Security Adaptation Based on Autonomic and Trust Systems for Ubiquitous mobile network and Green IT

Tewfiq El-Maliki
HEPIA Geneva
University of Applied Sciences Western Switzerland
tewfiq.elmaliki@hesge.ch

Jean-Marc Seigneur
University of Geneva
Advanced Systems Group
Jean-Marc.Seigneur@trustcomp.org

Abstract— Security in Wireless Sensor Network (WSN) or Internet of Things has become a hot research topic due to their wide deployment and the increasing new runtime attacks they are facing. Thereby, applications are unaware of what security mechanisms are as well as dynamic changing attacks. Accordingly, the concept that must cope with this new security challenge has to satisfy an overall performance such as power consumption, being actually a key issue for internet of things. This objective is completely compatible with green computing (Green 1.0). This research investigates methods mainly based on autonomic computing and adaption security to build a framework capable of determining appropriate security means for a highly dynamic wireless network with respect to context-aware, self-management, self-optimization and self-protection paradigms of autonomic system. Trust computing was the means used to mitigate the influence of attackers. Extensive simulations using agent based approach have been also conducted for a case study of pollution detection in Geneva city in concordance with Green 2.0. We have proved the performance of the framework in the case of mobile sensor network in the presence of different mobile attacks. The results clearly show that SARM is efficient in terms of survivability, overall network utilization and power consumption.

Keywords-Security adaptation; Autonomic; Trust; Green IT

I. INTRODUCTION

Ubiquitous computing is becoming more popular than ever, mainly by Internet of Things highlighted by large-scale embedded sensor devices. Indeed, trends are best observed by sensors and Radio Frequency Identification (RFID) in everyday life such as cars, refrigerators or even animals to track some useful information about them. This overflow of information coming from sensing and communication is fitting squarely within complex system and autonomic computing [1]. Furthermore, mobility of these devices exposes them to different security vulnerabilities.

However, there will be no acceptance of these new paradigms without security methods, which are main concerns of industry and consumers.

The increasing complexity of communication system and also of attacks makes the conventional static security almost obsolete. Whereby, it is resources consuming to maintain required security level. The overhead cost reaches high rate. Thus, new mechanisms need to be set up to achieve principle of adaptation security based on autonomic system in the field of security of Internet of Thing.

On the other hand, sustainable development has propelled the efficiency in using resources, which is one of the fundamental principles of green computing (Green 1.0). Indeed, it studies practices of efficient use of computing resources, motivated by reducing the use of materials harmful to nature, maximizing energy efficiency and life product [2]. In addition, Green IT (2.0) [3] initiative is also a good mean to contribute indirectly to catalyze economy of energy by using smart protocols and communications to reduce emission of other technologies and business sectors. In short, we would like to minimize the overall energy consumption when using security mechanisms (Green 1.0) as well as using ICT to contribute indirectly in reducing gas emission (Green 2.0).

In this paper, we introduce our security autonomic framework based on the concept of adaptation security, Green IT and explain its components and functionalities. In addition, we have evaluated the framework in the case study of pollution detection in Geneva based on mobile WSN to manage transport traffic and thus energy. In Section 2, the related work is reviewed. Section 3 gives the problem statement, highlighting the motivation of our work. Section 4 shows our proposed framework and Section 5 explains our Green-SARM, experiments and simulation implementation to validate our Framework for the case study. Our simulation results and performance analysis are presented in Section 6 and our conclusion is to be found in Section 7.

II. RELATED WORK

Security in sensor networks is complicated by the constrained capabilities of sensor node hardware and the properties of the deployment [4]. Individual sensor nodes in a WSN have the inherent limitations in resources, which make the design of security procedures more complicated. Each of these limitations is due in part to the two greatest constraints: limited energy and physical size [5].

Other security issues include security-energy assessment, data assurance, survivability, Trust, end to end security, Security Support for data centric sensor networks and node compromise distribution [5]. It is very important to study these areas due to a sensor network's special character, such as battery limitation, high failure probability nodes, easier compromised nodes, unreliable transmission media, etc.

