Security Key Management Model for Low Rate Wireless Personal Area Networks

Anass RGHIOUI *rghioui.anass-etu@uae.ac.ma*
Laboratory of Informatics, Systems and Telecommunications
Faculty of Science and Technology of Tangier
Abdelmalek Essaadi University, Morocco

Said BOUCHKAREN *sbouchakaren@uae.ac.ma*
Laboratory of Technology of Information and Communication
National School of Applied Sciences of Tangier
Abdelmalek Essaadi University, Morocco

Anass KHANNOUS *khannous@ensat.ac.ma*
Laboratory of Informatics, Systems and Telecommunications
Faculty of Science and Technology of Tangier
Abdelmalek Essaadi University, Morocco

Mohammed BOUHORMA *m.bouhorma@fstt.ac.ma*
Laboratory of Informatics, Systems and Telecommunications
Faculty of Science and Technology of Tangier
Abdelmalek Essaadi University, Morocco

Abstract

IEEE 802.15.4-based devices networks known by the name of LR-WPAN (Low Rate Wireless Personal Area Network) are characterized by low computation, memory and storage space, and they do not possess an infrastructure. This makes them dynamic and easy to deploy, but in the other hand, this makes them very vulnerable to security issues, as they are low energy so they cant implement current security solutions, and they are deployed in non-secure environments that makes them susceptible to eavesdropping attacks. Most proposed solutions draw out the security of the bootstrapping and commissioning phases as the percentage of existing of an intruder in this time is very low. In this paper, we propose a security model for LR-WPANs based on symmetric cryptography, which takes into account securing the bootstrapping phase, with an analysis of the effectiveness of this proposal and the measures of its implementation.

Keywords: LR-WPAN, Low Rate Wireless Personal Area Network, IEEE 802.15.4, Network Security, Key Management System.

1. INTRODUCTION

R WPAN [1] is a family of ad hoc networks for low-resource devices known by their low power consumption, low range and low debit. To communicate, these devices implement the IEEE 802.15.4 protocol [2] in the two lower layers, i.e. data link layer and physical layer. This protocol was designed specifically for this type of devices. It divides them into two types:

• FFD (Full Function Device) with all possible functions, must be at least one in a network, act as a PAN coordinator or a router, can communicate with all devices within the same network.

• RFD (Reduced Function Device) with limited functions, act as a sensor or actuator, can only communicate with FFDs.

802.15.4 defines two types of topologies: hierarchical and distributed. In hierarchical topologies devices are placed in groups as clusters, each cluster is managed by a cluster-head. Into a cluster, cluster-heads can communicate with each other, but devices can communicate only with their cluster-head.

In distributed topologies, all devices contribute to the formation of the network and every one of them can communicate with others who are within his reach.

Although LR WPAN characteristics helped greatly to the development of ubiquitous networks [3], they have a high security issues caused by the absence of a security infrastructure. Devices do not have sufficient resources to implement known security protocols that have proven their effective-ness [4]. One of the security deficiencies these networks suffer from, is the easy disclosure of exchanged information between devices into the network [5]. This information can be used by attackers in order to disrupt the functioning of the network. Among the solutions proposed to address this problem is the use of a specific cryptographic protocol, which respects the specificity of LR WPAN networks, as first line defense. Most solutions in this sense choose to deal with the hierarchical topologies because the devices are placed in an ordered manner and well controllable [6]. Also, these solutions neglect the security of the network deployment phase, the bootstrapping, as it takes a very little time to an attacker can intervene. This is true in a clustered networks, but in a distributed networks bootstrapping phase takes a very important time before the network being stabilized since the devices are placed in a disorderly manner. Securing this phase is indispensable, devices exchange important information if they are captured by a malicious, he can use them to attack the network.

We try to find a suitable solution to secure the bootstrap-ping phase in distributed LR WPAN. We propose a security model based on symmetric cryptography with a specific key establishment scheme. In the analysis part, we study the advantages of this solution in terms of its respect of: security metrics, flexibility, scalability, and energy-efficient.

After this introduction, the structure of the rest of the pa-per is as follows: Section 2 gives a brief overview of LR WPAN specifications, Section 3 discusses the proposed security model, and Section 4 presents a theoretical analysis of this model in terms of energy, flexibility and security. Finally, Section 5 concludes the paper.

