Security Policy Reconfiguration Solutions in Wireless Sensor Networks

UZH 655/678 Seminar: Internet Economics
- Prof. Dr. Burkhard Stiller

By Sanjiv Jha, Raphael Ochsenbein & Anastasia Ruvimova

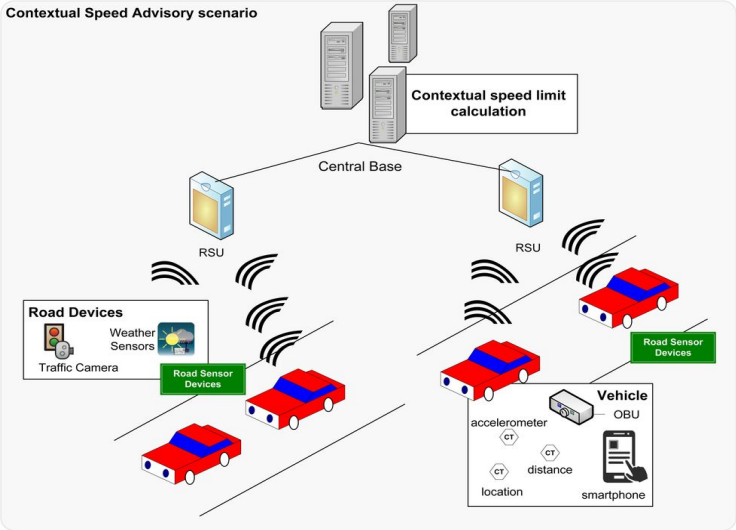
Supervisor: Dr. Corinna Schmitt

Table of Contents

- Introduction
- Applying Security Policies to WSN
  - Security Issues & Attack Vectors
  - Defense Mechanisms
- Practical Solutions
  - Effective Key Management for WSN's
  - Trust-based Enforcement of Security Policies
  - Dynamic Reconfiguration (Intra-trust and Famiware)
- Conclusion

Introduction

- Wireless Sensor Networks (WSN)?
- WSN Existing Network examples.
- WSN Security Policies needs.



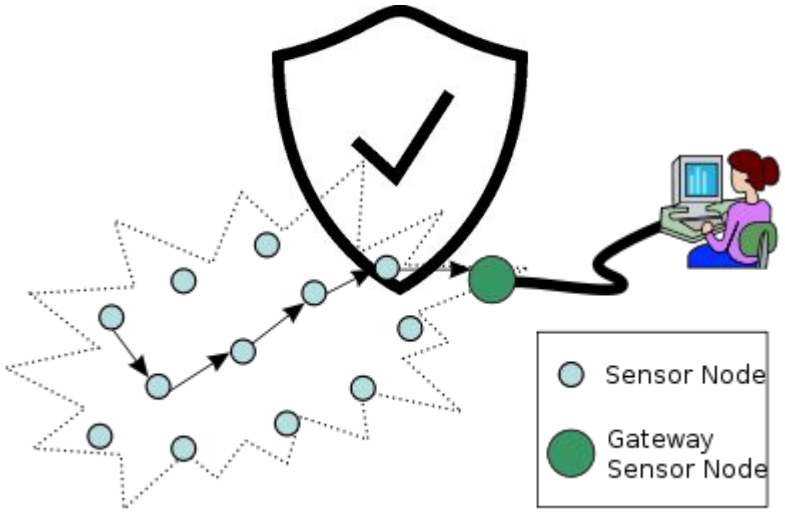
Intelligent transport system

Motivation for Security Reconfiguration in WSNs

a. Constraints and Issues with existing security policy.

b. Security Policy Reconfiguration?

c. Benefits of Re-configuring the security policies.



Terminology & Definitions

WSN

"Wireless sensor networks (WSNs) consist of hundreds or even thousands of small devices each with sensing, processing, and communication capabilities to monitor the real-world environment. They are envisioned to play an important role in a wide variety of areas ranging from critical military surveillance applications to forest fire monitoring and building security monitoring in the near future." - I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks", IEEE Communications Magazine, Vol. 40, No. 8, pp. 102-114, August 2002.

Internet of things (IoT)

"A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.