ISBN: 978-1-61208-289-9

Mobility greatly exacerbates the problem. Until now, there have been only a few approaches available, and more studies are needed in these areas. Furthermore, Trust [6] is a good path to explore because it gives in some cases better results. That's why we have carried out extreme simulation based on Trust to assess security requirements of our case study.

The best way to overcome this constraint is to implement the Framework capable of adapting security to the context based on the ideas similar to those described in [7] and consequently having an overall security control. We have been inspired by the concept of autonomic computing that was develop by IBM [1] to propose a new Security Adaptation security Frameworks based on autonomic computing and "Green IT" [2,3].

III. MOTIVATION

A. General Motivation

IT systems are resource consuming especially battery power [8]. This is because a lot of smart and useful mobile applications need significant power consumption, such ones using geo-localization. However, all actors avoid using or arming security means in attempt to reduce power and resource consumption. Accordingly, they put users' security at risk and thus facilitating also distributed attacks to be successful. In addition, in the smart 2020 report [3], it is illustrated the scale of the opportunity for IT to drive efficiency across the economy and deliver emission savings of 15% of global emissions in 2020. One of the biggest challenges is overcoming the lack of information about the emissions impacts of products and services, especially in the context of complex configurations and integration.

Furthermore, conventional security mechanisms such as cryptography are unable to protect against new attacks such as jamming mainly in WSN. Ref. [9] talk about hard security for conventional security mechanisms such as authentication versus soft security measures for trust and reputation systems.

Investigation of new techniques to deal with the trade-off between the use of security mechanisms and performance are highlighted as essential to computing [10, 11].

We also argue in this article that the spare processing and transmission resources are wasted in mobile 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 [12], context-aware access control systems [13] and security architectures [14]. This prompted us for the implementation of a completely reconfigurable architecture [15], which is fundamental to adapt the architecture to the terminal and network variability of the context and particularly in the security field [16]. J-M Seigneur [6] has introduced autonomic security pattern in his security design but only at the authentication level.

In [17], the author listed the main and typical problems for the security in complex system.

a) Inefficient and inadequate usage of available security methods and tools

b) Scattering of resources when trying to solve a lot of special security problems at the same time

These problems need efficient solutions, which lead to high demand for adaptive security methods.

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

IV. FRAMEWORK 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. All these are under policies and user real time intervention constraints. Thereby, our system differs from others by its [10]:

a) autonomic computing security feedback control system,

b) dynamic and evolving security mechanisms related to context-monitoring,

c) explicit energy consumption management,

d) dealing with mobility of attackers

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.

Our framework could work as a cross-layers program and thus it is not related to any layer. However, the best place to implement is in the kernel to avoid any compromising overall security.

To reduce the system complexity and to make the system incremental, we propose a feedback loop framework as introduced in [18] 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 with feedback loop. 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.

Security means are defined as any algorithm or mechanism that could ensure security. We have carried out a good synthesis survey on identity management security initiative used as means in [19].

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

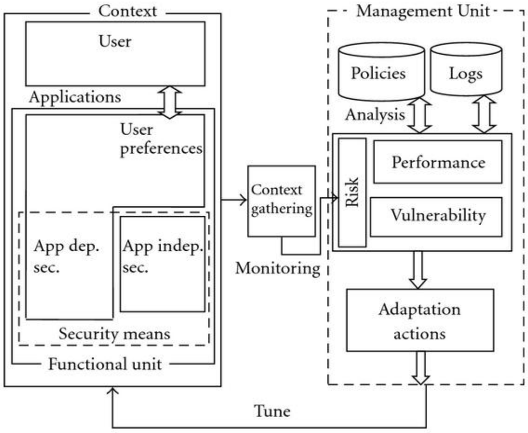

Figure 1. *SARM*.High level view

Security means can be application dependent such as a localized trust [20] or a distributed trust [21]. In [10], we have explicit all the details about SARM.

