International Scholarly Research Network
ISRN Communications and Networking
Volume 2012, Article ID 528374, 10 pages
doi:10.5402/2012/528374

Research Article

A Security Adaptation Reference Monitor for Wireless Sensor Network

Tewfiq El-Maliki[1] and Jean-Marc Seigneur[2]

[1] *Information Technology Department Hepia, University of Applied Sciences and Arts Western Switzerland, 1202 Geneva, Switzerland*
[2] *Advanced Systems Group, University of Geneva, 1211 Geneva 4, Switzerland*

Correspondence should be addressed to Tewfiq El-Maliki, tewfiq.elmaliki@hesge.ch

Received 14 March 2012; Accepted 19 April 2012

Academic Editors: K. Teh, Y. M. Tseng, and A. Vaccaro

Security in Wireless Sensor Network has become a hot research topic due to their wide deployment and the increasing new runtime attacks they are facing. We observe that traditional security protocols address conventional security problems and cannot deal with dynamic attacks such as sinkhole dynamic behavior. Moreover, they use resources, and limit the efficient use of sensor resources and inevitably the overall network efficiency is not guaranteed. Therefore, the requirements of new security mechanisms must be addressed in a flexible manner. Indeed, there is a lack of generic security adaptation protocols to deal with extremely dynamic security conditions and performances in a context of Wireless Sensor Network where reliability is a critical criterion for many applications. This paper proposes our Security Adaptation Reference Monitor for Wireless Sensor already validated in proximity-based wireless network. It is based on an autonomic computing security looped system, which fine-tunes security means based on the monitoring of the context. Extensive simulations using agent-based approach have been conducted to verify the performance of our system in the case of sensor network in the presence of sinkhole attacks. The results clearly show that we are efficient in terms of survivability, overall network utilization, and power consumption.

1. Introduction

A Wireless Sensor Network (WSN) consists of a large number of low-power, and multifunction sensor nodes that communicate as one hope, multihop, or cluster-based models to send data to one or many base stations (BSs) through wireless links [1]. These BSs are highly enriched with a large amount of energy. WSNs represent a challenging and an interesting research area due to the constraints involved. The small size of the sensors and the networking capability increase the appeal of WSNs for use in daily life. Distributed computing and routing could be well applied in case of multihope and cluster-based models. These capabilities enable WSNs to provide significant advantages for many applications that were not possible in the past. The WSN 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 unique properties of WSNs increase flexibility and reduce user involvement in operational tasks. Battlefield surveillance, forest fire detection, and smart environments are some well-known applications. Since the nodes in WSN are battery operated and have a limited lifetime to operate, there is a growing need of energy aware security algorithm performing low computational load to preserve the network lifetime.

WSN involves a huge number of interactions with its environment where security is also difficult to ensure against dynamic changing attacks. Indeed, it is highly challenging to maintain the overall security at the highest level due to the configuration complexity and the runtime changing context. In addition to the security challenge, data transfer in WSNs is more susceptible to loss due to the nature of sensors (power and processing, etc.) and the high error rate of wireless links. Moreover, sinkhole attackers 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.

In general, most applications cannot operate in case of high packet loss. Thus, reliability, being a key issue in sensor networks, is definitely one of the important criteria to evaluate the quality of WSNs. Accordingly, the concept that must cope with this new security challenge in terms of availability has to be based on dynamic adaptation security system to satisfy an overall performance such as network reliability and energy loss. We have already proposed a generic Security Adaptation Reference Monitor (SARM) as a compelling solution for such problems [2]. In this paper, we will apply it for WSN under 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.

2. Related Work

The concept of adaptive security in wireless network is used to mitigate the consequences of a substantial number of runtime threats, when it does not completely eliminate them.

Many systems rated at the higher levels of security for data are implemented according to the reference monitor concept. First introduced by 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.

Reference [4] has also proposed an adaptive security application in wireless ad hoc and sensor networks, where network conditions play a role in choosing relevant security mechanisms at runtime.

Chiang et al. [5] have proposed an approach to increase the availability of WSNs but they need additional hardware which generates more cost. Consequently, a suitable security service is must be 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 the sensor node hardware and the deployment properties [6–8].

All aspects of the wireless sensor network are being examined including secure and efficient routing [9–12], data aggregation [13–16], and group formation [17, 18]. Although there are some existing architectures for WSN that partially solve these problems, it is still possible to point out the neglected aspects that can be considered crucial for creating a satisfactory security system.

Other security issues include [19] security-energy assessment, data assurance, survivability, trust, end to end security, security and privacy support for data centric sensor networks (DCS), and node compromise distribution. It is very important to study these areas due to the sensor network's special character, such as battery limitation, high-failure probability nodes, easier compromised nodes, and unreliable transmission media. Until now, there have been only a few approaches available, and more studies are needed in these areas. Furthermore, trust [20] is a good path to explore because it gives in some cases better results.

3. Motivation for Our Framework

We argue that the spare processing and transmission resources are wasted in sensor environments if security is overprovisioned. 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 [21], context-aware access control systems [22], and security architectures [23]. This prompted us for the implementation of a completely reconfigurable architecture [24], which is adapted to terminal and network context variability, particularly in the security field [25]. Seigneur [20] has introduced autonomic security pattern in his security design but only at the authentication level.

Flexible security mechanisms are needed to respond to new types of attacks and to meet different network requirements by setting specific protection. The required flexible security assessment can be achieved by introducing a generic autonomic computing security framework according to Chess in [26, 27]. He describes the importance of automatically configuring the security of various parts of the system and automatically making various security trade-offs according to the value of the assets being protected and the cost of the measures being employed to protect them.

