WIRELESS SENSOR NETWORK: TOWARDS AN IMPROVEMENT OF SECURITY POLICY

[1]MOULAD Lamyaa, [1]CHAABITA Rachid, [1]BALAR Khalid

[1]Hassan II University/ FSJES AC, Casablanca, Morocco – (lamyaa.moulad@gmail.com, chabita@gmail.com, balarhalid@gmail.com)

KEY WORDS: WSN, Wireless Network, key management, LEAP, LEAP Enhanced, power consumption, symmetric key, asymmetric key

ABSTRACT:

The ad hoc network (or MANET, for Mobile Ad hoc NETwork) is a system containing a set of devices that organize themselves, thus forming an autonomous and dynamic network, communicating via radio interface. These devices can be fixed or mobile, no wired infrastructure is available, and so these objects have to dynamically discover their environment.
The design of these applications is based on trust between the nodes constituting the network. Unfortunately, when deploying randomly in difficult hostile areas, seeing impossible to monitor, not to mention the uncertainty of the communication channel, the sensor nodes are exposed to all types of attacks and intrusions, which can hinder and prevent the diffusion of the information between the sensor nodes of the network, and influencing its performance.
Many approaches have been proposed to solve security problems in wireless networks. The solutions can be mainly classified into two categories: symmetric and asymmetric key management schemes. Indeed it is clear, that the optimal solution in this case is to use symmetric shared key systems.
In this paper, the idea of LEAP improved is to apply the same Mechanisms used in LEAP Enhanced to overcome a compromised node and also prevent a compromised base station node while using a multiple base station network, this will, on the one hand, minimize power consumption, and secondly, to replace a base station in the event of a compromise, to ensure the continuity and proper functioning of the network. The evaluation of the proposed solution was carried out using the TOSSIM simulation tool.

1. INTRODUCTION

Wireless sensor networks (WSN) [1] consist of a large number of energy-constrained and storage-constrained small sensor nodes. Typically, sensor nodes are deployed randomly in special and hostile areas, dedicated to data collection and processing. And knowing that data packets are transmitted without physical support, sensors are exposed to numerous attacks that target the theft of information by listening to the channel.

It is therefore imperative to integrate a security mechanism to ensure the valid circulation of data in the WSN. However, this is difficult to implement, especially when the nodes are of limited hardware capacity, as they are very small sizes and powered by a small battery, in which case the resources, energy and storage, must be taken into account In any security strategy, in order to maximize the life and operating life of these devices without being obliged to replace them.

To ensure the confidentiality of the information transmitted between the nodes of these sensors, the messages must be encrypted before being

transmitted. It's a big challenge to implement encryption algorithms in wireless sensor networks because of the limited resource. In addition, malicious nodes can happen to be legitimate nodes and communicate with other valid nodes. This can overturn all networks. Therefore, a lightweight and efficient key management cryptography system should be used to solve all of the above mentioned problems.

In this work we will present a new lightweight and efficient solution for key management in WSNs. The proposed key management system is based on the LEAP and LEAP Enhanced [3] protocol, starting from the following principle: All network nodes will be treated in the same way in the event of a compromise.

2. ISSUE AND MOTIVATION

Wireless sensor networks are subject to numerous malicious acts and attacks due to their deployment in open environments in hostile areas and limited resources. In this sense, and to deal with these threats, a variety of protection systems exist. Among these solutions, cryptography is cited as the first line of defence against malicious behaviour.

To provide an appropriate cryptographic prevention process for wireless sensor networks at optimal cost, while ensuring better security, the choice of the appropriate cryptographic technique is a decisive phase affecting considerably the level of security of these networks.

According to the literature, there are generally two main forms of cryptography, each of which guarantees a certain number of properties: symmetrical cryptography or a secret key and asymmetrical cryptography, also known as public key. A third form called Hybrid based on the two main forms exists in the literature.

A typical detection node has only 4 KB of RAM, however, asymmetric key management systems cost too much energy. Indeed, it is necessary to design a key management scheme to balance the compromise between key storage space and energy consumption, hence the choice of using the symmetric key management system, based on the algorithm «LEAP Enhanced» in a multiple base station diagram.

