на постериорната условна веројатност да се добијат параметрите $\mathcal{M}$ во случај кога

набљудуваните податоци се $\mathcal{X}$, што се означува со $p_{\mathcal{X}}(\mathcal{M}|\mathcal{X})$ (Stankovski, Duggento, McClintock, & Stefanovska, 2014).

Односот помеѓу оваа постериорна условна веројатност, априорната густина на веројатност $p_{prior}(\mathcal{M})$ (која го опфаќа сите априорни информации за непознатите параметри базирани на претходни набљудувања), и функцијата на веројатност $\ell(\mathcal{X}|\mathcal{M})$ (која ја претставува условната густина на веројатност да се набљудуваат податоците $\mathcal{X}$ во случај на познати и одбрани параметри $\mathcal{M}$), е даден со Баесовата теорема:

$$p_{\mathcal{X}}(\mathcal{M}|\mathcal{X}) = \frac{\ell(\mathcal{X}|\mathcal{M})p_{prior}(\mathcal{M})}{\int \ell(\mathcal{X}|\mathcal{M})p_{prior}(\mathcal{M})d\mathcal{M}}, \quad (7)$$

што значи дека саканата постериорна условна веројатност може да се пресмета според оваа формула.

Со користење на доволно густо семплирање h, проблемот може да се реши со т.н. дискретизација со Ојлеров центар $x_n{}^* = (x_{n+1} + x_n)/2$ на (6), при што се добива:

$$x_{i,n+1} = x_{i,n} + hf\left(x_{i,n}{}^*, x_{j,n}{}^* \middle| c\right) + h\sqrt{D}z_n \ . \quad (8)$$

Тука, $z_n \equiv \int_{t_n}^{t_{n+1}} z(t)dt$ е стохастичкиот интеграл на шумот во времето помеѓу два семплирачки моменти. Шумот е статистички независен и веројатноста е дадена со производот на веројатноста за набљудување на x_{n+1} во секој временски момент, за сите вредности на n. Според тоа, заедничката густина на веројатност на z_n се користи за да се најде заедничката густина на веројатноста на процесот во однос на $x_{n+1} - x_n$.

Тогаш негативната логаритамска веројатност $S = -\ln \ell(\mathcal{X}|\mathcal{M})$ може да се изрази како:

$$S = \frac{N}{2}\ln|D| + \frac{h}{2}\sum_{n=0}^{N-1}\left(c_k \frac{\partial f_k(x_{.,n})}{\partial x} + \left[\dot{x}_n - c_k f_k\left(x.^*_{,n}\right)\right]^T (D^{-1})\left[\dot{x}_n - c_k f_k(x.^*_{,n})\right]\right), \quad (9)$$

каде што $\dot{x}_n = (x_{n+1} - x_n)/h$. Саканата вредност се добива со имплицитно сумирање на претходниот израз за индексот k.

Ако се дадени повеќевеличинска нормална распределба за априорната веројатност на параметрите c, со средна вредност $\bar{c}$, матрица на коваријанса Σ_{prior}, и матрица на концентрација $\Xi_{prior} \equiv \Sigma^{-1}{}_{prior}$, тогаш постериорната повеќевеличинска веројатност $\mathcal{N}_{\mathcal{X}}(c|\bar{c}, \Xi)$, а со тоа и густината на веројатност за секој од параметрите на моделот (6), може да се евалуира со користење на следните четири равенки за секој од секвенцијалните податочни блокови од $\mathcal{X}$:

$$D = \frac{h}{N}\left[\dot{x}_n - c_k f_k\left(x.^*_{,n}\right)\right]^T\left[\dot{x}_n - c_k f_k(x.^*_{,n})\right], \quad (10)$$

$$\Xi_{k\omega} = (\Xi_{prior})_{k\omega} + hf_k\left(x.^*_{,n}\right)(D^{-1})f_\omega(x.^*_{,n}),$$
$$r_\omega = (\Xi_{prior})_{k\omega} + hf_k\left(x.^*_{,n}\right)(D^{-1})\dot{x}_n - \frac{h}{2}\frac{\partial f_k(x_{.,n})}{\partial x},$$
$$c_k = (\Xi^{-1})_{k\omega} r_\omega .$$

Овде, точката во индексите го претставува соодветниот индекс *i* или *j*. Понатаму, *D* е матрицата на шумот, а *r* е привремена матрична променлива која служи за пресметување на конечната вредност на векторот на параметри *c*. Сумирањето преку $n = 1, 2, \dots, N$ се подразбира, почетната вредност на априорната распределба на веројатноста е дадена со $\Xi_{prior} = 0$ и $\bar{c}_{prior} = 0$, а сумирањето преку индексите *k* и *ω* е имплицитно. Итерациите на алгоритмот сопираат кога ќе се увиди дека нивното понатамошно извршување не ја менува вредноста на *c* и Ξ повеќе од некоја предефинирана вредност на праг *ε*.

Главниот концепт на овој пристап на користење на динамичка Баесова инференција за декрипција кај приемникот, се заснова на тоа дека заклучувањето мора да ја следи временската еволуција на параметрите *c* и истовремено да ги одвои динамичките ефекти од неизбежниот придружен шум.

Кога секвенцијалните податоци доаѓаат од низа од мерења во форма на повеќе последователни блокови на информации, тогаш (10) се применува на секој од тие блокови, во поединечни временски прозорци. Ако за системот се знае дека е стационарен, тогаш постериорната густина на секој блок се зема како априорна за секој следен. На тој начин, неизвесностите во параметрите на системот постепено се намалуваат со текот на времето, како што сé повеќе и повеќе податоци се вклучени во тековните пресметки.

Но доколку системот е временски променлив, тогаш методот за пропагација на познавањето на состојбата на параметрите мора да се рефинира, т.е. процесот на пропагација на информации помеѓу *n* - тата постериорна дистрибуција и *n+1* - та априорна дистрибуција мора да дозволи да се следи временската промена на системските параметри. Затоа се дефинира симетрична позитивно дефинитна матрица Σ_{diff}, која покажува колку вредноста на секој параметар дифузира. Така, следната априорна веројатност за параметрите е всушност конволуцијата од двете тековни нормални повеќевеличински распределби Σ_{post} и Σ_{diff} : $\Sigma_{prior}{}^{n+1} = \Sigma_{post}{}^{n} + \Sigma_{diff}{}^{n}$.

Матрицата на дифузија се дефинира како: $\Sigma_{diff}{}_{i,j} = \rho_{ij}\sigma_i\sigma_j$, каде што σ_i е стандардната девијација на дифузијата на c_i во тековниот временски прозорец, а ρ_{ij} е корелацијата помеѓу промените во параметрите c_i и c_j. Практично, ова всушност значи дека матрицата Σ_{diff} има нулеви вредности секаде освен во главната дијагонала, каде се сместени скалираните дијагонални вредности од матрицата Σ_{post}.

Понатамошни детали за динамичката Баесова инференција и нејзината софтверска имплементација и апликации можат да се најдат во (Stankovski, McClintock, & Stefanovska, 2014), (Stankovski, A., McClintok, & Stefanovska, 2012), (Stankovski, Duggento, McClintock, & Stefanovska, 2014), (Smelyanskiy, Luchinsky, Stefanovska, & McClintock, 2005), и во тамошните референци. Целата процедура на динамичко Баесово заклучување е изложена и во форма на алгоритам во следниот дел кој ја опишува практичната имплементација на протоколот за безбедна комуникација.

5.4. Практична имплементација на алгоритмот за безбедна комуникација во присуство на бел Гаусов шум

Како што беше нагласено претходно, главната предност на овој комуникациски алгоритам е неговата моќна енкрипција и практично неограниченото множество на можни вредности на клучот кој се користи за тоа. Ова значи дека протоколот може да најде примена во различни комуникациски апликации каде безбедноста на информациите е од клучно значење, а веќе беше изложено дека потребата од безбедност е честа кај индустриските вмрежени системи.

Сепак, се покажува дека предложениот алгоритам овозможува и значителна отпорност на шум на целокупниот систем, пред сé благодарение на користењето на динамичката Баесова инференција, која по природа претставува стохастичко заклучување. Овие резултати се очигледни при практична имплементација на алгоритмот со функции на спрега. Во овој дел ќе биде прикажан пример за еден таков практичен експеримент каде се тестирани перформансите на изложениот комуникациски протокол. Покрај тоа, целта на експериментот е и да се покаже можноста протоколот да се имплементира на хардвер кој е лесно и комерцијално достапен за општа употреба.

Од таа причина, експериментот е изведен така што испраќачот и приемникот на податоци се реализирани на два Raspberry PI 2 миникомпјутери. Станува збор за компјутери целосно имплементирани на една плоча (анг. single-board computer), составени од централна процесирачка единица со ARM архитектура, графичка процесирачка единица, SD картички за чување на оперативниот систем и програмската меморија, како и интерфејси за поврзување на голем број на дополнителни периферни уреди. Конкретно, се користи модел B од Raspberry PI 2, што претставува верзија со SoC Broadcom BCM2836 quad core Cortex A7 процесор од 900 MHz, со графичка процесирачка единица VideoCore IV, и системска меморија од 1 GB LPDDR2. Двата компјутери се поврзани преку 10/100M Ethernet врска и едниот игра улога на испраќач, а другиот на приемник на податоци. Според односот на перформансите и цената, овие уреди спаѓаат во категоријата во која се

и паметните телефони, па успешноста на протоколот за безбедна комуникација со функции на спрега на Raspberry PI 2 подразбира и дека се сосем реални можностите за негова идна практична апликација.

Сликовит приказ на целиот комуникациски алгоритам а со тоа и на експериментот може да се види на веќе дадената и претходно референцирана Слика 28.

На испраќачката страна треба да се испратат два временски променливи бинарни сигнали $s_1(t)$ и $s_2(t)$. За таа цел тука се наоѓа систем составен од два взаемно спрегнати хаотични Лоренцови осцилатори, при што првиот е даден со равенките:

$$\begin{aligned} \dot{x}_1 &= 10x_2 - 10x_1 + s_1(t)\cos(y_1)x_2 + s_2(t)x_1y_2/y_3 \,, \\ \dot{x}_2 &= 28x_1 - x_1x_3 - x_2 \,, \\ \dot{x}_3 &= x_1x_2 - 2.67x_3 \,, \end{aligned} \qquad (11)$$

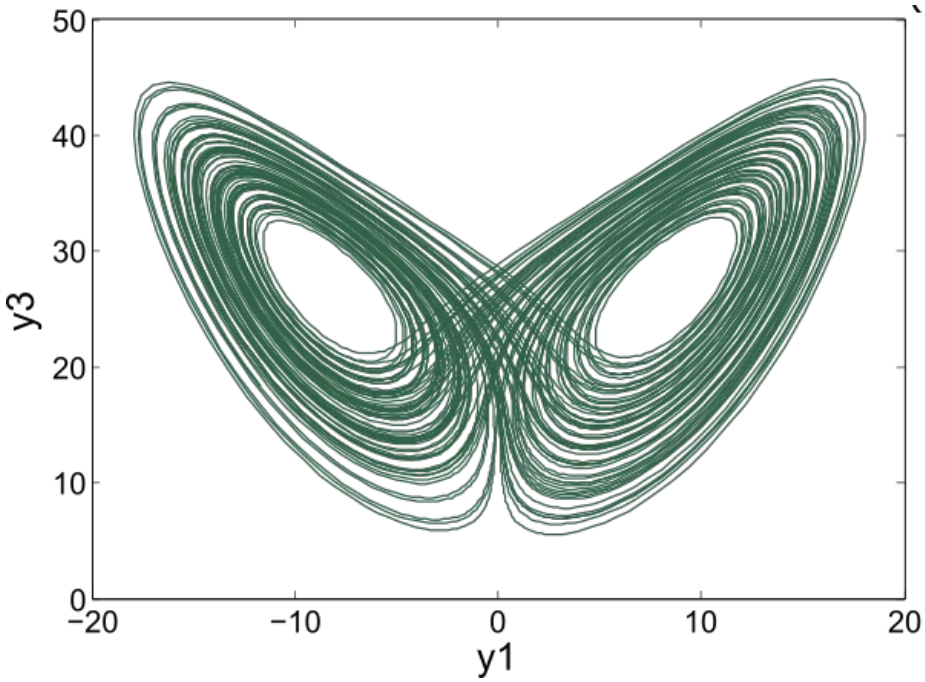
а вториот е даден со:

$$\begin{aligned} \dot{y}_1 &= 10y_2 - 10y_1 \,, \\ \dot{y}_2 &= 28y_1 - y_1y_3 - y_2 \,, \\ \dot{y}_3 &= y_1y_2 - 2.67y_3 \,. \end{aligned} \qquad (12)$$

Очигледно е дека во равенката за состојбата x_1 од првиот осцилатор има две функции на спрега. Секоја од нив содржи променливи од првиот но, што е уште поважно, и од вториот осцилатор. Мора да се напомене и дека овие две нелинеарни функции на спрега се само пример избран за конкретниот случај - наместо нив можат да се користат и други варијанти на линеарно независни функции.

Двата сигнали кои треба да се испратат се променливите коефициенти кај двете функции на спрега. Однесувањето на овие системи може да се види на Слика 29, Слика 30, и Слика 31, каде се прикажани Lissajou кривите за парот на осцилатори.

Најпрвин, на Слика 29 се прикажани траекториите на состојбите y_1 и y_3 од вториот автономен Лоренцов осцилатор (12). Графикот има очекувана форма, бидејќи траекториите на состојбите се привлечени кон стабилни точки, и обликот е типичен за хаотичните атрактори, меѓу кои секако спаѓа и Лоренцовиот.

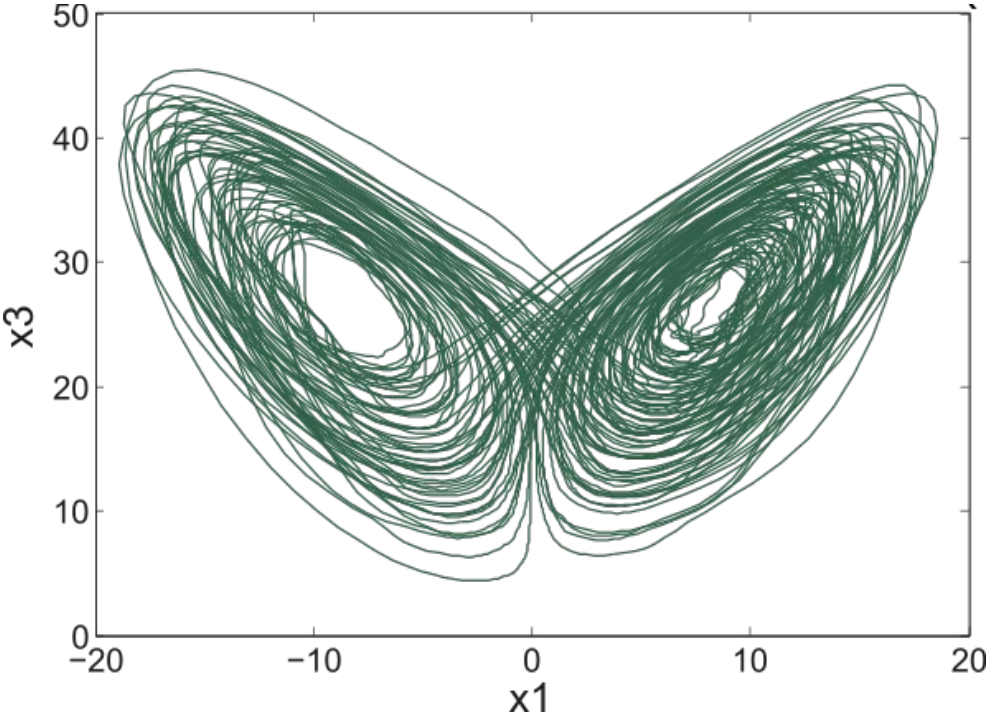


Слика 29 Траекториите на y_1 и y_3 од вториот осцилатор кај испраќачот

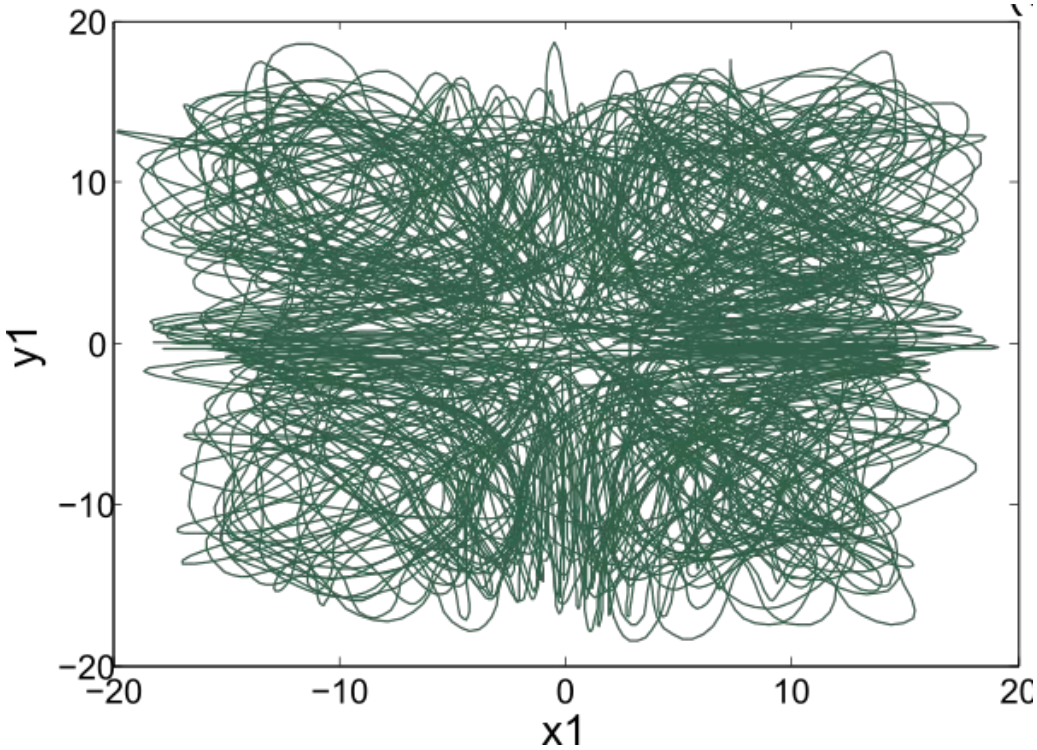
Понатаму, на Слика 30 се прикажани траекториите на состојбите x_1 и x_3 од првиот осцилатор (11). Графикот е сличен на претходниот, но сепак забележлива е грубоста на траекториите, што е очекувано со оглед на тоа што состојбата x_1 ги содржи елементите на спрегата.