2. LR-WPAN SPECIFICATIONS

2.1 Architecture and Security Specifications

In the studied network, it exists three types of devices:

• The base station BS, a powerful machine, is the network supervisor, collects data, manages the entire network, gathers information and updates devices. It can be protected from attacks by means of known security systems.

• FFDs act as routers for messages circulating in the network. These messages take one direction, from or to the base station.

• RFDs play the role of host devices; they represent either sensors or actuators.

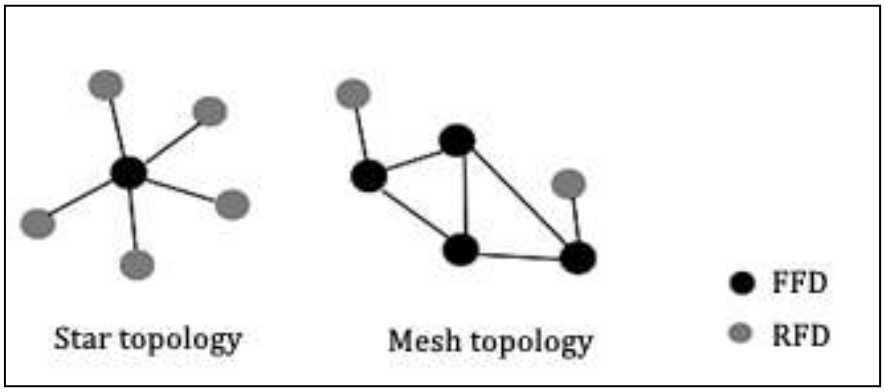

FIGURE 1: LR-WPAN topologies and devices.

LR WPANs do not possess an established secure infrastructure, in most cases; nodes are deployed in non-secure environments. These types of networks are vulnerable to Sniffing attacks without any difficulty to the attacker. There-from, the data exchanged within this network is non-confidential. To ensure it confidentiality, it is necessary to use a cryptographic system.

IEEE 802.15.4 defines two types of topologies: star and mesh (Fig 1). In star topology, devices are placed in groups as clusters, each cluster is managed by a cluster-head. Into a cluster, devices communicate only with their cluster-head. Cluster-heads can communicate with each other. In mesh topology, all devices contribute to the formation of the network and every one communicates with others who are within his reach.

2.2 Related Works

The cryptography solution ensures confidentiality, authentication and integrity of exchanged messages. By encrypting the data, no one can understand the message contents without mechanisms to decrypt it.

Applying cryptography in LR WPAN networks must take into consideration characteristics and constraints of devices implementing this technology, such as low power battery, low storage ability and low computing capacity, to optimize resources and provide to nodes longer life lasting. Even if efficient key management systems exist in today's internet, but their underlying cryptographic algorithms are either too heavy to run on resource-constrained nodes, or do not provide a satisfactory security level.

There are two types of cryptographic systems: symmetric and asymmetric. In symmetric cryptography, both communicating parties must share the same security key. However, for asymmetric cryptography, each unit has two keys: a public one that attributes to each device wants to communicate with it, and a private one that keeps it secret, used to decrypt messages encrypted by the public key. The ad-vantage of asymmetric cryptography is its security keys mechanism, instead of symmetric cryptography where the problem of how a device will share its key privately with the other one without being disclosed by unauthorized parties.

Since energy conservation is an essential element in LR WPANs, most of studies concerning LR WPANs [7], [8], [9], [10], [11] recommends the use of symmetric cryptography because, unlike asymmetric cryptography, it implements algorithms that do not require a lot of computation, as a benefit, it does not consume much energy. The difficult part in this kind of cryptography is security key management since each message sender must have the same shared key with the recipient to decrypt the encrypted messages. Both of them must have specific mechanism to exchange the security key without being unveiled by an intruder.

Existing solutions are based either on pre-shared information between nodes of the same network [12] [13] [14] [15] or depends on a trusted third party that manages the security keys between these nodes [16]. In the pre-shared based solutions, we find the use of a secret master key pre-shared between all nodes in the same network to use it as a basis for generation of session keys between them. Other solution based on multiple pre-shared keys that if a network gather N nodes, each node will hold N - 1 pairwise key shared with network nodes. In addition, there are solutions that use a random sharing key and depends on probability functions or nodes location to find at least one shared key between two nodes on the same network. Yet there are solutions that use a trusted third party to manage security keys, usually it is the base station or a local powerful nodes.