However, and contrary to the assumption used in LEAP and LEAP Enhanced [2], The base station is not supposed to be a

trusted entity, given that in turn and like any network sensor node , even if it is more powerful in terms of calculation and storage ,a base station may also be compromised, hence the need to deploy a multiple base station system.

It is a lightweight and efficient approach to the management of secret keys in sensor networks that will, on the one hand, minimize energy consumption and, on the other, replace a base station in the event of a compromise to ensure the availability and smooth operation of the network.

3. RELATED WORKS

Many key management systems have been proposed to establish secure links in the WSN. A probabilistic key pre-distribution scheme is proposed in [6]. In this diagram, a set of keys randomly selected from a pool of large keys is assigned to each sensor node prior to node deployment. Then, two sensor nodes can share at least one common key with some probability. This scheme is improved in [5].

Two sensor nodes are required to share at least q secret keys to establish a par-pair key (pairwise). A random pair scheme is also introduced in [5] to provide perfect security against node capture. [5,6] use a threshold-based technique: If the number of compromised nodes does not exceed a threshold value, the rest of the network is not affected by compromises. Recently, the researchers suggested using the planned location of the sensor nodes after the node deployment to improve the security and scalability of key facility systems [5,6].

[3] proposes LEAP Enhanced to identify the compromised node in the wireless sensor network and improve the resistance of the basic variant of the LEAP+ protocol against node capture. However, this work does not take into account the possibility of compromise of a base station, which can negatively influence the proper functioning of the WSN[7].

LEAP+ [8] is the extension of the original version of LEAP by the same author Zhu. LEAP+ [4] is a deterministic protocol key management for wireless sensor networks. The key management mechanism provided by LEAP+ supports internal processing "In network processing" while limiting the impact on the security of a compromised node on its immediate vicinity in the network.

Therefore, instead of assuming that the sensor nodes are "anti-burglary" which often prove to be untrue, the authors assume:

- That there is a lower limit on a time interval Tmin required an opponent to compromise a sensor node.
- This time test for a new sensor node reveals its immediate and established common key neighbors with each of them is smaller than Tmin.

In LEAP + compromise, the initial key at any time allows an opponent to deduce all key pairs through the network.

Chae Hoon et al. [9] proposed an improved variant of the LEAP+ protocol called LEAP ++. This new variant provides a mechanism against DoS attacks and manufacturing nodes when establishing the key. LEAP ++ offers a good compromise resilience node with master keys used only once in shorter time intervals and provides sufficient resistance against service node and manufacturing node attacks.

With the motivation to minimize the compromised part of the network when the initial IK key is revealed, Jang et al. [10] divides the life of a sensor into P-time slices and each time interval is assigned to an initial key.

Finally, a pair of sensor nodes that do not share any hardware manipulation, but the range of wireless communication can establish an associated key through proxy nodes.

In recent work, Aekre et al. [11] proposed to use more than one base station to overcome the limitations encountered for potential base station attacks and the improvement of the LEAP protocol in terms of detecting a compromised base station in the network.

4. PROPOSED MODEL

For critical applications of sensor networks, it is strictly necessary to have a security mechanism that ensures authentication and confidentiality. It is particularly difficult to ensure optimum security in this type of network because of the limited resources of the nodes. Bearing these limitations in mind, various studies of encryption protocols have been carried out with the aim of proposing a symmetrical encryption algorithm for key management. The basic algorithms for the proposed schemes are “Leap+” and “LEAP Enhanced”.

4.1. Schema has only one BS Vs multiple BS schema

After much excessive research, the literature usually covers the functionality of the WSN based on a base station participating in a system. It is important to remember that with an increase in a sensor network, there is an increase in the distance between the base station and its associated sensor nodes and the increase in distance may change the following:

- With long distances for packets to propagate, it can be lost due to network performance degradation.
- Transmission of data between the sensor nodes and a single base station in a large network requires high energy consumption leading to a reduction in the lifetime of the nodes.
- For nodes located in the vicinity of a base station, their energy is used up rapidly, which shortens the service life excessively. [axis discussed in the chapter energy management].

To overcome these problems, a network using multiple base stations shows potential to improve performance.