Конечно, на Слика 31 е прикажан односот помеѓу заемно спрегнатите состојби на двата системи x_1 и y_1 за време на преносот на информации помеѓу испраќачот и приемникот. Спрегнувачката Lissajous крива е хаотична.

Очигледно е дека решението не е врзано за ограничен и предвидлив простор на траекториите, туку напротив е добро сокриено во хаотичните и заплеткани спрегнувачки траектории и нелинеарни односи и зависности помеѓу системите. Токму ова е најпосакуваното својство на овој пристап кога е во прашање безбедноста на комуникацијата и моќноста на енкрипцијата на податоците и информациите кои се испраќаат.



Слика 30 Траекториите на x_1 и x_3 од вториот осцилатор кај испраќачот



Слика 31 Траекториите на x_1 и y_1 од двата осцилатори кај испраќачот

Од испраќачот не се испраќаат саканите s_1 и s_2, туку се испраќаат само сигналите x_1 и y_2 од двата осцилатори со чија спрега се енкриптираа s_1 и s_2. Пред испраќањето, x_1 и y_2 се претвораат во аналогни сигнали со помош на соодветен дигитално - аналоген конвертор, се засилуваат и се испраќаат преку вплетените парици на Ethernet конекцијата до приемникот. Во текот на комуникацијата на сигналите им се додава шум за да се испита неговото влијание врз нив. На приемната страна двата аналогни сигнали се враќаат назад во дигитална форма со аналогно - дигитален конвертор и се користат за комплетно синхронизирање на хаотичните системи кај приемникот (Pecora & Carroll, 1990). Така, системот u, преку x_1, ефективно станува идентичен на системот x (првиот осцилатор кај испраќачот):

$$\begin{aligned} u_1 &= x_1 \,, \\ \dot{u}_2 &= 28x_1 - x_1u_3 - u_2 \,, \\ \dot{u}_3 &= x_1u_2 - 2.67u_3 \,, \end{aligned} \qquad (13)$$

додека пак на истиот начин системот w, преку y_2, станува идентичен на системот y (вториот осцилатор кај испраќачот):

$$\begin{aligned} \dot{w}_1 &= 10y_2 - 10w_1 \,, \\ w_2 &= y_2 \,, \\ \dot{w}_3 &= w_1y_2 - 2.67w_3 \,. \end{aligned} \qquad (14)$$

Временските низи на шесте сигнали од двата реконструирани системи u и w кај приемникот всушност играат улога на влезови во алгоритмот за динамичката Баесова инференција, кој потоа на излез треба да ги даде заклучените вредности на параметрите c на функциите на спрега, кои се всушност оригиналните сигнали s_1 и s_2.

Алгоритмот за заклучување во рамките на еден временски прозорец всушност се состои од рекурзија на равенките дадени со (10) за системот даден со (13) и (14). Тој се состои од следните чекори:

i) алгоритмот стартува со почетните вредности на c_{prior} и Ξ_{prior} ;

ii) се пресметува матрицата на шум D_{new} со првата равенка од (10);

iii) се пресметува матрицата Ξ_{new} со втората равенка од (10);

iv) се пресметува r со користење на третата равенка од (10);

v) се пресметува c_{new} со користење на четвртата равенка од (10);

vi) алгоритмот се враќа на точка ii) со користење на c_{new} како c.

Условот за стопирање, како што беше споменато претходно, е достигнување на конвергенција со алгоритмот, т.е. ситуација кога понатамошни итерации на алгоритмот не ја менуваат повеќе значително вредноста на c и Ξ. Условот кој се користи за оваа проверка е даден со:

$$\sum \frac{(c_{old} - c_{new})^2}{c_{new}^{\ 2}} < \varepsilon \,, \qquad (15)$$

каде што ε е константа со многу мала вредност. Бидејќи проблемот е параболичен, оваа конвергенција се остварува многу брзо, најчесто за само неколку циклуси. За чекорот i) од алгоритмот, се зема дека иницијалната априорна распределба е неинформативна за процесот, т.е. дека $\Xi_{prior} = 0$ и $c_{prior} = 0$.

Во продолжение е даден алгоритмот за динамичка Баесова инференција во форма на псевдо-код кој може да се имплементира во било кој програмски јазик.

Првин е опишан главниот алгоритам:

Алгоритам 1: Баесова инференција

```
// пресметување на потребни променливи

calculate f
calculate v
c_pt = c_pr

FOR lp=1:MaxLoops  // главна рекурзивна јамка

   - calculate D
   - calculate c_pt

   IF SUM((c_pr-c_pt)^2/c_pt^2)<Epsilon  // ако е исполнет условот за конвергенција се запира
      RETURN
   ENDIF

   c_pr=c_pt

ENDFOR
```

Табела 2 Главен алгоритам за динамичка Баесова инференција

Овој алгоритам содржи два подалгоритми "*calculate f*" и "*calculate v*". Тие не се секогаш исти и зависат од обликот на моделот кој се заклучува. Притоа, f е основната функција на моделот (која може да се види во (6)), а v ги претставува нејзините парцијални изводи:

$$v\left(\mathcal{X}.^{*}{}_{,n}\right) = \frac{\partial f\left(\mathcal{X}.^{*}{}_{,n}\right)}{\partial \mathcal{X}}. \quad (16)$$

Останатите две функции во главниот алгоритам "*calculate D*" и "*calculate* c_{pt}" се изложени во продолжение.

Алгоритам 2: Пресметка на *D* // со користење на првата равенка од (10)

D = D+($\dot{\mathcal{X}}$-f*c)*(transpose of $\dot{\mathcal{X}}$-f*c)
D = (h/N)*D

Табела 3 Пресметување на матрицата на шумот

Конечно, во следниот алгоритам е дадена пресметката на векторот на параметри c. За неговото пресметување се потребни и вредностите на Ξ и r.

Алгоритам 3: Пресметка на *c*

invD = D^{-1}

// пресметување на Ξ со користење на втората равенка од (10)

FOR i=1:*l*
  FOR j=1:*l*

    Ξ_{pt}((i-1)·K+1 TO i·K,(j-1)·K+1 TO j·K) =
    Ξ_{pr}((i-1)·K+1 TO i·K,(j-1)·K+1 TO j·K) + h*invD(i,j)*f*(transpose of f)

  ENDFOR
ENDFOR

// пресметување на r со користење на третата равенка од (10)

ED=invD*$\dot{\mathcal{X}}$

FOR i=1:*l*
  FOR j=1:*l*
    $r(ALL,i) = r(ALL,i)+\Xi_{pr}((i-1)\cdot K+1 \text{ TO } i\cdot K,(j-1)\cdot K+1 \text{ TO } j\cdot K)*c(ALL,j)$
  ENDFOR
  $r(ALL,i) = r(ALL,i)+h\cdot P*(\text{transpose of ED})-(h/2)\cdot sum(v(ALL,i))$
ENDFOR

// пресметување на c со користење на четвртата равенка од (10)

$c = (\Xi_{pt}^{-1})*r$

Табела 4 Инференција на параметрите *c*

Тука, *l* е бројот на временски низи, а K=M/*l* каде што M е вкупниот број на основни функции кои се користат. Операторите * и · се однесуваат на матрично и скаларно множење соодветно. За пресметките во рамките на матриците, TO го претставува линеарниот распон на целобројни индекси во еден ред или една колона на матрицата, а соодветно ALL ги претставува сите индекси во еден ред или една колона на матрицата.

Трите алгоритми кои се користат на приемната страна во протоколот се аплицирани на еден прозорец од примени податоци. Временската низа се дели во повеќе последователни податочни блокови и алгоритмите се применуваат на секој од нив по ред. Суштината на динамичката Баесова инференција е во тоа дека ги користи информативните априори, односно евалуацијата на секој последователен податочен блок зависи од (и ги користи) евалуациите и резултатите од претходниот блок. Процесот на пропагација на информациите помеѓу *n*-тата постериорна и следната *n+1*-а дистрибуција ја следи временската промена на параметрите преку матрицата на концентрација Ξ_{pt}. Тоа е изложено во последниот алгоритам.

Алгоритам 4: Пропагација

$c_{pr}^{n+1} = c_{pt}^{n}$

$inv\Xi n = (\Xi_{pt}^{n})^{-1}$
$invDiff^{n} = 0$

FOR i=1:K
  $invDiff^{n}(i,i) = p_{\omega}^{2}*inv\Xi^{n}(i,i)$
ENDFOR

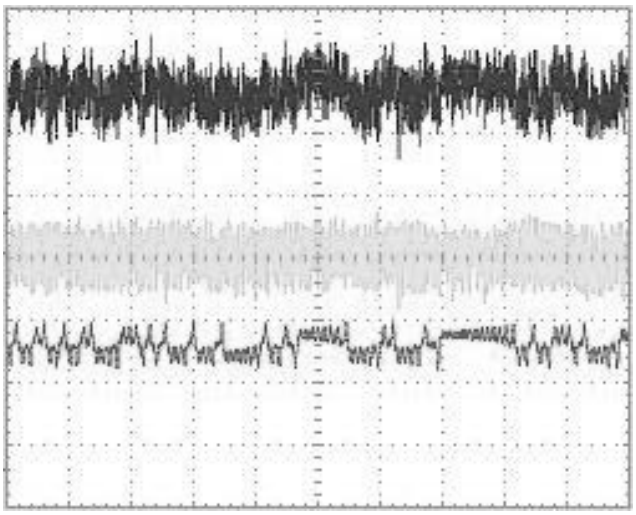
$\Xi_{pt}^{n+1} = (invDiff^{n} + (\Xi^{n})^{-1})^{-1}$

Табела 5 Пропагација на веројатностите во рамките на инференцијата

Нумеричките симулации за генерирање на сигналите кај испраќачот (и за нивна реконструкција кај приемникот) се извршени со помош на Runge-Kutta шема од четврти ред, со семплирање $h = 0.01$.

Што се однесува до хардверскиот аспект, дигитално - аналогниот и аналогно - дигиталниот конвертор кои се користат се имплементирани на ADC-DAC Pi картички кои се базирани на MCP3202 А/Д конверторот на Microchip, (содржат два аналогни влеза со 12 битна резолуција) за А/Д конверзија, и на MPC4822 Д/А конверторот на Microchip (со 12 битна резолуција на два канали и внатрешен извор на референтен напон) за Д/А конверзија. За засилување на сигналите се користени општонаменски операциски засилувачи TL084N со стандардни вредности за отпорниците и кондензаторите.

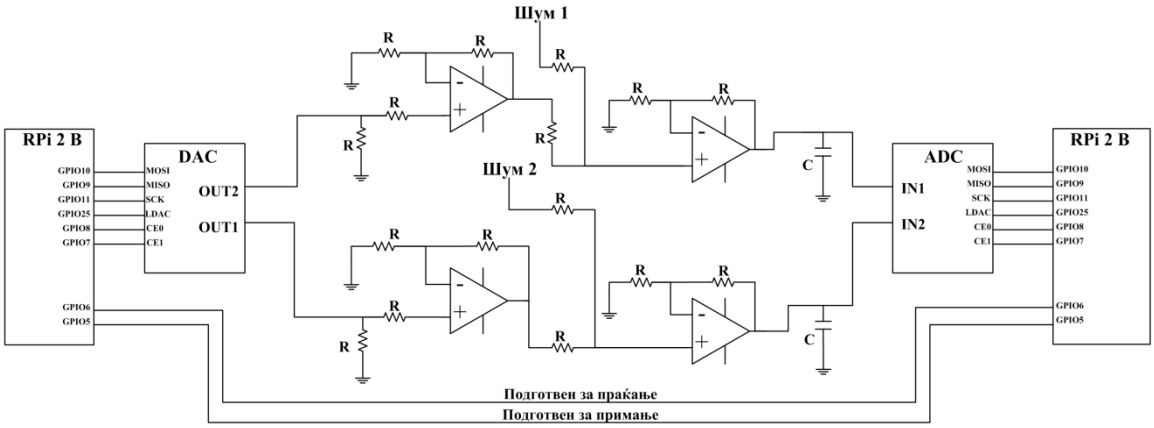
Шумот кој се додава на двата испратени сигнали во текот на комуникацијата се генерира во Matlab и се испраќа на два одвоени и независни аналогни излези од компјутерска звучна картичка со семплирачка фреквенција од 100 kHz. Двата сигнали на шум се со иста амплитуда, а анализата на нивната средна вредност, автокорелација, и на нивниот фреквентен спектар јасно укажува дека генерираниот шум ги поседува својствата на експериментален бел шум. На Слика 32 можат да се видат временски исечоци од три сигнали снимени со помош на осцилоскоп: најдолниот сигнал е испратениот аналоген сигнал $y_2(t)$, во средината е додадениот бел шум, а на врвот е сигналот $y_2(t)$ откако шумот е додаден на него. Ова дава добра визуелна претстава за директниот ефект на генерираниот шум врз испратените сигнали (информации) во временски домен.



Слика 32 Осцилоскопски снимки во реално време од испратениот сигнал y_2 (долу), генерираниот шум за него (средина), и y_2 по додавањето на шумот (горе)

Логиката на пренос на податоците подразбира и користење на т.н. "ракување" (анг. handshaking) преку директни дигитални поврзувања помеѓу испраќачкиот и примачкиот компјутер. Преку овие линкови, испраќачот праќа дигитален бинарен индикатор кога е подготвен за испраќање на податоци, по што приемникот враќа соодветен бит за да индицира дали е подготвен за нивен прием. Сето ова се прави со цел да се овозможи сигурна комуникација и да се минимизира можноста за грешки и нивното влијание врз процесот. Бидејќи брзината на комуникација не е во фокусот на ова истражување, временскиот прозорец во кој се применува Баесовото заклучување е 250 s со семплирање $h = 0.01$, т.е. секој бит {0 или 1} се испраќа во рамките на ова времетраење.

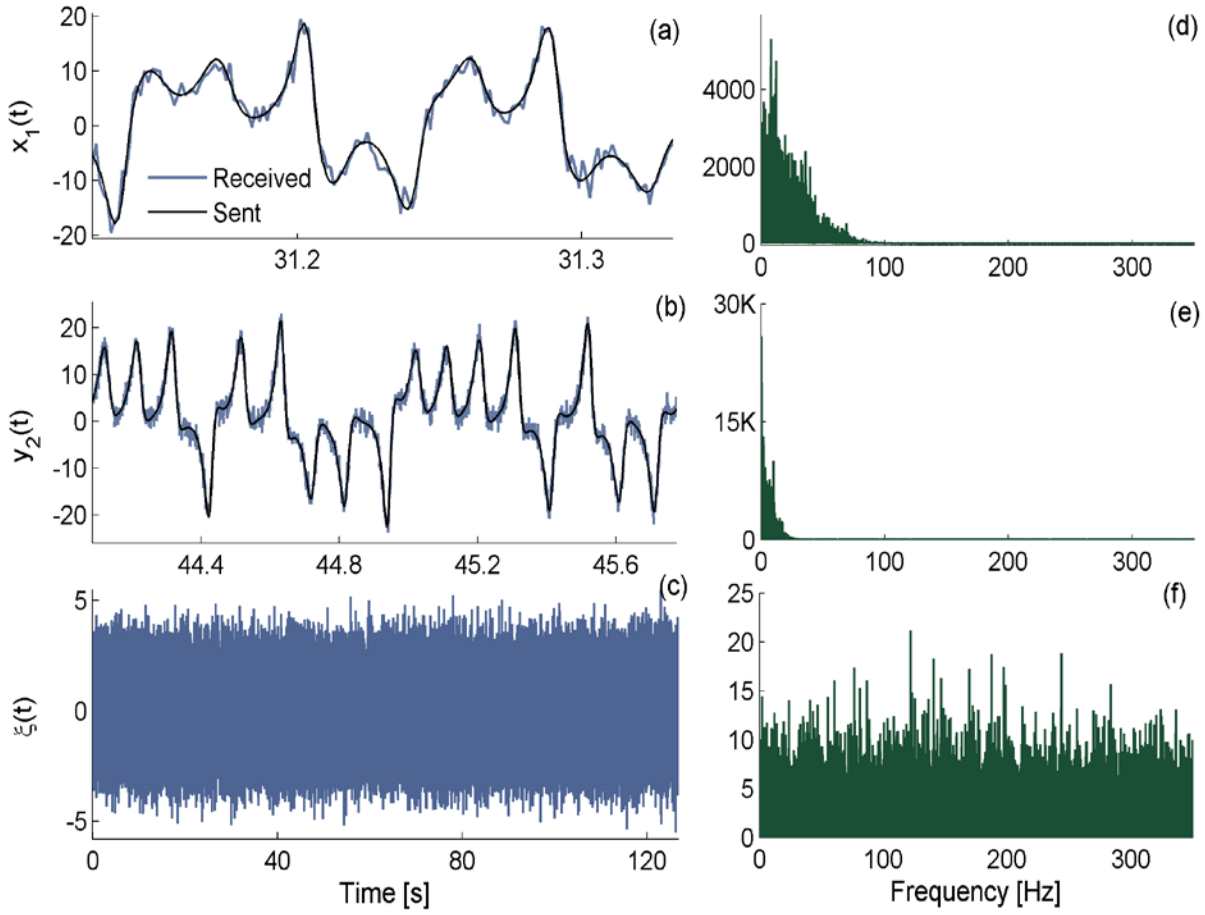
На Слика 33 може да се види детална електрична шема од електронската имплементација на комуникацискиот систем кој се користи за експериментот и за истражувањето. Сигналот x_1 се пренесува преку горниот, а сигналот y_2 се пренесува преку долниот комуникациски канал на сликата.