3. LR-WPAN SPECIFICATIONS

Our main purpose is not to offer a complete security solution for LR WPAN networks, but the aim of our study is to pro-pose a security model based on symmetric cryptography, providing a key establishment solution, for distributed LR WPANs, taking into account the security of the bootstrap-ping phase. So our scheme can be adapted and implemented by any symmetric cryptographic system as needed, de-pends on the used application.

3.1 Assumptions

We suppose that LR WPAN consists of following units: a base station, routers and hosts. Each one of routers and hosts has a unique identifier. Hosts do not communicate with each other.

Notation	Description
BS	Base Station
ID	Unique IDentication number
D_i	Device i
L	Device level in network, relative to the *BS*
S_{BS}	Generated seed by *BS*
S_{Di}	Generated seed by a device D_i
K^{Di}	Symmetric key generated by a device D_i
$K^{Di,BS}$	Symmetric key shared between D_i and *BS*
(A) $K^{Di,BS}$	Encrypted message A by $K^{Di,BS}$

TABLE 1: List of Notations.

All devices are located in the network in a distributed way, but no one is outside the reach of other network devices. Thus, each host is connected to at least one router.

Communications within the network are of two types: communications exchanged between the devices and the base station, and those exchanged between the devices themselves to establish connections and update the network topology.

In the base station, we create a database of devices that will be in the network, it is implemented by data concerning these devices. The both information necessary for our solution are the identifier and the address of each device.

Every device D_i has two type of security keys: $K^{Di,BS}$ a pairwise key between D_i and the base station *BS*, and $K^{Di,j}$ between two devices D_i and D_j. To generate a $K^{Di,BS}$ key, we use a base station generated seed S_{BS} and the device ID. To generate $K^{Di,j}$, we use a device generated seed S_{Di}.

The choice of the cryptographic algorithm is left to the user, also the choice of the method to which it will combine between S and the device ID to generate the key, according to its needs and its deployment environment.

3.2 Solution Purpose

During the network start-up, the bootstrapping phase, devices need to exchange them identities and other information to make connections and update them routing scheme. An attacker can easily steal this information at this stage and use them after in his attacks.

Our solution purpose is to develop a security model suggesting a scheme for pairwise key establishment at bootstrapping phase, which will secure the two kinds of communication existing in this network: communication be-tween a device and the base station, and communication between two devices, a host and a router, or two routers.

4. SECURITY KEYS ESTABLISHEMENT

4.1 $K^{Di,BS}$ Establishment

As described in Fig. 2, the base station *BS* generates a seed S_{BS}, sends it to the devices in the first row, the message is determined as a message of level L_1 since it belongs to the *BS*, which represents the head of the network.

A device D_i that receives this message will keep the seed, increment the level L of the received message and make it as its level, so if the first message that is generated by the base station equal to 1. The first devices that receive this message will have L_2 , and so on, each node that receives this message for the first time will increment its level. Thus, it records the sender address of this message as its gateway to the *BS*. Thereafter, each node will send the received seed to other devices, in this case: if a node has already received the seed, it will check the level of the sender, if it is less than or equal to its level, it will reject it, otherwise it will record the sender address as its second gateway. If a device receives the message for the first time, it will proceed as cited before.

So on, until all the devices in the network receives the seed S_{BS}. This way, each device will use the seed with its own ID to generate the secret key to encrypt its communications with the *BS*. Since the base station has the seed and all devices IDs in its database, it will generate for each one its appropriate security key. Upon receiving an encrypted message, it will check the address of the sender to know its key that will use to decrypt the message.