V. GREEN-SARM

We have used an adapted version of SARM called Green-SARM to the application domain of wireless sensor network applied to a case study of pollution detection in the city of Geneva, which is an application for both Green 1.0 and 2.0 initiatives.

A. *Sensors Energy Consumption*

A typical sensor node processor is of 4 MHz at 916 MHz frequency [5]. Table I shows that receiving costs almost half the energy of sending, which are almost 5 to 25 time average computing energy. That is why, our computing energy for trust and detection is really insignificant compared to transmission.

TABLE I. CHARACTERISTIC DATA FOR THE MICA2DOT SENSOR(

Field	Value
Effective data rate	12.4 kbps
Energy to transmit (5dBm)	59.2 µJ/byte
Energy to receive	28.6 µJ/byte

A. *The Main Problem : use case*

Geneva is an international financial city, and worldwide centre for diplomacy and for UN agency. It is the most popular and the second most populous city in Switzerland.

During summer, traffic jam is making the city unfortunately polluted. To apply Green IT 1.0 and 2.0 objectives, we would like to minimize this pollution by implementing:

a) A sensor network will be deployed based on a cheap Zigbee transmitter to monitor the level of pollution (CO2).

b) Every transmitter is placed in a car or a pedestrian

c) There are many fixed base stations that collect information about CO2 from sensors

d) Some information is exchanged within a fixed range and an evaluation of data consistency is rated as a trust

e) Obtained data will be aggregated by weighted average according to the trust on collected information

f) Therefore, recommendations will be overspread to conductor and walker to avoid the places where the pollution overpasses a certain level and simultaneously a trust about every transmitter will be send to the participant.

g) Finally, the traffic is managed in real time to initiate action plans crescendo capable of reducing the emission and thus avoiding in advance pollution peaks.

B. *Implementatin of Green-SARM*

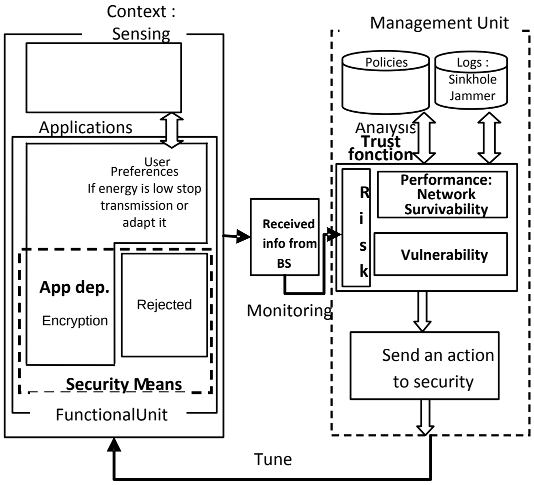

Figure 2. Adapted SARM.: Green-SARM

The control system of SARM Framework is ideal for a collaborative environment where the decision making trust function for the security must interact with other users to find the adequate decision. In Fig. 2, we describe module by module, how SARM is applied to the application domain of our validation, becoming the Green-SARM version. First of all, the security means are tuned efficiently by SARM. However, the application could use or not authentication and encryption with all rejected sensors. 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 (BS) and Nodes (sensors). These values represent the trust of a sensor about its neighbors (summarized in Table II)

TABLE II. BEHAVIOR AND RECOMMENDED VALUE SENT BY BASE STATION TO SENSOR UNDER SINKHOLE AND JAMMER ATTACKS

Sensor Behavior over neighbors According to a scenario	Recommended value to Sensor
Normal	Good (1) = Pos
Sinkhole or Jamming to neighbors "Who are you"	Bad (-1) = Neg
Unkwon	Neutral (0.5)= Neu

Attackers are detected when they are within a given range to the BS. The network is configured with messages following a given communication protocol to establish a connection as describe in Fig 3. In fact according to it, only the BSs and the attackers send messages "Who Are You?" As the BSs are too far from each others, if a message of this type is received it means that it is send necessarily by an attacker. In this case, the base sends a "Bad" message to everyone to indicate an intruder is present and BS updates its trust in a centralized database.