Слика 33 Детална електронска шема од практичната имплементација на комуникацискиот систем

Во продолжение ќе биде дадена анализата на резултатите од претходно опишаниот експеримент за практична имплементација на протоколот за безбедна комуникација со функции на спрега.

За време на генерирањето, енкрипцијата, преносот, и дескрипцијата на податоците, сите сигнали се зачувани за подоцнежна offline анализа. Затоа е можно детално да се анализираат временските облици на испратените сигнали: на Слика 34 е прикажана оваа анализа на неколку графици.



Слика 34 Графици на испратените сигнали x_1 и y_2 и на генерираниот шум во временски и во фреквентен домен

Најпрвин, на a) и b) се прикажани испратените $x_1(t)$ и $y_2(t)$, пред и откако е додаден шумот, при што шумната верзија е суперпонирана врз оригиналните сигнали соодветно. На c) пак е прикажана дигитализирана временска форма на аналогниот бел шум кој се додава на сигналите. Од овие графици е очигледно влијанието на шумот врз сигналите во временскиот домен.

На десната страна од сликата се наоѓаат соодветните Фуриеви трансформации (направени со помош на брзи Фуриеви трансформации, анг. fast Fourier transform - FFT) на двата испратени сигнали на d) и e), и на додадениот шум на f). Може да се види дека спектрите на хаотичните сигнали $x_1(t)$ и $y_2(t)$ се проширени но немаат изразени хармоници.

Во контраст на ова, спектарот на шумот ги содржи сите фреквенции распространети низ целиот набљудуван домен, како што и може да се очекува од процес

на бел шум. Ова е и потврда повеќе дека вештачки генерираниот шум има сакани карактеристики и е верен репрезент на природниот бел шум.

5.5. Анализа на работата на протоколот во присуство на нискофреквентен шум кој не е Гаусов

Пречките кои се јавуваат во комуникациските мрежи најчесто се моделираат како случаен Гаусов процес (со нормална распределба). Ваквиот пристап е коректен и соодветен во случаи каде шумот е причинет од повеќе различни сигнали во околината кои се меѓусебно независни и некорелирани, при што ниту еден од нив не доминира во нивното целокупно акумулирано влијание. Еден виден и најчесто среќаван пример за ваквите случаи е топлинскиот шум во електрониката, кој се моделира како адитивен бел Гаусов шум. Како што беше изложено претходно, протоколот за безбедна комуникација со функции на спрега успешно се справува со ваквиот шум во комуникациските мрежи.

Сепак, во многу ситуации во реалноста постојат доминантни извори на интерференција, најчесто како резултат на слабеењето на моќноста на сигналите при нивното ширење низ просторот (El Sawy, Sultan-Salem, Alouini, & Win, 2017). Во вакви случаи, апроксимацијата со бел Гаусов шум не е задоволителна затоа што функцијата на густина на веројатноста на реалните пречки има "задоцнет" и пострмен прираст од онаа на Гаусовиот модел. Постојат различни пристапи за моделирање на шумови од ваква природа, какви што се користењето на мешани Гаусови модели, на просторен Поасонов процес (Win, Pinto, & Shepp, 2009), на т.н. розов шум (Bak, Tang, & Wiesenfeld, 1987), уште и наречен "1/f шум", чиј спектар на моќност е обратно пропорционален од фреквенцијата, и конечно користењето на процесот Ornstein-Uhlenbeck (Hanggi, Mroczkowski, Moss, & McClintock, 1985), на кој овде ќе му се обрне најмногу внимание.

Историски, Ornstein-Uhlenbeck процесот бил прв пат искористен за моделирање на брзините на Брауновото движење на честички во течност, и притоа дал модел кој бил подобар и пореален во однос на моделирањето со бел шум (Bibbona, Panfilo, & Tavella, 2008). Општо гледано, еден Ornstein-Uhlenbeck процес може да се дефинира со:

$$\dot{\eta}(t) = \xi(t) - \frac{1}{\gamma}\eta(t)\ , \qquad (17)$$

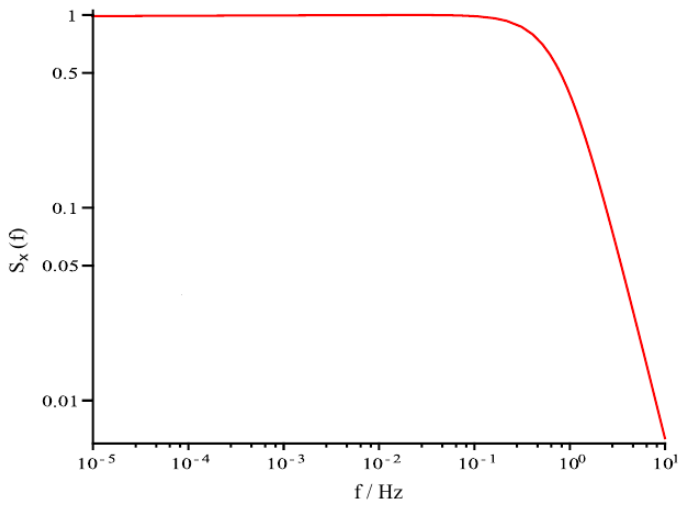
со автокорелација $\langle \eta(t)\eta(t') \rangle = \sigma^2 e^{-\frac{t-t'}{\gamma}}$. Овде, $\xi(t)$ е бел Гаусов шум со јачина (или во статистичка смисла варијанса) D, а γ е времето на корелација на случајниот процес. Оваа величина всушност означува колку време е потребно да помине за случајниот сигнал "да

се повтори" во статистичка смисла. Во граничен случај кога $\gamma \to 0$, очигледно е дека случајниот процес конвергира кон бел Гаусов шум. Сепак, во реалноста шумот често има ненулево време на корелација кое не може да се занемари, па така овој процес е всушност еден вид на природно генерализирање на белиот Гаусов шум и може да се искористи за моделирање на пречките кои се јавуваат во комуникациските системи во реалниот свет (Lehle & Peinke, 2017).

Фреквентниот спектар на ваквиот процес го дале и самите автори (Wang & Uhlenbeck, 1945), и може да се претстави со:

$$S_x(f) = \frac{\sigma^2\gamma^2}{1+4\pi^2\gamma^2 f^2}, \qquad (18)$$

каде што σ е јачината на шумот, а γ е времето на корелација. Спектарот уште може да се види и на Слика 35, и тоа за јачина $\sigma = 5$ и за време на корелација $\gamma = 0.2$.



Слика 35 Фреквентен спектар на стационарен Ornstein-Uhlenbeck процес со јачина 5 и време на корелација 0.2 (од (Bibbona, Panfilo, & Tavella, 2008))

Процесот Ornstein-Uhlenbeck има тенденција на т.н. лебдење (анг. drift) кон својата средна вредност со тек на време (на англиски уште и се нарекува mean-reverting process). Сепак, во текот на релативно кратките временски прозорци за време на кои се одвива комуникација помеѓу два ентитети, а и за доволно големи вредности на времето на корелација γ, оваа спомената тенденција може целосно да се занемари и шумот да се третира како целосно различен од нормалниот бел Гаусов шум, иако по дефиниција го содржи истиот во својата основа и се претвора во него во стационарен режим. Ова е и

соодветно потврдено со помош на користење на Kolmogorov-Smirnov и Anderson-Darling тестовите, кои се непараметарски тестови кои имаат за цел да проверат дали случајните вредности на податоците од даден процес потекнуваат од нормална распределба. Со повторување на овие тестови за различни вредности на времето на корелација γ, се заклучува дека за шумовите генерирани со (17) може со сигурност да се смета дека не доаѓаат од нормална Гаусова распределба за вредности $\gamma \geq 0.09$. Со други зборови, шумот е реален и не е бел Гаусов шум за времиња на корелација поголеми од 90 ms.

Од горенаведените причини, и со цел да се испита робустноста на протоколот за безбедна комуникација изложен во оваа глава на шумови кои многу почесто можат да се најдат во реални услови, извршена е анализа базирана на нумеричките симулации дадени во (Stankovski, McClintock, & Stefanovska, 2014). Поставеноста на системот е концептуално иста како онаа опишана на Слика 28, но значителната разлика е во тоа што сега наместо бел Гаусов шум, на испратените сигнали им е придружен нискофреквентниот Ornstein-Uhlenbeck шум $\eta(t)$. Осцилаторите кај испраќачот се повторно оние дадени со (11) и (12), и повторно сигналите кои се испраќаат се x_1 и y_2, што значи дека при преносот важи:

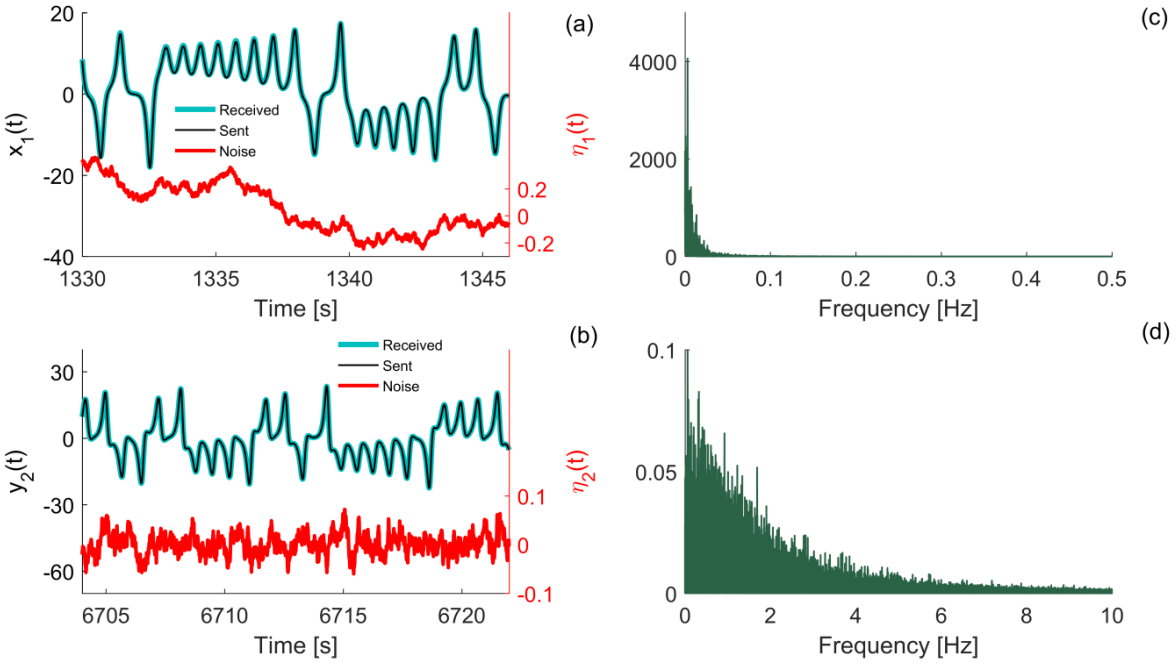
$$\begin{aligned} x_1 &= x_1 + \eta_1(t), \\ y_2 &= y_2 + \eta_2(t). \end{aligned} \qquad (19)$$

Притоа, сигналот на шумот $\eta_1(t)$ е генериран со јачина од $D_1 = 20$ и со време на корелација $\gamma_1 = 30$, а сигналот на шумот $\eta_2(t)$ е генериран со јачина од $D_2 = 20$ и со време на корелација $\gamma_2 = 0.09$, на самата граница на преминување во Гаусов шум која е претходно утврдена од Kolmogorov-Smirnov и Anderson-Darling тестовите.

Во продолжение се дадени резултатите од нумеричките симулации извршени за време од 20000 секунди, за време на кои вкупно 400 битови од податоци се енкриптирани со помош на функции на спрега, потоа испратени, и конечно декриптирани во 400 прозорци на Баесова инференција на приемната страна, при што секој прозорец трае по 50 секунди, сето тоа при периода на семплирање од $h = 0.01$.

На Слика 36 се прикажани испратените и примените сигнали при симулацијата, како и временскиот облик и фреквентниот спектар на генерираните шумови. Најпрвин на a) се прикажани временските облици на испратениот (со црна боја) и приемниот (со сина боја) сигнал $x_1(t)$, а на истиот график со црвена боја е прикажан и шумот $\eta_1(t)$. Слично, на b) се прикажани соодветните временски облици на испратениот и приемниот сигнал $y_2(t)$ и на шумот $\eta_2(t)$. Влијанието на шумот може да се забележи по малите, но сепак видливи разлики во временските серии на испратениот и приемниот сигнал на двата графици. На c) и d), пак, се прикажани фреквентните спектари добиени со брза Фуриева трансформација на $\eta_1(t)$ и $\eta_2(t)$ соодветно. Од приложеното може да се види дека подолгото време на корелација шумот на првиот сигнал го прави нискофреквентен и значително поразличен

од Гаусовиот шум - има повидливо лебдење (drift) кон средната вредност во временски домен (a) и спектар на моќност концентриран во појас на многу ниски фреквенции (c). Од друга страна, пократкото време на корелација (кое кај шумот на вторичниот сигнал е на границата востановена со Kolmogorov-Smirnov и Anderson-Darling тестовите) сега го прави шумот многу посличен на бел Гаусов - и во временски домен (b), и во фреквентен домен, каде сега спектарот е распространет по поширок фреквентен појас (d). Од овде може и да се забележи зошто изборот на начин на моделирање на реален шум паѓа на Ornstein-Uhlenbeck процесот: со едноставно менување на параметарот на времето на корелација, целиот генериран шум може ефективно да се трансформира од бел Гаусов во нискофреквентен.



Слика 36 Графици на испратените сигнали x_1 и y_2 и на генерираниот шум во временски и во фреквентен домен

За соодветно да се види перформансот на протоколот за безбедна комуникација во услови на нискофреквентен шум, неопходно е да се испита неговата успешност во декрипцијата на кодираните податоци, што е направено со помош на средната квадратна грешка дадена со:

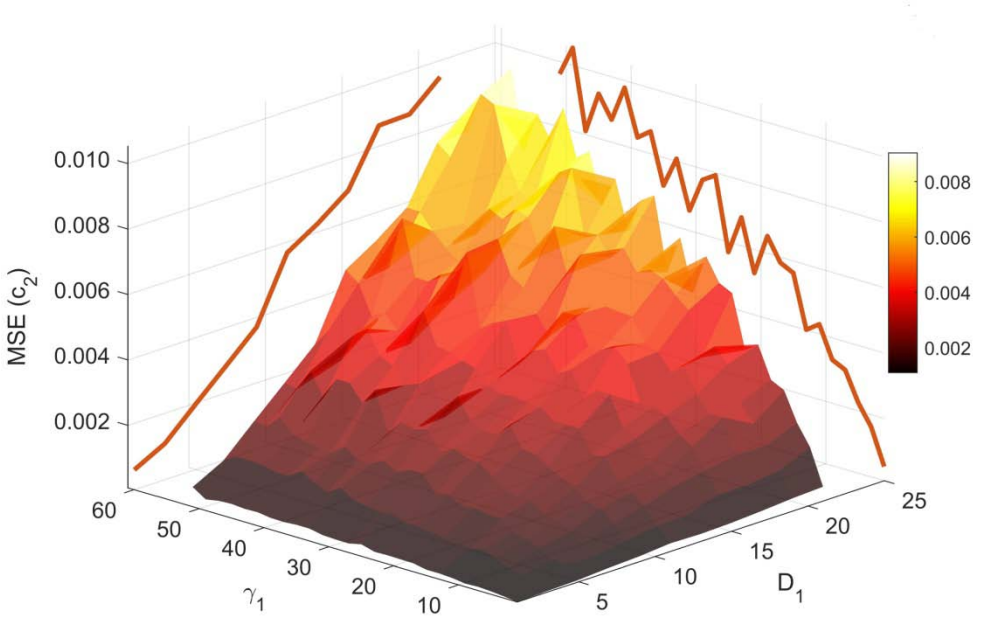
$$MSE(c) = \frac{1}{n}\sum_{i=1}^{n}(c_{j,\text{декриптирано}} - c_{j,\text{енкриптирано}})^2 \,, \qquad (20)$$

која го претставува отстапувањето помеѓу оригиналната вредност на испратените битови c_j пред енкрипцијата, и нивната декриптирана вредност до која приемникот дошол по применување на динамичката Баесова инференција.