Because of the following limitations [17], layered security solutions are inadequate and/or inefficient:

(i) Redundant Security Provisioning: systematic security at each layer consumes more resources than necessary;

(ii) Nonadaptive Security Services: because attacks on a WSN come from any layer and any protocol, a countermeasure scheme at only one layer is unlikely to guarantee security all the time;

(iii) Power Inefficiency: energy efficiency must be addressed because it is a crucial issue in WSN. The power efficiency design cannot be addressed completely at any single layer in the networking stack.

In WSN case, the sensors have limited resources in terms of energy. Since the spending of energy dramatically increases with the range of transmission, the sensors usually forward their messages to a Base Station (BS) [28] in a hop-by-hop fashion. It is quite easy for an attacker as a sinkhole [29] to defeat the WSN purpose by dropping messages when received rather than forwarding them or to consume energy of other sensors by requesting them to continuously send information.

As mentioned earlier, it is highly challenging to keep the overall security due to the configuration complexity and the runtime changing context. Moreover, assuring reliable data delivery between the sensor nodes and the BS in wireless sensor networks is also a challenging task as it affects the ability to sense event. In fact, the reliability of data transfer is impacted by data loss due to nature of sensors in addition to high error rate of wireless links. The problem of achieving reliable communication between nodes is further aggravated by the presence of sinkhole attackers whenever they are changing dynamically their behavior. Therefore, the most crucial constraint in WSN, which is reliability, cannot be guaranteed.

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. Thereby, the concept that must cope with this new security challenge in term of availability has to be based on dynamic adaptive security system to satisfy an overall performance such as network reliability and energy loss.

Thus, to lengthen the lifetime of wireless sensor network, an efficient protocol needs to support reliable network in most energy efficient manner under sinkhole attacks.

We propose a generic framework called Security Adaptation Reference Monitor (SARM) as a compelling solution for this problem, because it is a looped system developed especially for highly dynamic wireless network.

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 which leads to an overall security control.

Since the following constraints: energy limitation, decentralized collaboration, and fault tolerance are imposed in sensor networks, algorithms for network security tend to be quite complex and usually defy analytical methods that have been proved to be fairly effective for traditional networks. Furthermore, applying new methods and mechanisms in real networks is very difficult and not operational. It appears that simulation is the only feasible approach to the quantitative analysis of new algorithms in the wireless networks.

We propose SARM for wireless environments based on an autonomic computing security looped system, which fine-tunes security means based on the monitoring of the context including the application environment and energy consumption aspects. It is aimed to offer a global adaptation security scheme for any application instead of a classical layered security mechanism.

4. SARM Description

We would like with SARM to fine-tune security means as best as possible taking into account the risk of the current 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.

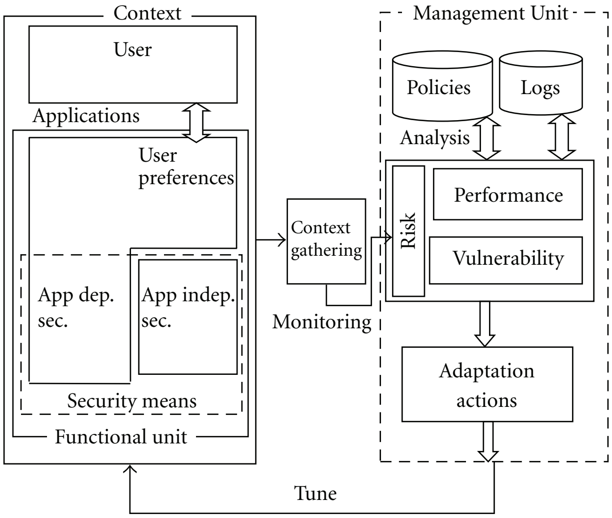


Figure 1: SARM components high-level view.

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 nonrealistic 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 users 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 [27] to design SARM by dividing it into a functional unit and a monitoring unit.

To reduce the system complexity and to make the system incremental, we propose a looped framework as introduced in [20] at the authentication level, that is, the system automatically tunes to its best configuration based on the current monitored context, thus avoiding any static decision making. Hence, we split SARM into two units looped as a servo control system model to fine tune the adequate security measures/means, which we will discuss later. One unit called management or monitor unit is for monitoring the context by evaluating and analyzing risks, performances, and energy consumption, which are significant for detecting attacks and tuning the adequate security means using the second module called functional unit.

We have depicted in Figure 1 the different components of SARM and their interconnections.

Security means are defined as any algorithm or mechanism that could ensure security but it could also be a no security action when it is not necessary. It includes also the choice of the adequate network access too because some network communication technologies are more secure

Table 1: Characteristic data for the Mica2dot sensor platform: 3 V, 4 MHz, 915 MHz transceiver, and transmit power 5 dBm.

Field	Value
Effective data rate	12.4 kbps
Energy to transmit	59.2 μJ/byte
Energy to receive	28.6 μJ/byte

with higher energy consumption and others less secure with lower energy consumption. Security means can be application dependent such as a localized trust [30, 31] or a distributed trust [32] or application independent such as cryptographic protocols. Indeed, localized and distributed trusts are good paths to explore because they generate low-computing charge (less energy consumption) and give in some cases better results. Thereof, we are fitting perfectly the context of WSN.

