IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 04, Issue 11 (November. 2014), ||V2|| PP 40-47

An optimized algorithm for a secured Wireless Sensor Networks integration into Enterprise Information System

Ouail Abroun[1], Abderrahim Tahiri[2], Noura Aknin[3], Kamal Eddine El Kadiri[4]
[1] *Abdelmalek Essaadi University Tetouan, Morocco* [2] *Abdelmalek Essaadi University Tetouan, Morocco*
[3]*Abdelmalek Essaadi University Tetouan, Morocco 4Abdelmalek Essaadi University Tetouan, Morocco*

Abstract: - Due to it wide range of applications, Wireless Sensor Networks (WSN) represent a rapidly growing technology promising to resolve problems that were impossible in the near past. At the level of enterprises, the integration of WSN technology to their information system is an issue which stills under research, and many challenges face such merging. In this paper, we focus on the security aspect of WSN integration to Enterprises Information System (EIS) through the discussion of the different components of security that should be covered in order to consider a system as secured. From another level, our aim in this paper is to suggest an optimized algorithm that can lead to a secure use of WSN inside enterprises. To attain this purpose, we diagnose the main threats that face WSN security in those enterprise and compare the different WSN security related algorithms.

Keywords: - *Attacks; Authentication; EIS; Middleware; Security; WSN.*

I. INTRODUCTION

WSN is considered to be one of the rapidly growing technologies and the most widely used network for physical and environmental conditions such as temperature, humidity noise and others [18] [14]. The confidence which was gained by WSN is due to the easy network topology, low cost and availability of the components of the network. This technology can be seen in many fields such as military, healthcare, building monitoring and much more. At the level of Enterprises, WSN integration to this world is still under research [15] [6], and efforts are made in order to find the optimal way to make such integration as much as efficient as possible. In a previous article [17], we suggested a middleware architecture that allows to integrate WSN to Enterprises, especially to their information system and to overcome the different challenges that face this merging. In accordance to this work, we discuss in this paper the security side of this architecture, and detail the optimal manner that may increase the collected data security. To attain this purpose, we enumerate the different concepts that should be respected when adopting a security policy (section 1), the attacks and threats that concern WSN security (section 2), what make WSN different than the classical network, the role of this difference in data security and the advantages that Enterprise give to WSN (section 3 and 4) and finally we present our vision about providing a secured WSN based data collection inside Enterprises Information System, through an optimized algorithm and we evaluate it efficiency in term of memory and energy consumption.

II. SECURITY IN WSN

1. WSN Security requirements

WSN is used mainly for environment conditions monitoring through data collecting and also data aggregation in order to provide the needed highly accurate data for decision making. In the enterprise world, data exchange is very sensitive and need to be carefully considered. What asks for a security policy that should be adopted by those enterprises.

Based on the work of [1], in order to name a WSN as secured, the following components should be fulfilled:

- Data confidentiality

Confidentiality means to keep relevant information hidden from outside parties. In other words, data should not be leaked to any of the neighboring networks, what makes every network independent from the external environment.

In order to maintain this concern, the encryption of the exchanged data is adopted using a secret key. However in term of resources, such approach is considered to be too expensive to be perfectly applied in WSN [6].

- Data authenticity

In order to guarantee that the received data is originated from a trusted source, authentication allows to secure the network from intruders that are trying to inject false data into the information process. Based on SPINS [1] principles, most proposals in term of data authenticity, rely on asymmetric digital signatures which is also a resources consuming approach that needs high computational abilities that are not available at the level of WSN.

- Data integrity

A property that can be provided also by authenticated data. The major role here is to guarantee that data when received is not changed, in any way, by an external intruder.

- Data availability [5]

At this level, the ability of a node to use resources and whether the network is available for the messages to communicate.

- Data freshness

In WSN, where the transmitted data change rapidly, it is very important to allow that the received data is in the most recent form and old messages weren't injected during the communication process.

- Robustness and Survivability

Since no network is secured from external attacks, having a survivability property and robustness against such attacks is a needed component, especially for a vulnerable network such as WSN.
Those components represent the highly needed principles in WSN, and as shown by [21] and [6].