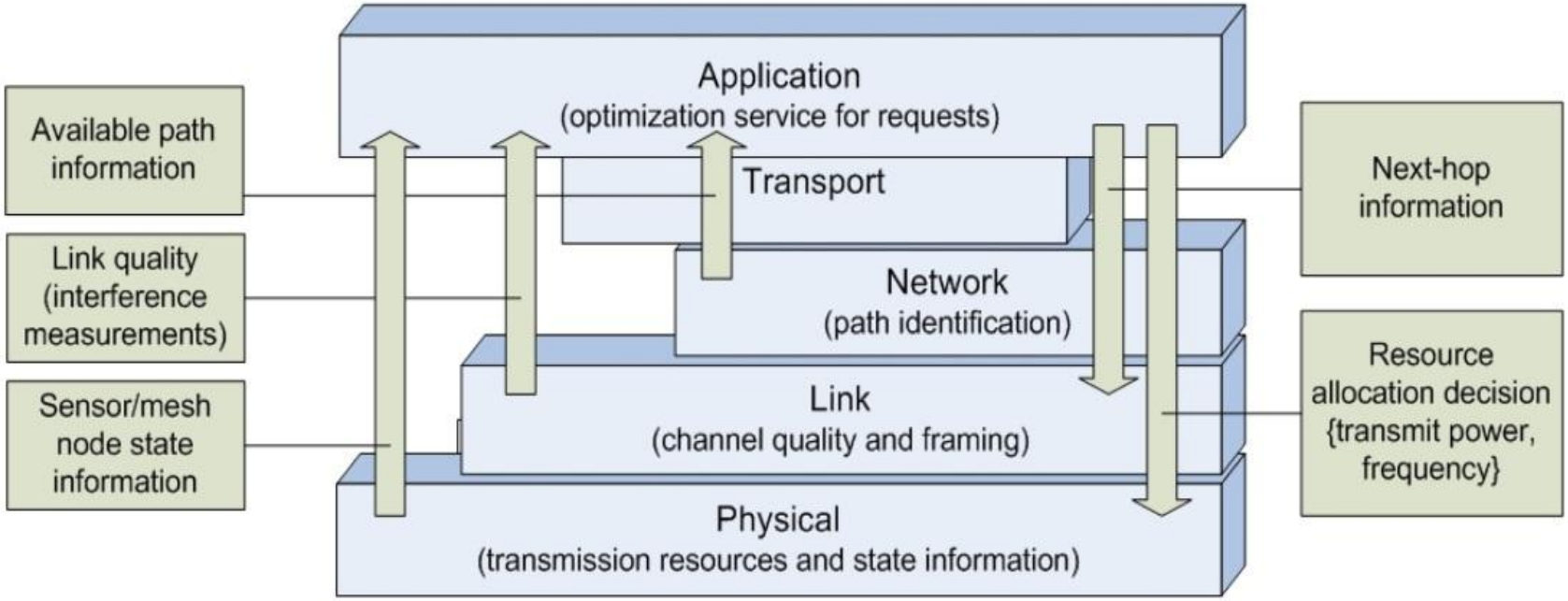
NOTE 1 – Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.

NOTE 2 – From a broader perspective, the IoT can be perceived as a vision with technological and societal implications."

- ITU-T: Y2060 - Overview of the Internet of things, 2012. https://www.itu.int/rec/T-REC-Y.2060-201206-I.

Security Issues & Attack Vectors

- ❑ **DoS Attacks**
- ❑ **Attacks on Secrecy and Authentication**
  - ❑ Node Replication
  - ❑ Privacy



DoS Attacks - Denial of Service

Physical Layer

- ❑ Jamming
- ❑ Tampering

Link Layer

- ❑ Link Layer
- ❑ Purposefully Created Collisions
- ❑ Resource Exhaustion
- ❑ Unfairness in Allocation

DoS Attacks (cont.)