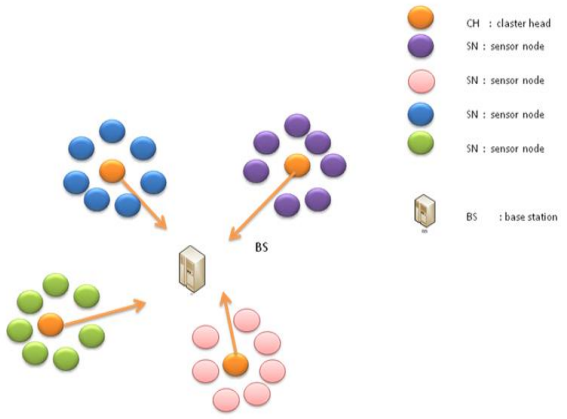

Figure 1. Single BS scenarios

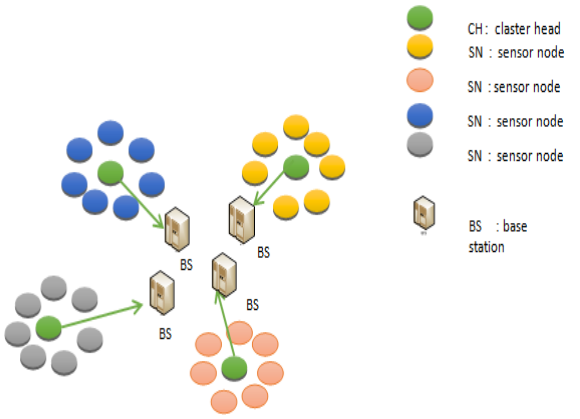

Figure 2 . Scenarios with multiple BSs

By deploying more than several BSs (Figure 2), the distance between the sink wells and its associated sensor nodes will be reduced by providing more successful paths for data transmission as well as eliminating the disadvantages of high energy consumption and safety hazards.

4.2. Detection and revocation of the compromised node

Detection and revocation of the compromised node [12]

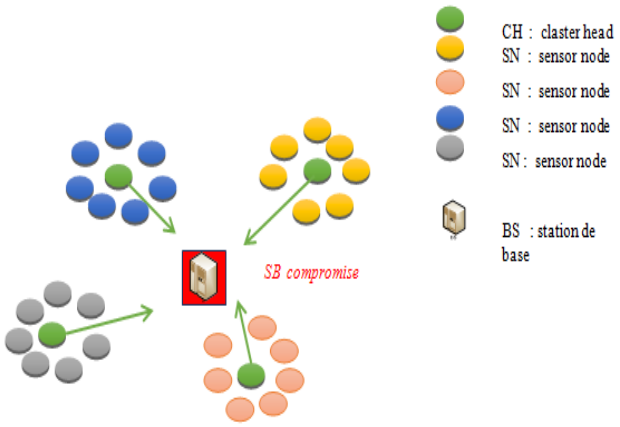

Figure 3.. Scenario with a single BS (BS compromised)

The periodic operation "PERIODIC-CHECK (Tp)" is executed in each node to check whether it is attacked or not. The "Tp" duration is the compromise of the "complexity " where the Tp could be increased to minimize the complexity of the network in terms of packet exchange, and the "threat of the attacker""where Tp could be minimized to have more frequent checks on node compensation. Now suppose a node is compromised exactly after the end of the “periodic CHECK”, which is “Tp + t”, in this case, rather than waiting for the next period (t = 2Tp), the node itself sends a “Help broadcast” message to the base station. Once this message is received, the base station broadcasts an ALERT message. This contains the id of the HELP issuing node. A node receiving an “ALERT” message, then compares the id of the node under attack with the list of ids present in its list of neighbors. If a match is detected, it removes the pair key already established with this node. Otherwise, the node maintains this id for a given amount of time, and each time it initiates the per-pair key exchange process, it compares this key so as not to establish a per-pair key with a node that is infected. In Figure 4, we present our proposed enhanced model for the detection of the compromised node.