The above principles can be summarized in the following figure:

Fig. 1. WSN Security issues

2. WSN limitations and challenges

One of the major issues that we see are asking for the creation and adoption of entirely WSN devoted security policy is that WSN have particularities and differences when compared to other networks. In this section we discuss the major limitations that made WSN particular when compared to other networks.
According to [2], the major challenges that influence on the security of WSN are the size of sensors that belong to a certain network, the processing power, energy, memory and the type of tasks that are expected from sensors to accomplish.

- Deployment environment

In most of the cases, the sensors, that are the major components of WSN, are deployed in less secure and dangerous areas. For example, in order to prevent forest fires, [10], sensors are placed inside forest, with all the risks that such environment can represent. In other scenarios, WSN are deployed in the wild life, battle fields, under sea and much more [2]. With such conditions, an important limitation can be found only in WSN.

- A wireless nature

As concluded by [12], by having a wireless nature, security became a major concern for data exchange in WSN. Due to this nature, vulnerability increase with the size of the network. In general, a WSN is composed with tiny microcontrollers with limited capabilities, named motes. Those motes are wirelessly interconnected, with no intermediate layer between them, what make it a perfect attack opportunity.

- Self-configuring Network

Wireless Ad hoc networks are self-configuring, what means that nodes can leave and enter the network depending on their needs, what opens the door for outside attacks.

- Ad hoc topology

As stated in [16], Ad hoc network is a decentralized type of wireless network, nodes within each other radio range communicate directly via wireless links while these which are far apart rely on other nodes to relay messages.

- Energy, computation and memory

Those three component are the major concerns of research in WSN field. Wireless motes, have a life time of their battery, which is dependent on the energy consuming computation tasks (communication and data aggregation) that are assigned to those mote. Memory is also another limitation of WSN, when knowing that those microcontrollers have only the memory needed for processing and transmission, so implementing security related algorithms on those motes in addition to their tasks is going to be a complex task.

To summarize, due to the different limitations and challenges, WSN can be considered a unique system with a unique architecture that needs to be treated differently. On the other hand, those limitations encouraged the existence of different attacks targeting the security of the transmitted data inside the network.

3. Attacks on WSN

Based on the work in [16], attacks on ad hoc wireless networks can be classified under two classes, passive and active attacks.

- Passive attacks:

Where the attackers spoof the exchanged data in the network without altering it, what harms the confidentiality component of network security.

- Active attacks:

At this level data integrity and authenticity are under question, since the attacker purpose is to alter or completely destroy the exchanged data in the network.

Regarding their type (active or passive), their source (external or internal) and also the attacked targeted level of the wireless network (the security mechanisms or basic mechanisms [2]. According to the finding in [6], attacks against WSN can be classified under the following types:

- Spoofed, altered, or replayed routing information

Where the main purpose of the attacks is to create routing loops, generate false error messages and partition the network.

- Selective Forwarding

Benefiting from the multi hop nature of WSN, malicious nodes can ensure that information is not propagated properly by refusing to forward certain received messages from other nodes.

- Sinkhole attacks:

Considered in [9] as the most severe attacks against sensor networks. In this attack, a node tries to attract as much traffic as possible from a particular area, by making itself look attractive to the surrounding nodes. In this way it manages to attract all traffic that is destined to the base station, where many attacks can be launched to modify or drop the received data.

- Sybil attacks:

In this type of attacks, a node illegitimately claims multiple identities [11], and behaves as if it were a larger number of nodes, for example by impersonating other nodes or by claiming false identities. This attack represents a dangerous threat to routing mechanisms; reduce the effectiveness of fault-tolerant schemes, dispersity and topology maintenance in WN according to [4].

- Wormholes:

According to [23], an attacker records packets at one location in the network, transfers them to another location, and retransmits them there into the network. As a result, communication inside the network will be disrupted, what causes a major collapse in delivering the sensed data.