Network Layer

- Spoofed routing information
- Selective forwarding
- Sinkhole
- Sybil attack
- Wormhole
- Hello flood
- Acknowledgment spoofing

Transport Layer

- Flooding
- De-synchronization

Defense Mechanisms

Defense Mechanisms

- **Cryptography in WSNs**
  - Public key cryptography
  - Symmetric key cryptography
- **Key management protocols**
  - Key management based on network structure
  - Key management on probability of key sharing
    - Deterministic key distribution schemes
    - Probabilistic key distribution schemes
- **Defense against DoS attacks**
  - Defense in the physical layer
  - Defense in the link layer
  - Defense in the network layer
    - Secure broadcasting and multicasting protocols
- **Defense against attacks on routing protocols**

Defense Mechanisms (cont.)

- Defense against the Sybil attack
- Detection of node replication attack
- Defense against traffic analysis attack
- Defense against attacks on sensor privacy
- Intrusion detection
- Secure data aggregation
- Defense against physical attacks
- Trust management

Solution 1:

Effective Key Management in Dynamic Sensor Networks

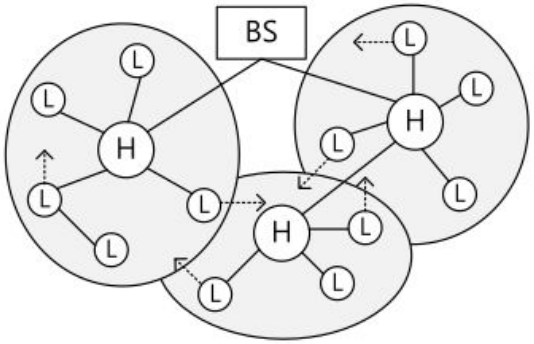
Seo, Seung-Hyun, Jongho Won, Shabana Sultana, and Elisa Bertino. Effective key management in dynamic wireless sensor networks, Information Forensics and Security, IEEE Transactions on 10, no. 2 (2015): 371-383. http://docs.lib. purdue. edu/cgi/viewcontent.cgi? article=1640&context=ccpubs.

Effective Key Management in dynamic WSN's (cont.)

- Symmetric key encryption drawbacks:
  - i high communication overhead
  - ii large memory space
  - iii not scalable
  - iv not resilient to node compromise
- Asymmetric key encryption (public key cryptography (PKC))
  - i ECC (elliptic curve cryptography): feasible performance-wise
  - ii resilient to node compromise attacks
  - iii more scalable and flexible
  - iv vulnerable to message forgery, key compromise known-key attacks
- Certificateless effective key management (CL-EKM) scheme
  - i certificateless public key cryptography (CL-PKC)
  - ii the user's full private key is a combination of a partial private key generated by a key generation center (KGC) and the user's own secret value
  - iii pairwise key between nodes: a pairing-free certificateless hybrid signcryption scheme (CL-HSC)

Effective Key Management in dynamic WSN's (cont.)

- **3 Node Types**
  - i BS: Manages Network, collects Data, hosts a Key Generation Center (KGC)
  - ii nodes with high processing capabilities (H-Sensors)
  - iii nodes with low processing capabilities (L-Sensors)
- **4 Key Types**
  - i a certificateless public/private key pair
  - ii an individual key
  - iii a pairwise key
  - iv a cluster key
- **7 Network Phases**
  - i system setup
  - ii pairwise key generation
  - iii cluster formation
  - iv key update
  - v node movement
  - vi key revocation
  - vii addition of a new node
- **BS Role**
  - i issues certificateless public/private key pairs for each node
  - ii a unique individual key, shared only between the node and the BS is assigned to each node
  - iii certificateless public/private key of a node is used to establish pairwise keys between any two nodes
  - iv a cluster key is shared among the nodes in a cluster



Effective Key Management in dynamic WSN's (cont.)

