Optimal Security Adaptation in Proximity-Based Wireless Networks

Tewfiq El Maliki and Jean-Marc Seigneur

Abstract. Nowadays, the number of wireless networks available is increasing dramatically throughout the world, mainly in cities (airports, train stations and hotels). However, mobile wireless connections are still risky and the performance varies a great deal depending on the different nearby networks connections. For example, new soft Access Points (AP) may easily spoof the identity of another AP and thus compromise the privacy or the power consumption of users' mobiles. This paper presents an Optimal Security Adaptation Proximity-based wireless network (OSAP) taking into account the published security value of each user and accessed APs. Moreover, this autonomous security configuration can be adapted dynamically during runtime depending on the security parameters. We have analyzed the network utilization and power consumption of mobile devices in the case of Geneva Hotspot AP locations. We have validated our proposed solution for resource-constrained devices through simulation based on a dynamic simulation tool called AnyLogic. The result shows that OSAP is optimal in terms of overall network utilization and power consumption.

1 Introduction

In the past few years, Wireless Local Area Networks (WLANs) have increasingly become major wireless networks in many cities. Their spread in many locations like airports, cafes, businesses and university campuses has expanded their utilization. This ongoing spreading, coupled with the inherent vulnerabilities of the deployed protocols, has provoked more breach of security. In addition to typical network threats, wireless networks present several challenges and attacks. This is due to the wide open air nature of the channel allowing more attacks, bandwidth limitations and constant topology change because of node mobility. In such networks, security requirements are high as they are opened to many kinds of attacks. In this case the basic security mechanisms may not be sufficient. To tackle the above-mentioned constraint problems, we need new and simple security-adapted mechanisms to be implemented; respecting overall performances.

In this paper, we introduce the concept of local dichotomy security value in the wireless access network and different solutions exploiting this value, and we compare it to normal security solutions. 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 mechanisms and Section 5 explains our experiments and simulation implementation. Our simulation results and performance analysis are presented in Section 6 and our conclusion is to be found in Section 7.

2 Related Work

Ganz has already introduced a security broker architecture for WLANs [10]. This framework uses security services versus security requirements specified by the user, available network performance as well as the performance of security routines. [7] has also proposed an adaptive security application in mobile ad-hoc networks, where network conditions play a role in choosing relevant security mechanisms at runtime. In the Chigan Chunxioo & all's article [6], the authors report that often a highly secure mechanism inevitably consumes a large amount of system resources, which in turn may unintentionally cause a security attack. Consequently, 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 WLAN and Sensor networks operation. Another contribution to the adaptation of security mechanisms in WLANs was published by Saxena in [15]. The required security level depends mainly on the level of trust in the environment and describes how hostile one expects the environment to become. The article argues 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. More complex solutions have been proposed, such as in Moustafa's article [12]. Even new models, such as the Zhou and al. concept [18] which use threshold cryptography to distribute trust in ad-hoc networks, or Davis' concept [8] that proposes the use of certificates to manage trust, are resource-consuming. In this field, however, there is still a lot to be done.

3 Problem Statement

Applications for adaptive security have been proposed in areas such as mobile ad-hoc networks, where current network conditions play a role in choosing relevant security mechanisms at runtime. In WLAN the same principle can be applied and evaluated to ensure security and performance [2]. There have also been proposals to provide adaptive security system through system-event monitoring [3].

Most deployments of public WLAN access solutions are not based on global network utilization and energy economy. This is of great interest to network operators. Also, this would require the change or the extension of the existing security mechanism to fulfill the security adaptation requirements. For example, the concept of trust needs some resources to establish and maintain trust between the nodes of a wireless network, by using either centralized or decentralized architecture. Therefore, it is very important to develop a secure mobile mechanism based on simple concept that saves energy compared to others and maximizes the overall utilization. This can only be done step by step. In addition, when we trade-off between security and performance, it is security in general that suffers. If we introduce adaptive security, at least we ensure better balance between them. Moreover, adaptive security is based on the observation that the security requirements of a system or service depends greatly on the environment in which they operate and should therefore be dynamically adjusted to best operate within that environment. Using adaptive security, we can allow a system to exist in a less secure, more performing state until it comes under attack. Therefore, we can adapt the system to a more secure, less performing implementation.