- Hello flood attacks

This attack take advantage of the need of many routing protocols to require nodes to broadcast "HELLO" packets to announce themselves to their neighbors, and that when such message is received, the node assumes that it is within the transmission range of the sender. Attackers broadcast large number of HELLO messages in order to convince other nodes to be their neighbor, what creates false links between network nodes and the attacker. When an attacker succeed in creating such false links within the network, this operation continues from one contaminated node to another, rapidly propagating as a flood. And finally the network enter a state of confusion.

Considered to be the major attacks for whom researchers are trying to find the optimal solution, those attacks show also many weak sides of WSN that may represent major fears to adopt such technology, especially where information privacy is a very important issue, as it the case in the enterprise world.

4. WSN in Enterprise Information systems and security

The development of information technology have provided new solutions that fulfill the growing needs of business processes and manufacturing. According to [13], today, not only large and medium sized companies but also small companies are quickly learning that a highly integrated ES is a requirement for the global operation. ES has become a basic information processing requirement for many industries.

From another side, information play a major role in directing the architecture of the whole enterprise. In order to improve the architecture of the enterprise in accordance with it strategies, according to [7] enterprise architects adopt a set of techniques to bring about the different changes in the organizations. These techniques are classified under four major types:

- Business architecture.
- Information architecture.
- Applications architecture.
- Technology architecture.

Those types show that information does not only contribute to the success of business, but also to a major issue as the architecture and the identity of the enterprise.

Due to this high value that Information systems have for enterprises, it became essential to conduct research for the goal of improving those systems and open new opportunities for accurate data collection. For this reason, we proposed in [17] the integration of a rapidly growing technology WSN, which is the base of tomorrow technology through it major role in the internet of things and many other applications as discussed in section1. In that work, and based on information system definition in [8], we envisioned enterprise information system to have the following form:

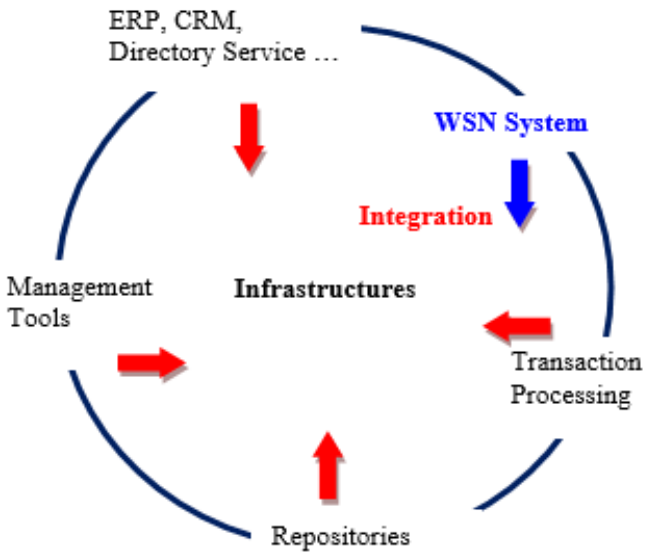

Fig. 2. Enterprise Information System and WSN integration.

The integration of WSN to Enterprises information system needs to overcome major challenges that face such merging, and security is one of them. As discussed in section 3, WSN is characterized by an entirely different architecture, and it faces different types of attacks that may lead to crashes and failures in the delivery of the needed information. At the level of enterprises, if willing to adopt the use of WSN inside them, those risks represent a major challenge that need to be overcome. However, inside enterprises, many limitations of WSN can be reduced.

- Deployment environment:

Sensors when deployed inside the enterprise (for employees presence or work environment conditions monitoring for example) they are considered to be in a safer place then being exposed to external dangers such as in the wild life or military. With less human interaction, another advantage is added to the integration of WSN to enterprises.

- Energy:

Based on [4] energy is identified as a crucial resource in wireless sensor networks, and the problem is coming from the difficulty to recharge the sensors because they are usually deployed in a hostile environment.

In Enterprises, it is not the case, the batteries can be easily replaced in a small amount of time.