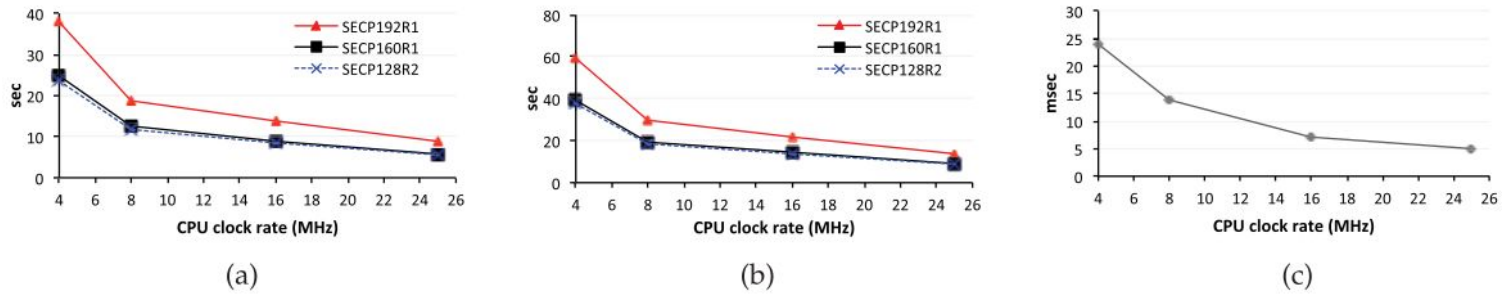


Fig. 2. Computation overhead for pairwise master/encryption key establishment. (a) Encapsulating key information. (b) Decapsulating key information. (c) Pairwise encryption key establishment.

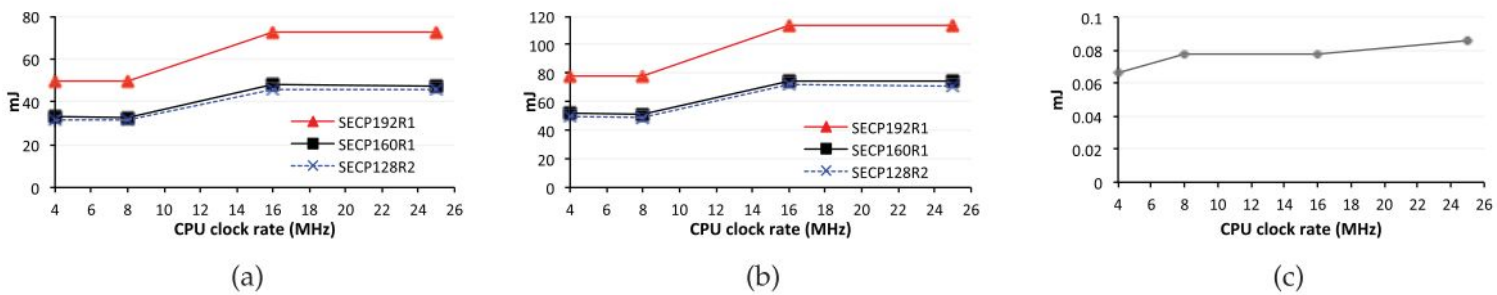
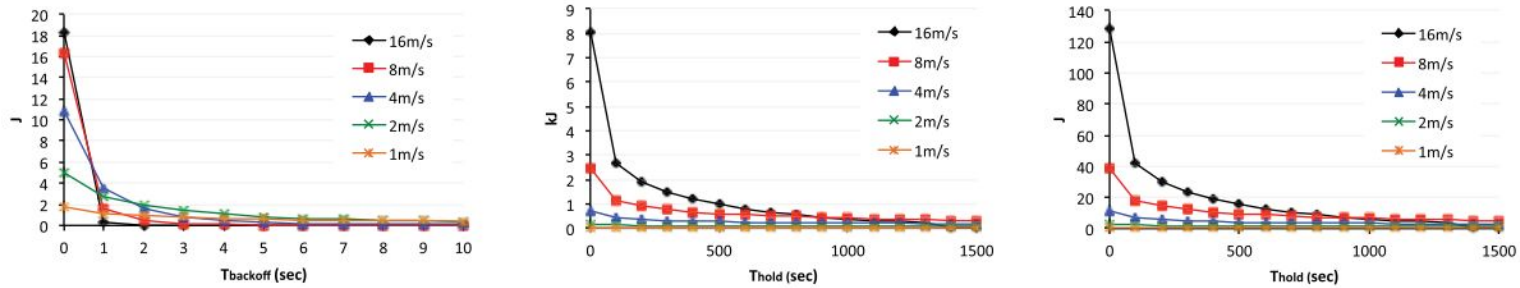