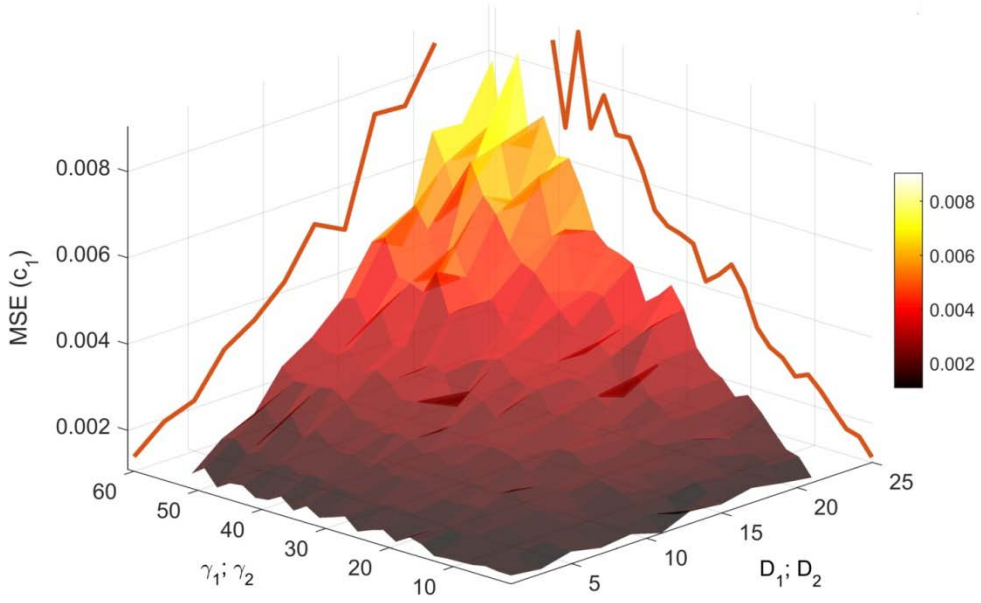
На Слика 37 е прикажана средната квадратна грешка MSE (анг. mean squared error) на вториот енкриптиран и испратен бит $c_2(t)$ во услови кога при симулацијата параметрите на шумот $\eta_2(t)$ се држени на константни вредности $D_2 = \gamma_2 = 1$, а менувани се само параметрите на шумот $\eta_1(t)$ кој влијае на $x_1(t)$, и тоа интензитетот D_1 во границите [0;22] и времето на корелација γ_1 во границите [0;52]. Средната грешка е одредена за секој можен целобројен пар на вредности на D_1 и γ_1 со што е добиена површината на зависност прикажана на графикот. Очигледно е дека грешката расте со порастот на јачината и/или времето на корелација на шумот, што значи дека со оддалечувањето на шумот од бел Гаусов по своите карактеристики, прецизноста на механизмот за динамичка Баесова инференција се намалува.

На истата слика се дадени и проекциите на тридимензионалната површина на страничните рамнини, кои дополнително покажуваат дека грешката расте порамномерно и речиси линеарно со зголемувањето на силината на шумот D, за разлика од зголемувањето на времето на корелација γ кое придонесува за многу похаотично и непредвидливо поведение на грешката. Слични графици на зависност на грешката при декрипцијата на оригиналните податоци се добиваат и со менување на останатите параметри и водат до истите заклучоци, но овде не се вклучени во интерес на простор и едноставност на презентирањето на резултатите.

Втор тип на ситуација е симулирана со истовремено зголемување на јачината и времето на корелација на двата шумови $\eta_1(t)$ и $\eta_2(t)$. На Слика 38 е прикажана зависноста на средната квадратна грешка при примањето и декрипцијата на податочните битови $c_1(t)$ од промената на параметрите на двата шумови. Од страничните проекции на површината може да се забележи дека грешката повторно расте на сличен начин како и претходно, и дека повторно зголемувањето на јачината на шумовите придонесува за многу помирно и порамномерно растење, а пак менувањето на времето на корелација предизвикува турбулентно и непредвидливо менување на оваа зависност.



Слика 37 Зависноста на средната квадратна грешка на испратените и примените сигнали $c_2(t)$ од јачината D и времето на корелација γ на генерираниот шум $\eta_1(t)$



Слика 38 Зависноста на средната квадратна грешка на испратените и примените сигнали $c_1(t)$ од јачината D и времето на корелација γ на двата генерирани шумови $\eta_1(t)$ и $\eta_2(t)$

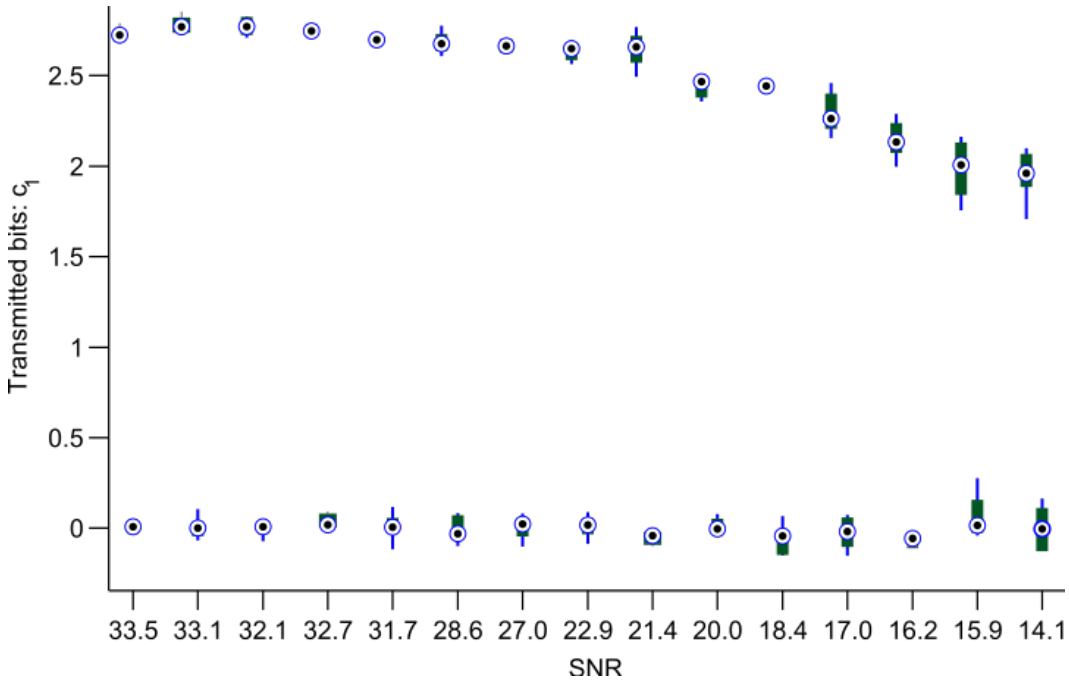
За крај, треба да се напомене дека симулациите извршени во исти вакви услови во кои доаѓа до зголемување на времето на корелација на било кој од шумовите на вредности над времетраењето на еден бит (во случајов 50 секунди), покажуваат крајно нелинеарно и непредвидливо менување на грешката при декрипција. Ова е и очекувано, затоа што динамичката Баесова инференција кај приемникот нема како да се справи со шум чие време на корелација е подолго од траењето на праќањето и декрипцијата на секој бит, и во таков случај нејзината успешност е целосно препуштена на случајноста.

6. МОЌНОСТ НА ПРАЌАЊЕ НА ПОДАТОЦИТЕ ПРИ КОМУНИКАЦИЈА СО ПРОТОКОЛОТ СО ФУНКЦИИ НА СПРЕГА И ДИНАМИЧКА БАЕСОВА ИНФЕРЕНЦИЈА

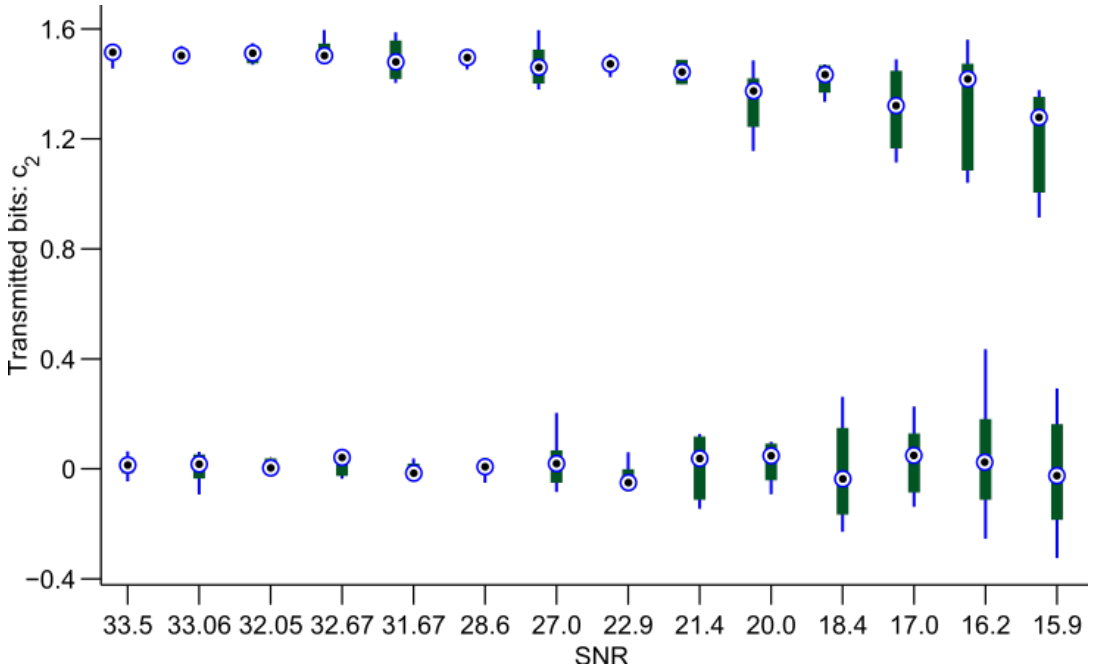
6.1. Анализа на отпорноста на комуникацискиот протокол на бел Гаусов шум

Главната цел на извршениот експеримент е тестирање на робустноста и ефикасноста на протоколот за комуникација во присуство на шум, и со тоа да се испита неговата практична применливост. Затоа при експериментот, додека се одвива комуникацијата (се генерираат случајни бинарни секвенци од 0 и 1 за $s_1(t)$ и $s_2(t)$), нивото на шум кој се генерира и додава во системот систематски се зголемува, и истовремено се набљудуваат неговите ефекти преку следење на односот сигнал - шум (анг. signal to noise ratio - SNR).

На Слика 39 и Слика 40 се прикажани девијациите на бинарните вредности на 0 и 1 за декриптираниот сигнал $s_1(t)$ (означен уште како $c_1(t)$, како параметар на заклучениот модел), и за декриптираниот сигнал $s_2(t)$ (означен уште како $c_2(t)$, како параметар на заклучениот модел) како функции од односот сигнал - шум. Така, за секоја испитана точка на SNR (чија вредност е добиена со донесување на шумот на соодветна вредност), c_1 и c_2 се цртаат во т.н. boxplots, кои ги прикажуваат средната вредност и дистрибуцијата на параметрите, за сите вредности на "0" и "1". Притоа, за сигналот $s_1(t)$ и параметарот c_1, бинарната вредност за "1" е претставена со $c_1 = 2.7$, а за сигналот $s_2(t)$ и параметарот c_2, бинарната вредност за "1" е претставена со $c_2 = 1.5$.



Слика 39 Девијација на декриптираниот сигнал $s_1(t)$ од иницијалните бинарни состојби под дејство на шум, како функција од односот сигнал - шум (SNR), претставен со boxplot



Слика 40 Девијација на декриптираниот сигнал $s_2(t)$ од иницијалните бинарни состојби под дејство на шум, како функција од односот сигнал - шум (SNR), претставен со boxplot

За големи вредности на SNR (што значи слаб шум), дистрибуциите на параметрите се компресирани околу нивната средна вредност, без разлика дали станува збор за 0 или 1. Од друга страна, за мали вредности на SNR (што значи силен шум), дистрибуциите стануваат многу пошироки, што значи дека заклучената вредност на параметрите е многу понеизвесна. Доколку дистрибуциите на 0 и на 1 се доближат доволно близу една до друга или почнат да се преклопуваат, тоа значи дека нивната вредност веќе не може апсолутно да се разликува, т.е. не може со сигурност да се знае кој симбол бил испратен - за таа ситуација, уште се вели дека стапката на грешка во битовите (анг. bit error rate - BER) веќе не е нула и станува позитивна. Како што може да се види од приложените графици за анализа на заклучените вредности на параметрите, во сите испитани случаи за кои е нацртан boxplot не доаѓа до преклопување на дистрибуциите и BER има нулева вредност.

Процесот на енкрипција и декрипција при постепено зголемување на шумот се повторува сé до достигнување на SNR = 15 dB за двата параметри c_1 и c_2. За помали вредности на односот сигнал - шум (т.е. за посилен шум), експериментот веќе станува неостварлив заради физичките ограничувања и несовршености, предизвикани меѓу другото и од 12-битната резолуција на аналогно - дигиталниот и дигитално - аналогниот конвертор. Треба да се напомене дека претходни чисто нумерички симулации на протоколот за безбедна комуникација го поставија прагот на нулев BER на шум одреден со SNR = 4 dB (Stankovski, McClintock, & Stefanovska, 2014), што значи дека практичната имплементација на протоколот го крева овој праг на послаби но реални SNR ≈ 15 dB.

Со енкрипцијата/декрипцијата на само првиот параметар c_1, ефективна комуникација практично се остварува сé до SNR = 14.1 dB, што е релативно добра вредност за толерантност кон шум, пред сé имајќи предвид дека стандардниот праг пред прекин на комуникација е околу 15 dB за безжична комуникација, и околу 40 dB за комуникација преку кабел (Alvarez & Li, 2006).

Понатаму, со цел да се одреди ефективноста на протоколот со функции на спрега, тој е спореден со претходно добро познат комуникациски протокол базиран на комплетна синхронизација на хаотични динамички системи, наречен протокол со маскирање на сигналот (анг. signal masking protocol) (Cuomo & Oppenheim, 1993). Овој протокол е еден од најчесто користените во класата на протоколи за безбедна комуникација со хаотични системи, па затоа оваа споредба е релевантна за сите протоколи во таа класа. Бидејќи пристапот даден во овој труд исто така користи комплетна синхронизација со функции на спрега за пренос на сигналите, оваа споредба тестира и како комуникацијата со функциите на спрега функционира во услови на околина со шум и интерференција без користење на динамичка Баесова инференција. Со други зборови, оваа споредба ги демонстрира придобивките од аспект на робустност кон шум од користење на Баесовиот метод за декрипција на податоците, што е главната разлика помеѓу протоколот изложен во овој

труд и останатите протоколи за безбедна комуникација со синхронизација на хаотични системи.

Сепак, при ваквата компарација не смее да се пропушти и да се напомене дека протоколот со маскирање на сигналот има понизок степен на комплексност бидејќи се состои само од целосна синхронизација, а не и од Баесова инференција за декрипција на сигналот и отстранување на шумот. Ваквата комплексност на методот со функции на спрега имплицира и неопходна потреба од повисока пресметувачка моќ и неизбежна појава на соодветни помали брзини на функционирање во споредба со останатите методи за безбедна комуникација.

Со цел да се постигне значајна споредба, истиот број на битови со случајна вредност се емитува од испраќачот во истата временска рамка, со користење на идентичното хардверско поставување на експериментот, и со идентично систематско приложување на истите нивоа на шум врз емитуваните сигнали. Резултатите укажуваат дека при користење на протоколот со маскирање на сигналите, ненулеви вредности за BER почнуваат да се јавуваат за околу SNR = 20 dB, што е значително помало ниво на шум кој овој протокол може да го толерира во споредба со вредностите како што се SNR = 14.1 dB и SNR = 15 dB, кои беа добиени со протоколот со функции на спрега и динамичка Баесова инференција.