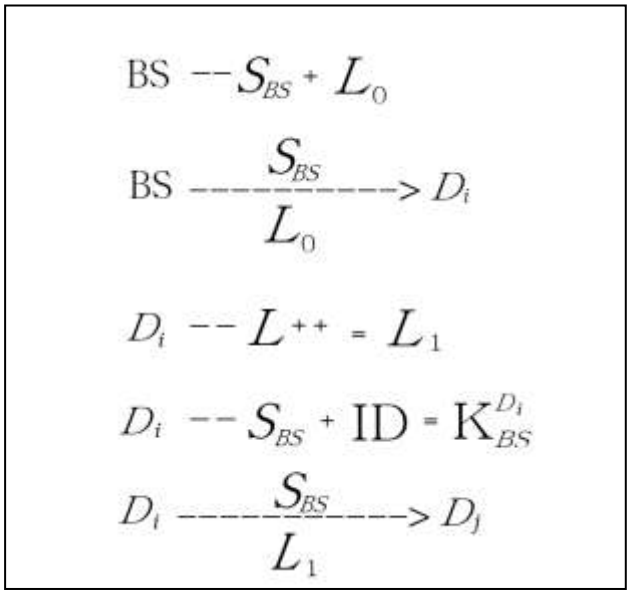

FIGURE 2: $K^{Di,BS}$ generation messages exchange protocol.

4.2 $K^{Di,j}$ Establishment

After that each device in the network has a symmetric key $K^{Di,BS}$ shared with the base station, they will need to communicate with each other to share some information to up-date them routing tables. For this (Fig. 3), each device generates its own seed S_{Di} and use it with its ID to generate a symmetric key K^{Di} in order to share it with its nearest devices. If a two devices D_i and D_j want to establish a secure communication, firstly, they exchange hello messages, including them level L. The device that has the level less than the other, which is to say it is in a position nearest to the base station, will deal with authentication procedures and key exchange.

As described in Fig. 2, assuming that D_i level less than D_j. In this case, D_i records in a message D_j address and its own key K^{Di}, encrypts this message by its key $K^{Di,BS}$ and transfers it to the base station. The latter, i.e. the *BS*, decrypting this message will understand that the node owner of the address contained in the message, i.e. D_j, wants to communicate with the node sending the message, which is D_i. The base station will check them in its database, if it is OK, it encrypts the key of the sender node K^{Di} with the solicited node key $K^{Di,BS}$ and sends it to this latter, i.e. D_j, to use it to communicate securely with the other node D_i.

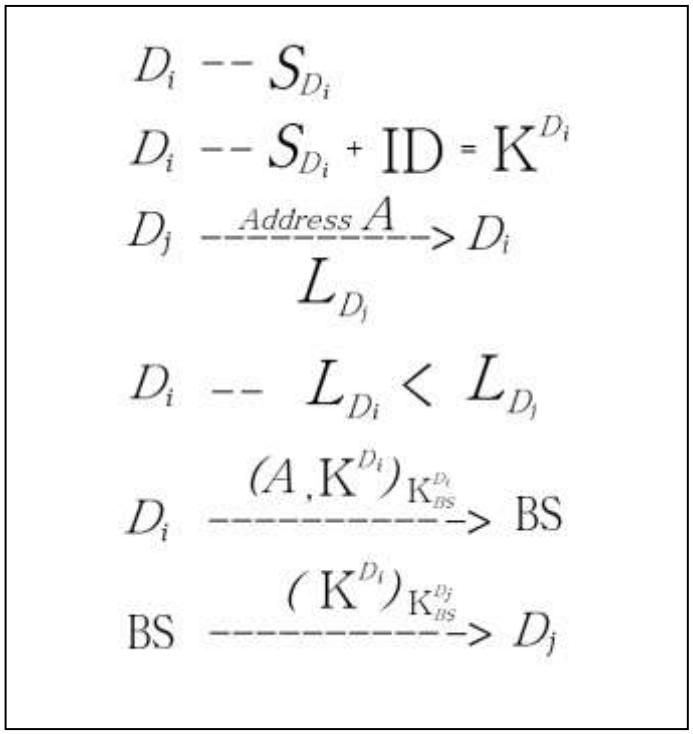

FIGURE 3: $K^{Di,j}$ generation messages exchange protocol.

5. PERFORMANCE EVALUATION

We evaluate our work relative to three criteria: energy and time efficiency, an essential element for LR WPAN networks, flexibility and scalability of this model in a dynamic network like distributed networks and security our main objective of this study.