New, simple and efficient mechanisms are important to use in the case of AP wireless network. To that aim, we implement and evaluate an adaptation security mechanism, called Optimal Security Adaption Proximity-based (OSAP) WLAN.

In this paper, we propose original and simple security mechanisms. Their main advantages are:

i) to maximize the overall utilization;
ii) to minimize the power consumption;
iii) to allow a simple implementation without compromising the network security features.

4 System Model

In IEEE 802.11, the privacy of devices in a given radio domain can be compromised if the AP identity is spoofed. This security breach is now very easy to deploy by using a soft AP. In addition, the temptation is high to use a PKI to secure the channel. However, it is so time and energy consuming that a more easily deployable solution should be proposed.

Based on trust management [14, 9], some solutions could be implemented but they need to hold and manage a lot of values. Simple solutions should be implemented, evaluated and eventually strengthened to save energy and maximize the use of overall resources of the network.

As some values should be published to decide whether or not to use security, one could be tempted to cheat by behaving maliciously, firstly by enforcing users to secure the connection even if no security is necessary because there is no risk in depleting the mobile user device energy; secondly to push users not to be secured to compromise their privacy or security in general. The paper investigates how to determine when to use a secure connection and when to use a non-secure connection, especially considering the trade-off between security and performance.

4.1 Decision-Making Function

We assume that each AP periodically collects information related to active users during short interval of time that we named monitoring periods (the choice of their length is not discussed in this paper). A series of binary values that are published by each user assuming some of them are collected by each AP. These values are then fed into a Decision Making Function (DMF) that decides whether a secure connection is necessary or not.

This method presents several advantages. First, the tests are very simple with minimum time and energy-consumption. Second, new tests could be easily added to mitigate other malicious behaviors.

The DMF is typically a statistical test that determines the security of the connection between the AP and the users. Trust values are previously collected in order to judge whether a transfer should be secured or not. DMF can be as simple as a comparison of two values or a more complicated technique.

The general objective of OSAP architecture is to support mobile clients' security and a seamless access to the Internet, near public WLAN Hotspots, even when some attacks are performed. The locations of Hotspot APs created in our simulation correspond to real positions based on GPS coordinates in Geneva.

The basic concept of OSAP is to exchange binary values of the users' devices within the range of access point. These values assert the fact that the security has to be used or not.

The modularization taken from Hotspot Access Point in Geneva could be applied anywhere. We use the existing APs of the network, and the potential danger comes from some users' devices that could compromise the network security by being Soft APs. As depicted in Figure 1, the devices of category (b) influence the energy consumption of all devices in their range. Other devices have a normal behavior and no direct influence.

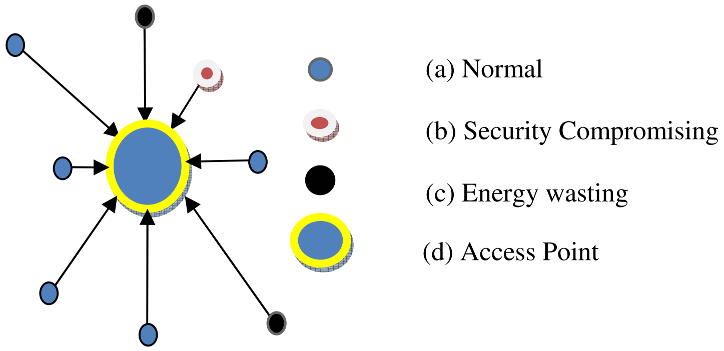

Figure 1. OSAP Simulation Scenario

Each device, before using an AP will publish a binary value and it will read the published value of other devices within range to the access point.

Our solution consists in choosing a function that predicts whether or not to use a secure connection depending on the average value of the published values of each device within range.

P_a(v, threshold) = Sum(value/number of devices within a given range); if $P_a(v) >$ threshold then we use a secure connection if not, we use a non-secure connection.