Firstly, the application uses communication means. The default preferences related to the chosen application are taken. Secondly, the context gathering module will collect all information about the current context of the application. This information is sent to the Monitoring/Management Unit, which is responsible for all security analysis in accordance with the security policies based on log files in a first stage, risks, vulnerabilities, and energy consumption in a second stage. The Logs are used to store all the information about the system: mainly the security problems. Risks, performances, and energy consumption analysis with policies is a key issue in the framework because it is responsible for detecting a potential unsecure context, a probable energy wasting environment, and/or a very vulnerable application.

Thereby, the analysis could trade-off between all these constraints to choose an efficient action to tune the functional unit. Individual sensor nodes in a WSN have the inherent limitations in resources, which make the design of security procedures more complicated.

4.1. Sensors Energy Consumption. A typical sensor node processor is of 4–8 MHz, having 4 KB of RAM, 128 KB flash, and ideally 916 MHz of radio frequency. Each of these limitations is due in part to the two greatest constraints: limited energy and physical size [33]. Table 1 shows that receiving costs almost half the energy of sending.

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

4.2.1. Validation 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. Indeed, sensor nodes are usually battery powered [34–36]. In order to increase the lifetime of sensor networks, various energy saving schemes have been proposed.

One of known possibility for prolonging network lifetime is energy balancing, which is the approach that we have implemented in our framework SARM for WSN. In an energy balanced network, all the nodes deplete their energy at the same rate. It is an efficient method to implement a data-gathering algorithm for WSN's.

Indeed, a data-gathering WSN is deployed over a region to be monitored and when a sensor detects an event, it needs to report to the BS which is not limited in energy in our case study.

We send messages to the BS in a hop-by-hope 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.

Thus, it creates bottleneck region in the network. Unfortunately, when too many of those nodes run out of energy, the sink becomes disconnected from the network, This leads to put the network down while there may be plenty of energy remaining in nodes away from the sink. Therefore, it seems that energy balancing is a particularly promising way of maximizing the lifespan of networks accomplishing a data-gathering task.

Another problem that challenges all the proposed solution is sinkhole attack. Indeed, it compromises the balancing effect on the lifespan of any WSN. That's why a countermeasure is necessary in this case

We propose as an efficient solution our SARM with its feedback mechanisms and its Trust Function to balance the energy through all reachable nodes to overcome sinkhole attacks. Then, we compare it with simple equidistribution (uniform packet repartition) without any feedback.

4.2.2. Validation. 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 utilization,

(c) and minimizing the power consumption.

4.2.3. WSN-SARM Description. In Figure 2, we describe module by module, how SARM is applied to the application domain of our validation, becoming the WSN-SARM version.

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 distance 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 2.

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 or not. In addition, the performance

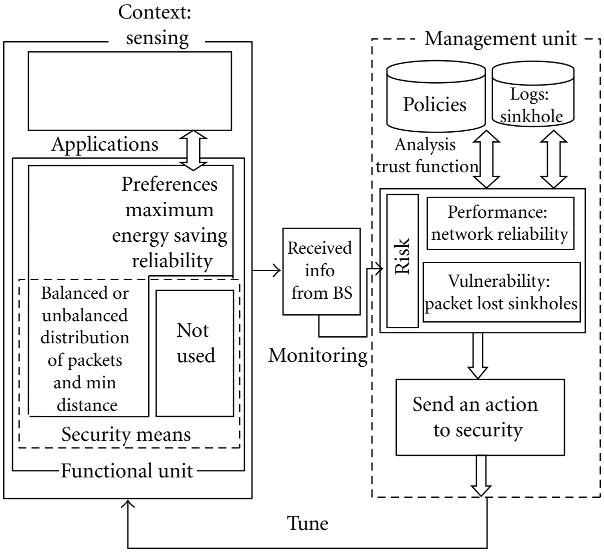


Figure 2: WSN-SARM Modules.

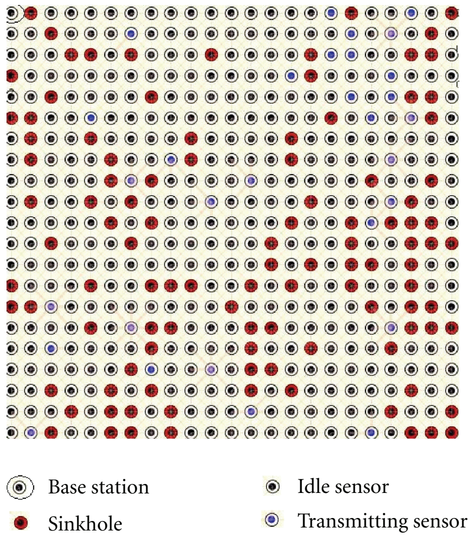


Figure 3: Context of WSN-SARM.

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 defined range according to threshold used as policy. Thanks to its context gathering module the Trust Function has all information to evaluate the trust. Figure 3 gives a representation of the context of each Sensor and behavior of some of them.

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* $v_{i,j}$ (i packets) sent by the BS to sensor z about his neighbor sensor j within defined range.

(i) $T_j^z(v_{ij}) = (\Sigma_{i=1}^{N} v_{ij})/N$ [$T_j^z(v_{ij})$: 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 the BS]

Table 2: 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)

(ii) Threshold = rand()

```
For all $j$ sensors
    if ($T_j^z(v_{ij}) > 0$)
        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
```

The system consists of one to many sensors with different behaviors that could change randomly. Therefore, we should have analyzed the overall system characteristics in a real world but that was very difficult. The complexity of analysis comes from the fact that every nodes acts independently from others. Therefore, our model will be studied using simulation tools in order to compare it with reference cases.