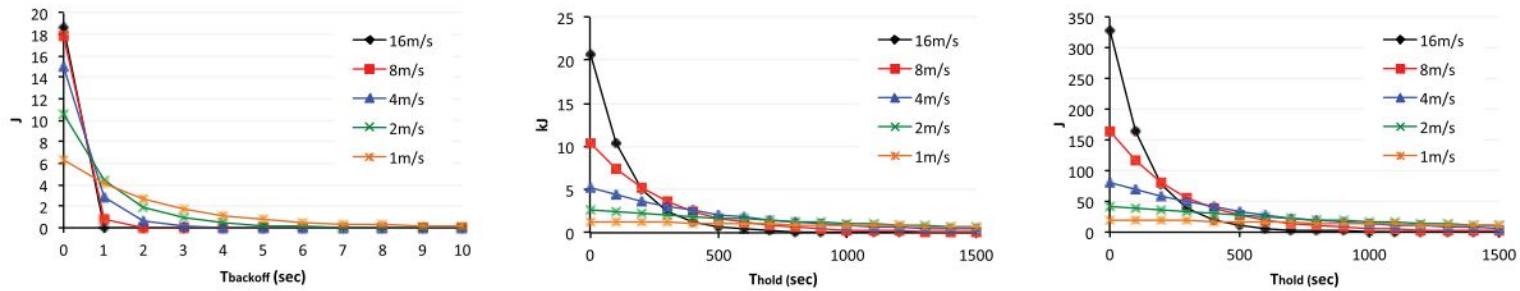
Fig. 3. Energy consumption for pairwise master/encryption key establishment. (a) Encapsulating key information. (b) Decapsulating key information. (c) Pairwise encryption key establishment.

Effective Key Management in dynamic WSN's (cont.)



(a) (b) (c)

Fig. 8. Node movement simulation results in random walk mobility model. (a) Energy consumption of one H-sensor for cluster key update for one day ($T_{hold} = 100$ sec). (b) Energy consumption of one H-sensor for pairwise key establishment for one day ($T_{backoff} = 6$ sec). (c) Energy consumption of one L-sensor for pairwise key establishment for one day ($T_{backoff} = 6$ sec).



(a) (b) (c)

Fig. 9. Node movement simulation results in Manhattan mobility model. (a) Energy consumption of one H-sensor for cluster key update for one day ($T_{hold} = 100$ sec). (b) Energy consumption of one H-sensor for pairwise key establishment for one day ($T_{backoff} = 6$ sec). (c) Energy consumption of one L-sensor for pairwise key establishment for one day ($T_{backoff} = 6$ sec).

Solution 2:

Trust-based Enforcement of Security Policies

Roberto Vigo , Alessandro Celestini , Francesco Tiezzi , Rocco De Nicola , Flemming Nielson , and Hanne Riis Nielson

Overview

- Security Policies are strengthened/loosened based on node's reputation system
- Finding appropriate balance between resource consumption and security strength
- Trust is calculated stochastically, through probabilistic calculus

The Logic & Logistics

- Implemented in modelling language StoKlaim
- Signature check determines trust score: reputation based on number of positive interactions
- Either:
  - no policy is enforced (action denied)
  - one policy is enforced (at base, but not target)
  - two policies are enforced (at base and target)

Table 2. Syntax: Aspects and Policies.

$\pi ::= \mathsf{do} \mid \mathsf{skip} \mid [?_{rcp(u)} rec \text{ if } cut : cond] \mid \pi_1.\pi_2$	(Policy)
$cut ::= l :: a@u$	(Aspect trigger)
$cond ::= \mathsf{true} \mid \mathsf{false} \mid d_1 = d_2 \mid \mathsf{readp}(T)@u : \lambda$	(Applicability condition)
$\mid \neg cond \mid cond_1 \wedge cond_2 \mid cond_1 \vee cond_2$	
$rec ::= \mathsf{skip} \mid \mathsf{do} \mid P$	(Recommendation)

[8]

Probabilities

Table 3. Results of the analysis of the formula $true\ U^{\leq t} \phi_{FwdCorrupted}$.