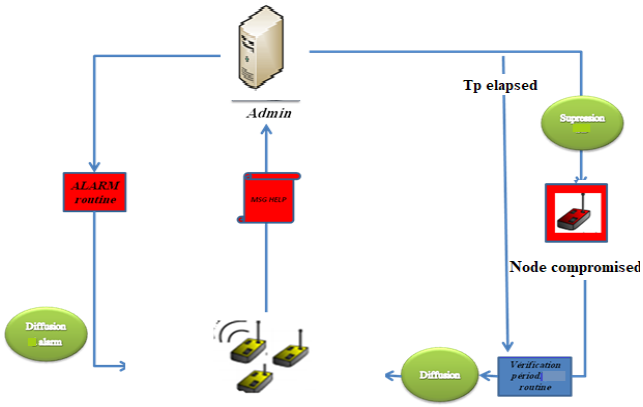

Figure 4. Diagram for the detection of the compromised node (Scenario with a BS)

Detection and revocation of a compromised base station node

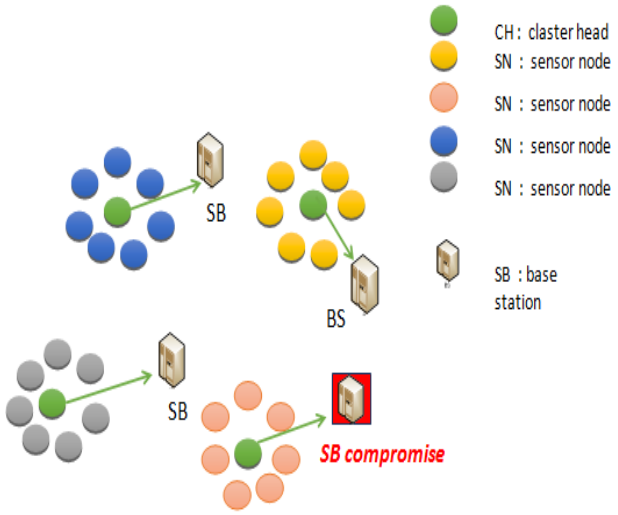

Figure 5 . Scenario with multiple BSs, and one compromised

Like the sensor nodes, the periodic operation is performed in each element of the network, the nodes and the base station, to check if it is infected or not.a hacked base station can be detected and revoked by the other base stations in case of compromise and exactly after the end of the “periodic CHECK”, the base station itself sends a “Help broadcast” message at other base stations. Once this message is received, a base station broadcasts an ALERT message. This contains the HELP issuer id. A BS node receiving an “ALERT” message, then compares the id of the BS node under attack with the list of ids present in its list of neighbouring BSs. If a match is detected, the latter will send the administrator a help message indicating that one of the base stations is hacked. In turn, the administrator removes it from the system and proceeds to replace it with another. However, the administrator validates that one of the base stations is hacked if at

least more than one of the three base stations states , therefore, the base station will not be involved in the data transmission once the other base stations discover a compromised BS. Otherwise, the BS node maintains this id for a given period of time, and each time it initiates the pairwise key exchange process, it compares this key so as not to establish a pairwise key with a node that is infected.

In Figure 6, we present the proposed model for the detection of the compromised base station node.

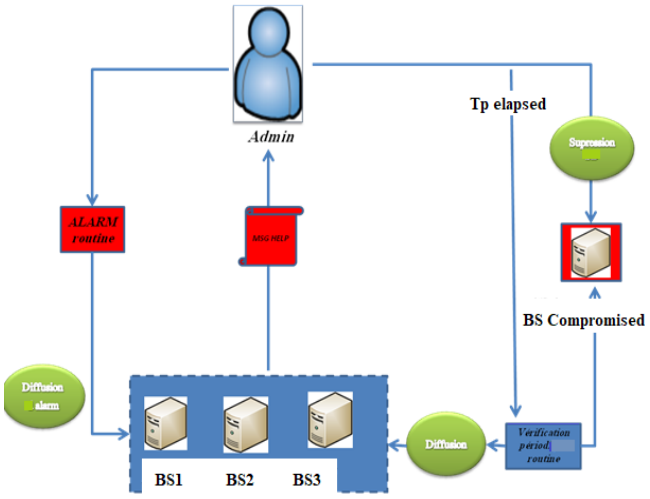

Figure 6. Diagram for the detection of a compromised BS node - Scenario with several BSs

By using multiple base stations, system performance is improved by minimizing data transmission loss, and improves security since the proposed solution could detect a compromised base station.

5. ANALYSIS AND DISCUSSION

5.1. Analysis of the proposed scheme

In this part, we will try to analyze evaluate the performance of our solution with some existing schemes in the literature. Four criteria should be taken into consideration in order to compare the performance of different key management schemes.