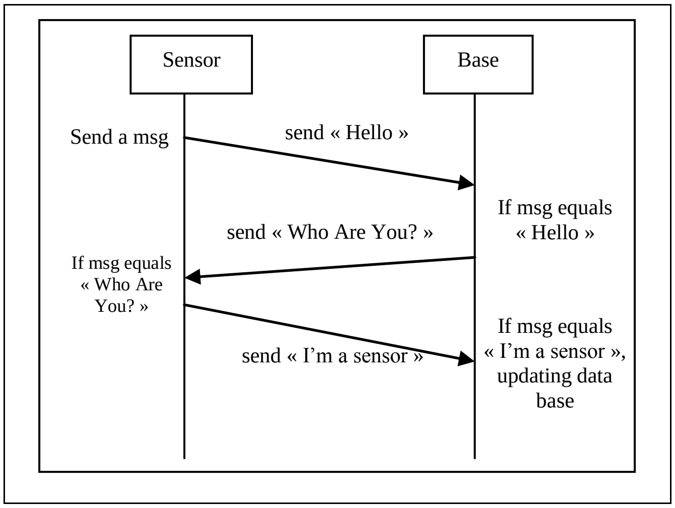

Figure 3. Communication protocol based on soft security

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 is fixed as energy saving in accordance with Application Preference, which is lifespan maximizing.

One of our used TF is explained in “(1)”:

$$TF_j = (2*Pos-2*Neg)/ (2*Pos+2*Neg+ Neu) \qquad (1)$$

```
For all j sensors
if ($TF_j$ > **threshold** )
    Accept connection
    else{ $TF_j$ =< **threshold**}
        then {rejected and use encryption and authentication if required}
End for
```

The TF will be used to calculate the weighted average of pollution values gathered from sensors and it will be also used to minimize overall energy consumption.

The implementation and the system analysis are difficult and complex. This comes from the fact that every sensor acts independently from others. Therefore, our model will be studied using simulation tools in order to compare it with reference cases. Indeed, each Sensor sends data packets to a number of Sensors within a defined range according to threshold used as policy. Thanks to its context gathering module the TF has all information to evaluate the trust.

B. *Attackers*

The behavior of a node is fixed in the starting of the simulation based on a uniform distribution, which has an average equal to rate of attackers .There are many attacks but we will consider only two attacks:

- Jamming attack: given the sensitivity of the wireless medium to noise, a node can cause a denial of service by transmitting signals at a certain frequency. It is implemented just by sending packet repeatedly.
- Sinkhole attack: the node tries to attract to it the most possible path like a concentrator to have control over most of the data through the network. To do this, the attacker must appear to others as being very attractive, presenting optimal routes. It is implemented by imitating any BS or any good node.

Note that we do not treat Sybil attacks.

C. *Metrics*

Due to the characteristics of WSN, their major objective is to fulfill their mission even though some nodes are out of use due to attackers. Indeed, this means to ensure survivability of WSN, which can be defined as: “the capability to fulfill its mission, in a timely manner, in the presence of intrusions, attacks, accidents and failures” [22] Gain of survivability is the ratio between: Duration time when 75% of nodes are out of battery using our framework and same case but without using our framework

VI. Implementation and Validation Methodology

We have implemented Green-SARM and validated it in a mobile Sensor wireless network simulation developed with AnyLogic, which is a simulation tool that supports all different simulation methodologies. It is based on Real-time UML, Java object-oriented language and agent based model.