5. 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 (a.k.a. Discrete Event), and Agent-Based modeling. It is based on Real-time UML and Java object-oriented language.

5.1. Model Setup. The basic element of an Agent-Based model is the agent itself. By using an Agent-Based model, we have created a new class that behaves as Sensor. Each Sensor is associated to a given agent matching with its location. As a sensor is placed randomly, we have modeled its coordinates using X and Y random variables.

Setting up our security model using Table 2, we can take advantage of state chart by monitoring the behavior of agents. The state of our agents is controlled by state charts, which represents the exact behavior of sensors, as shown in Figure 4.

Setting up our security model using Table 2, 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.

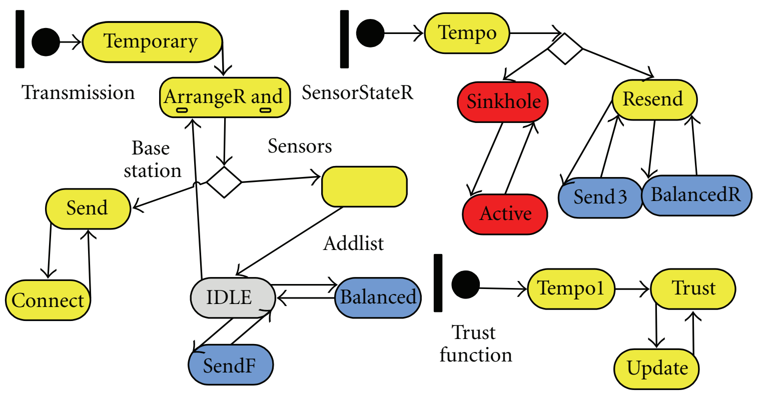


Figure 4: State-charts: "Transmission" of agents "SensorStateR"and "TF".

In Figure 4, 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,

(b) sinkhole.

Each agent is then processed depending on the decision of the monitor unit to choose a security means or not. Therefore, the agent could transit to another state or stand in the same state. When completing the transfer, the Agent returns to its initial state and so on. The state-chart trust updates 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 an attack by any sinkhole.

5.2. Validation Methodology. 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 all paths that have the shortest Euclidian distance to the BS. Indeed, if the topology of sensors is uniformly distributed and the sensors are not in the border of the square, there are 3 possible sensors that have the near-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 [37] 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.

In our experiments, we have validated our proposed solution and analyzed the extended performance under a range of various scenarios. All sensors are spread over a square (520 m of each side) topology and operating over one day of simulation time. In our simulations, we considered that the Base Station was taken at the origin. The Base Station coverage 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.

We have also used an algorithm in the Base Station to calculate for each sensor his suboptimal routing hops to the BS. It needs to send packet step-by-step power emission and could be implemented by a sector antenna.

The number of sensors can be selected from 10 to 1000 and their display can be selected between arranged uniformly or randomly.

Figure 5 shows a very powerful animation interface using AnyLogic. Note that the BS and sensors' forms are described in Figure 3. Arranged sensors means that they are placed in an equidistant manner as depicted in Figure 3. Random distributed sensors means that the sensors are placed physically in a random manner as depicted in Figure 5.

We carried out our experiments considering thirty cases. In each studied case, we ran our simulations with different conditions. Our performance evaluation was the result of different simulations.

5.3. 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.

Assuming dropped packets have a direct relation with energy wastage, the energy loss per node can be measured by [38]

$$E(i) = \frac{(\text{nbr of packets dropped by node})}{(\text{all packets rvd node})}. \tag{1}$$

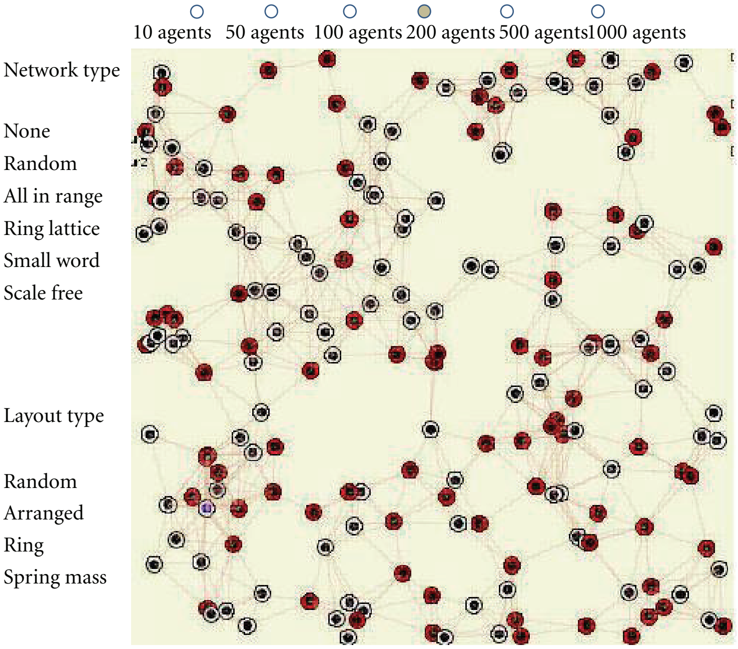


Figure 5: Animation interface and results of Random WSN-SARM.

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

$$E_{\text{net}} = \frac{(\text{nbr of packets dropped by net})}{(\text{all packets rvd BS})}. \tag{2}$$

Reliability of the entire network is defined as

$$R_{\text{net}} = \frac{(\text{nbr of packets rvd by BS})}{(\text{total packets send by all})}. \tag{3}$$

Please note, $R_{\text{net}} = 1/(E_{\text{net}} + 1)$ and rvd = received.