The complexity of communication: the proposed key management scheme must ensure the needs of the nodes relating to a deployed WSN, in terms of memory space to store their data and considerable energy resources.

Scalability: this is an essential metric, allowing the measurement of the flexibility of the protocol with the size of the wireless sensor network.

Connectivity: this metric gives the probability that two or more nodes share a key. Deterministic key management protocols like the LEAP model are based on the initial key generation and which achieves full connectivity (100%) with a low cost in terms of memory storage space, unlike probabilistic protocols which require a higher cost. high in terms of memory storage, and their connectivity depends on the size of the keyring preloaded in the nodes.

Resilience Against Node Capture: This setting allows you to assess the impact of a compromised node on the security of the rest of the wireless sensor network.

5.2. Results and comparison

- Resilience against compromised nodes

Resilience is measured by the fraction of links compromised on the rest of the message exchange in the network. We calculate the fraction of corrupted links Fx when x sensor nodes are captured in a 100 node network. Let Nx be the number of corrupted links when the attacker captures x sensor nodes.

$$Fx = Nx / N * d$$

Figure 7 illustrates the resiliency of the enhanced LEAP +, LEAP, and our scheme to attacks that compromise nodes when an attacker randomly captures 1 to 10 nodes. It is clear that our improved scheme performs better than the others it is compared to.

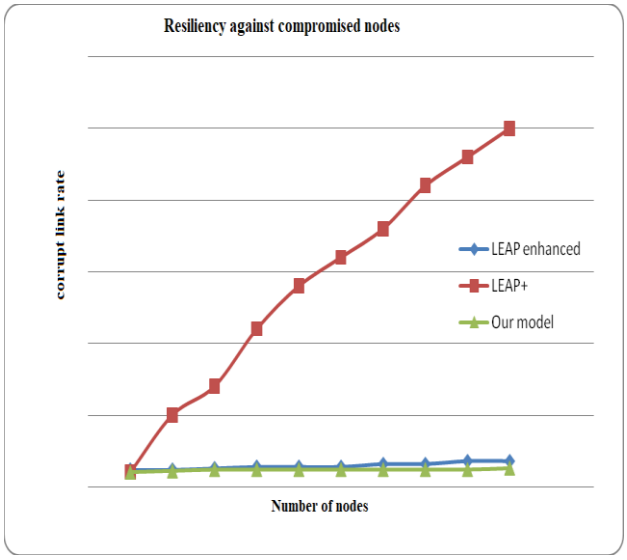

Figure 7. Resiliency against compromised nodes

- Energy consumption

La Figure 8 illustrates the variation in the energy consumed. After evaluating the average energy consumption of a node during the step of discovering neighbourhood and installing session keys, it is deduced that the amount of energy expended increases with the growth of the size of the network. This increase in power consumption is mainly due to the increasing number of packets exchanged for tuning, calculation and verification of encryption keys by sensor nodes. The energy consumed using LEAP + and LEAP Enhanced is higher compared to that of our proposed model.

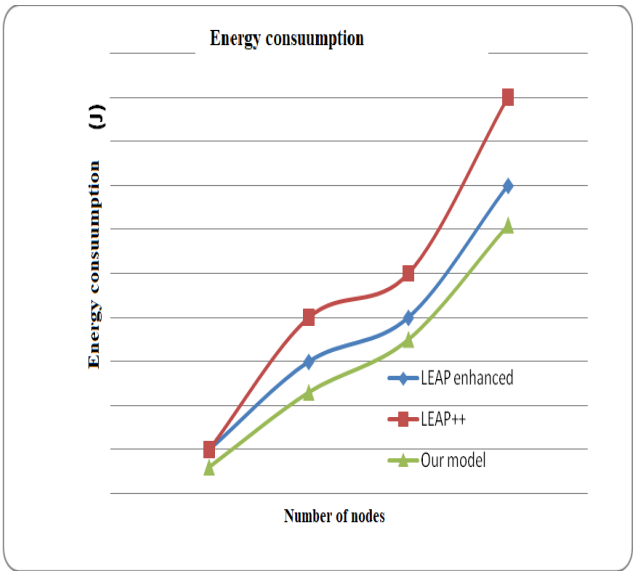

Figure 8. energy consumption

After a comparative analysis carried out in this section, we can deduce that our scheme of the LEAP improved, provides an interesting level of security against attacks, compared to other schemes cited in the literature. The experiment obtained shows the following results :

- A low cost of key memory storage space.
- A minimum rate of lost packets.
- A very reduced consumption of energy resources compared to other schemes due to the installation of multiple BSs.
- Our proposed diagram shows a reduced generation of the number of packets exchanged.
- Efficiency in terms of security thanks to the per-pair key established between two nodes, limiting the effect of a compromised node on the wireless sensor network.
- Enhanced deterministic key management protocols based on initial key generation ensure 100% connectivity.