A. *Model Set-up*

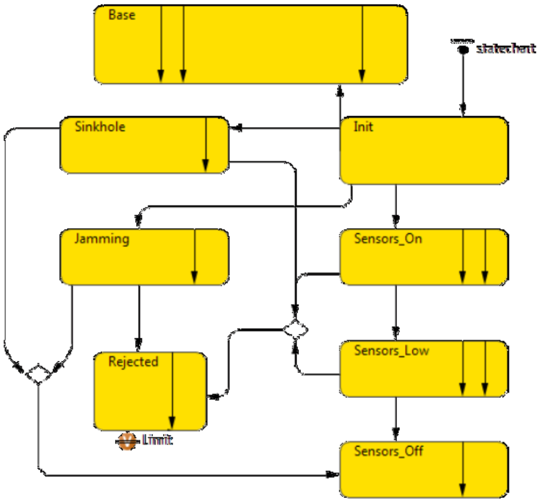

Figure 4. Statechart of sensors

Each Sensor is associated to a given agent matching with its location and behavior.

Setting up our security model using Table II, 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

Fig. 4. Using AnyLogic as implementation platform agents and state-charts can be programmed very conveniently. Particular modifications and/or extensions of the final model can be handled in a simple way.

In Fig. 4, each Agent (Sensor) starts at state Init. The Agents are switched to their relative state (Sinkhole, Jamming, Base Station, Sensors) according to percentage of attackers, BS and 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 and Jamming as attakers

Each Agent is then processed depending on the decision of the monitor unit to choose a security means or not. When arriving at a minimum defined level of Energy according to the real consumption of Sensor (see table [1]), the Agent transits to Sensor_low; and then transit to Sensor_off when the Agent has not enough energy to transmit data. The Agent transits to Rejected state when its TF is lower than a Threshold. The state-chart Trust updates the trust each time the Base Station received information about a sensor. The BS is not limited in energy and has also access to trust database to spread it over its range.

In order to have a deep study of the model, we have introduced factors :

a) ImmunityRate: when TF of a Sensor reaches this value it has double influence on its values "Good". It is a catalyst to accelerate convergence.

b) Limit: it is the Threshold of TF to reject sensors.

c) JudgementError: it defines an error rate among the large number of messages received and helps to study the robustness of the model. It is useful in our case where errors are very frequent due to the media.

B. Validation Methodology

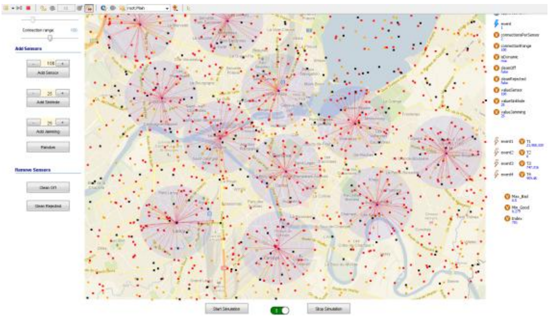

Figure 5. Simualtion interface for Geneva pollution use case

Fig. 5 depicts the context of the simulation interface. In this respect, we have carried out simulations under 0%, 20%, 40%, 60% and 80% half-half sinkhole and jammer attackers. Furthermore, the network topology was set to random spreading of sensors. We have taken a uniform packet distribution over the neighbors.

The BSs are randomly spread over the network. In our experiments, we have validated our proposed solution and analyzed the extended performance under a range of various scenarii, where we have fixed to ten BSs. All sensors are spread over a square topology and operating over 35 days of simulation time. The Base Station coverage a large circle but it has no contact over the coverage of other BSs. We deployed the Sensors in an incremental mode, from S1 to Sn. As the device is not static, we have modeled his mobility using random variables model. The movement pattern of mobile clients was totally randomized, in order to comply with a real application. To achieve this, we used the Random WayPoint (RWP) mobility model [23]. All nodes are mobile and their pause time is a randomly uniform variable. The time is in minutes and is in a range [0; 50'000] adapted to the battery of sensors.

C. Scenarii

We have used three scenarii to validate our model. In our scenarii, sensors (agents) were divided in four categories.

A normal behavior, they are composed of N sensors set in the range of [100; 1000]. The trust threshold is optimized after many series of simulation to 0.3.

