Faculty of Electrical Engineering - Skopje

Evaluation issues of different cryptography algorithms in Wireless Sensor Networks

Kire Trivodaliev
Biljana Stojkoska
Ace Dimitrievski
Danco Davcev

kire.trivodaliev@etf.ukim.edu.mk

Semptember 6,2006

NATO-ARW, Suceava, September 4-8, 2006

WSN applications VS. traditional wireless network applications

- Generating data when monitoring phenomena
- Collaboratively processing the data into useful information
- Either storing the information within the network for later retrieval or communicating the information directly to a user

Holistic approach of security

- Security is to be ensured for all the layers of the protocol stack
- The cost for ensuring security should not surpass the assessed security risk at a specific time
- Physical security ensured
- Security measures should be developed to work in a decentralized fashion

Requirement specific adaptation

- QoS parameters
- WSN security constraints
- Using both analytical expressions and simulations

QoS parameters

- System lifetime
- Response Time
- Data Freshness
- Detection Probability
- Data Fidelity
- Data Resolution

WSN security constraints

- Hostile environment
- Random topology
- Power restrictions
- Limited Computational power
- Storage Restrictions

Evaluation model

- Analytical model
- Simulation
- Validation
- Results feedback

Analytical model

- Performance parameter, ***P***
- Set of QoS parameters, ***Q***
- Set of constraints, ***C***
- Tradeoffs
  - Impact of the constraints on the QoS, ***QxC***
  - Relationship between different QoS parameters, ***QxQ***

Analytical model - Tradeoffs

- System lifetime is affected by the energy consumption rate of the entire system
- Response time is impacted by the latency of transmission and data processing
- Data freshness is impacted by the latency of transmission and data processing
- Detection probability is affected by loss and error of data transmission
- Data fidelity is an aggregated measurement reflecting not only the accuracy of sensing data but also the accuracy of location and time information associated with the data
- Data resolution is impacted by the amount of processed data to describe real world phenomena

