Reliablity and Survivability of Wireless Sensor Network Using Security Adaptation Reference Monitor (SARM)

Tewfiq El Maliki
Information Technology department-hepia
University of Applied Sciences Western Switzerland
1202 Geneva - Switzerland
tewfiq.elmaliki@hesge.ch

Jean-Marc Seigneur
Advanced Systems Group
University of Geneva
1211 Geneva 4 – SWITZERLAND
Jean-Marc.Seigneur@trustcomp.org

Abstract —Security has become a key issue for any huge deployment of Wireless Sensor Network (WSN). Moreover, data reliability combined with energy loss minimization is really a challenging task, particularly to maintain survivability of the WSN under attacks such as sinkhole. Therefore, new security mechnisms must be in accordance with energy consumption constraint. This paper proposes to address this task using our Security Adaptation Reference Monitor (SARM) which is an efficient Framework capable of trading-off between security and energy optimization. SARM is based on an autonomic computing security looped system, which fine-tunes security means based on the monitoring of the context including energy consumption aspects. We evaluate SARM in the context of WSN through a simulation tool to verify the performance of overall reliability and energy loss in the presence of sinkhole attackers. The results clearly show that SARM is efficient in terms of reliability, overall network utilization and power consumption.

Keywords – Framework, Autonomic, Security adaptation, Sinkhole, Sensor Network

I. INTRODUCTION

Wireless sensor network (WSN) is a versatile network for supporting variety of important applications, consisting of a large number of low-power and multifunction sensor nodes that communicate as one hop, multi-hop or cluster-based models to send data to one or many base stations (BS)s through wireless links [1]. The BS is highly enriched system with a large amount of energy. This network is built by deploying the sensing nodes in the area of interest to form a self configured network and start acquiring the necessary information. The nodes in this network are battery operated and have limited lifetime to operate. Therefore, there is a need of energy aware security algorithm which should not perform heavy computation on the nodes since it shortens the network lifetime.

In general, many applications could not operate under significant packet loss. Thus, reliability is one of the most important criteria to evaluate the quality of wireless sensor networks. Unfortunately, packet loss is increased by two major factors: less coverage of sensors due to less power and high error rate of wireless links. Moreover, dynamic power attacks such as sinkhole are fatal to the survivability of the network. Therefore, the concept that must cope with this new security challenge has to be based on dynamic adaptation security system to satisfy an overall performance such as network reliability, being a key issue especially in sensor networks. We have already proposed a generic security adaptation reference monitor (SARM) as a compelling solution for such problems [2]. In this article, we will apply it for WSN in case of sinkhole attacks.

Please note: we use security in general term including availability, reliability and survivability.

In Section 2, we survey other related works. Section 3 gives the problem statement, highlighting the motivation of our work. Section 4 introduces SARM for WSN and explains its components and functionalities. Section 5 explains our experiments and simulation implementation to validate SARM in the case of sensor network. Our simulation results and performance analysis are presented in Section 6 and Section 7 concludes our paper.

II. RELATED WORK

Many systems rated at the higher levels of security for data are implemented according to the reference monitor concept. First introduced by James Anderson [3], a reference monitor is a concept that has proven to be a useful tool for computer security experts. It is the only effective tool known for describing the abstract requirements of secure system design and implementation.

A suitable security service is provisioned in a progressive way to achieve the maximum overall security services against network performance services throughout the course of sensor networks operation. Security in sensor networks is complicated by the constrained capabilities of sensor node hardware and the properties of the deployment [4], [5] and [6].

We argue that the spare processing and transmission resources are wasted in sensor environments if security is over-provisioned. Hence the trade-off between security and performance is essential in the choice of security services. Adaptive security mechanisms are also found in flexible protocol stacks for wireless networks [7], context-aware access control systems [8] and security architectures [9]. This prompted us for the implementation of a completely reconfigurable architecture [10], which is fundamental to adapt the architecture to the terminal and network variability of the context and particularly in the security field [11]. J-M

 ISBN: 978-1-61208-010-9

Seigneur [12] has introduced autonomic security pattern in his security design but only at the authentication level.

III. MOTIVATION FOR OUR FRAMEWORK

Flexible security mechanisms are needed to respond to new types of attacks and to meet different network setting-specific protection requirements. The required flexible security assessment can be achieved by introducing a generic autonomic computing security framework.