The evaluation of our scheme is based on simulations made on the TOSSIM simulator of TinyOS. The simulations were compiled for the TelosB platform. TelosB is based on the low-power microcontroller MSP430 16-bit with a clock frequency of 4 MHz. It implements the IEEE 802.15.4

transceiver CC2420 with a claimed data rate of 250 Kbps. We used AES 128-bit as the symmetric cryptography protocol. We used PowerTOSSIM plugin for energy analysis.

5.1 Energy Cost

From energy point of view (Fig. 4), which is an essential metric for LR WPAN networks, and a critical criterion of choice to adopt or not a solution, our model does not require a lot of calculation or exchange between devices to establish security keys, it can be considered as an energy-economizer.

Our model is based on symmetric cryptography that is recommended by experts in the field as an appropriate solution for LR WPANs. Our proposal for key management in our scheme has two key types to secure two important types of communication within this network communication between the base station and network devices, and communication between these devices, so, any device have to store only its symmetric key shared with the base station, and the keys of these gateways, i.e. the router devices with a level less than it and convey its messages to the base station. Network device uses its ID to establish the key; it does not need to store other additional information that will charge its space storage. In terms of computation, a device only needs to combine between the Seed and its ID to have the key, an operation that not require many computation processes.

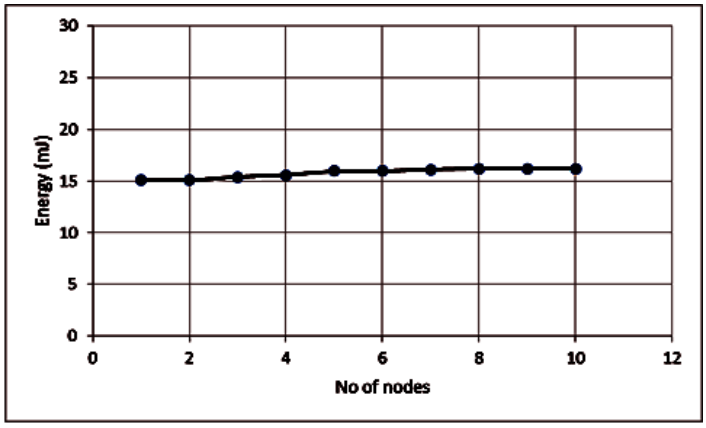

FIGURE 4: Key protocol energy cost.

5.2 Time Evaluation

The time of generation of a symmetric key is negligible. However, the key distribution takes a significant time, with the increase in the number of nodes, the time spent in key distribution increases linearly, and this makes the graph follow a linear trend (Fig. 5).

Several factors can influence the time of the distribution key as devices gathering, network topology, routing protocol, a device response time, total number of devices on a net-work, average number of neighboring devices, etc.. This will affect any used key distribution protocol. To accelerate time distribution and key management, we used the idea of levels. During the generation and distribution of keys, the devices need to exchange messages between them, so more than the number of devices increase the more it will take much time, and we fall into a redundancy in processing the same information several times. Separate devices in levels, where each level device communicates only with the upper or lower level devices, will limit the number of communicating to each device and therefore transmit faster the information. Thus, the same information will propagate from one level to another instead of spread from one device to another that will accelerate the distribution of information through the entire network in a very short time.