Behaviour θ	Time t	Threshold th	Probabilities	Time t	Probabilities
0.2	20	1%	0.6534	40	0.8894
0.2	20	5%	0.4693	40	0.6087
0.2	20	10%	0.2378	40	0.2565
0.5	20	1%	0.8974	40	0.9869
0.5	20	5%	0.7256	40	0.8584
0.5	20	10%	0.3747	40	0.4010
0.8	20	1%	0.9279	40	0.9928
0.8	20	5%	0.5535	40	0.6151
0.8	20	10%	0.1379	40	0.1382

[8]

- Policy enforcement is dependent on threshold

Solution 3:

Dynamic Reconfiguration - Intra-trust and Famiware

Dynamic Reconfiguration of Security Policies in Wireless Sensor Networks

*Mónica Pinto *, Nadia Gámez , Lidia Fuentes , Mercedes Amor , José Miguel Horcas and Inmaculada Ayala*

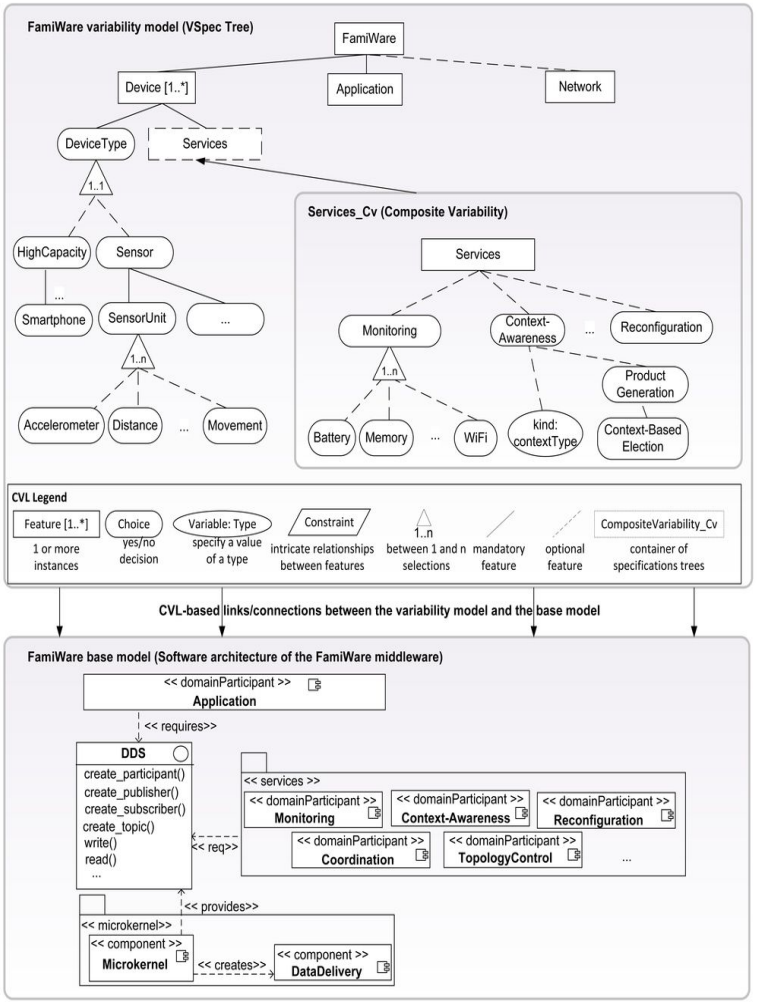
Dynamic Approach

WSN is a network with myriad of sensors,·have constraints can be overcome by using Dynamic approach:

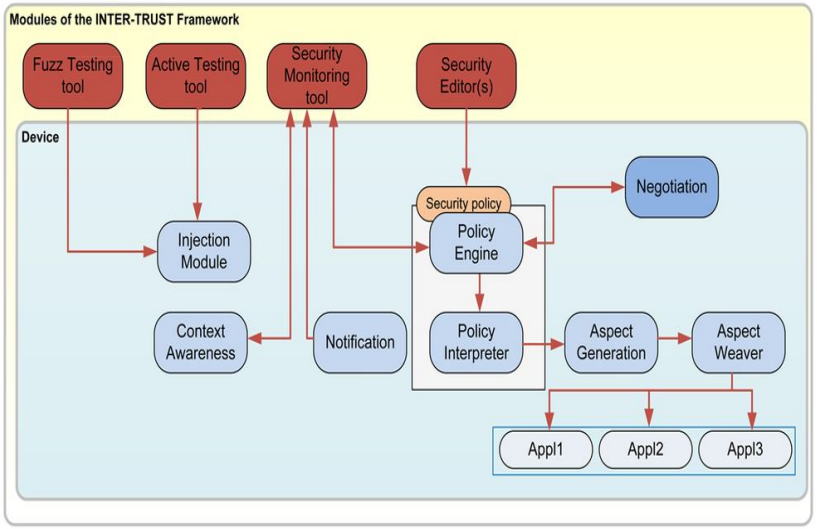
- Build secure applications that run on heterogeneous nodes with limited capabilities.
- Dynamic negotiation of security policies for WSNs.
- Monitor the changes in the context.
- Dynamic reconfiguration service to endow applications with self-protection.