In the case of sensor networks, the sensors usually forward their messages to a Base Station (BS) [13] in a hop-by-hop fashion because they are resource-constrained in terms of energy and the spending of energy dramatically increases with the range of transmission. It is quite easy for an attacker as a Sinkhole [14] to defeat the WSN purpose by dropping messages when received rather than forwarding them to consume energy of other sensors by requesting them to continuously send information.

It is highly critical to keep the overall security at the highest level due to the configuration complexity and the runtime changing context. In general, data transfer in WSNs is more susceptible to loss due to the nature of sensors (power, processing, etc) in addition to the high error rate of wireless links. Moreover, sinkhole attacks by means of dynamic changing behavior skyrocket the packet loss. Therefore, the most crucial constraint in WSN which is reliability is not at all guaranteed

Assuring reliable data delivery between the sensor nodes and the BS in Wireless Sensor Networks is a challenging task as it affects the ability to sense event. A reliable protocol in WSN is a protocol that allows reliably data transfer from source to BS with reasonable packet loss. The problem of achieving reliable communication between nodes is further aggravated by the presence of sinkhole attackers whenever they are changing dynamically their behavior.

In addition, most applications cannot operate in case of high packet loss. Thus, reliability, being a key issue especially in sensor networks, is definitely one of the important criteria to evaluate the quality of wireless sensor networks. Accordingly, the concept that must cope with this new security challenge in term of availability has to be based on dynamic adaptation security system to satisfy an overall performance such as network reliability and energy loss.

Briefly, to lengthen the lifetime of wireless sensor network, an efficient protocol needs to support reliable network combined with energy efficiency under sinkhole attacks.

We propose a generic Framework called Security Adaptation reference monitor (SARM) as a compelling solution for this problem, because it is looped system developed especially for highly dynamic wireless network. It is aimed to offer a global adaptation security scheme for any application instead of a classical layered security mechanism.

Implementing this security scheme at each application level is not feasible because the change will interfere in each communication program in each sensor. The best way to overcome this constraint is to implement it in the kernel that leads to an overall security control.

IV. SARM DESCRIPTION

We would like with SARM to fine-tune security means as best as possible taking into account the risk of the current application environment and the performance of the system especially regarding the optimization of its energy consumption. Thereby, our system differs from others by its [2]:

a) Autonomic computing security looped system

b) Dynamic and evolving security mechanisms related to context-monitoring

c) Explicit energy consumption management

The concept of isolating various functions and restricting their access to specific system can also be applied to security in wireless environment integrated in the operating system itself. The best way to overcome the non realistic constraint of implementing the framework in each communication program is to integrate it in the kernel and consequently having an overall security control. Thus, all communication programs go through SARM at some stage in order to gain access to communication resources.

The key challenge of SARM is the adaptation of Reference Monitor (RM) [3] concept for wireless communication and beyond data access control. The goal of a RM is to enforce security by forcing all processes and also to prevent applications from accessing any data but only through the reference itself. The security kernel is managed by security policies. We have also chosen to apply the autonomic computing security pattern [15] to design SARM by dividing it into a functional unit and a monitoring unit. In addition, localized trust [17] or distributed trust [18], [19] and [20] are good paths to explore because in some cases they generate low computing charge (less energy consumption) and give better results. Thereof, we are fitting perfectly the context of WSN.

In [2], we could find all information about SARM high-level components view.

A. WSN- SARM

To validate SARM, we have applied an adapted version of SARM, called WSN-SARM, to the application domain of wireless sensor network.

1) Application Domain Main Problem

In Wireless Sensor Networks (WSN), one of the main constraints is to minimize energy consumption in order to maximize the lifespan of the network.

We send messages to the BS in a hop-by-hop routing method. While this method searches to minimize the overall network utilization of energy, since the power cost is in function of distance to the power of a parameter ranged from 2 to 5.

This heavy load of traffic on nodes near the BS brings them to deplete their energy rapidly. Thereby, it is a bottleneck region for the network. Unfortunately, when too many of those nodes run out of energy, the BS becomes disconnected from the network, and putting the network down while there may be plenty of energy remaining in nodes away from the BS. Therefore, it seems that energy

 ISBN: 978-1-61208-010-9

load balancing is a particularly promising way of maximizing the survivability of the network.