There are also other interesting functions that are taken as references:

The first is security in every case even when there is no threat and the second is no security in all cases. Another interesting case is a random chosen value to use security or not. At the end we introduce a 50% threshold security case which is useful for comparison purpose.

$P_1(v) = 1$ the result is equal to one for whatever the values published by users; secure connection in all cases

$P_0(v) = 0$ the result is equal to zero for whatever the values published by users; non-secure connection in all cases

$P_r(v) = \text{random}(0,1)$ for any published value; if $P_r(v) = 1$ then we use a secure connection and if $P_r(v) = 0$ then we use a non-secure connection

$P_a(v, 50\%) = \text{Sum}(\text{value/number of devices within a given range})$; if $P_a(v) > 50\%$ then we use a secure connection if not, we use a non-secure connection.

The system consists of one to many devices of different behaviors that could move randomly from one place to another within Geneva region and the real locations of its public APs.

5 Experiments and Simulation

We first explain how we have tried to quantify the energy consumption overhead between secure and non-secure mobile connections. Then we describe our simulation set-up.

5.1 Energy Impact

We have implemented a testbed based on WLAN network and mobile phones. The main goal is to know the time consumption difference between secure and non-secure connections. The results are shown in Figure 2. The set-up of this experience are:

- E65 telephone
- WLAN 802.11b, D-link Access Point
- Tomcat server
- SAML Token and SSL secure connection

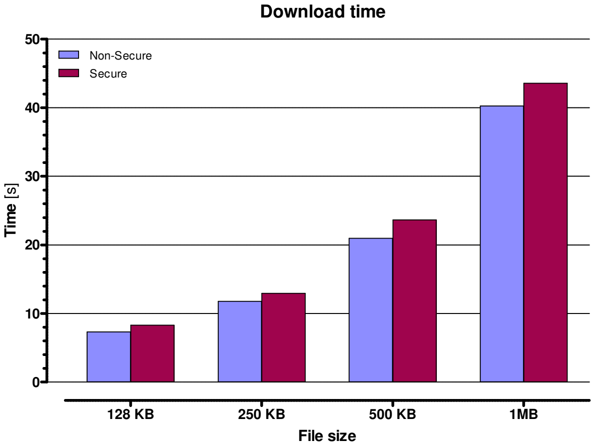

Figure 2. Download time of different files (sec, non-sec.)

Figure 2 shows the download time average difference between secure and non-secure for different file sizes. In all cases, the difference between secure and non-secure is ranged from 10% to 15%.

For more details, Figure 3 gives the min-max and the standard-deviation for the same average results plotted in Figure 2. Refer to [5, 13] for more comprehensive discussion of energy consumption of symmetric ciphers and hash algorithms.

Table 1 gives the energy level consumption by byte for a secure connection and the amount of energy used for transmission [1].

Field	Value
Effective data rate	12.4 kbps
Energy to transmit	59.2 µJ/byte
Energy to receive	28.6 µJ/byte
SHA-1 secu.	5.9 µJ/byte
AES-128 Enc/Dec	1.62/2.49 µJ/byte

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

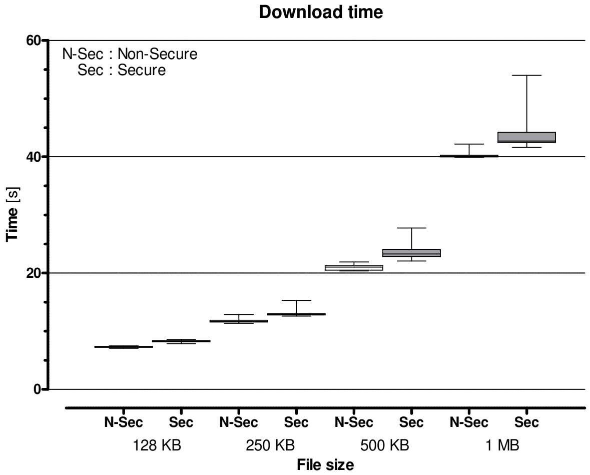

Figure 3. Min-Max & std-dev. of download time

In all cases, the energy consumption for security represents less than 15% over normal energy. This is a significant saving of energy allowing us to look further for an optimal security adaptation solution.