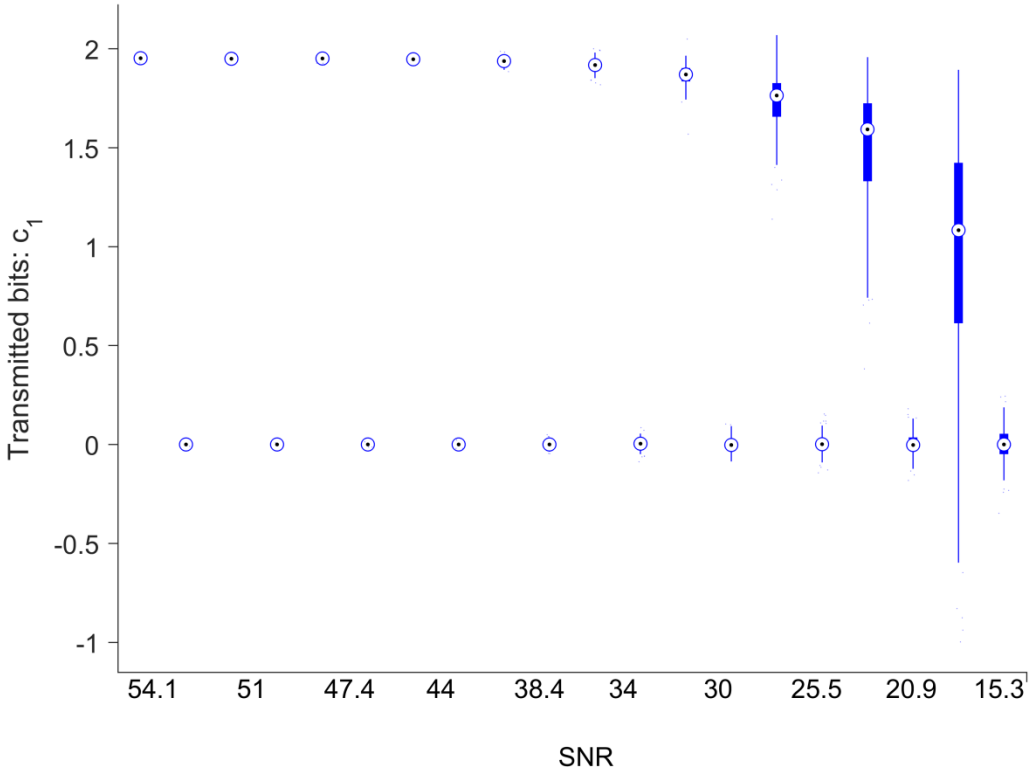
6.2. Анализа на отпорноста на комуникацискиот протокол на нискофреквентен Ornstein-Uhlenbeck шум

Извршена е и анализа на влијанието на нискофреквентниот Ornstein-Uhlenbeck шум врз квалитетот на комуникацијата која се одвива со помош на изложениот протокол. Притоа, може да се забележат резултати кои се очекувани со оглед на заклучоците извлечени во претходната глава.

Имено, од Слика 37 и Слика 38 стана евидентно дека средната квадратна грешка при декрипцијата расте со порастот на времето на корелација на случајниот процес (т.е. со "оддалечувањето" на генерираниот шум од нормалната Гаусова распределба). Затоа, не треба да изненади фактот дека границите на толеранција на протоколот кон шумот кој е генериран од случаен Ornstein-Uhlenbeck процес се намалени.

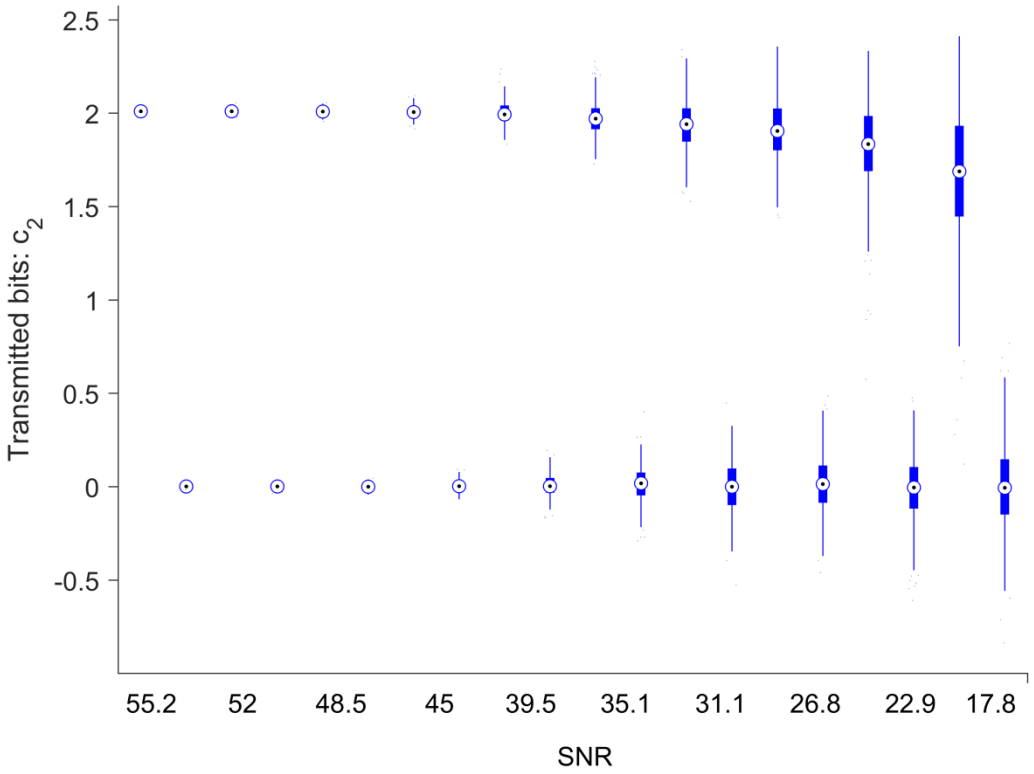
На Слика 41 е дадена девијацијата на бинарните вредности на декриптираниот сигнал $s_1(t)$ за различни вредности на односот сигнал-шум. Повторно, прикажани се средните вредности и девијациите на секој од декриптираните битови за вредност 0 и за вредност 1. Од графикот може да се забележи дека за ниски вредности на шумот (високи

вредности на односот сигнал-шум), границата помеѓу вредностите на битовите е јасна и утврдена. До појава на претходно споменатата bit error rate доаѓа кога SNR достигнува вредност од приближно 20dB до 25dB. Овој праг на толеранција на шумот е понизок од прагот од SNR = 15dB установен во ситуацијата на бел Гаусов шум, што значи дека присуството на интерференција која по природа не е Гаусова ја намалува отпорноста на протоколот кон шум, но сеуште ја одржува во граници кои се прифатливи и споредливи со толеранцијата на други комуникациски протоколи кои се почесто користени во реални и во индустриски услови (Alvarez & Li, 2006).



Слика 41 Девијација на декриптираниот сигнал $s_1(t)$ од иницијалните бинарни состојби под дејство на Ornstein_Uhlenbeck шум, како функција од односот сигнал - шум (SNR), претставен со boxplot

На Слика 42 е дадена девијацијата на бинарните вредности на декриптираниот сигнал $s_2(t)$ за различни вредности на односот сигнал-шум. Резултатите се слични како и претходно; од графикот може да се забележи дека до преклопување на девијациите од декриптираните вредности на сигналот доаѓа кога SNR достигнува вредност од приближно 23dB, што повторно претставува праг на толеранција кој е понизок од прагот од SNR = 15dB установен во ситуацијата на бел Гаусов шум.



Слика 42 Девијација на декриптираниот сигнал $s_2(t)$ од иницијалните бинарни состојби под дејство на Ornstein_Uhlenbeck шум, како функција од односот сигнал - шум (SNR), претставен со boxplot

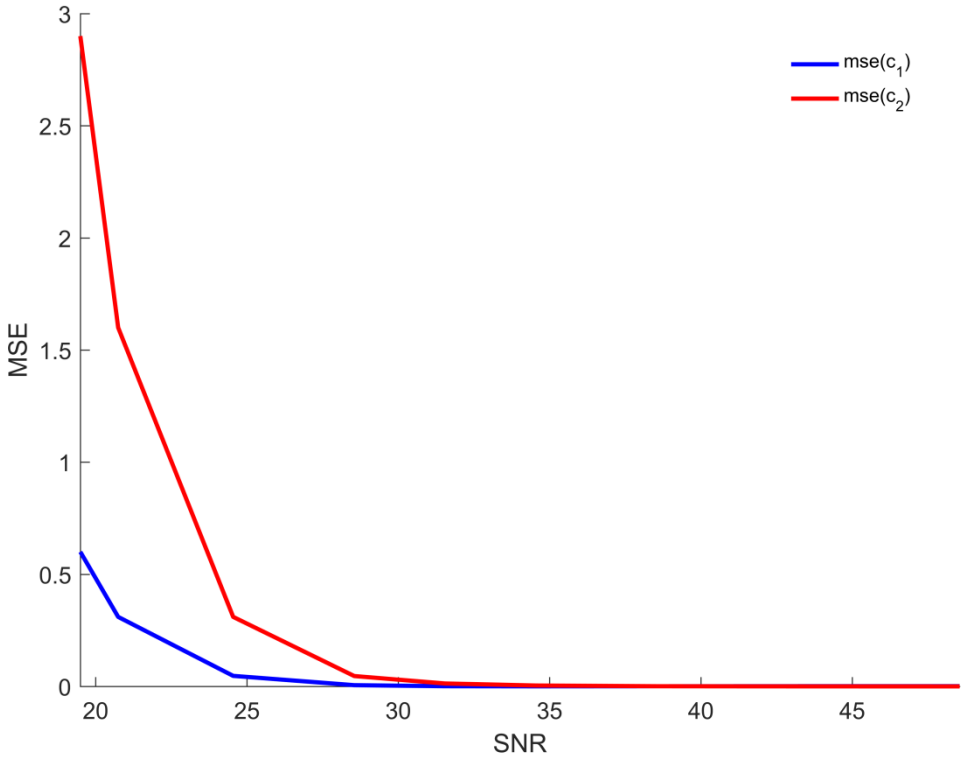
Од приложеното во овој дел може да се сумира дека динамичката Баесова инференција како механизам, поради својата стохастичка природа, е повеќе способна да се справува со шум кој е Гаусов, односно кој има пократко време на корелација (што е потврдено симулациски, но и практично и експериментално).

Сепак, резултатите покажуваат дека таа прикажува сосем задоволително поведение и во услови на појава на нискофреквентен шум, кој овде е симулиран со помош на случаен Ornstein-Uhlenbeck процес, а е честа појава во реалноста, особено карактеристичен кај комуникациските системи во индустриски услови.

6.3. Анализа на резултатите од аспект на моќноста на емитување на податоците при комуникација

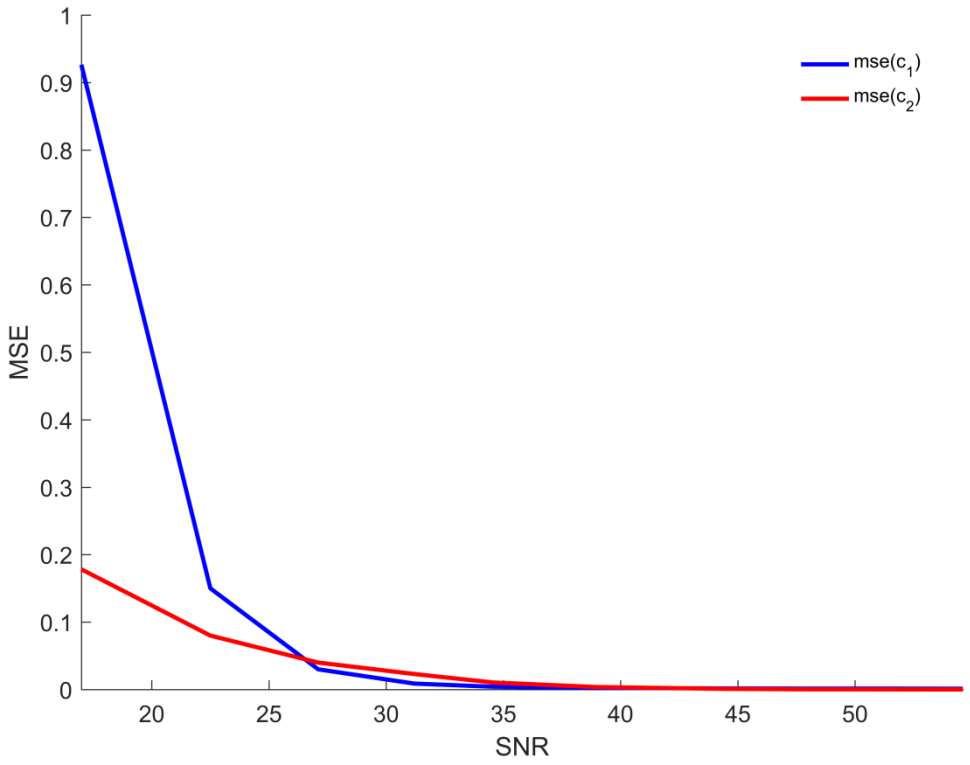
Влијанието на шумот во комуникацискиот канал од вмрежениот систем каде се користи протоколот врз прецизноста и точноста на динамичката Баесова инференција, може да се покаже и со помош на графиците дадени во продолжение.

Најпрво, на Слика 43 е дадена зависноста помеѓу средната квадратна грешка помеѓу енкриптираната и декриптираната вредност на сигналите s_1 (со сина боја) и s_2 (со црвена боја), т.е. на параметрите c_1 и c_2, и нивото на односот сигнал-шум во комуникацискиот канал, при влијание на интерференции предизвикани од бел Гаусов шум. Очекувано, со зголемување на квалитетот на овој однос, односно со намалување на интензитетот на шумот, средната квадратна грешка значително се намалува.



Слика 43 Зависност на средната квадратна грешка (mse) при декрипцијата на параметрите c_1 (сина боја) и c_2 (црвена боја), од нивото на односот сигнал-шум во комуникацискиот канал во кој има пречки предизвикани од бел Гаусов шум

На Слика 44, пак, дадена е зависноста помеѓу средната квадратна грешка помеѓу енкриптираната и декриптираната вредност на сигналите s_1 (со сина боја) и s_2 (со црвена боја), т.е. на параметрите c_1 и c_2, и нивото на односот сигнал-шум во комуникацискиот канал, при влијание на интерференции предизвикани од случаен Ornstein-Uhlenbeck процес.



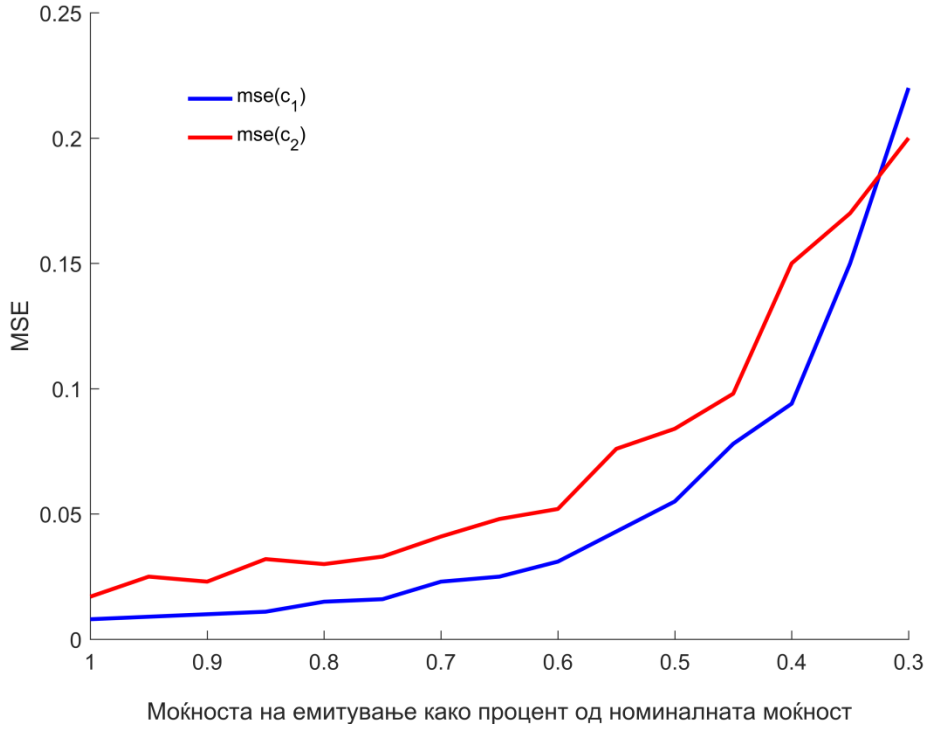
Слика 44 Зависност на средната квадратна грешка (mse) при декрипцијата на параметрите c_1 (сина боја) и c_2 (црвена боја), од нивото на односот сигнал-шум во комуникацискиот канал во кој има пречки предизвикани од нискофреквентен Ornstein-Uhlenbeck шум

Со оглед на ќешто досега беше изложено во врска со отпорноста на шум на презентираниот протокол за безбедна комуникација, едно интересно прашање кое се наметнува е можноста за искористување на оваа отпорност за заштеда на енергија. Имено, во случај на присуство на шум со одредена јачина во комуникацискиот канал, намалувањето на моќноста на емитуваните сигнали ќе придонесе за намалување и на односот сигнал-шум. Сепак, знаејќи ги границите на толеранција на вредностите на SNR за кои протоколот сеуште функционира коректно, би можела да биде одбрана таква отстапка која сеуште ќе го остави односот во некоја "безбедна" зона. На овој начин, гледано на подолг рок, може да се оствари заштеда на енергија при испраќањето на податоците во вмреженият систем на автоматско управување кој го користи овој

комуникациски протокол. Се разбира, притоа не треба да се занемари и фактот дека намалувањето на моќноста на емитувањето на сигналите може и негативно да влијае на точноста и прецизноста на динамичката Баесова инференција.

На Слика 45 се прикажани резултатите од ваквото испитување. Во системот влијае нискофреквентен Ornstein-Uhlenbeck шум со интензитет $D = 100$ и со време на корелација $\gamma = 10$, што во нормални услови претставува ниво на сигнал-шум од $\mathrm{SNR} \approx 31\mathrm{dB}$, а протоколот за безбедна комуникација ги користи функциите на спрега дадени со (11) и (12).

Со намалување на моќноста на емитување на сигналите $x_1(t)$ и $y_2(t)$, а при исти карактеристики на шумот, нивото на сигнал-шум разбирливо опаѓа. Ова резултира во менување на прецизноста и точноста на декрипцијата со динамичката Баесова инференција на приемната страна.