Sinkhole and jammer attackers are composed of the same amount of sensors. In the first scenario, we fixed the percentage as: N of normal behavior and 10 % of sinkhole and 10% jammer attackers. In the second scenario, we fixed the percentages as: N of normal behavior and 20 % of sinkhole and 20% jammer attackers. In the third scenario, we fixed the percentages as: N of normal behavior and 40 % of sinkhole and 40% jammer attackers

VII. RESULTS ANALYSIS

During our analysis, we firstly studied the performance of Green-SARM in the three defined scenarii where sensors were arranged at random. Secondly, we studied the scalability of the model. Thirdly, we studied robustness of the model based on the factor Error.

For comparison purpose, we plotted the Green-SARM for 1000 sensors in Fig. 6 and without trust in Fig. 7 for the same first scenario. We can easily conclude that SARM is largely better than normal case without security trust; a ratio of 6.5 is reached and we can see that in short time 1000min compared to the maximum time 50'000min. Indeed, we have obtained the desired effect of the feedback mechanism of the SARM. An example of 500 sensors without Green-SARM security is plotted in Fig. 8. We see clearly that the attackers diminish quickly the survivability of the network.

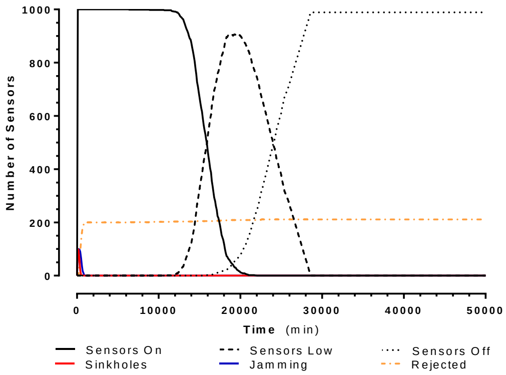

Figure 6. 1000 sensors for the first scenario (Green-SARM)

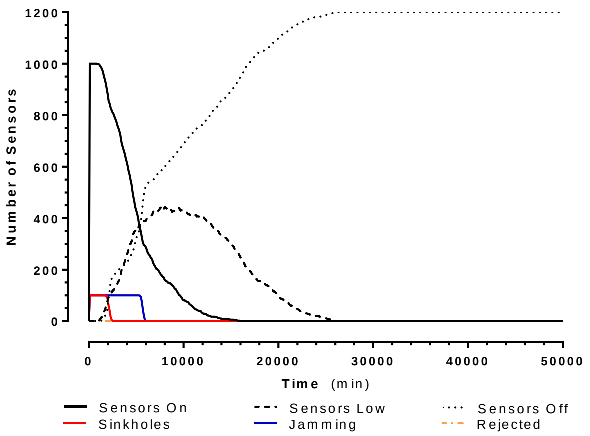

Figure 7. Network of 1000 Sensors for the first scenario (without SARM)

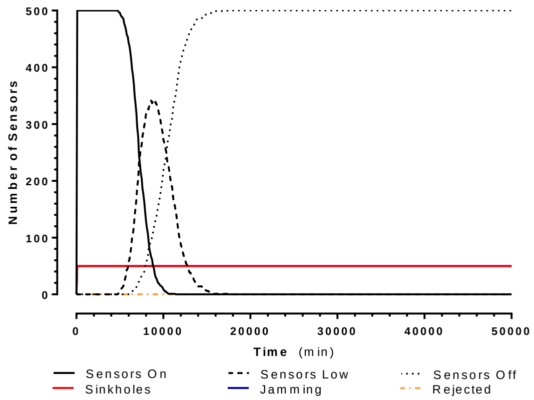

Figure 8. 500 sensors for the first scenario (without SARM)

In Fig. 9, we plotted the scalability of the model in function of number of sensors using Green-SARM for the first scenario. This graph shows clearly that our model is scalable. The number of sensors goes higher as the network survivability goes higher.