Analytical model

$$P = f(Q)$$

- Degree to which the desired QoS parameters are met, $f(Q)$

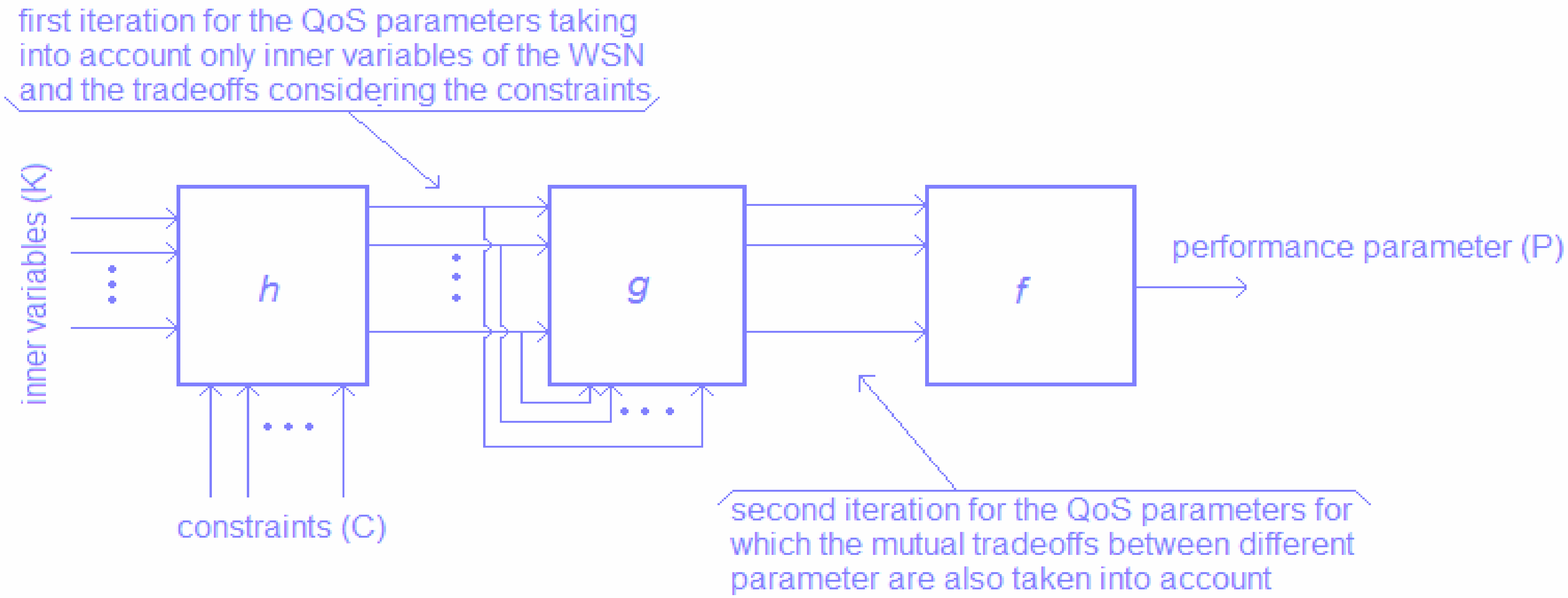
$$f(Q) = h(QxC)\,g(QxQ)$$

- $g(QxQ)$ analytically describes relationships between different QoS parameters (possible degradation or amplification)
- $h(QxC)$ analytically describes the influence of the constraints and inner variables on the QoS parameters

Analytical model

$$h(QxC) = KxC$$

- K depicts the influence of the inner variables of the WSN which can be altered as desired


first iteration for the QoS parameters taking into account only inner variables of the WSN and the tradeoffs considering the constraints
inner variables (K)
h
g
f
performance parameter (P)
constraints (C)
second iteration for the QoS parameters for which the mutual tradeoffs between different parameter are also taken into account

Simulation

- Simulation challenges
- Effects of detail
- Repeatable simulation
- Statistical validity
- Estimation of target property
- Precision
- Problems
  - we can never be sure we've accounted for all aspects (we can't know what we don't know)
  - simulation package differences
  - incorrect parameter settings
  - improper level of detail

Validation

- Properly validating simulation models against the intended real-world implementation and environment
- Identifying the platform used in measurements
- Proposing measurement methodology
- Problem
  - newly developed algorithm that doesn't have an actual implementation or testbed to serve as a baseline
  - validation against algorithm specification or mathematical calculations
  - lower reliability (difficult to include environmental conditions and channel contention)

Results feedback

- If a simulation is valid, real-life performance should correlate with the simulated performance
- Results should point out the design adaptations, if needed
- Possible issue
  - validation results refer to networks with less nodes, smaller density, different environmental conditions etc.
  - if experimentally measured performance for WSN, in research lab conditions, correlates with simulation is the simulation valid?

Example case study scenario

- We plan to evaluate the implementation of different cryptographic algorithms that use symmetric keys (*SkipJack*, *RC5, RC6, TEA, BlowFish*)
- WSN performance using these algorithms should meet QoS parameters, especially energy efficiency and data robustness (System Lifetime, Data Freshness, Data Fidelity, Data Resolution)
- Simulations will be carried out of WSN with 100 stationary and homogenous nodes, in which a secure application is implemented

Example case study scenario

- The verification process will be performed on a seven node WSN consisted of MicaZ wireless sensors with the following features:
  - ATMega128L microcontroller operating at 7.3728 MHz
  - 128 kB program memory
  - 4 kB data memory
  - CC2420 radio operating at 2.4 GHz with maximum data rate of 250 kbits/sec
  - typical battery capacity 2000mA-hr
- In the feedback phase, the verification results will possibly confirm the usage of the evaluated cryptography algorithms in WSN

Summary

- Holistic approach of security
- Requirement specific adaptation
- Evaluation model
  - – Analytical model
  - – Simulation
  - – Validation
  - – Results feedback