5.2 Simulation Tool

AnyLogic [19] is a simulation tool that supports all the most common simulation methodologies in place today: 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. AnyLogic is a programming and simulation environment, mainly aiming at modeling of hybrid systems. These characteristics matched exactly with our simulation development needs. We have used Agent Based modeling because it corresponds to our final goal of simulating the overall characteristics by describing only the behavior of each category of devices describe in Figure 1. Moreover, the mobility is based on a random mobility model and excludes, in the chosen area of Geneva, other locations, such as the crossing of the lake.

5.3 Model Set-Up

The basic element of an Agent Based model is the agent itself. This is done in AnyLogic by creating a new class than behaves as an Access Point. Each device is associated to a given agent matching with it location. As the device is not static, we have modelised its mobility using X and Y random variables.

The movement and the status of our agents are controlled by state-charts which represent the exact behavior of the device as described in Figure 4.

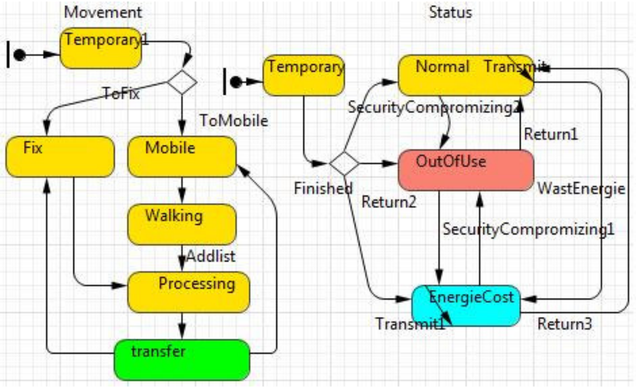

Figure 4. State-charts: “Movement” of agents and “Status”

We used Agents that were in one of the 3 states:

a. Normal state,
b. Security compromising state and
c. Energy wasting state.

In Figure 4, each Agent starts simultaneously in a “Temporary” state in the “Movement” and “Status” state-charts. The Agents are switched to their relative state (Normal, Security compromise, Energy consuming). A number of them are Access Points, so they are switched to the state “Fix” and placed in the map according to their GPS positions taken from Swiss hotspots reference [20]. All others are considered as mobile nodes and each of them follows a random mobility model. They are then added to a list of an Access Point whenever they are within the range of this AP.

Each Agent was then processed depending on the value of the Decision Making Function. Therefore, the Agent transited to other states or stood in the same state. When completing the transfer, the Agent returned to its initial state.

5.4 Simulated Scenarios

We have used two scenarios to validate our model. In our first scenario, devices which have access to APs are divided in three categories.

- A normal behavior, they represent 50% of all devices. Note that half of them are mobile devices (25%).
- An energy wasting behavior asking a security access even if it is not necessary, these are devices that try to push other devices to waste energy (25% of the devices).
- A security compromising behavior asking not to use security to access the network in order to compromise the privacy and security of anyone within a given range. They make the connection out-of-use during a period of time equal to the time of network access and data transfer (25% of the devices).

Behavior	**Given value to neighbors**	**Real value**
Normal	Don’t secure access: 0	true
Energy wasting	Secure access: 1	false
Security compromising	Don’t secure access: 0	false
Not used in this paper	Secure access: 1	true

Table 2. Devices Behavior

In the second scenario, we fixed the percentages of each category to:

a. 80% for normal behavior, half of them are mobile devices
b. 10% for energy wasting behavior
c. 10% for security compromising behavior

In our experiments, we validated our proposed mechanisms and analyzed the extended performance under a range of various mobility scenarios. All simulations were run using a wireless network composed of 1,000 nodes moving over a rectangular Geneva region of 8.69 km x 6.08 km topography, and operating over one day of simulation time. We also considered that the WLAN APs showed more reliability over mobile nodes, in having a non-limited amount of energy and a uniform transmission range. The communication range of APs was configured to be 100 meters. Each mobile device was also configured to have a communication range equal to 100 meters. We deployed the APs in an incremental mode, from AP_1

to AP_n, in the exact position taken from the true GPS position. Thus we estimated the impact of our mechanisms for an existing network depending on the behavior of mobile devices and on overall network performance.