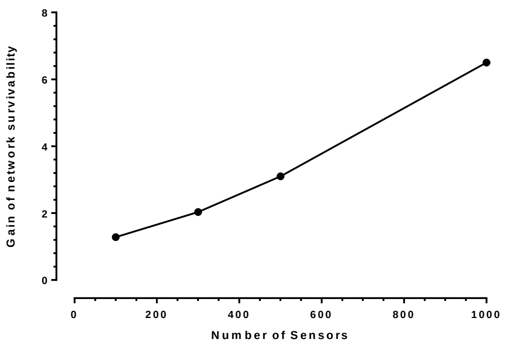

Figure 9. Gain of survivability for 20 % of attackers for number of sensors from 100 to 1000

For comparison purpose, we plotted the Green-SARM under 20% of sinkhole attackers (the second scenario) using our TF in Fig. 10 and also without trust in Fig. 11. The results clearly demonstrate that the survivability is boosted.

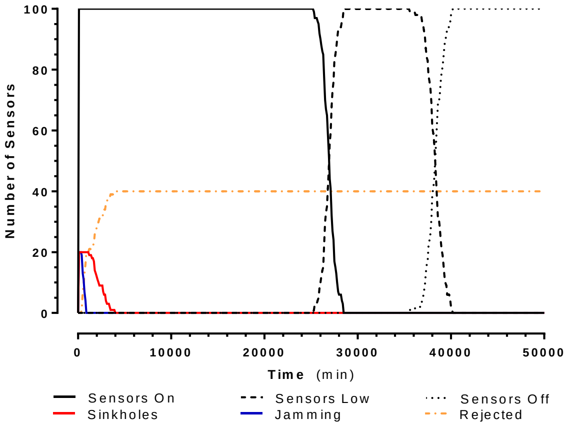

Figure 10. Number of 100 sensors for the 2nd scenario using Green-SARM

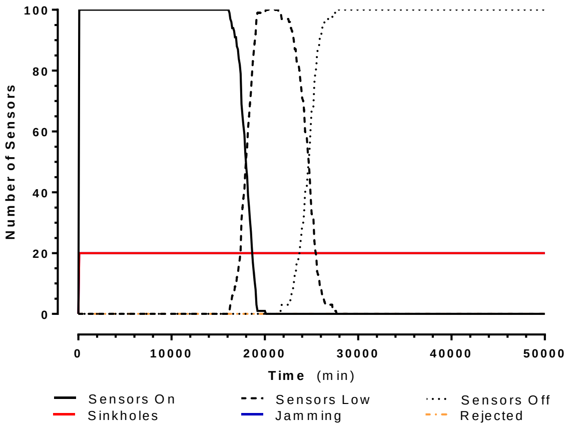

Figure 11. 100 sensors for the 2nd scenario (without Green-SARM)

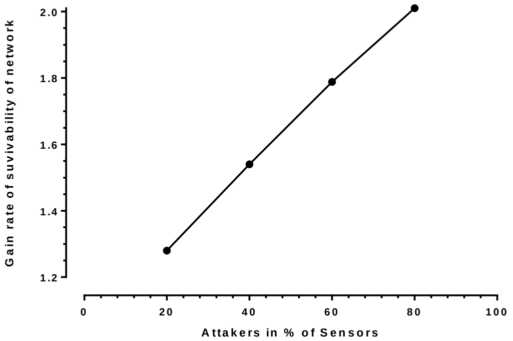

Figure 12. Survivability of 100 sensors for different scenarii

In Fig. 12, we plotted the gain of survivability of the model in function of the percentage of attackers using Green-SARM. Therefore, we have the proof that Green-SARM is ameliorating the survivability to up a rate of about 2 when the network is under more attackers compared to a passive security network.

The *JudgmentError* factor, which designs errors on TF, was set to 10% but the variation of results was less than 1%. This shows clearly the robustness of the Green-SARM.