Femi Ware and Inter-trust Framework

Dynamic Software Product Lines

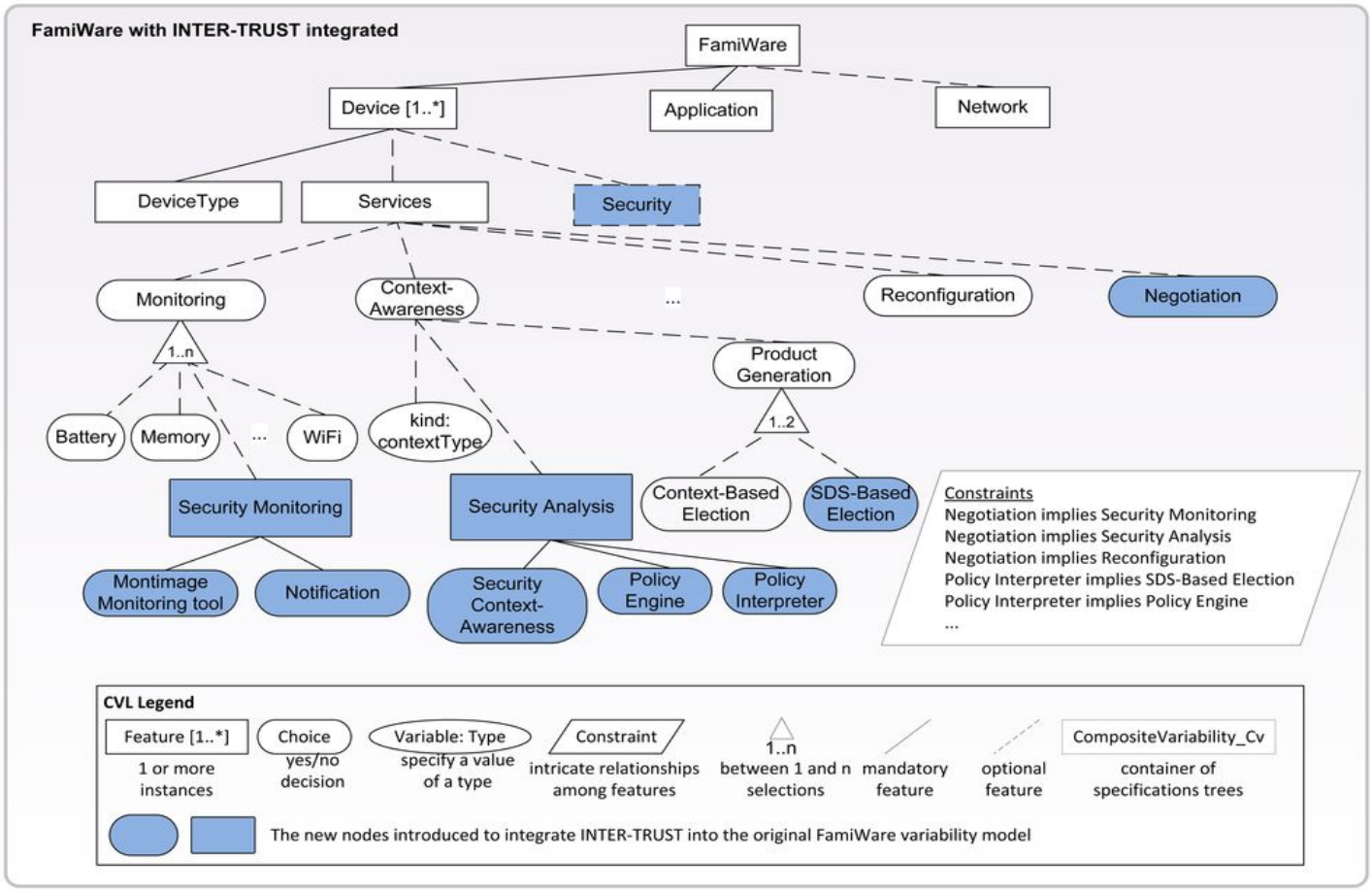


Dynamic Security Framework



Dynamic Security Adaptation

Fami Ware with Inter-Trust Integration:



Conclusion

- The approaches and policies to be applicable not only for all sensors or the Internet of things, but also to the Mobile phones. This can be extended to e-voting and ambient home applications.
- Choose the right tool for the right situation

Questions?

Discussion

Question 1: What level of security is needed for the following scenarios:

a. Ambient control in homes
b. Patient-monitoring in hospitals
c. Disaster response (fire, earthquakes)
d. Airplanes

Discussion

Question 2: In this wirelessly-connected world, do you trust currently employed security mechanisms?

Discussion

Question 3: Which of the presented practical solutions is the most useful?

Discussion

Question 4: How do you see the future of WSN's?

- Where will WSN's bring a lot of added value?
- What kind of products could be enabled by WSN's?
- For these products, what security mechanisms would be relevant?

Thank You!

Appendix 1

Table 2 Classification of key management protocols [97]

Prot. Type	Protocol Name	Ref	Master Key	Pairwise Key	Path Key	Cluster Key	Scalability	Robustness	Proc. Load	Comm. Load	Storage Load
Deterministic											
	All pairwise		NA	Yes	No	No	Low	Low	Low	Low	High
	LEAP	[59]	Yes	Yes	Yes	Yes	Good	Low	Low	Low	Low
	BROSK	[122]	Yes	Yes	No	No	Good	Low	Low	Low	Low
	LKHW	[63]	Yes	Yes	No	Yes	Limited	Low	Low	Low	Low
	CDTKeying	[123]	NA	Yes	No	No	Good	Good	Medium	Medium	High
	IOS & DMBS	[124]	NA	Yes	No	No	Good	Good	Medium	Medium	High
Probabilistic											
	Basic	[19]	NA	Yes	Yes	No	Good	Good	Medium	Medium	High
	q-composite	[22]	NA	Yes	No	No	Good	Good	Medium	Medium	High
	Polynomial based	[46]	NA	Yes	No	No	Good	Good	Medium	Medium	High
	Blom based	[9]	NA	Yes	No	No	Good	Good	Medium	Medium	High
	Deployment knowledge based	[129]	NA	Yes	No	No	Good	Good	Medium	Medium	High
	Cluster key grouping	[130]	NA	Yes	No	No	Good	Good	Medium	Medium	High
	Location based	[132	NA	Yes	No	No	Good	Good	Medium	Medium	Medium

Appendix 2

Table 1. Attacks on WSNs and countermeasures

Layer	Attacks	Defense
Physical	Jamming	Spread-spectrum, priority messages, lower duty cycle, region mapping, mode change
Link	Collision	Error-correction code
	Exhaustion	Rate limitation
	Unfairness	Small frames
Network	Spoofed routing information & selective forwarding	Egress filtering, authentication, monitoring
	Sinkhole	Redundancy checking
	Sybil	Authentication, monitoring, redundancy
	Wormhole	Authentication, probing
	Hello Flood	Authentication, packet leashes by using geographic and temporal info
	Ack. flooding	Authentication, bi-directional link authentication verification
Transport	Flooding De-synchronization	Client puzzles Authentication

Source: Y. Wang, G. Attebury, and B. Ramamurthy, IEEE Communications Surveys and Tutorials, Vol. 8, No. 2, pp. 2-23, 2006