The movement pattern of mobile clients was totally random, to conform to a real Hotspot application. To achieve this, we used the Random WayPoint (RWP) mobility model [4] with pause time equal to the time of network access and data transfer. In our simulation, each mobile device initially published its security value and calculated its own Decision Making Function to decide whether or not to use a secure channel. In case of a security failure, the device was ranked as security compromising and in the case of power failure; it was ranked as energy wasting.

We carried out our experiments considering thirty cases. In each studied case, we ran our simulations with different Decision Making Functions. Our performance evaluation was the result of 1000x30 different simulations.

The total number of nodes is 1000; therefore the sum up of the only three states (“utilization” “Sec.Comp” and “Energy Wasting) will be 1000.

The measurement of “utilization” state is based on the number of times the node is connected to the access point without any security compromising. Figure 5 shows the animation interface to monitor the simulations.

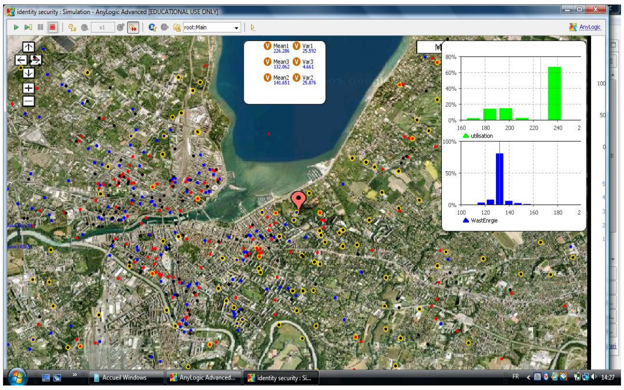

Figure 5. Animation interface and results of OSAP

6 Results Analysis

During our analysis, we firstly studied the performance of Geneva Hotspots network in terms of relative utilization, energy wasting and security compromising under the constraint of a fixed percentage (25%) of devices in energy wasting state and idem for security compromising (25%). Two threshold values (50%) and 5%) were taken as references for OSAP evaluation. Secondly, we studied the same performance but in the case of our second scenario which is based on 10% of energy wasting devices and 10% of security compromising devices. Finally, we studied the effect of the threshold on the overall network utilization. For comparison purpose, we plotted the five Decision Making Functions and their relative average number of Agents’ states in Figure 6.

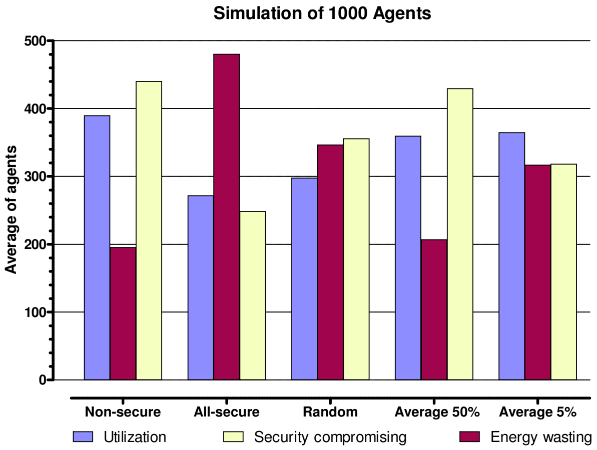

Figure 6. Performance results of different DMFs

As we can see from the result depicted in Figure 6, the best relative utilization rate happened in the case of "Non-secure" DMF, but unfortunately this result is compromised with the huge amount of security compromising devices (out-of-use). In the other hand, "All-secure" DMF is of course optimal in security compromising and it is the worst case in term of energy wasting. For more detail, Figure 7 gives the min-max and the standard-deviation for the same average results plotted in Figure 6.