Слика 45 Зависност на средната квадратна грешка (mse) при декрипцијата на параметрите c_1 (сина боја) и c_2 (црвена боја), од нивото на моќноста на емитување на сигналите x_1 и y_2 во комуникацискиот канал во кој има пречки предизвикани од нискофреквентен Ornstein-Uhlenbeck шум

Точноста на алгоритмот повторно најсоодветно се одликува преку средната квадратна грешка, која повторно се користи како метрика за споредба. На графикот на Слика 45, на апсцисата е прикажано намалувањето на моќноста на емитувањето на податоците како однос помеѓу реалната и номиналната моќност. Работата на протоколот останува прифатлива за вредности на средната квадратна грешка помали од приближно 0.075, кога девијациите на вредностите на "1" и "0" на битовите c_1 и c_2 почнуваат да се преклопуваат. Според графикот, таа вредност на грешката одговара на вредност на моќноста на емитување од приближно една половина од номиналната. Ова значи дека, за споменатите услови на никскофреквентен шум кој ги предизвикува интерференциите во комуникацискиот канал, можно е да се заштеди и до 50% од енергијата потребна за испраќање на сигналите. Сепак, мора да се има предвид и дека менувањето на моќноста на емитување на податоците, освен што го слабее сигналот, истовремено и влијае на точноста на декрипцијата кај динамичката Баесова инференција преку функциите на спрега, што всушност значи дека достигнувањето на одредено ниво на односот сигнал-шум во системот, не значи и дека средната квадратна грешка на вредностите на битовите (а со тоа и успешноста и прецизноста на декрипцијата кај приемникот) ќе биде еднаква со средната квадратна грешка за истото ниво на односот сигнал-шум, во услови на истиот шум, и при емитување со номинална моќност. Од таа причина, при користење на намалена моќност на испраќање со цел на заштеда на енергија, веројатно е пожелно одредување на нејзина поконзервативна вредност која ќе се осигура дека нема да дојде до грешки во декрипцијата на приемната страна.

Оваа можност може да се искористи така што ваквиот пристап за нагодување на моќноста на емитување на сигналите би можел да се подобри и/или усовршии на неколку можни начини, меѓу кои се и динамичко нагодување на моќноста врз основа на карактеристиките на шумот во комуникацискиот канал, или пак врз основа на инкрементот во информацијата на податоците кои треба да се испратат, што всушност претставува квалитативна мерка за промената во нивната "важност" (Wu, Li, Quevedo, Lau, & Shi, 2015). Методи за динамичко одредување на моќноста на емитување на податоците кај вмрежените системи на автоматско управување можат да се најдат во литературата (Gatsis & Ribeiro, 2014), но никој од нив не се однесува (и не е тестиран) на конкретниот комуникациски протокол кој е изложен овде. Според тоа, ова останува интересно и отворено прашање за понатамошно истражување.

Конечно, на овој комуникациски протокол како недостаток би можела да му се припише комплексноста а оттаму и зголемената побарувачката за пресметувачка моќ, па можноста за намалување на моќноста на испраќање на сигналите резултира во добредојдена заштеда на енергија при работата, што придонесува за подобрување на степенот на енергетска ефикасност на протоколот и на целокупниот систем во чии рамки тој функционира.

6.4. Завршна анализа на резултатите

Како заклучок и целокупно сумирање на резултатите од анализата на претходните две глави, може да се каже дека предложениот протокол за безбедна комуникација имплементира уникатна енкрипција на податоците кои треба да се пренесат, преку нивно комплексно нелинеарно мешање овозможено од механизмите на интеракција дефинирани со функциите на спрега кај хаотичните осцилатори. Клучот кој се генерира всушност се зема од неограничено множество на негови можни форми и вредности, што го прави овој алгоритам исклучително безбеден.

Понатаму, протоколот е тестиран и практично и испитана е неговата робустност во услови на шум. Шумот, како што беше изложено претходно, е честа појава со сериозни негативни ефекти во работата и комуникацијата во реални индустриски услови, при што секој комуникациски пристап кој нуди робустност и ефикасно справување со последиците од шумот е добредојден. Во случајов, протоколот покажа високо ниво на толеранција на шум, подобро или во најмала рака на еднакво ниво со други слични протоколи кои користат сличен концепт на синхронизација на хаотични системи, но со впечатливо отсуство на Баесовиот механизам за декрипција на податоците. Токму користењето на динамичка Баесова инференција на приемната страна од комуникациската врска се покажува како клучно за одвојување на ефектите на околниот бел шум од детерминистичките информации во системот, и тоа за нивоа на шум повисоки од праговите на толеранција на слични протоколи, како што е signal masking протоколот.

Конечно, сето ова е реализирано на едноставен и комерцијално лесно достапен хардвер и софтвер, со цел да се покаже дека протоколот и покрај својата моќност е доволно едноставен за да може да се имплементира на опрема од рангот на миникомпјутери, вградливи системи, и/или паметни телефони. Сепак, токму поради едноставноста на експериментот, неизбежни и очекувани се одредени ограничувања кои можат да се надминат со користење на хардвер и софтвер со посилни перформанси и повисока цена. Такви на пример би биле компјутери со повисока подобра процесирачка моќ (GPU или FPGA), кои би овозможиле меѓу другото и конверзија со поголема резолуција и поголема прецизност од 12-битната верзија која е достапна на искористената верзија од Raspberry PI.

Понатаму, целосната и комплетна синхронизација, каква што користи овој комуникациски протокол, не е едноставна за одржување во реални услови, каде испраќачот и приемникот на податоците се физички прилично одвоени. Сепак, и за таков случај постојат веќе познати и развиени методи за одржување на синхронизација на

податоци во комуникациски мрежи, како што на пример се дадени од страна на (Worsley & Edem, 1997) и (Halim & Stossel, 2001).

Инаку теоретски, процесниот шум (анг. process noise) влијае како динамичка пертурбација на динамичките состојби на системот, но во експериментите се забележува и одредено ниво на шум при мерењето (анг. measurement noise), што го прави заклучувањето на приемната страна помалку прецизно. Идните варијанти на овој протокол би требало во делот на динамичка Баесова инференција да содржат и дополнителни пресметки и процедури за одвојување на ефектите и од овој шум.

7. ЗАКЛУЧОК

Еволуцијата на системите на автоматско управување во вмрежени системи подразбира и појава на многу претходно непостоечки ранливости и проблеми во нивното функционирање. Дигиталната комуникација како фактор сега овозможува брз и ефикасен пренос на големи количини на податоци помеѓу компонентите на системот, што придонесува за подобрување на неговата ефикасност, но истовремено и претставува слаба точка ранлива на влијанијата од интерференциите предизвикани од околниот шум, и на намерни малициозни напади чија цел е пресретнување или корупција на податоците и информациите во системот.

Ова може лесно да се заклучи од прегледот на историскиот развој на вмрежените системи на автоматско управување како гранка на автоматиката која во денешниот свет на брзи дигитални комуникации има исклучително значење. Во оваа дисертација (а пред ќе во втората глава) детално ги изложуваме главните проблеми кои се јавуваат кај вмрежените системи на автоматско управување, но и големиот број на различни постоечки пристапи за нивно решавање или за неутрализирање на нивните ефекти. Покажавме дека главните недостатоци, како што се доцнењата, губењата на податочни пакети, делегирањето на пристапот кон мрежата и негативните ефекти од квантизацијата се проблеми кои науката ги сфаќа сериозно и е способна да ги решава.

Голем дел од овие недостатоци се предизвикани од влијанијата на шумот и интерференцијата во комуникациските системи, особено во индустриските услови кои изобилуваат со извори на шум од најразлична природа, а истовремено бараат неопходно присуство на вмрежените системи за подигнување на ефикасноста и флексибилноста на управуваните процеси и постројки. Во оваа дисертација директно ги прикажавме ефектите од шумот типичен за индустриските средини врз еден реално имплементиран индустриски вмрежен систем за автоматско управување. Практичниот експеримент опишан во третата глава покажа дека иако постоечката индустриска управувачка опрема е дизајнирана да се справува со ваквите интерференции, сепак комуникациската мрежа останува главна ранливост на целокупниот систем во вакви услови бидејќи присуството на макар краток (иако по магнитуда интензивен) шум предизвикува непредвидливо доцнење на податочните пакети или пак нивно губење и/или изобличување. Истовремено, дополнителна придобивка од извршениот експеримент е и одредувањето на прагот на толеранција на шум за конкретната класа на индустриски системи, односно на рамките во кои системот може коректно да функционира кога е во прашање интензитетот на електростатичкиот шум.

Дополнителен проблем кај денешните вмрежени системи на автоматско управување претставува и нивната ранливост кон намерни и малициозни напади

предизвикани од човекот. Видот на постројки и процеси кои овие системи денес ги управуваат подразбира дека значењето на податоците кои минуваат низ комуникациските мрежи имаат исклучителна важност како никогаш досега, и дека нивното намерно менување и компромитирање или неавторизирано пресретнување и надгледување може да има катастрофални последици. Во оваа дисертација, и тоа конкретно во четвртата глава, дадовме преглед на голем број од најмодерните и најчесто користени методи за осигурување на безбедноста на податоците во рамките на SCADA системите како најкарактеристичен репрезент на вмрежените системи на автоматско управување.

Главниот придонес на оваа докторска дисертација е зголемувањето на степенот на безбедност на индустриските комуникациски протоколи и подигнувањето на нивото на нивната отпорност кон интерференцијата предизвикана од околниот шум или од човечки фактори. Како што беше презентирано во петтата и шестата глава, ова е постигнато со развој на алгоритам кој користи функции на спрега помеѓу два динамички системи за енкрипција, и динамичка Баесова инференција за декрипција на податоците. Ваквиот пристап резултира во комуникација која е криптографски безбедна бидејќи врските помеѓу вистинските енкриптирани сигнали и испратените (и евентуално пресретнати) сигнали е добро сокриена во хаотичните траектории и односи помеѓу двата спрегнати динамички системи. Истовремено, ваквата комуникација е и отпорна на електромагнетен шум од различна природа - и бел и нискофреквентен, како што покажавме теоретски, симулациски, и практично. Ова е очекувано со оглед на тоа што самата динамичка Баесова инференција која се користи како механизам за декрипција на податоците на приемната страна е инхерентно стохастичка. Отпорноста на шумот подразбира дека комуникацијата реализирана со предложениот протокол е способна да функционира во индустриски услови, но и дека се одликува со намалени моќности на емитување а според тоа и со одреден степен на енергетска ефикасност, особено надоместувајќи за зголемената побарувачка за пресметувачка моќ која произлегува од пристапот.

Резултатите од истражувањето можат да се применат за подобрување на безбедноста на комуникациите и интегритетот на податоците кај вмрежените системи на автоматско управување во индустриски услови. Комуникациски протоколи за индустриски ВСАУ кои се грижат и за безбедноста веќе постојат, но овој конкретен протокол се одликува со висок степен на сигурност на енкриптираните податоци која произлегува од неброената бесконечност на можни комбинации при избор на функциите на спрега на испраќачката страна, и со инхерентна отпорност на шум и интерференции која произлегува од стохастичката природа на Баесовата инференција која се користи на приемната страна.

7.1. Можности за понатамошна работа и истражување

Развојот и тестирањето на комуникацискиот протокол опишан во оваа дисертација остава и неколку доста интересни прашања и можности за понатамошна работа и истражување.

Пред ќе, останува да се испита отворено прашање во врска со комплексноста на протоколот. Тој покажува подобра безбедност и толеранција кон шум во споредба со слични протоколи (signal masking протоколот, на пример), но се одликува и со додатно ниво на сложеност, предизвикана од механизмот за динамичка Баесова инференција за декрипција на примените податоци. Протоколот беше имплементиран физички, на комерцијално достапни уреди без висока сметачка моќ, и очигледно е дека има практична вредност, но останува ова понатаму и подетално да се испита за различни видови на (пософистицирана) опрема.

Интересно би било да се проучи и перформансот на овој протокол во услови на шум и интерференции од различна природа. Дисертацијата покажа дека успешно функционира во околини на бел Гаусов шум и на нискофреквентен (во конкретниот случај Ornstein-Uhlenbeck) шум, но останува да се испита и како би се справил во ситуации каде пречките се предизвикани од шум кој не е Гаусов по природа (примери за процеси кои генерираат ваков шум беа дадени во делот 5.5 и во соодветните референци споменати таму).

Во дисертацијата беше прикажана и експериментална верификација на предложениот протокол со помош на едноставна и комерцијално достапна опрема. Ваквата практична реализација на протоколот претставува само еден чекор при неговиот развој, но придонесува за премостување на јазот помеѓу теоретското истражување на ваквата комуникација и нејзината целосна реална имплементација во иднина. Еден од следните предизвици по целосната реализација е остварување на детална и прецизна споредба на развиениот протокол со постоечки и утврдени протоколи кои се користат за комуникација во индустриски услови (и генерално во околини со изразито присуство на шум и интерференција), и тоа не само од аспект на отпорноста кон пречките туку и од аспект на сигурноста и безбедноста на информациите од малициозни акции предизвикани од човечки фактор.

Конечно, зголемената отпорност на шум на протоколот за безбедна комуникација во одредени услови би можела да значи и отворање на можност за намалување на моќноста на емитување на податоците. Во таква ситуација, очекувано би се намалила вредноста на односот сигнал-шум во околината, но теоретски протоколот би продолжил

успешно да функционира ѐ додека овој однос остане во границите во кои не се јавува стапка на грешка во битовите (bit error rate). Сето ова би имало корисен долготраен ефект врз потрошувачката на моќност и со тоа и врз енергетската ефикасност на целокупниот вмрежен систем на управување во кој е имплементиран самиот протокол.

8. ЛИТЕРАТУРА

Al-Hammouri, A., Branicky, M., Liberatore, V., & Phillips, S. (2006). Decentralized and Dynamic Bandwidth Allocation in Networked Control Systems. *Proceedings of 20th International Parallel Distrib. Process. Symp*, (pp. 8).

Almutairi, N., Chow, M., & Tipsuwan, Y. (2001). Network-based Controlled DC Motor with Fuzzy Compensation. *The 27th IECON*, (pp. 1844-1849). Denver, Colorado.

Alvarez, G., & Li, S. (2006). Some Basic Cryptographic Requirements for Chaos-based Cryptosystems. *International Journal on Bifurcation and Chaos* , 2129-2151.

American Gas Association. (2005). *Cryptographic Protection of SCADA Communications.* Washington, DC.

Amin, S., Cardenas, A., & Sastry, S. (2009). Safe and Secure Networked Control Systems under Denial-of-service Attacks. *Hybrid Systems: Computation and Control* , 31-45.

Amin, S., Litrico, X., Sastry, S., & Bayen, A. (2010). Stealthy Deception Attacks on Water SCADA Systems. *Hybrid Systems: Computation and Control*, (pp. 161-170). Stockholm.

Anderson, R. (2001). *Security Engineering - A Guide to Building Dependable Distributed Systems.* Wiley.

Azimi-Sadjadi, B. (2003). Stability of Networked Control Systems in the Presence of Packet Losses. *Proceedings of 42nd IEEE Conferece on Desicion and Control, 2003*, (pp. 676-681).

Bak, P., Tang, C., & Wiesenfeld, K. (1987). Self-organized Criticality: An Explanation of 1/f Noise. *Physics Review Letters* , 381-384.

BCIT Industrial Security Database. (н.д.). Повратено од http://www.bcit.ca/appliedresearch/security/services.shtml

Bennett, C. H. (2000). Quantum Information and Computation. *Nature* , 247-255.

Beresford, D. (2001). *The Sauce of Utter Pwnage.* Повратено од http://thesauceofutterbwnage.blogspot.com/

Besada-Portas, E., Lopez-Orozco, J. A., Besada, J., & de la Cruz, J. M. (2011). Multisensor Fusion for Linear Control Systems with Asynchronious out-of-Sequence and Erroneous Data. *Automatica* , 1399-1408.

Bian, X. L., & Xia, Y. Q. (2014). Energy Efficient Data Fusion Over Wireless Channels with Power Control. *IET Signal Processing* .

Bian, X. L., Xia, Y. Q., Deng, Z. H., & Fu, M. Y. (2014). One-channel Networked Data Fusion with Communication Constraints. *Journal of the Franklin Institute* , 156-173.

Bianchi, C., & Meloni, A. (2007). Natural and Man-made Terrestrial Electromagnetic Noise: An Outlook. *Annals of Geophysics* .

Bibbona, E., Panfilo, G., & Tavella, P. (2008). The Ornstein-Uhlenbeck Process as a Model of a Low-pass Filtered White Noise. *Metrologia, no. 45* , 117-126.

Byres, E., & Nguyen, T. (2000). Using OPC to Integrate Control Systems from Competing Vendors. *Canadian Pulp and Paper Association Technical Conference.*

Byres, E., Carter, J., Elramly, A., & Hoffman, D. (2002). Worlds in Collision: Ethernet on the Plant Floor. *ISA Emerging Technologies Conference.* Chicago, IL: Instrumentation Systems and Automation Society.

Byres, E., Hoffman, D., & Kube, N. (2006). On Shaky Ground - A Study of Security Vulnerabilities in Control. *5th American Nuclear Society International Topical Meeting on Nuclear Plant Implementation, Controls, and HMI Technology.*

Castanon, D., & Tenekzis, D. (1985). Distributed Estimation Algorithm for Nonlinear Systems. *IEEE Transactions on Automatic Control* , 418-425.