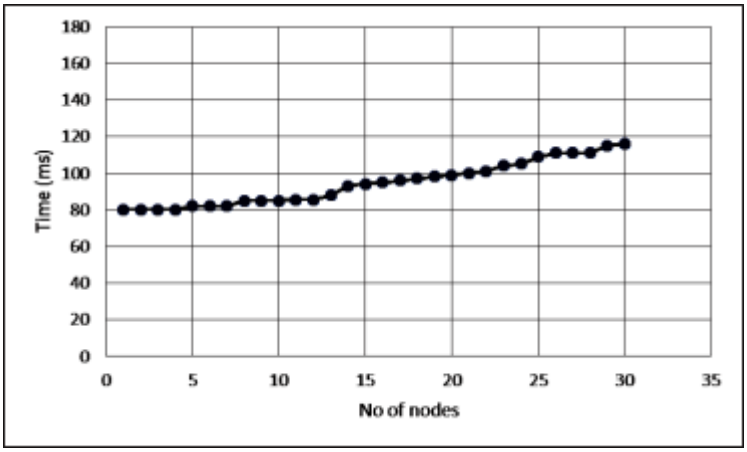

FIGURE : Key management (generation and distribution) time

5.3 Scalability

In distributed networks, two key elements are important to take into consideration, flexibility and scalability; we deal with these two concepts by designing a model that tolerates changes in topology and do not depend in a specific infrastructure. Our model is flexible towards changes in: topology, devices positions, and network density, because each device has a specific key sharing with the base station, in any physical position the device takes in the network, both can establish a secure communication using their shared key. A device can easily change a gateway by another, for any reason: optimization, due to a malfunction of an equipment, a change of position, or for some other reason, it will request the connection establishment with this new router, it has only forward its request to the base station for verification and exchanging keys. In case of a new device is being add to the network, it must be previously added to the base station database, if it is OK, it only has to make a solicitation to join the network to the more nearest router to establish a connection in the same way mentioned above.

5.4 Adaptability

Our schema can be adapted to any LR WPAN network, it has been designed is based on the exchange of information between the devices themselves, without relying on a given infrastructure or specific devices.

Our solution facilitates the establishments of new trust relationships between devices without sharing pre-shared information, devices must only be subscribed in the base station database to join the network and communicate with network devices. In addition, the key distribution method in our schema does not depend on a specific topology; even clustered or mesh topology can implement this solution.

Key generation mechanism are simple and used in all symmetric cryptography algorithms, the device has only to combine between the received seed and its ID to generate a key; we left to the user the choice of the appropriate function according to its context. Even generated key function can be negotiated between the base station and a device . For example, if network devices generate a key with a hush function and does not implement this function, the base station can ordred it to generate the key only by XORing the seed and its ID.

5.5 Security

Our solution ensures confidentiality, authentication and authorization of communications within the network. All communications and data exchanged in the network are encrypted, the only information exchanged in plaintext is the seed generated by the base station that represents only one element among others that are well secured to establish the key. Thus, no outside device unless those defined in the base station database has permission to join the network, or has the possibility of establishing a security key because it does not have mechanism that make it able to

generate the key, the thing that will make it legitimate and can join the network as a normal device. To generate the key, an intruder must be subscribed in the base station, i.e. the base station database must possess its ID, which is difficult as for non-authorized person to add or modify in this database as it is localized in the base station, a powerful and well secured machine.

In addition, a compromised device and a disclosure of its secrets presents no danger to the network since it does not affect any other device. Our solution proposes two types of keys: a unique pairwise key shared between the network device and the base station, and a pairwise key shared only between communicated nodes. Unlike solutions that are based on group key or network key solutions, a compromised node divulge only its own key and its shared key with its neighboring nodes. Even if, as devices change and update their keys and their neighbors frequently, the attacker can only decrypts the actual and new encrypted messages as he is not possess the old keys, the keys of ended sessions.

We avoided sharing of any information that may present a risk to the network; the key generation is done in the device itself. Thus, we do not share in the network devices IDs, so no intruder can take a legitimate device ID by a sniffing at-tack. The base station is a powerful machine; it was given the role of monitoring the network basing on its database of legitimate network devices.

6. CONCLUSION

We presented a settlement security keys for symmetric cryptography in order to secure the bootstrapping phase of LR WPANs. This model is based on the establishment of two security pairwise keys: The first is generated by a single device with a seed sent by the base station, shared between the two in order to secure them communication. The second is also unique to each device; it can be share with one or more other adjacent devices to update their routing tables.

This model ensures the confidentiality and devices authentication as no intruder cannot get a false ID or set the security key to integrate the network. The analysis showed that this model meets the measures that must be taken into account for LR WPANs, such as energy conservation, adaptation to the network flexibility and scalability.

We have not defined symmetric cryptography algorithms or used of specific applications, to give to the user the choice according to his needs. This model can also be used for hierarchical network topologies, and able to add additional security features to make it more robust.

We estimate subsequently try our scheme to other platforms to compare the results we get. Thus, we intend to try it with other technologies that use the IEEE 802.15.4 standard as Zigbee and 6LoWPAN.