5.4. Scenarios. We have used three scenarios to validate our model. In our scenarios, sensors (agents) were divided in two categories.

A normal behavior, they are composed of x% of all sensors.

An energy wasting behavior sinkhole attackers are composed of $(1 - x)$% of all sensors.

In the first scenario, we fixed the percentage as

100% of normal behavior and

0% of sinkhole attackers.

In the second scenario, we fixed the percentages as

80% of normal behavior and

20% of Sinkhole behavior.

In the third scenario, we fixed the percentages as:

50% of normal behavior and

50% of sinkhole behavior.

6. Results Analysis

During our analysis, we firstly studied the performance of WSN-SARM in the three defined scenarios 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 the rapidity of convergence to 100% (how WSN-SARM tends to 1) and compared it to suboptimal routing paths.

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

For comparison purpose, we plotted the WSN SARM in Figure 6 and the uniform balancing (no trust: uniform distribution of parquets over neighbors) in Figure 7 for the same three predefined scenarios. We can easily conclude that SARM is largely better than uniform balancing; a ratio of 20 is reached in short time 50 s. Indeed, we have obtained the desire effect of the feedback mechanism of the SARM.

In Figure 8, we plotted the long-term convergence trend of SARM for the second scenario. Unfortunately, the convergence is very long due to the use of links with many hops. Moreover, in the second and third scenarios with respectively 20% and 50% of sinkhole attackers reliability of SARM is exceeding the case of 0% sinkhole because sensors within the Base Station detect any sinkhole neighbor and eliminate it from its connections.

For comparison purpose, we plotted the WSN-SARM under 20% of sinkhole attackers (the second scenario) using

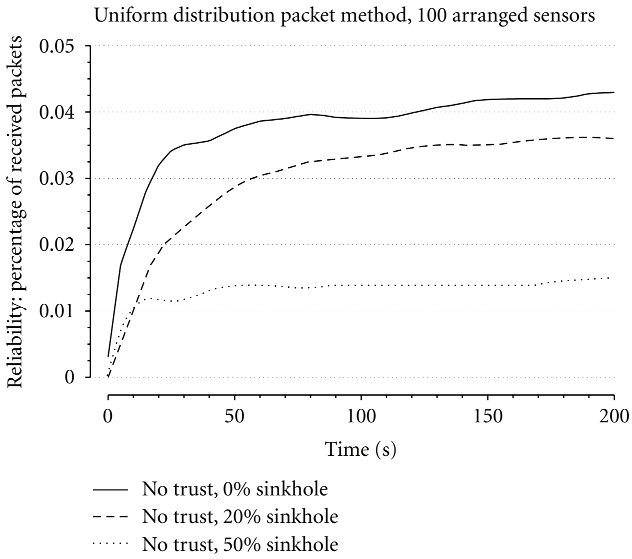


FIGURE 6: Reliability of references for the 3 scenarios.

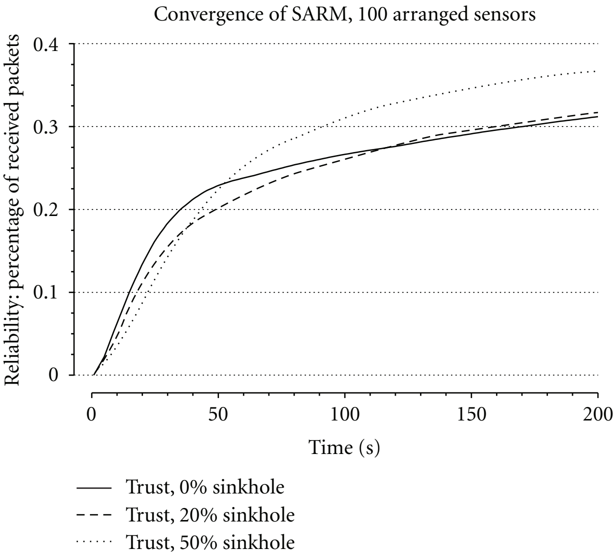


FIGURE 7: Reliability of WSN-SARM for the 3 scenarios.

our Trust Function and also without trust in Figure 9. We have used all suboptimal routing paths to the Base Station. The results clearly demonstrate that the convergence is boosted.

In Figure 10, we have depicted the network energy loss as defined by our metrics. We have an average ratio of 5.2 between the two cases. We can conclude that using SARM with trust Function converges rapidly than without trust. Thereby, the reliability is guaranteed and the overall energy cost is minimized even under a number of 20% of sinkhole attackers.

Please note: there are significant differences between Trust used by WSN-SARM and uniform packet distribution reference.

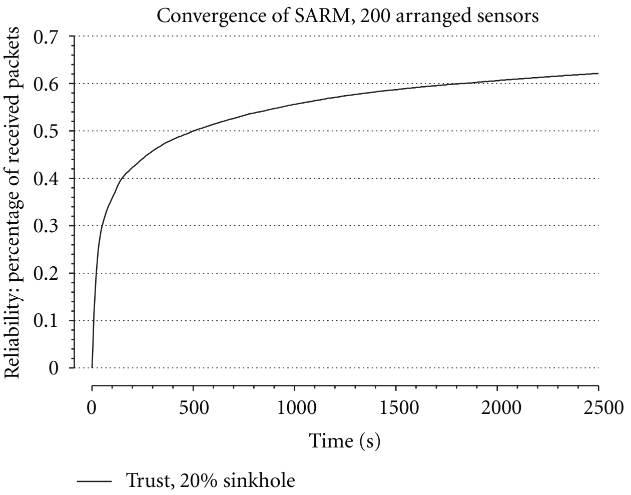


FIGURE 8: Long-term reliability of WSN-SARM for 2nd scenarios.