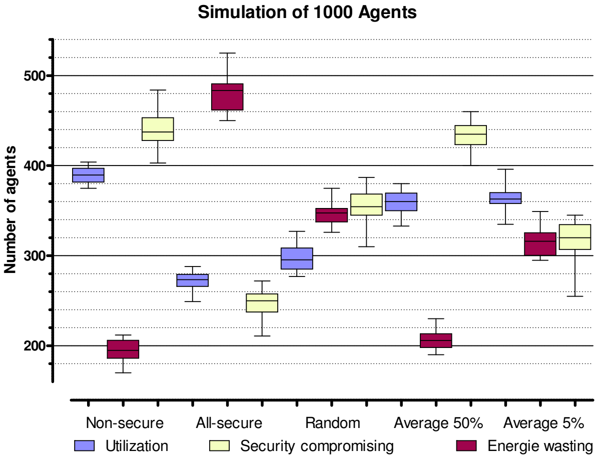

Figure 7. Min-Max & std-dev. performance for all DMFs

Optimal Security Adaptation Proximity-based WLAN references values (50% and 5%) are almost at the same level of relative utilization rate, but the case of "Average50%" is the nearest one to "None-secure" in all terms due to the threshold's level 50% which is too high to change anything. However, it just starts to change the level of the three categories.

The “Random” values related to the three categories are well distributed and almost equal. However, the utilization rate is lower than both Averages and the energy wasting rate is higher than “Average 5%”. This last “Average” constitutes a good trade-off for all studied cases because it offers simultaneously a high overall utilization and a lower energy wasting. Therefore, it is interesting to plot the three categories for different threshold values to find the exact value that optimizes the overall network utilization. Then, it is easy to prove that the OSAP is optimal in terms of overall utilization.

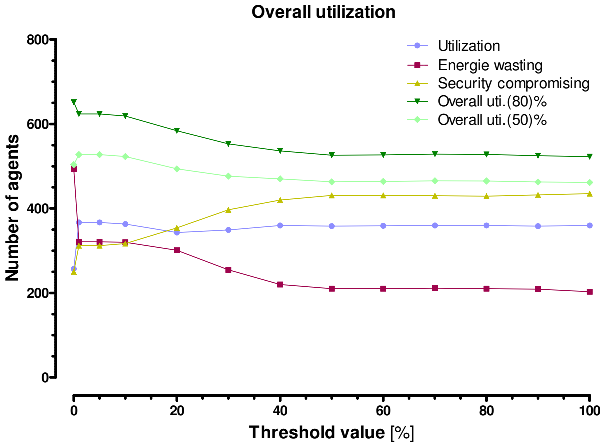

Figure 8. Effect of threshold on overall utilization 1st Scenario

Figure 8 illustrates the evolution of the three categories when we varied the threshold value between 0% (“All-secure”) to 100% (“Non-secure). We also plotted the overall utilization for two cases under the constraint of our first scenario. In one case, we counted only 80% of the energy wasting devices in the overall utilization, and in the other case only 60%. Indeed, when a device is in energy wasting status, only a part of it offered bandwidth and allocated time are used. That was the reason why we counted only a part of them.

In the Figure 9, we plotted the same case as in Figure 8 with the only difference being that the second scenario was applied. The results showed that our OSAP was optimal in term of overall utilization. It improved the overall utilization by 10% in the case of 60% of energy wasting devices. Almost no improvement was realized in the case of 80% of energy wasting devices.

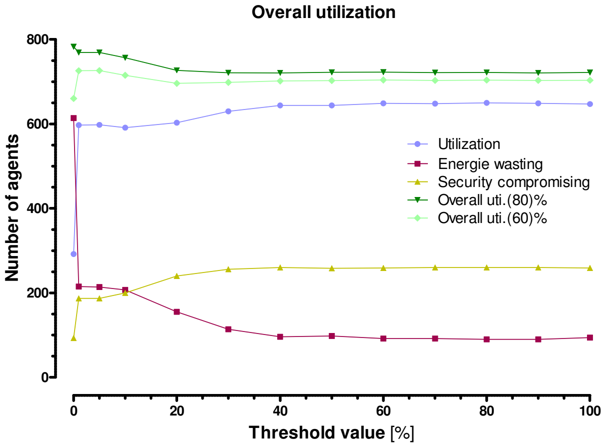

Figure 9. Effect of threshold on overall utilization 2nd Scenario

The overall utilization was better for OSAP when the threshold was in the interval of]0;0.2]. The overall utilization difference was clear when using OSAP instead of "All-secure" method. The obtained gain of OSAP was almost 10%. The threshold in this case was 0.01.