7. REFERENCES

[1] F. Chen, N. Wang, R. German, et F. Dressler, Performance Eval-uation of IEEE 802.15.4 LR-WPAN for Industrial Applications , in Fifth Annual Conference on Wireless on Demand Network Sys-tems and Services, 2008. WONS 2008, 2008, p. 89-96.

[2] J. A. Gutierrez, M. Naeve, E. Callaway, M. Bourgeois, V. Mitter, et B. Heile, IEEE 802.15.4: a developing standard for low-power low-cost wireless personal area networks , IEEE Netw., vol. 15, no 5, p. 12-19, sept. 2001.

[3] J. Zheng et M. J. Lee, Will IEEE 802.15.4 make ubiquitous net-working a reality?: a discussion on a potential low power, low bit rate standard , IEEE Commun. Mag., vol. 42, no 6, p. 140-146, juin 2004.

[4] S. Tennina, M. Tiloca, J.-H. Hauer, M. Bouroche, M. Alves, A. Koubaa, P. Jurcik, N. Pereira, R. Severino, E. Tovar, G. Dini, and R. Daidone, Amendments to the IEEE 802.15.4 Protocol,

in IEEE 802.15.4 and ZigBee as Enabling Technologies for Low-Power Wireless Systems with Quality-of-Service Constraints, Springer Berlin Heidelberg, 2013, pp. 85112.

[5] T. Kennedy et R. Hunt, A Review of WPAN Security: Attacks and Prevention, in Proceedings of the International Conference on Mobile Technology, Applications, and Systems, New York, NY, USA, 2008, p. 56:156:8.

[6] S. Ullah, M. Mohaisen, et M. A. Alnuem, A Review of IEEE 802.15.6 MAC, PHY, and Security Specifications , Int. J. Distrib. Sens. Netw., vol. 2013, avr. 2013.

[7] Y. Wang, G. Attebury, et B. Ramamurthy, A Survey of Security Issues In Wireless Sensor Networks , CSE J. Artic., janv. 2006.

[8] P. Boyle et T. Newe, Security Protocols for Use with Wireless Sensor Networks: A Survey of Security Architectures , in Third International Conference on Wireless and Mobile Communications, 2007. ICWMC 07, 2007, p. 54-54.

[9] X. Chen, K. Makki, K. Yen, et N. Pissinou, Sensor network security: a survey , IEEE Commun. Surv. Tutor., vol. 11, no 2, p. 5273, Second 2009.

[10] An Liu, Mihui Kim, Leonardo B. Oliveira, and Hailun Tan, Wireless Sensor Network Security, International Journal of Distribut-ed Sensor Networks, vol. 2013, Article ID 362385, 1 pages, 2013. doi:10.1155/2013/362385

[11] R. Daidone, G. Dini, and G. Anastasi, On evaluating the performance impact of the IEEE 802.15.4 security sub-layer, Comput. Commun., vol. 47, pp. 6576, Jul. 2014.

[12] K. Zhang, C. Wang, and C. Wang, “A secure routing protocol for cluster-based wireless sensor networks using group key management,” In Proc. 4th IEEE International conference on Wireless Communications, Networking and Mobile Computing (WiCOM’08), 2008, pp. 1–5.

[13] I. S. Gawdan, C. O. Chow, T. A. Zia, Q. I. Sarhan, “A Novel Secure Key Management for Hierarchical Wireless Sensor Networks,” In Proceeding of 2011 Third Conference on Computational Intelligence, Modeling and Simulation (CIMSiM), 2011 , pp. 312 - 316.

[14] F. Kausar, A. Masood and S. Hussain. “An Authenticated Key Management Scheme for Hierarchical Wireless Sensor Networks,” In Advances in Communication Systems and Electrical Engineering, Lecture Notes in Electrical Engineering, Vol. 4, 2008, pp. 85-98.

[15] Y. Cheng and D. Agrawal, “An improved key distribution mechanism for large-scale hierarchical wireless sensor networks,” Ad Hoc Networks (Elsevier), Vol. 5, No. 1, 2007, pp. 35–48.

[16] T. Landstra, S. Jagannathan, and M. Zawodniok, “Energy-efficient hybrid key management protocol for wireless sensor networks," International Journal of Network Security, vol. 9, no. 2, pp. 121-134, Sep. 2009.