Chan, H., & Ozguner, U. (1995). Closed-loop Control of Systems Over a Communication Network with Queues. *Int. J. Control* , 493-510.

Chen, B., Zhang, W. A., & Yu, L. (2014). Distributed Fusion Estimation with Missing Measurements, Random Transmission Delays, and Packet Dropouts. *IEEE Transactions on Automatic Control* , 1961-1967.

Chou, H. G., Chuang, C. F., Wang, W. J., & Lin, J. C. (2013). A Fuzzy Model Based Chaotic Synchronization and its Implementation on a Secure Communication System. *IEEE Transactions on Information Forensics and Security* , 2177-2185.

Creery, A., & Byres, E. (2005). Industrial Cybersecurity for Power System and SCADA Networks. *Proc. Ind. Appl. Soc. 52nd Petroleum Chem. Ind. Conf.*, (pp. 303-309).

Crutchfield, J. P. (2012). Between Order and Chaos. *Natural Physics, vol. 8, no. 1* , 17-24.

Cuomo, K. M., & Oppenheim, A. V. (1993). Circuit Implementation of Synchronized Chaos with Application to Communications. *Physics Review Letters* , 65-68.

Cuomo, K. M., Oppenheim, A. V., & Strogatz, S. H. (1993). Synchronization of Lorenz-based Chaotic Circuits with Applications to Communications. *IEEE Transactions on Circuits and Systems II* , 626-633.

Dan, G., & Sandberg, H. (2010). Stealth Attacks and Protection Schemes for State Estimators in Power Systems. *IEEE International Conference on Smart Grid Communication*, (pp. 214-219). Gaithersburg, MD.

Davis, D., & Swick, R. (1990). Network Security via Private Key Certificates. *Operating Systems Review* , 64-67.

Decotignie, J. D. (1996). *Local Area Networks: Fieldbus, the Industrial Electronic Handbook.* CRC Press.

DeMarco, C. L., Sariashkar, J. V., & Alvarado, F. (1996). The Potential for Malicious Control in a Competitive Power Systems Environment. *IEEE International Conference on Control Applications*, (pp. 462-467). Dearborn, MI.

Digital Bond. (н.д.). *Securing the Critical Infrastructure.* Повратено од http://www.digitalbond.com/

El Sawy, H., Sultan-Salem, A., Alouini, M. S., & Win, M. Z. (2017). Modeling and Analysis of Cellular Networks Using Stochastic Geometry: A Tutorial. *IEEE Communications Survey of Tutorials* , 167-203.

Elia, N., & Mitter, S. K. (2001). Stabilization of Linear Systems with Limited Information. *IEEE Transactions on Automatic Control* , 1384-1400.

Eliades, D. G., & Polycarpou, M. M. (2010). A Fault Diagnosis and Security Framework for Water Systems. *IEEE Transactions on Control Systems Technology* , 1254–1265.

Falliere, N., Murchuand, L., & Chien, E. (2010). *W32.Stuxnet Dossier.* Symantec Security Response.

Fang, H., Yang, F., & Zheng, Y. (2006). Fuzzy Modelling and Fault Detection for Networked Control Systems. *6th IFAC Symposium on Fault Detection, Supervision, and Safety of Technical Processes*, (pp. 1153-1158).

Fang, H., Zhang, H., Fang, Y. W., & Yang, F. (2006). Quasi T-S Fuzzy Models and Stable Controllers for Networked Control Systems. *6th World Congress on Intelligent Control and Automation*, (pp. 220-223). Dalian.

Fu, M. Y., & Xie, L. H. (2005). The Sector Bound Approach to Quantizied Feedback Control. *IEEE Transactions on Automatic Control* , 1689-1711.

Gatsis, K., & Ribeiro, A. (2014). Optimal Power Management in Wireless Control Systems. *IEEE Transactions on Automatic Control, vol. 59* , 1495-1510.

Goktas, F. (2000). Distributed Control of Systems over Communication Networks. *PhD Dissertation* . University of Pennsylvania.

Goktas, F., Smith, J., & Bajcsy, R. (1996). Mu-synthesis for Distributed Control Systems with Network-induced Delays. *Proceedings on 35th IEEE Conference on Desicion Control*, (pp. 813-814).

Greason, W. (2009). Analysis of Cable Discharge Events. *Electrostatics Joint Conference.*

Grime, S., Durrant-Whyte, H. F., & Ho, P. (1992). Communication in Decentralized Data Fusion Systems. *American Control Conference*, (pp. 3299-3303). Chicago.

Gupta, R. A., & Chow, M.-Y. (2010). Networked Control System: Overview and Research Trends. *IEEE Transactions on Industrial Electronics* , 2527-2535.

Gupta, R., & Chow, M. (2008). Performance Assessment and Compensation for Secure Networked Control Systems. *Proceedings of IECON '08*, (pp. 2929-2934).

Halevi, Y., & Ray, A. (1988). Integrated Communication and Control Systems. *Journal of Dynamic Systems, Measurement and Control* , 367-373.

Halim, C., & Stossel, J. W. (2001). *Патент бр. Remote Data Access and Synchronization, 6,304,881*. USA.

Hamza, F., Tabuada, P., & Diggavi, S. (2011). Secure State Estimation for Dynamical Systems under Active Adversaries. *Allerton Conference on Communications, Control, and Computing.*

Hanggi, P., Mroczkowski, T. J., Moss, F., & McClintock, P. V. (1985). Bistability Driven by Colored Noise: Theory and Experiment. *Physics Review A* , 695-698.

Hansman, S., & Hunt, R. (2004). A Taxonomy of Network and Computer Attacks. *Computers and Security* .

Haroun, M. F., & Gulliver, T. A. (2015). Secret Key Generation Using Chaotic Signals Over Frequency Selective Fading Channels. *IEEE Transactions on Information Forensics and Security* , 1764-1775.

Hayakawa, T., Ishii, H., & Tsumura, K. (2009). Adaptive Quantized Control for Linear Uncertain Discrete-time Systems. *Automatica* , 692-700.

Hayakawa, T., Ishii, H., & Tsumura, K. (2009). Adaptive Quantized Control for Nonlinear Uncertain Systems. *Systems and Control Letters* , 625-632.

Hespanha, J., Haghshtabrizi, P., & Xu, Y. (2007). A Survey of Recent Results in Networked Control Systems. *Proceedings of IEEE* , 138-162.

Hirai, K., & Satoh, Y. (1980). Stability of a System with Variable Time Delay. *IEEE Transactions on Automatic Control* , 552-554.

Hong, S. (1995). Scheduling Algorithm of Data Sampling Times in the Integrated Communication and Control Systems. *IEEE Transactions on Control Systems Technology* , 225-230.

Huang, D., & Nguang, S. K. (2010). Robust Fault Estimator Desgin for Uncertain Networked Control Systems with Random Time Delays: an ILMI Approach. *Information Sciences* , 465-480.

Huang, W., Tichenor, J., & et al, e. (2014). An Ethernet Cable Discharge Event Test and Measurement System. *IEEE International Symposium on Electromagnetic Compatibility*.

Huo, Z., & Fang, H. (2006). Fault Tolerant Control Research for Networked Control Systems under Communication Constraints. *Acta Automatica Sinica* , 659-666.

Huo, Z., & Fang, H. (2005). Robust H-infinity Filter Design for Networked Control Systems with Random Delays. *10th International Conference on Engineering of Complex Computer Systems*, (pp. 333-340). Shanghai.

Iatsenko, D., Bernjak, A., Stankovski, T., Shiogai, Y., Owen-Lynch, P. J., Clarkson, P. B., и др. (2013). Evolution of Cardio-respiratory Interactions with Age. *Phil. Trans. R. Soc. Lond. A.*

Imer, O., Yuksel, S., & Basar, T. (2006). Optimal Control of LTI Systems over Unreliable Communication Links. *Automatica* , 1429-1439.

Instrumentation Systems and Automation Society. (2004). *Security Technologies for Manufacturing and Control Systems.* Research Triangle Park, NC.

Irakiza, D., Karim, M. E., & Phoha, V. V. (2014). A Non-interactive Dual Channel Continuous Traffic Authentication Protocol. *IEEE Transactions on Information Forensics and Security* , 1133-1140.

Ishii, H., & Basar, T. (2005). Remote Control of LTI Systems Over Networks With State Quantization. *Systems and Control Letters* , 15-31.

Kamrani, E., & Mehraban, M. (2006). Modeling Internet Delay Dynamics Using System Identification. *Proceedings of ICIT*, (pp. 716-721).

Kilpatrick, T., Gonzalez, J., Chandia, R. P., & Shenoi, S. (2005). An Architecture for SCADA Network Forensics. Bo M. Olivier, & S. Shenoi, *Advances in Digital Forensics II* (pp. 273-285). New York, NY: Springer.

Kish, L. B. (2006). Totally Secure Classical Communication Utilizing Johnson's Noise and Kirchoff's Law. *Phys. Lett. A.* , 178-182.

Kiss, I. Z., Rusin, C. G., Kori, H., & Hudson, J. L. (2007). Engineering Complex Dynamical Structures: Sequential Patterns and Desynchronization. *Science* , 1886-1889.

Kiss, I. Z., Y., Z., & Hudson, J. L. (2005). Predicting Mutual Entrainment of Oscillators with Experiment-based Phase Models. *Physics Review Letters* , 248-301.

Klinkhieo, S., Kambhampati, C., & Patton, R. (2007). Fault Tolerant Control in NCS Medium Access Constraints. *Proc. IEEE Int. Conf. Netw. Sens. Control*, (pp. 416-423).

Kocarev, L., & Parlitz, U. (1995). General Approach for Chaotic Synchronization with Applications to Communication. *Physics Review Letters* , 5028-5031.

Kralemann, B., Fruhwirth, M., Pikovsky, A. S., Rosenblum, M., Kenner, T., Schaefer, J., и др. (2013). In Vivo Cardiac Phase Response Curve Elucidates Human Respiratory Heart Rate Variability. *Nat. Commun.* , 2418.

Kuypers, M. A., Maillart, T., & Pate-Cornell, E. (2015). *An Empirical Analysis of Cyber Security Incidents at a Large Organization.*

Lehle, B., & Peinke, J. (2017). Analyzing a Stochastic Process Driven by Ornstein-Uhlenbeck Noise. *arXiv[physics.data-an]* , 1702.00032.

Levanjic, Z., & Pikovsky, A. S. (2011). Network Reconstruction from Random Phase Resetting. *Physics Review Letters* , 34-101.

Li, J., & Al-Regib, G. (2007). Rate-constrained Distributed Estimation in Wireless Sensor Networks. *IEEE Transactions on Signal Processing* , 1634-1643.

Li, L., Xia, Y. Q., Qiu, J. Q., & Yang, H. J. (2012). Robust H-infinity Networked Control for Discrete-time Fuzzy Systems with State Quantization. *International Journal of Systems Science* , 2249-2260.

Li, Q., & Mills, D. (2001). Jitter-based Delay-boundary Prediction of Wide-area Networks. *IEEE/ACM Transactions on Networking* , 578-590.

Li, Q., Yi, G., Wang, C., Wu, L., & Ma, C. (2006). LMI-based Stability Analysis of Networked Control Systems with Large Time-varying Delays. *Proceedings of IEEE International Conference on Mechatronics and Automation*, (pp. 713-717).

Li, Z., & Chow, M. (2007). Sampling Rate Scheduling and Digital Filter Co-design of Networked Supervisory Control System. *Proceedings of ISIE*, (pp. 2893-2898).

Liu, B., & Xia, Y. Q. (2011). Fault Detection and Compensation for Linear Systems over Networks with Random Delays and Clock Asynchronism. *IEEE Transactions on Industrial Electronics* , 4396-4406.

Liu, G., Xia, Y., Chen, J., Rees, D., & Hu, W. (2007). Networked Predictive Control of Systems with Random Network Delays in both Forward and Feedback Channels. *IEEE Transactions on Indian Electronics* , 1282-1297.

Liu, Y., Reiter, M. K., & Ning, P. (2009). False Data Injection Attacks Against State Estimation in Electric Power Grids. *AMC Conference on Computer and Communications Security*, (pp. 21-32). Chicago, IL.

Lorenz, E. N. (1963). Deterministic Non-periodic Flow. *J. Atmos. Sci. vol. 20* , 130-141.

Luchinsky, D. G., McClintock, P. V., & Dykman, M. I. (1998). Analogue Studies of Nonlinear Systems. *Rep. Prog. Phys.* , 889-997.

Luck, R., & Ray, A. (1990). An Observer-based Compensator for Distributed Delays. *Automatica* , 903-908.

Luck, R., & Ray, A. (1994). Experimental Verification of a Delay Compensation Algorithm for Integrated Communication and Control Systems. *Int. J. Control* , 1357-1372.

Mahmoud, M. S., & Xia, Y. Q. (2014). *Networked Filtering and Fusion for Wireless Network Sensors.* Chemical Rubber Company Press.

Mandia, K., Prosise, C., & Pepe, M. (2003). *Incident Response and Computer Forensics.* McGraw-Hill/Osborne: Emeryville, CA.

Mao, Z., Jiang, B., & Shi, P. (2009). Protocol and Fault Detection Design for Nonlinear Networked Control Systems. *IEEE Transactions on Circuits and Systems - II: Express Briefs* , 255-259.

Marti, P., Yez, J., Velasco, M., Villa, R., & Fuertes, J. (2004). Managing Quality-of-control in Network-based Control Systems by Controller and Message Scheduling Co-design. *IEEE Transactions on Indian Electronics* , 1159-1167.

McGarry, M., Maier, M., & Reisslein, M. (2004). Ethernet PONs: A Survey of Dynamic Bandwidth Allocation (DBA) Algorithms. *IEEE Communications Magazine* , 8-15.

Mendes, M., Santos, B., & da Costa, J. (2007). Multi-agent Platform for Fault Tolerant Control Systems. *Proc. IEEE Int. Conf. Syst.*, (pp. 1321-1326).

Millerioux, G., Amigo, J. M., & Daafouz, J. (2008). A Connection Between Chaotic and Conventional Cryptography. *IEEE Transactions on Circuits and Systems I: Regular Papers* , 1695-1703.

Mitsubishi. (2013). *MELSEC - FX3GE Programmable Controller.* Tokyo, Japan: Mitsubishi Electric Corporation.

Miyazaki, J., & Kinoshita, S. (2006). Determination of a Coupling Function in Multicoupled Oscillators. *Physics Review Letters* .

Mo, Y., & Sinopoli, B. (2010). Secure Control Against Replay Attacks. *Allerton Conference on Communications, Control, and Computing*, (pp. 911-918). Monticello, IL.

Modbus IDA. (2004). *MODBUS Application Protocol Specification.* North Grafton.

Mohsenian-Rad, A. H., & Leon-Garcia, A. (2011). Distributed Internet-based Load Alerting Attacks Against Smart Power Grids. *IEEE Transactions on Smart Grids* , 667-674.

Montestruque, L., & Antsaklis, P. (2005). Quantization in Model-based Networked Control Systems. *Proceedings of IFAC '05.*

Montestruque, L., & Antsaklis, P. (2004). Stability of Model-based Networked Control Systems with Time-varying Transmission Times. *IEEE Transactions on Automation and Control* , 1562-1572.

Murray, R. (н.д.). *http://www.cds.caltech.edu/~murray/wiki/Main_Page*. Повратено од http://www.cds.caltech.edu/~murray/wiki/Main_Page: http://www.cds.caltech.edu/~murray/wiki/Main_Page

Murray, R. M. (2006). *An Introduction to Networked Control Systems.* California Institute of Technology.

Natori, K., & Ohnishi, K. (2008). A Design Method of Communication Disturbance Observer for Time-delay Compensation, Taking the Dynamic Property of Network Disturbance into Account. *IEEE Transactions on Indian Electronics* , 2152-2168.

Nilsson, J., Bernhardsson, B., & Wittenmark, B. (1998). Stochastic Analysis and Control of Real-time Systems with Random Delays. *Automatica* , 57-64.

Park, H., Kim, Y., Kim, D., & Kwon, W. (2002). A Scheduling Method for Network-based Control Systems. *IEEE Transactions on Control System Technology* , 318-330.

Parlitz, U., Junge, L., Lauterborn, W., & Kocarev, L. (1996). Experimental Observation of Phase Synchronization. *Phys. Rev. E* , 2115-2117.

Pasqualetti, F., D'Orfler, F., & Bullo, F. (2011). Cyber-Physical Attacks in Power Networks: Models, Fundamental Limitations, and Monitor Design. *IEEE Conference on Decision and Control and European Control Conference*, (pp. 2195-2201). Orlando, FL.

Patankar, R. (2004). A Model for Fault-tolerant Networked Control System using TTP/C Communication. *IEEE Trans. Veh. Technol.* , 1461-1467.

Pecora, L. M., & Carroll, T. L. (1990). Synchronization in Chaotic Systems. *Physics Review Letters* , 821-824.

Peng, C., & Tian, Y. (2009). Delay-dependent Robust H-infinity Control for Uncertain Systems with Time-varying Delay. *Information Sciences* , 3187-3197.

Pereira, N., Andersson, B., & Tovar, E. (2007). WiDom: A Dominance Protocol for Wireless Medium Access. *IEEE Transactions on Indian Informatics* , 120-130.

Persis, C. D. (2009). Robust Stabilization of Nonlinear Systems by Quantized and Ternary Control. *Systems and Control Letters* , 602-608.