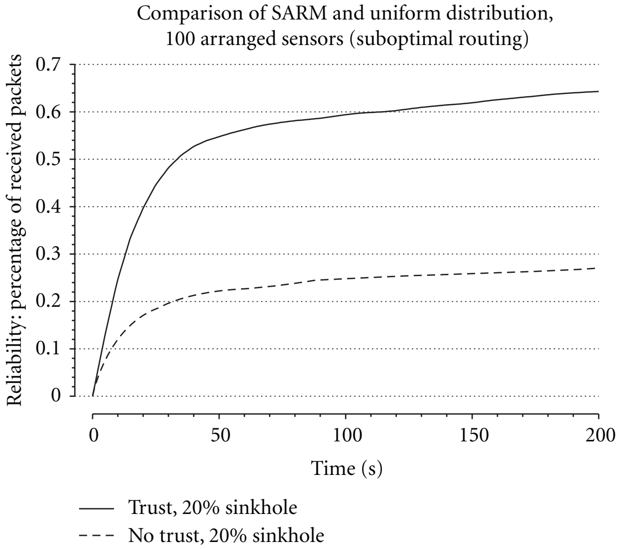


FIGURE 9: Reliability of WSN-SARM for the 2nd scenario.

We have depicted in Figure 11 the proof that WSN-SARM is converging to 100% in term of reliability and to a 0% in term of network energy loss.

All the results show clear advantages of WSN-SARM arranged sensor network or random sensor network even at 50% of sinkhole attackers. We can conclude that our security monitor helps the WSN to operate even under 50% of sinkhole attackers thanks to the looping system connected to the context gathering monitor and the Trust Function.

7. Conclusion and Future Work

We have proposed a Security Adaptation Reference Monitor based on the reference monitor concept and the autonomic computing Security pattern to support both context monitor and behavior control. This paper presents also the validation

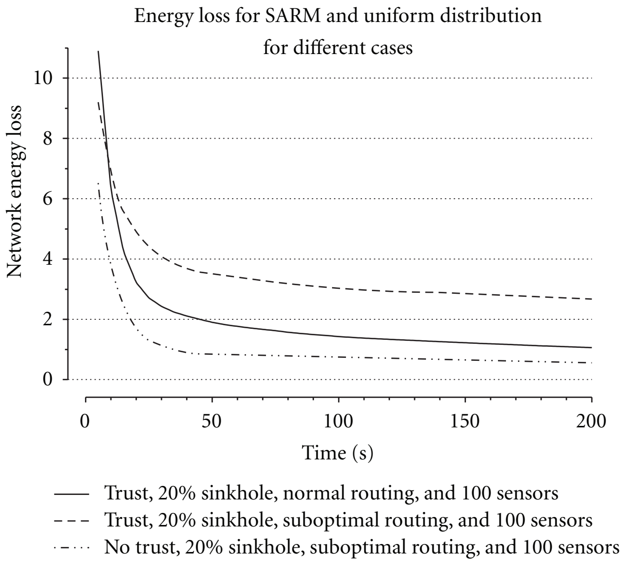


Figure 10: Energy loss of WSN-SARM for the 2nd scenario and no trust.

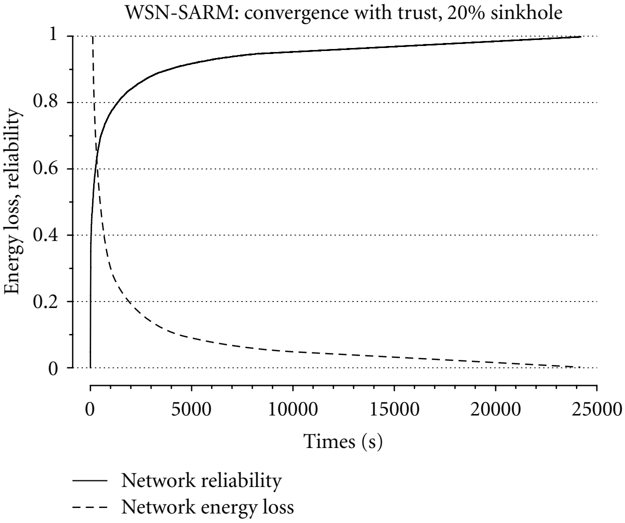


Figure 11: Reliability and energy loss of WSN-SARM for the 2nd scenario.

of SARM in WSN. The results clearly 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 within the Base Station to detect any sinkhole and eliminate it from its connections and put it into log file, thanks to the context gathering monitor and the looped regulation system. Therefore, we show that our framework is efficient in this context and is tuning to achieve the best trade-off between security and performance according to application preferences. In addition, the network is well energy balanced.

These results encourage us to further research on other strategies that could automatically optimize the trade-off between security and energy consumption under other important attacks.

References

[1] J. Ibriq and I. Mahgoub, "Cluster-based routing in wireless sensor networks: issues and challenges," in *Proceedings of the International Symposium on Performance Evaluation of Computer and Telecommunication Systems*, San Jose, Calif, USA, July 2004.