Another problem that challenges all proposed solution is sinkhole attack which is a node that does not retransmit any received packet.

The goal of this validation is to show that SARM adapts security as efficiently as possible by:

a) keeping an appropriate level of security depending on the context ;

b) whilst maximizing the overall reliability;

c) and minimizing the power consumption.

2) Metrics

Energy metrics are Packet loss ratio that affects energy loss per node and the whole network energy loss which is important to evaluate energy efficiency at transport protocol for any application.

Assuming dropped packets have a direct relation with energy depletion, the energy loss per node can be measured by [16]:

$$E(i) = \frac{\text{nbr of packets dropped by node}}{\text{total nbr packets received by node}}$$

Whereas the energy loss for the whole network can be calculated by total number of packet received by:

$$F_{network} = \frac{\text{nbr of packets dropped by the network}}{\text{total nbr of packets received by BS}}$$

Reliability of the entire network is defined as:

$$R_{network} = \frac{\text{nbr of packets received by BS}}{\text{total nbr packets Send by all nodes}}$$

We can show easily that $R_{network} = 1/(E_{network} + 1)$

3) WSN-SARM Description

In Fig. 1, we describe module by module, how SARM is applied to the application domain of our validation, becoming the WSN-SARM version.

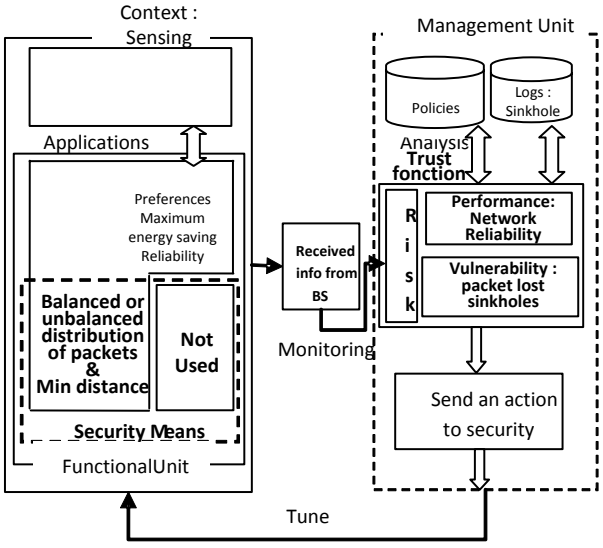

Figure 1. WSN-SARM Modules

First of all, the security means, which can be tuned by SARM, are uniform packet repartition or unbalanced neighbors packet repartition or a set of suboptimal routing paths. The application preference is to maximize the usage time whilst keeping enough security. The gathering context module is used to collect and distribute trust values between the Base Station and Nodes (sensors). These values represent the trust of a sensor about its neighbors. They are summarized in Table I.

TABLE I. BEHAVIOR AND RECOMMENDED VALUE SENT BY BASE STATION TO SENSOR UNDER SINKHOLE ATTACK

Sensor Behavior over neighbors	Recommended value to Sensor
Normal	The packet is received (1)
Sinkhole to neighbors' by not sending packet	The packet is lost (-1)

The values are sent to the management unit for analysis using a Trust Function (TF) that will assert the fact which algorithm has to be used. In addition, the performance is fixed as energy saving in accordance with Application Preference, which is lifespan maximizing.

Each Sensor sends packets uniformly to a number of Sensors within a define range according to thresholds used as policy. Thanks to its context gathering module the TF has all information to evaluate the trust.

The management unit will integrate the Trust Function TF that predicts whether or not to use uniform or unbalanced connections depending on the **output** of the TF depending on historical **values** $v_{i,i}$ (i packets) sent by the BS to sensor z about his neighbor sensor j within defined range.

- $T_j^z(v_{i,j}) = \frac{\sum_{i=1}^{N} v_{i,j}}{N}$ [$T_j^z(v_{i,j})$: trust of sensor z in sensor j and v_i are sent by BS as ACK, N : number of all packets sent by sensor z and received by BS]
- Threshold = rand()

For all j sensors

if ($T_j^z(v_{i,j}) > 0$

TF is the summation of all positive Trust over j neighbors

if (TF ==0)

then {we send uniformly}

else{TF> **threshold**}

then {we send the packet to sensor j}

End for

V. IMPLEMENTATION AND VALIDATION METHODOLOGY

We have implemented WSN-SARM and validated it in a Sensor wireless network simulation developed with AnyLogic, which is a simulation tool that supports all different simulation methodologies: System Dynamics, Process-centric, and Agent Based modeling. It is based on Real-time UML and Java object-oriented language.