Pikovsky, A., Rosenblum, M., & Kurths, J. (2001). *Synchronization - A Universal Concept in Nonlinear Sciences.* Cambridge: Cambridge University Press.

Pommerenke, D., Fan, J., & Drewinak, J. (2016). Simulation Challenges in System Level Electrostatic Discharge Modelling. *International Conference on Wireless Information Technology and Systems and Applied Computational Electromagnetics.*

Ragnathan, S., Spaiser, V., Mann, R. P., & Sumpter, D. J. (2014). Bayesian Dynamical Systems Modelling in the Social Sciences. *PLoS ONE* .

Renzo, M., Imbriglio, L., Graziosi, F., & Santucci, F. (2009). Distributed Data Fusion Over Correlated Log-normal Sensing and Reporting Channels: Application to Cognitive Radio Networks. *IEEE Transactions to Wireless Communications* , 5813-5821.

Risley, A., Roberts, J., & LaDow, P. (2003). Electronic Security of Real-time Protection and SCADA Communications. *Annual Western Power Delivery Automation Conference.* Spokane, WA.

Rosenblum, M. G., & Pikovsky, A. S. (2001). Detecting Direction of Coupling in Interacting Oscillators. *Phys. Rev. E.*

Sauter, T., & Schwaiger, C. (2002). Achievement of Secure Internet Access to Fieldbus Systems. Bo *Microprocessors & Microsystems* (pp. 331-339). Netherlands: Elsevier.

Schwabedal, J. T., & Pikovsky, A. S. (2010). Effective Phase Dynamics of Noise-induced Oscillations in Excitable Systems. *Phys. Rev. E.* , 46-218.

Schwaiger, C., & Treytl, A. (2003). Smart Card Based Security for Fieldbus Systems. *IEEE Conference on Emerging Technologies and Factory Automation*, (pp. 398-406).

Segaran, T., & Hammerbacher, J. (2009). *Beautiful Data: The Stories Behind Elegant Data Solutions.* O'Reilly Media.

Seiler, P., & Sengupta, R. (2005). An Hinf Approach to Networked Control. *IEEE Transactions on Automatic Control* , 356-364.

Shakkottai, S., Kumar, A., Karnik, A., & Anvekar, A. (2001). TCP Performance Over End-to-end Rate Control and Stochastic Available Capacity. *IEEE/ACM Transactions on Networking* , 377-391.

Shanmugasundaram, K., Bronnimann, H., & Memon, N. (2005). Integrating Digital Forensics in Network Architectures. Bo M. Pollitt, & S. Shenoi, *Advances in Digital Forensics I* (pp. 127-140). New York, NY: Springer.

Shanmugasundaram, K., Memon, N., Savant, A., & Bronnimann, H. (2003). Fornet: A Distributed Forensics System. *Proceedings of the Second International Workshop on Mathematical Methods, Models, and Architectures for Computer Network Security.*

Shannon, C. E. (1948). A Mathematical Theory of Communication. *Bell Systems Technologies Journal* , 379-423.

Shannon, C. E. (1949). Communication in the Presence of Noise. *Proc. IRE* , 10-21.

Shannon, C. E. (1949). Communication Theory of Secrecy Systems. *Bell Systems Technology Journal* , 656-715.

Sharon, Y., & Liberzon, D. (2012). Input to State Stabilizing Controller for Systems with Coarse Quantization. *IEEE Transactions on Automatic Control* , 830-844.

Siemens. (2012). *SIMATIC S7-1200 Programmable Controller* . Nuernberg, Germany : Siemens AG.

Silberschatz, A., Baer Galvin, P., & Gagne, G. (2005). *Operating System Concepts.* Wiley & Sons.

Smelyanskiy, V. N., Luchinsky, D. G., Stefanovska, A., & McClintock, P. V. (2005). Inference of a Non-linear Stochastic Model of the Cardiorespiratory Interaction. *Physics Review Letters* , 98-101.

Smith, M., & Copps, M. (1993). *DNP3 V3.00 Data Object Library Version 0.02.* Pasadena, CA: DNP Users Group.

Smith, R. (2011). A Decoupled Feedback Structure for Covertly Appropriating Network Control Systems. *IFAC World Congress*, (pp. 90-95). Milan.

Soucek, S., Sauter, T., & Koller, G. (2003). Effect of Delay Jitter on Quality of Control in EIA-852-based Networks. *Proceedings of IECON*, (pp. 1431-1436).

Sridhar, S., Hahn, A., & Govindarasu, M. (2012). Cuber-physical System Security for the Electric Power Grid. *Proceedings of the IEEE* , 1-15.

Stankovski, T., A., D., McClintok, P. V., & Stefanovska, A. (2012). Inference of Time-evolving Coupled Dynamical Systems in the Presence of Noise. *Physics Review Letters* , 24-101.

Stankovski, T., Duggento, A., McClintock, P. V., & Stefanovska, A. (2014). A Tutorial on Time-evolving Dynamical Bayesian Inference. *European Physics Journal on Special Topics* , 2685-2703.

Stankovski, T., McClintock, P. V., & Stefanovska, A. (2014). Coupling Functions Enable Secure Communications. *Physics Review* , 11-26.

Stankovski, T., McClintock, P. V., & Stefanovska, A. (2014). Dynamical Inference: Where Phase Synchronization and Generalized Synchronization Meet. *Phys. Rev. E* .

Stankovski, T., Pereira, T., McClintock, P. V., & Stefanovska, A. (2017). Coupling Functions: Universal Insight into Dynamical Interaction Mechanisms. *Rev. Mod. Phys.*

Stankovski, T., Petkoski, S., Raeder, J., Smith, A. F., McClintock, P. V., & Stefanovska, A. (2016). Alterations in the Coupling Functions Between Cortical and Cardio-respiratory Oscillations due to Anaesthesia with Propofol and Sevoflurane. *Phil. Trans. R. Soc. A* .

Stankovski, T., Stefanovska, A., Young, R. J., & McClintock, P. V. (2016). *Патент бр. 14/910,547.* USA.

Stankovski, T., Ticcinelli, V., McClintock, P. V., & Stefanovska, A. (2015). Coupling Functions in Networks of Oscillators. *New J. Phys.*

Stankovski, T., Ticcinelli, V., McClintock, P. V., & Stefanovska, A. (2017). Neural Cross-frequency Coupling Functions. *Front. Syst. Neurosci.* , 33.

Sun, Z., Li, H., & Wang, J. (2007). Recent Advances in Networked Control Systems. *International Conference on Control, Automation and Systems.* Seoul, Korea.

Tarn, T., & Xi, N. (1998). Planning and Control of Internet-based Teleoperation. *Proceedings of SPIE: Telemanipulator and Telepresence Technologies*, (pp. 189-193). Boston, Massachusetts.

Teixeira, A., Amin, S., Sandberg, H., Johansson, K. H., & Sastry, S. (2010). Cyber Security Analysis of State Estimators in Electric Power Systems. *IEEE Conference on Decision and Control*, (pp. 5991-5998). Atlanta, GA.

The Vulcan Story. (1958). *Flight Magazine* .

Tian, E., Yue, D., & Zhao, X. (2007). Quantised Contol Design for Networked Control Systems. *IET Control Theory & Applications* , 1693-1699.

Tipsuwan, Y., & Chow, M. (2003). Control Methodologies in Networked Control Systems. *Control Engineering Practice 11* , 1099-1111.

Tipsuwan, Y., & Chow, M. (2001). Network-based Controller Adaptations Based on QoS Negotiation and Deterioration. *Proceedings of IECON '01*, (pp. 1794-1799).

Tipsuwan, Y., & Chow, M. (2004). On the Gain Scheduling for Networked PI Controller Over IP Network. *IEEE/ASME Transactions on Mechatronics* , 491-498.

Tokuda, I. T., Jain, S., Kiss, I. Z., & Hudson, J. L. (2007). Inffering Phase Equations from Multivariate Time Series. *Physics Review Letters* , 64-101.

Tsang, C., & Kwong, S. (2005). Multi-agent Intrusion Detection System in Industrial Network using Ant Colony Clustering Approach and Unsupevised Feature Extraction. *Proc. IEEE. Int. Conf. Ind. Technol.*, (pp. 51-56).

US Government Accountability Office. (2004). *Critical Infrastructure Protection Challenges and Efforts to Secure Control Systems.* Report to Congressional Requesters.

Walsh, G., Beldiman, O., & Bushnell, L. (1999a). Asymptotic Behavior of Networked Control Systems. *Proceedings of the IEEE International Conference on Control Applications*, (pp. 1448-1453). Kohala Coast, Hawaii.

Walsh, G., Ye, H., & Bushnell, L. (1999c). Stability Analysis of Networked Control Systems. *Proceedings of the 1999 American Control Conference*, (pp. 2876-2880). San Diego, California.

Wang, M. C., & Uhlenbeck, G. E. (1945). On the Theory of the Brownian Motion II. *Review of Modern Physics, vol. 17* , 323-342.

Wang, Y., Ye, H., & Wang, G. (2006). A New Method for Fault Detection of Networked Control Systems. *Proceedings of IEEE Conference on Indian Electronics* , 1-4.

White, T. (2012). *Hadoop: The Definitive Guide.* O'Reilly Media.

Win, M. Z., Pinto, P. C., & Shepp, L. A. (2009). A Mathematical Theory of Network Interference and its Applications. *Proceedings of the IEEE* , 205-230.

Worsley, D. J., & Edem, B. C. (1997). *Патент бр. Method of Maintaining Frame Synchronization in a Communication Network, 5,668,811*. USA.

Wu, J., Deng, F.-Q., & Gao, J.-G. (2005). Modeling and Stability of Long Random Delay Networked Control Systems. *Proceedings of International Conference of Machine Learning and Cybernetics*, (pp. 947-952).

Wu, J., Li, Y., Quevedo, D. E., Lau, V., & Shi, L. (2015). Data-driven Power Control for State Estimation. *Automatica 54* , 332-339.

Xia, Y. Q. (2014). Cloud Control Systems. *IEEE/CAA Journal of Automatica Sinica* .

Xia, Y. Q. (2012). From Networked Control Systems to Cloud Control Systems. *31st Chinese Control Conference*, (pp. 5878-5883). Hefei.

Xia, Y. Q., & Liu, B. (2013). Maximum Likelihood Ratio Detection of Abrupt State Change for MIMO Linear Systems Based on Frequency Domain Data. *International Journal of Robust and Nonlinear Control* , 858-877.

Xia, Y. Q., Amann, A., & Liu, B. (2010). Detection of Abrupt Changes in Electrocardiogram with Generalized Likelihood Ratio Algorithm. *IET Signal Processing* , 650-657.

Xia, Y. Q., Gao, Y. L., Yan, L. P., & Fu, M. Y. (2015). Recent Progress in Networked Control Systems - A Survey. *International Journal of Automation and Computing* , 343-367.

Xia, Y. Q., Shang, J. Z., Chen, J., & Liu, G. P. (2009). Network Data Fusion with Packet Losses and Variable Delays. *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics* , 1107-1120.

Xia, Y. Q., Yan, J. J., Shang, J. Z., Fu, M. Y., & Liu, B. (2012). Stabilization of Quantized Systems Based on Kalman Filter. *Control Engineering Practice* , 954-962.

Xia, Y. Q., Yan, J. J., Shi, P., & Fu, M. Y. (2013). Stability Analysis of Discrete-time Systems with Quantized Feedback and Measurements. *IEEE Transactions on Industrial Informatics* , 313-324.

Xia, Y., Liu, G., & Rees, D. (2006). Hinf Control for Networked Control Systems in Presence of Random Network Delay and Data Dropout. *Proceedings of Chinese Control Conference*, (pp. 2030-2034).

Xie, L., Fang, H., & Zheng, Y. (2004). Guaranteed Cost Control for Networked Control Systems. *Journal of Control Theory and Applications* , 143-148.

Xiong, J., & Lam, J. (2007). Stabilization of Linear Systems over Networks with Bounded Packet Loss. *Automatica* , 80-87.

Yan, J. J., Xia, Y. Q., & Li, L. (2014). Stabilization of Fuzzy Systems with Quantization and Packet Dropout. *International Journal of Robust and Nonlinear Control* , 1563-1583.

Yan, J., & Xia, Y. (2012). Stabilization of Nonlinear Continous System with Input Quantization and Packet Dropout. *IET Control Theory & Applications* , 2426-2433.

Yan, L. P., Li, X. R., Xia, Y. Q., & Fu, M. Y. (2013). Optimal Sequential and Distributed Fusion for State Estimation in Cross-correlated Noise. *Automatica* , 3607-3612.

Yan, L. P., Xiao, B., Xia, Y. Q., & Fu, M. Y. (2012). State Estimation for Asynchronous Multirate Multisensor Nonlinear Dynamic Systems with Missing Measurements. *International Journal of Adaptive Control and Signal Processing* , 516-529.

Yang, H. J., Xia, Y. Q., & Liu, B. (2011). Fault Detection for T-S Fuzzy Discrete Systems in Finite-frequency Domain. *IEEE Transactions on Systems, Man and Cybernetics, Part B: Cybernetics* , 911-920.

Ye, H., & Ding, S. X. (2004). Fault Detection of Networked Control Systems with Network-induced Delay. *8th International Conference on Control, Automation, Robotics, and Vision*, (pp. 294-297).

Yorke, J. A. (1970). Asymptotic Stability for One Dimensional Differential-delay Equations. *Journal of Differential Equations* , 189-202.

You, K. Y., & Xie, L. H. (2011). Minimum Data Rate for Mean Square Stabilizability of Linear Systems with Markovian Packet Losses. *IEEE Transactions on Automatic Control* , 772-785.

You, K. Y., & Xie, L. H. (2010). Minimum Data Rate for Mean Square Stabilization of Discrete LTI Systems Over Lossy Channels. *IEEE Transactions on Automatic Control* , 2373-2378.

You, K. Y., Su, W. Z., Fu, M. Y., & Xie, L. H. (2011). Attainability of the Minimum Data Rate for Stabilization of Linear Systems via Logarithmic Quantization. *Automatica* , 170-176.

Yuan, G., Qigong, C., Ming, J., & Yiqing, H. (2013). Modeling of Random Delays in Networked Control Systems. *2013*.

Yue, D., Han, Q., & Lam, J. (2005). Network-based Robust Hinf Control of Systems with Uncertainty. *Automatica* , 999-1007.

Yue, D., Han, Q., & Lam, J. (2008). Robust H-infinity Control and Filtering of Networked Control Systems. Bo F. Wang, & D. Liu, *Networked Control Systems: Theory and Applications* (pp. 121-151). London: Springer.

Yue, D., Peng, C., & Tang, G. (2006). Guaranteed Cost Control of Linear Systems over Networks with State and Input Quantizations. *IEEE Proceedings on Control Theory and Applications* , 658-664.

Zampieri, S. (2008). Trends in Networked Control Systems. *Proceedings of the 17th IFAC*, (pp. 2886-2894). Seoul, Korea.

Zhang, C., Feng, G., & Qiu, G. J. (2011). Generalized H2 Filter Design for TS Fuzzy Systems with Quantization and Packet Loss. *Proceedings of IEEE Symposium on Computational Intelligence in Control and Automation*, (pp. 52-59). Paris, France.

Zhang, C., Feng, G., & Qiu, G. J. (2011). H-infinity Filtering for Nonlinear Discrete-time Systems Subject to Quantization and Packet Dropouts. *IEEE Transactions on Fuzzy Systems* , 353-365.

Zhang, H., Yang, J., & Su, C. (2007). T-S Fuzzy-model-based Robust Hinf Design for Networked Control Systems with Uncertainties. *IEEE Transactions on Indian Informatics* , 289-301.

Zhang, L., Gao, H., & Kaynak, O. (2013). Network-induced Constraints in Networked Control Systems - A Survey. *IEEE Transactions on Industrial Informatics* , 403-416.

Zhang, L., Shi, Y., Chen, T., & Huang, B. (2005). A New Method for Stabilization of Networked Control Systems with Random Delays. *American Control Conference*, (pp. 633-637). Portland, OR, USA.

Zhang, W. A., Feng, G., & Yu, L. (2012). Multi-rate Distributed Fusion Estimation for Sensor Networks with Packet Losses. *Automatica* , 2016-2028.

Zhang, W., Branicky, M. S., & Phillips, S. M. (2001). Stabillity of Networked Control Systems. *IEEE Control Systems Magazine* , 84-99.

Zheng, Y., Fang, H., & Wang, H. O. (2006). Takagi-Sugeno Fuzzy-model-based Fault Detection for Networked Control Systems with Markov Delays. *IEEE Transactions on Systems, Man and Cybernetics - Part B: Cybernetics* , 924-929.

Zhu, C., Xia, Y. Q., Yan, L. P., & Fu, M. Y. (2012). Centralized Fusion over Unreliable Networks. *International Journal of Control* , 409-418.

Zhu, C., Xia, Y. Q., Yan, L. P., & Fu, M. Y. (2010). Multi-channel Networked Data Fusion with Intermittent Observations. *29th Chinese Control Conference*, (pp. 4317-4322). Beijing.

Zhu, X., & GH, Y. (2009). Networkpbased Robust H-infinity Control of Continous-time Systems with Uncertainty. *Asian Journal of Control* , 21-30.

Zhu, Z., & Zhou, X. (2007). Fault Detection Based on the State Observer for Networked Control Systems with Uncertain Long Time-delay. *Proc. IEEE Int. Conf. Autom. Logistics*, (pp. 2320-2324).