7 Conclusion and Future Work

WLAN has been increasingly deployed in various locations because of the convenience of wireless communication and decreasing costs of the underlying technology. However, the existing security mechanisms in wireless communication are vulnerable to attacks, seriously threaten privacy and are particularly resource consuming. The emergence of wireless networks brings many open issues to network designers.

Therefore, several challenges are opened particularly in the field of security and energy consumption. This paper presents the simulation of a new dichotomy mechanism called Optimal Security Adaptation Proximity-based (OSAP) WLAN applied to Geneva Hotspots network Access Points based on random mobility and AnyLogic simulations. Our work shows that OSAP is in many cases optimal in term of overall network utilization, almost a gain of 10%. The "All secure" Decision Making Function has got the best overall security compromising rate but it is the worst case in utilization. On the other hand, "Non-secure" has got the best relative utilization rate but it is the worst case in energy wasting. Our work shows that our solution is optimal in term of overall utilization rate because it tackles at the same time the worst cases of "Non-secure" and "All-secure". These results encourage us to further research on other strategies that could automatically optimize the trade-off between security and performance particularly in energy consumption and overall network utilization.

References

[1] Arvinderpal S. Wander & al., Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks, Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications, 2005.

[2] Balfanz, D., Smetters, D., Stewart, P., and Wong, H., Talking to Strangers: Authentication in Ad-hoc Wireless Networks, NDSS, San Diego, 2002.

[3] Barbeau, M., WiMax/802.16 Threat Analysis, Proceedings of the 1th ACM Int. Workshop on Quality of Service & Security in Wireless and Mobile Networks, Q2SWinet '05.

[4] Bettstetter C. and al., Stochastic Properties of the Random Waypoint Mobility Model, 2004.

[5] Carman, D. W., Kruus, P. S., and Matt, B. J., Constraints and Approaches for Distributed Sensor Security, Network Associates Labs Tech. Rep. 2000.

[6] Chigan Chunxiao & all, Balancing security against performance in wireless ad-hoc and sensor networks, 60 IEEE Vehicular Technology Conference, ETATS-UNIS (2004)

[7] Chigan, C., Li, L. and Ye, Y., Resource-aware Self-adaptive Security Provisioning in Mobile Ad-Hoc Networks, Proc. IEEE Wireless Communications and Networking Conference, pp.2118–2124, 2005.

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

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

[10] Ganz (Z.) Ganz (A.), Park (H.). Security broker for multimedia wireless LANs: Design, implementation and testbed. 1998.

[11] Johnston, D., and Walker, J., Overview of IEEE 802.16 Security, Security & Privacy Magazine, vol. 2, Issue 3, IEEE Computer Society Press, pp. 40-48, 2004.

[12] Moustafa, H., and al., Authentication, Authorization and Accounting (AAA) in Hybrid Ad-hoc Hotspot's Environments. WMASH'06, September 29, 2006, Los Angeles.

[13] Potlapally, N., and al., "Analyzing the Energy Consumption of Security Protocols", ISLPED 2003.

[14] Seigneur, J.-M., "Trust, Security and Privacy in Global Computing", PhD Thesis, Trinity College Dublin, 2005.

[15] SAXENA, B., An adaptive security framework for wireless ad-hoc networks. Wireless World Research Forum (WWRF), 2004. Euro-Labs.

[16] Yixin, J., & al., A mutual authentication and privacy mechanism for WLAN security: Research Articles, Jan. 2008 Wireless Communications & Mobile Computing.

[17] Yuan, L., and Qu, G., Design Space Exploration for Energy- Efficient Secure Sensor Network, ASAP 2002.

[18] Zhou, L., and Z. J. Haas, Securing ad-hoc networks, IEEE Network Magazine, vol. 13, no. 6, pp. 24–30, Nov.'99.

[19] http://www.xjtek.com/anylogic/

[20] http://www.swiss-hotspots.ch/