[2] T. El Maliki and J. M. Seigneur, "A security adaptation reference monitor (SARM) for highly dynamic wireless environments," in *Proceedings of the 4th International Conference on Emerging Security Information, Systems and Technologies (SECURWARE '10)*, pp. 63–68, July 2010.

[3] J. Anderson, "ComputerSecurity Technology Planning," http://seclab.cs.ucdavis.edu/projects/history/papers/ande72.pdf, 1972.

[4] C. Chigan, Y. Ye, and L. Li, "Balancing security against performance in wireless Ad Hoc and sensor networks," in *Proceedings of the 60th IEEE Vehicular Technology Conference (VTC '04)*, pp. 4735–4739, ETATS-UNIS, September 2004.

[5] M. W. Chiang, Z. Zilic, K. Radecka, and J. S. Chenard, "Architectures of increased availability wireless sensor network nodes," in *Proceedings of the International Test Conference 2004*, pp. 1232–1241, October 2004.

[6] H. K. D. Sarma and A. Kar, "Security threats in wireless sensor networks," in *Proceedings of the 40th Annual IEEE International Carnahan Conference on Security Technology (ICCST '06)*, pp. 243–251, 2006.

[7] E. Shi and A. Perrig, "Designing secure sensor networks," *IEEE Wireless Communications*, vol. 11, no. 6, pp. 38–43, 2004.

[8] Y. Zhou, Y. Fang, and Y. Zhang, "Securing wireless sensor networks: a survey," *IEEE Communications Surveys & Tutorials*, vol. 10, no. 3, pp. 6–28, 2008.

[9] J. Deng, R. Han, and S. Mishra, "INSENS: intrusion-tolerant routing in wireless sensor networks," Tech. Rep. CU-CS-939-02, Department of Computer Science, University of Colorado, 2002.

[10] B. Karp and H. T. Kung, "GPSR: greedy perimeter stateless routing for wireless networks," in *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MOBICOM '00)*, pp. 243–254, ACM Press, August 2000.

[11] P. Papadimitratos and Z. J. Haas, "Secure routing for mobile Ad Hoc networks," in *Proceedings of the SCS Communication Networks and Distributed System Modeling and Simulation Conference (CNDS '02)*, 2002.

[12] S. Tanachaiwiwat, P. Dave, R. Bhindwale, and A. Helmy, "Secure locations: routing on trust and isolating compromised sensors in location-aware sensor networks," in *Proceedings of the 1st International Conference on Embedded Networked Sensor Systems (SenSys '03)*, pp. 324–325, ACM Press, November 2003.

[13] D. Estrin, R. Govindan, J. S. Heidemann, and S. Kumar, "Next century challenges: scalable coordination in sensor networks," in *Proceedings of the Mobile Computing and Networking Conference*, pp. 263–270, 1999.

[14] L. Hu and D. Evans, "Secure aggregation for wireless networks," in *Proceedings of the Symposium on Applications and the Internet Workshops (SAINT '03 Workshops)*, p. 384, IEEE Computer Society, 2003.

[15] S. Madden, M. J. Franklin, J. M. Hellerstein, and W. Hong, "Tag 'a tiny aggregation service for Ad-Hoc sensor networks'," *ACM SIGOPS Operating Systems Review*, vol. 36, pp. 131–146, 2002.

[16] B. Przydatek, D. Song, and A. Perrig, "SIA: secure information aggregation in sensor networks," in *Proceedings of the 1st International Conference on Embedded Networked Sensor Systems (SenSys '03)*, pp. 255–265, November 2003.

[17] M. Xiao, X. Wang, and G. Yang, "Cross-layer design for the security of wireless sensor networks," in *Proceedings of the 6th World Congress on Intelligent Control and Automation (WCICA '06)*, pp. 104–108, June 2006.

[18] S. Rafaeli and D. Hutchison, "A survey of key management for secure group communication," *ACM Computing Surveys*, vol. 35, no. 3, pp. 309–329, 2003.

[19] X. Chen, K. Makki, K. Yen, and N. Pissinou, "Sensor network security: a survey," *IEEE Communications Surveys & Tutorials*, vol. 11, no. 2, pp. 52–73, 2009.

[20] Seigneur J. M., *Trust, security and privacy in global computing*, Ph.D. thesis, 2005.

[21] C. Hager, *Context aware and adaptive security for wireless networks*, Ph.D. thesis, Virginia Polytechnic Institute and State University, 2004.

[22] M. Lacoste, G. Privat, and F. Ramparany, "Evaluating confidence in context for context-aware security," in *Proceedings of the European Conference on Ambient Intelligence (AmI '07)*, 2007.

[23] J. Al-Muhtadi, D. Mickunas, and R. Campbell, "A lightweight reconfigurable security mechanism for 3G/4G mobile devices," *IEEE Wireless Communications*, vol. 9, no. 2, pp. 60–65, 2002.

[24] E2R Deliverable D2.2, "Equipment Management Framework for Reconfiguration: Architecture, Interfaces, and Functions," 2005.

[25] T. Jarboui, M. Lacoste, and P. Wadier, "A component-based policy-neutral authorization architecture," in *Proceedings of the French Conference on Operating Systems (CFSE '06)*, 2006.

[26] D. M. Chess and IBM Thomas J. Watson Research Center, "Security in autonomic computing," *ACM SIGARCH Computer Architecture News*, vol. 33, no. 1, 2005.

[27] D. M. Chess, C. C. Palmer, and S. R. White, "Security in an autonomic computing environment," *IBM Systems Journal*, vol. 42, no. 1, pp. 107–118, 2003.