A. Model Set-up

Setting up our security model using table 1, one can take advantage of state charts to control the behavior of Sensors. Using AnyLogic as implementation platform agents and especially state-charts can be programmed very conveniently. In particular modifications and/or extensions of the final model can be handled in a simple way.

In Fig. 2, each Agent (Sensor) starts simultaneously in a "Transmission" state in the "SensorStateR" and "Trust function" state-charts. The Agents are switched to their relative state (Sinkhole, Base Station, Sensors). They are then added to a list of the sensor whenever they are within his range.

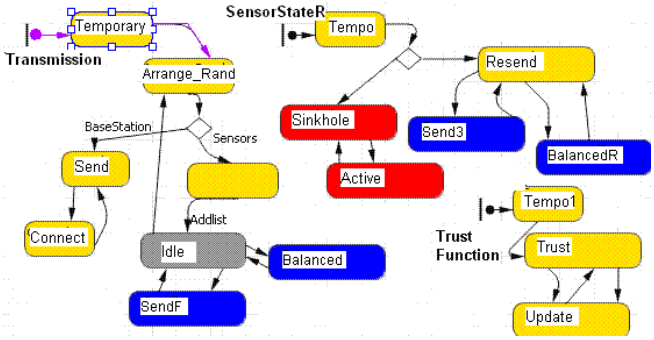

Figure 2. State-charts: "Transmission" of agent "SensorStateR" and "TF"

In Fig. 2, each Agent (Sensor) starts simultaneously in a "Transmission" state in the "SensorStateR" and "Trust Function" state-charts. The Agents are switched to their relative state (Sinkhole, Base Station, Sensors). They are then added to a list of the sensor whenever they are within his range.

We used Agents having one of the following behaviors:

a) Normal state and

b) Sinkhole

Each Agent is then processed depending on the decision of the monitor unit to choose a security mean or not. Therefore, the Agent transits to another state depending on the transition conditions or stand in the same state. When completing the transfer, the Agent returns to its initial state and so on. The state-chart Trust update the trust each time the Base Station sends an Ack. Of course, the BS is not limited in energy and thus is not subject to any sinkhole attack.

B. Validation Methodology

In our experiments, we have validated our proposed solution and analyzed the extended performance under a range of various scenarios.

We have carried out simulations under 0%, 20% and 50% sinkhole attackers. Furthermore, the network topology was set to random spreading or arranged uniform spreading of sensors. We have taken as a reference uniform packet distribution over the neighbors. In addition, a Time-To-Live TTL counter is used to avoid that a packet stay forever in the network and to guarantee that the consumed energy is limited to a maximum value when a packet is sent from the farthest sensor to the BS.

To minimize the transit delay and the energy consumption, we have also introduced suboptimal routing paths as paths that have the shortest Euclidian distance to the BS. Indeed, if the topology of sensors is uniformly distributed and the sensors aren't in the border of the square, there are 3 possible sensors that have the shortest distance to the BS.

Normally, the BS is in the middle of the network to minimize the distance to the farthest sensor. Additionally, 90 degree sector antennas are used to cover each of four squares to lengthen the BS range and minimizing the energy consumption. Sector directional antennas can be also added to sensors to take advantage of this technique in term of energy consumption [21] Therefore, we do not lose any generality if we put the BS in the upper left side of the square; rather we gain in survivability of WSN.