All the results show clear advantages of Green-SARM even at 80% of sinkhole and jammer attackers. We can conclude that our security monitor helps the WSN to operate even under 80 % of attackers thanks to the looping system connected to the context gathering monitor and the TF.

VIII. CONCLUSION & FUTURE WORK

We have proposed a Security Adaptation Reference Monitor based on security adaptation and the Autonomic Computing Security pattern to support both context monitor and behavior control. This paper also presents the validation of SARM in WSN applied to support Green IT concepts. The results clearly show that Green-SARM copes with survivability and network Energy loss under sinkhole and jamming attacks even at 80% of attackers. Indeed, Green-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 feedback control and 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 implement the model in a tamper-resistant security module based on a Secure Digital card.

ACKNOWLEDGMENT

I would like to thank my students O. Oudom and M. De Azevedo who have worked in computer model implementation.

REFERENCES

[1] M. Parashar and S. Hariri, “Autonomic Computing : An overview”, Spring-2005

[2] L. Wilbanks, “Green, My Favorite Color”, IT Pro v.10, n.6., 2008, pp.63-64. IEEE Comp Soc. Press

[3] SMART 2020, “Enabling the low carbon economy in the information age”, Global e-Sustainability Initiative, 2008

[4] H. K. D. Sarma and A. Kar, “Security Threats in Wireless Sensor Networks”, In proceeding of: Carnahan Conferences Security Technology, Oct. 2006, pp. 243-251, Proceedings 40th Annual IEEE International, 2006

[5] X. Chen, K. Makki, K. Yen, and N. Pissinou, “Sensor Network Security: A Survey”, IEEE Communications Surveys & Tutorials, Vol. 11, No. 2, Second Quarter 2009, pp. 52–73, 2009.

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

[7] B. Badrinath,. A. Fox, L Kleonrock, G. Popek, and M. Satyanarayanan, “A conceptual Framework for Network and Client Adaptation”, Mobile Networks and applications, v.5 n.4, Dec. 2000, pp. 221-231, 2000.

[8] A. S. Wander, N. Gura, H. Eberle, V. Gupta, and S. C. Shantz, “Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks”, Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications, March 2005, pp. 324-328, 2005

[9] A. Josang, R. Ismail, and C. Boyd, “A Survey of Trust and Reputation Systems for Online Service Provision”, Decision Support Systems, 43(2) 2007, pp. 618-644, 2007

[10] 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, Jul. 2010, pp. 63-68

[11] A.V. Taddeo, “Gradual Adaptation of Security for Sensor Networks”, IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks, June. 2010, pp. 1-9

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

[13] M. Lacoste, G. Privat, and F. Ramparany, “Evaluating Confidence in Context for Context-Aware Security”, European Conference on Ambient Intelligence (AmI'07), Nov. 2007, pp. 211-229.

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

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

[16] M. Lacoste, T. Jarboui, and R. He, “A Component-Based Policy-Neutral Architecture for Kernel-Level Access Control,” Annals of Telecommunications, vol. 64, no. 1-2, Feb. 2009, pp. 121–146

[17] A. Shnitko, “Practical and Theoretical Issues on Adaptive Security”, WOLFASI, Turku, Finland, 2004.

[18] D. M. Chess, “Security in Autonomic Computing”, IBM Thomas J. Watson Research Center, 2005.

[19] T. El-Maliki, J.-M. Seigneur, “A survey of user-centric identity management technologies”, Emerging Security Information, Jul. 2007, pp. 12-17, ieeexplore.ieee.org, 2007.

[20] 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, pp. 44-66.

[21] A. Rahman and A. Hailes, “A Distributed Trust Model”, New Security Paradigms Workshop, 1997, pp. 48-60, ACM, 1997.

[22] R. Ellison, D. Ficher, R. Linger, H. Lipson, T. Longstaff, and N. Mead, “Survivable Network System: An Emerging Discipline”, CMU/SEI-97-TR-013, 1997

[23] C. Bettstetter, “Stochastic Properties of the Random Waypoint Mobility Model”, 2004.