6. CONCLUSION

Wireless sensor networks are prone to many malicious threats and attacks due to their deployment in an open environment in hostile areas, and their limited resources. In this sense, and to face these threats, a panoply of protection systems exists. Among these solutions, we cite cryptography as being the first line of defense against malicious behaviour in order to ensure security for this type of networks, it is in this sense that this chapter is written.

This contribution comes to improve the security of cryptographic protocols; We have presented a new lightweight and efficient solution for key management in WSNs. The proposed key management system is based on the LEAP and LEAP Enhanced protocol [7], starting from the following principle : All network nodes will be treated in the same way in the event of a compromise, the idea is to apply the same Mechanisms used in LEAP Enhanced to overcome a compromised node, and also to prevent a base station node being hacked while using a multiple base station network, has on the one hand minimized power consumption and reduced power consumption. on the other hand, to replace a base station in the event of a compromise. The results showed that this low power consumption scheme presents a strong line of defence against the majority of attacks against all network components, even for the base station and shows good performance in terms of connectivity, management of memory resources and resistance to attacks with a small generation of the number and size of exchanged packets. So we can conclude that our proposed scheme of LEAP improved, provides a high level of security against attacks and low power consumption compared to those described in the literature.

7. REFERENCES

[1] F. Akyildiz, W. S. Sankarasubramaniam, E. Cayirci, “A survey on sensor networks,” IEEE Communications, Aug 2002.

[2] ”Google”. ”google.ca,”. ” http ://images.google.ca/”, ”consulte le 5 sep 09”.

[3] Y. Maleh, A. Ezzati, “A review of security attacks and intrusion detection schemes in wireless sensor network”, International Journal of Wireless & Mobile Networks (IJWMN) Vol. 5, No. 6, December 2013.

[4] S. Zhu, S. Setia, et S. Jajodia, « LEAP+: Efficient security mechanisms for large-scale distributed sensor networks », ACM Trans. Sen. Netw., vol. 2, no 4, p. 500–528, nov. 2006.

[5] D. Liu, P. Ning, et R. Li, ‘’Establishing pairwise keys in distributed sensor networks’’, ACM Trans. Inf. Syst. Secur., vol. 8, no 1, p. 41–77, févr. 2005

[6] Sarmad Ullah khan, “ Key management in wireless sensor networks, IP-Based sensor networks, content centric networks”, March 14, 2013 .

[7] Y. Maleh, A. Ezzati, “An Efficient Key Establishment Protocol for Wireless Sensor Networks”, Advances in Ubiquitous Networking, Springer Lecture Notes in Electrical Engineering, 2011.

[8] S. ZHU, S. SETIA, S. JAJODIA, “LEAP+: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks”, ACM Transactions on Sensor Networks, Vol. 2, No. 4, pp. 500-528, November 2006.

[9] Chae Hoon Lim, “LEAP++: A Robust Key Establishment Scheme for Wireless Sensor Networks 2008 IEEE DOI 10.1109/ICDCS.Workshops, 2008.

[10] J. Jang, T. Kwon, and J. Song, "A Time-Based Key Management Protocol for Wireless Sensor Networks", Third International Conference, ISPEC 2007, Springer LNCS, pp 314-328 Hong Kong, China, May 7-9, 2007.

[11] S. A. Aekre, R. K. Krishna, “Improved LEAP Protocol with Experimental Results and Conclusion”, International Journal of Scientific and Research Publications, Volume 5, Issue 8, August 2015.

[12] Y. Maleh and A. Ezzati, “An Efficient Key Establishment Protocol for Wireless Sensor Networks’’, The International Symposium on Ubiquitous Networking, LNEE 2015, p. 273-281, 2015.