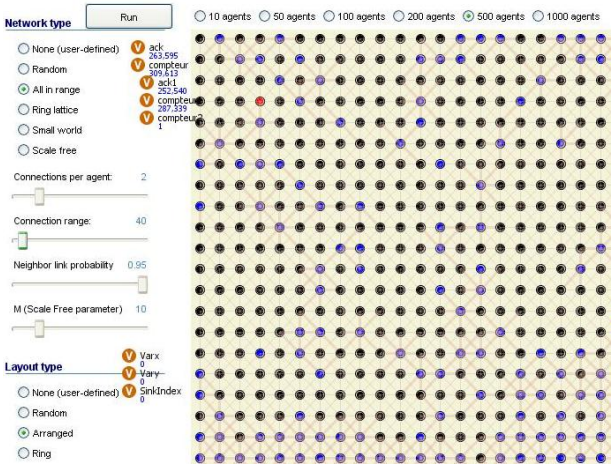

Figure 3. Animation interface of Arranged WSN-SARM

Fig. 3 shows a very powerful animation interface using AnyLogic. The BS is placed in the upper left side of the square.

Arranged sensors means that they are placed in an equidistant manner as depicted in Fig. 3. Random sensors

repartition means that the sensors are physically placed in a random manner.

All sensors are over spread over a square topology of 520m side length, and operating over one day of simulation time. In our simulations, we considered that the Base station was taken at the origin. The coverage of the Base Station is over the entire network. We fix the connection number of neighbors from 1 to 7. Indeed, depending on the topology of the network (arranged or random distributed sensors positions), each sensor was configured to have a maximum communication range equal to 50 meters. We deployed the Sensors in an incremental mode, from S_1 to S_n. The number of sensors can be selected from 10 to 1000 and their arrangement can be selected between arranged uniformly or randomly.

VI. RESULTS ANALYSIS

During our analysis, we firstly studied the performance of WSN-SARM in the defined scenarii where sensors were arranged uniformly or at random. The performance metrics are network Reliability Ratio and overall network Energy loss within the constraints:

a. Thanks to TTL almost the same average energy consumption for any packet and
b. Balancing overall traffic over all the neighbors to guaranteed the network survivability.

Secondly, we studied long-run convergence of TF used in WSN-SARM.

We have depicted in Fig.4 and Fig. 5 the results of the simulation of WSN-SARM and uniform traffic balancing under respectively 0%, 20% and 50% of sinkhole attackers. We can easily conclude that SARM is largely better than uniform balancing. A ratio of 10 is reached within short time. Indeed, we have the obtained the desired effect of the feedback mechanism and Trust Function implemented in WSN-SARM.

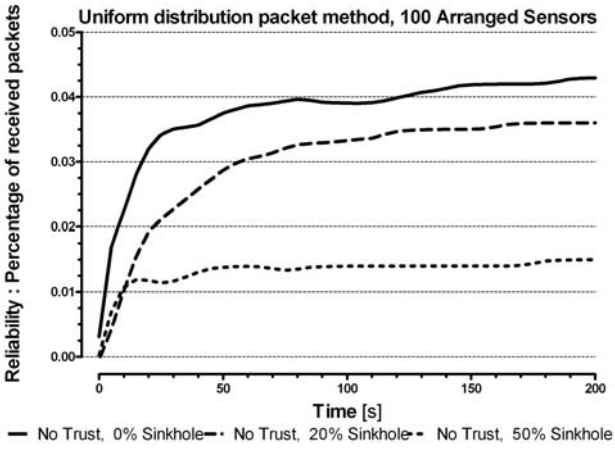

Figure 4. Reliability of WSN-SARM under different sinkhole attacks.

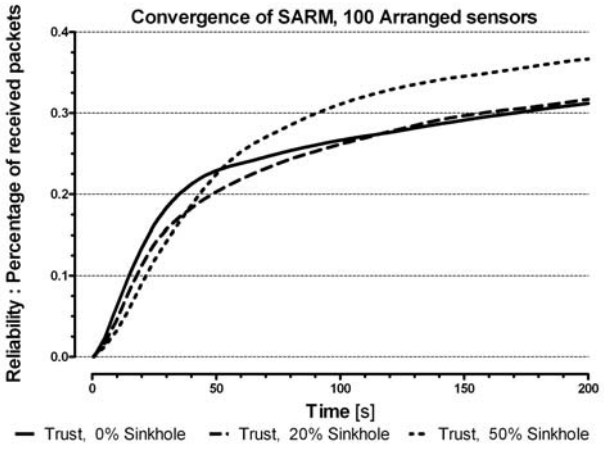

Figure 5. Reliability of WSN-SARM under different sinkhole attacks.