[28] O. Powell, J. M. Seigneur, and L. Moraru, "Trustworthily forwarding sensor networks information to the internet," in *Proceedings of the International Conference on Emerging Security Information, Systems, and Technologies (SECURWARE '07)*, pp. 30–35, October 2007.

[29] A. A. Pirzada and C. McDonald, "Circumventing sinholes and wormholes in wireless sensor networks," in *Proceedings of the International Workshop on Wireless Ad-Hoc Networks*, 2005.

[30] C. Davis, "A localized trust management scheme for Ad-Hoc networks," in *Proceedings of the 3rd International Conference on Networking (ICN '04)*, March 2004.

[31] L. Eschenauer, V. Gligor, and J. Baras, "On trust establishment in mobile Ad-Hoc networks," in *Proceedings of the 10th International Workshop of Security Protocols*, Springer Lecture Notes in Computer Science (LNCS), April 2002.

[32] A. Rahman and A. Hailes, "A distributed trust model," in *Proceedings of the New Security Paradigms Workshop 1997*, ACM, 1997.

[33] T. El Maliki and J. M. Seigneur, "Optimal Security Adaptation in Proximity-Based Wireless Networks," Advance System Group Publication. Mobile Quality of Service. University of Geneva, 2009.

[34] J. M. Rabaey, M. J. Ammer, J. L. da Silva, D. Patel, and S. Roundy, "PicoRadio supports Ad Hoc ultra-low power wireless networking," *Computer*, vol. 33, no. 7, pp. 42–48, 2000.

[35] B. Warneke, M. Last, B. Liebowitz, and K. S. J. Pister, "Smart dust: communicating with a cubic-millimeter computer," *Computer*, vol. 34, no. 1, pp. 44–51, 2001.

[36] M. J. Sailor and J. R. Link, "'Smart dust': nanostructured devices in a grain of sand," *Chemical Communications*, no. 11, pp. 1375–1383, 2005.

[37] E. Felemban, S. Vural, R. Murawski et al., "SAMAC: a cross-layer communication protocol for sensor networks with sectored antennas," *IEEE Transactions on Mobile Computing*, vol. 9, no. 8, pp. 1072–1088, 2010.

[38] M. A. Rahman, A. E. Saddik, and W. Gueaieb, "Wireless sensor network transport layer: state of the art," in *Sensors: Advancement in Modeling, Design Issues, Fabrication and Practical Applications*, Springer, Berlin, Germany, 2008.

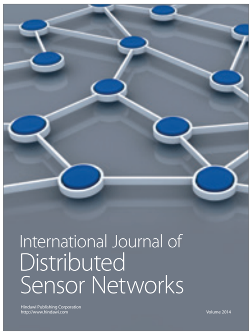
The Scientific World Journal

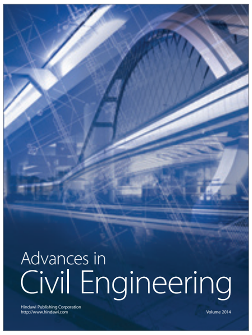
International Journal of Rotating Machinery

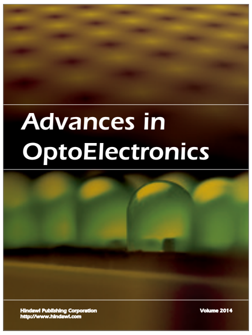
Journal of Engineering

Journal of Sensors

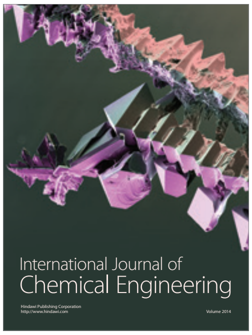
Advances in Mechanical Engineering


International Journal of Distributed Sensor Networks


Advances in Civil Engineering

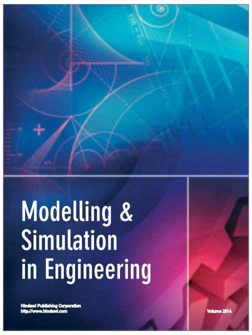

Advances in OptoElectronics

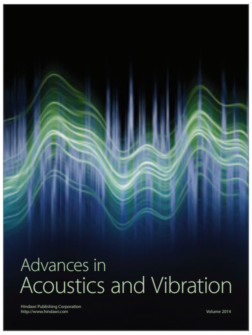
Journal of Robotics


International Journal of Chemical Engineering

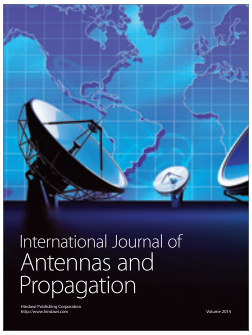
VLSI Design

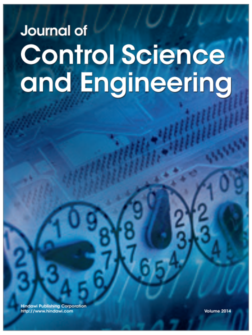
International Journal of Navigation and Observation

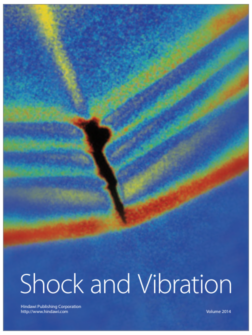

Modelling & Simulation in Engineering


Advances in Acoustics and Vibration

Active and Passive Electronic Components


International Journal of Antennas and Propagation


Journal of Control Science and Engineering


Shock and Vibration

Journal of Electrical and Computer Engineering