For comparison purpose, we plotted the WSN-SARM under 20% of sinkhole attackers using our Trust Function and without trust (No Trust) in Fig. 6. We have used all suboptimal routing paths to the Base Station. The results clearly demonstrate that the convergence is boosted to reach 100% of Network Reliability.

Remark: WSN-SARM constitutes a good algorithm to detect any sinkhole with the help of the Base Station and eliminates it from its connections. We can see that when the Sinkhole attackers are detected and inhibited by the message sent by BS to all sensors, the reliability of the network is raised and especially in case of 50% sinkhole attackers (many attackers) get a significant step for its convergence. Therefore, simulation shows that our Framework is efficient in this context and is tuning to achieve the best trade-off between security in one side and, energy loss and reliability in other side.

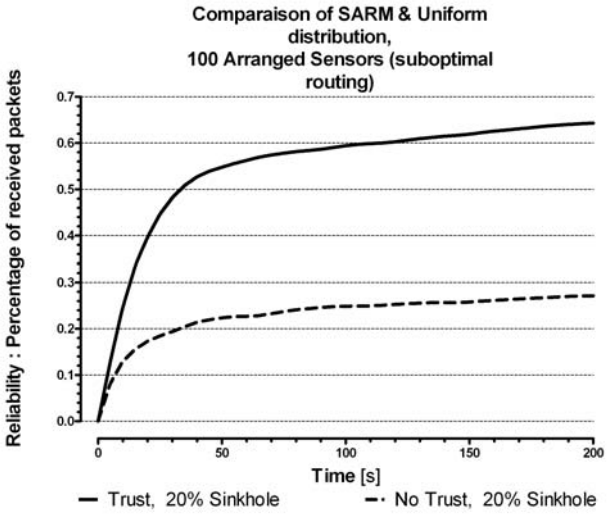

Figure 6. Reliability of WSN-SARM and reference.

We have noticed that there are significant differences between Trust Function used by WSN-SARM and uniform packet distribution reference in the case of arranged Sensors.

 ISBN: 978-1-61208-010-9

We have an average ratio of 2.4 between the two cases. The convergence is also boosted for WSN-SARM.

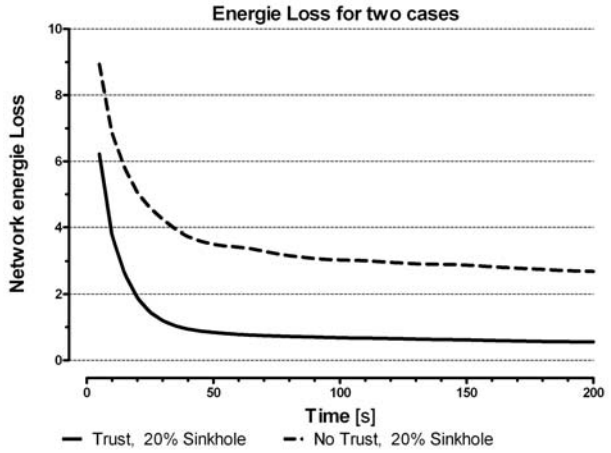

Figure 7. Network Energy Loss for WSN-SARM and uniform balancing

We have depicted in Fig. 7 energy loss of WSN-SARM using Trust Function and a reference case without trust under 20% of sinkhole attackers. The convergence is rapid and the overall Energy loss is very rapidly minimized within WSN-SARM.

Since long-run simulation has a Network reliability of 1 (estimated with an error of less than 0.1%), the system convergence is guaranteed.

All the results show clear advantages of WSN-SARM under sinkhole attackers thanks to the looped system and the Trust Function efficiently.

VII. CONCLUSION AND FUTURE WORK

We have proposed a Security Adaptation Reference Monitor (SARM) based on the Reference Monitor concept and the Autonomic Computing Security pattern to support both context monitor and behavior control. The results show that WSN-SARM copes with reliability and network Energy loss under sinkhole attack even at 50% of attackers. Indeed, WSN-SARM constitutes a good Platform to detect within the Base Station any sinkhole and eliminates it from its connections. The results clearly show that our platform copes with reliability and security of the network under sinkhole attack, by efficiently tuning the adequate means whilst minimizing energy loss.

These results encourage us to further research on other strategies that could automatically optimize the trade-off between security and energy consumption in other important application domains, such as mobile wireless sensor networks under other attacks.

REFERENCES

[1] J. Ibriq and I. Mahgoub, “Cluster-based routing in wireless sensor networks: Issues and challenges” Proceedings of the International Symposium on Performance Evaluation of Computer and Telecommunication Systems, July 25-29, 2004, San Jose, California, USA

[2] T. El Maliki and J.-M. Seigneur “A Security Adaptation Reference Monitor (SARM) for Highly Dynamic Wireless Environments” The International Conference on Emerging Security Information, Systems, and Technologies SECURWARE July 2010

[3] J. Anderson, “Computer Security Technology Planning,” http://seclab.cs.ucdavis.edu/projects/history/papers/ande72.pdf, 1972.

[4] Hiren Kumar Deva Sarma, Avijit Kar, “Security Threats in Wireless Sensor Networks”, IEEE 2006

[5] E. Shi and A. Perrig, “Designing Secure Sensor Networks,” Wireless Commun. Mag., vol. 11, no. 6, pp. 38–43, Dec. 2004

[6] Yun Zhou; Yuguang Fang; Yanchao Zhang, “Securing Wireless Sensor Networks: A Survey”, IEEE Communications Surveys & Tutorials, Vol:10, Issue 3, PP: 6 –28, Third Quarter 2008.

[7] C. Hager, “Context Aware and Adaptive Security for Wireless Networks,” PhD thesis, Virginia Polytechnic Institute and State University, 2004.

[8] M. Lacoste, G. Privat, and F. Ramparany. “Evaluating Confidence in Context for Context-Aware Security,”. European Conference on Ambient Intelligence (AmI'07), 2007.

[9] J. Al-Muhtadi, D. Mickunas, and R. Campbell, “A Lightweight Reconfigurable Security Mechanism for 3G/4G Mobile Devices,” IEEE Wireless Communications, 9(2):60–65, 2002.

[10] E2R Deliverable D2.2., “Equipment Management Framework for Reconfiguration: Architecture, Interfaces, and Functions,” Dec. 2005.

[11] T. Jarboui, M. Lacoste, and P. Wadier, “A Component-Based Policy-Neutral Authorization Architecture,” French Conference on Operating Systems (CFSE), 2006.

[12] J.-M. Seigneur, “Trust, Security and Privacy in Global Computing,” PhD Thesis, 2005.

[13] Olivier Powell, Jean-Marc Seigneur and Luminita Moraru,“Trustworthy Forwarding Sensor Networks Information to the Internet” The International Conference on Emerging Security Information, Systems, and Technologies (SECURWARE 2007).

[14] Asad Amir Pirzada and Chris McDonald “Circumventing Sinholes and Wormholes in Wireless Sensor Networks” the Int. Workshop on Wireless Ad-hoc Networks, 2005.

[15] D.M. Chess, C.C. Palmer, and S.R. White, “Security in an autonomic computing Environment,” IBM Systems Journal, VOL 42, N1, 2003.

[16] Anylogic 38M. A. Rahman, A. E. Saddik and W. Gueaieb, “Wireless Sensor Network Transport Layer: State of the Art”, Sensors, Springer-Verlang Berlin Heidelberg, 2008.

[17] C. Davis, “A localized trust management scheme for ad-hoc networks,” Proc. 3rd International Conference on Networking (ICN'04), Mar. 2004.

[18] L. Eschenauer, V. Gligor, and J. Baras, “On Trust Establishment in Mobile Ad-Hoc Networks,” Proc. 10th International Workshop of Security Protocols, Springer Lecture Notes in Computer Science (LNCS), Apr. 2002.

[19] A. Rahman and A. Hailes, “A Distributed Trust Model,” New Security Paradigms Workshop 1997, ACM, 1997.

[20] X. Titi, Tewfiq EL MALIKI, Jean-Marc Seigneur, “Trust-Based Hotspot Selection” IADIS International Jounal onComputer Science and Information System. V V,2 , 2010

[21] E. Felemban, S. Vural, R. Murawski, E. Ekici, K Lee, Y. Moon, and S. Park, ”SAMAC: A Cross-Layer Communication Protocol for Sensor Networks with Sectored Antennas” Mobile Computing, IEEE Transactions on, August 2010

 ISBN: 978-1-61208-010-9