- Computation capability:

Since it is highly related with energy consumption, when dealing when a big number of data, and processing is required to take place at the level of sensors then energy and time to deliver response will be in question. Based on the work of [24] we suggest using the idea of outsourcing tasks in order to reduce the overall energy consumption as well as the energy consumption of the sensors with low remaining energy

What can be revealed from those different issues, is that enterprise present many advantages that can be motivating for the integration of WSN, especially that it allow to overcome the major problem facing this technology, energy. However still another side that we discuss in the next section, which is security.

5. WSN security strategy inside EIS

When analyzing the different attacks that WSN are exposed to we can find that the existence of malicious nodes is the main source of the attacks (Spoofing, selective forwarding, sink holes, Sybil, wormholes and hello flood attacks). At security level, we are talking about authentication or identity verification. Therefore, to prevent those attacks from crashing the network and injecting false information, a highly secured authentication mechanism should be provided. According to [22] three main methods of authentication are used in wireless networks:

- Open authentication

A weakly secured mechanism because that it only requires that the end device be aware of the Service-Set Identifier (SSID) used on the network.

- Shared authentication

Used in individual and small wireless LAN implementations, based on shared key that is given to both sides of the connection

- Extensible Authentication Protocol (EAP) based authentication:

This is the most common method used by enterprises, it is based on the use of an authentication server that take the responsibility of authentication based on different credential options.

What can be obvious is that the use of EAP may bring many benefits and help to resolve the problem of authentication for wireless sensor networks, however this method consumes resources and it is not suited for such type of networks, even that the main idea can be very useful.

Consequently, the work in [20] suggested the use of Wireless Extensible Authentication Protocol (WEAP) which is an adapted version of EAP to the WSN constraints. This work suggested an authentication process between wireless client and a RADIUS server, where the server send the dynamic encryption key to the access point via a secured channel (through sensors). This protocol shown many advantages in term of increasing security for WSN. However, the major limitation that we found in this method is the dependency in the communication between the server and the client on the secured channel, even that it suggests the use of multiple base stations to resolve the problem; however this solution is more expensive in term of time and complexity. Another limitation of this method is that more the distance between the client and the server grows, the needed transmission time and complexity also grows.

To overcome those problems we suggest to take advantage of today trends, with the growing number of internet connectivity ability under Internet of things principles to accomplish the following goal: The independency of the sensors from the network in term of authentication of data senders. Consequently, no matter where the sensor is located the process of authentication consumes the same amount of time and resources.

Noting that communication for authentication should be exclusively encrypted.

6. The suggested algorithm

Today, accomplishing such task is possible because of the existence of protocols such as 6LowPAN that have been already implemented in many cases [18], and we adopt that protocol because of the different advantages that it provide as stated in [3]:

- Future trend: IPv6 is the next generation for the internet.
- Bigger Address Space: the presence of a huge address space that can be used for large-scale and dense WSNs.
- Stateless Address Configuration: 6LoWPAN bases IPv6 addresses on their MAC addresses.
- Ease of Access: using 6LoWPAN protocol can be accessed easily by other IP-based networks than a proprietary WSN protocol. Consequently, there is no need for gateway servers.

In order to implement our main idea, the solution of security problem can be explained in the following algorithm:

1. Sensor A receives message from one of its neighbors B.
2. Sensor A checks the identity of Sensor B by sending Sensor B encrypted ID (with a unique private key) to remote middleware.

3. Middleware send a Boolean response to Sensor A.
4. Based on the received response, the sensor A accept or reject Sensor B message.

This approach can be illustrated in the following schema:

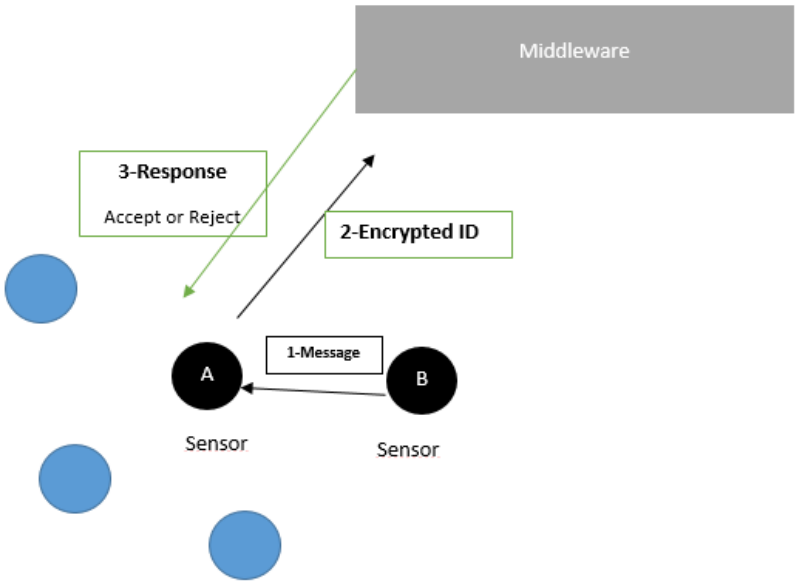

Fig.3. The proposed authentication improved protocol.

As it can be noticed for this proposed security mechanism, it provides many advantages:

- The rapid response compared to other protocols
- The high resulted security.
- The independence from the size of the network, so there is no need for adding any more base stations or to pass through a secure channel.

6. Evaluation:

In order to evaluate the suggested approach, we base our study on the work of [3] where a performance evaluation was made for the 6LoWPAN protocol compared to the mesh networks famous ZigBee protocol. Through their study, it was proven that 6LoWPAN protocol presents more possibilities in term of Network size, Internet connectivity and importantly RAM requirements. The following table summarizes these findings:

	Zigbee	6LoWPAN
Code Size with mesh	32K to 64K+	22K
Code Size w/o mesh	N/A	12K
RAM Requirements	8K	4K
Header Overhead	8-16 bytes	2-11 bytes
Network Size	65K	2^{64}
RF Radio Support	802.15.4	802.15.4
Transport Layer	None	UDP/TCP
Mesh Network Support	Zigbee	Many
Internet Connectivity	Zigbee Gateway	Bridge/Router

Table 1: Comparison of 6LoWPAN to Zigbee [3]

From another level, as discussed in the previous section, memory and energy consumption grows with the size of the network and the number of the needed hops to authenticate a node on the WEAP protocol. Consequently, we conclude that the suggested algorithm accompanies the developments and the trend of technology toward the internet of things principle adoption. As a result, solution for many problems

III. CONCLUSION

Because of the different vulnerabilities that exist in WSN, security aspect is a side that attracted the major concerns of researches. For this reason, many protocols and solutions were suggested in order to bypass the obstacle that holds the adoption of WSN in many fields; however those works had many limitations.

In this paper, we discussed the different limitations of the security aspect of WSN, especially when integrated to EIS. Since information inside enterprises is a sensitive issue, the discussion lead us to the conclusion that a mechanism should be made in place in order to bring higher standards to make information exchange highly secured. As a result, we focused in this work on the improvement of the authentication process inside WSN. Therefore, based on the different advantages that WSN will have when integrated to EIS, we suggested an algorithm that should, theoretically, realize a highly secured data exchange of WSN.

Additionally, the suggested algorithm was evaluated in terms of memory and energy consumption and proven theoretically it efficiency, however a practical case study is required in a future work. To conclude, what can be derived from this work is the importance and the need for improving security mechanisms in the field of WSN, and taking in consideration the particularities of WSN when compared with the other types of networks

REFERENCES

[1] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, & Culler, D. E. (2002). SPINS: Security protocols for sensor networks. Wireless networks, 8(5), 521-534.

[2] A. S. K. Pathan, H. W. Lee & C. S. Hong, (2006, February). Security in wireless sensor networks: issues and challenges. In Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference (Vol. 2, pp. 6-pp). IEEE.

[3] B Cody-Kenny, D. Guerin, D. Ennis, R. Simon Carbajo, M. Huggard, & C. Mc Goldrick. (2009, October). Performance evaluation of the 6LoWPAN protocol on MICAz and TelosB motes. In Proceedings of the 4th ACM workshop on Performance monitoring and measurement of heterogeneous wireless and wired networks (pp. 25-30). ACM.

[4] C.Karlof, & D. Wagner, (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. Ad hoc networks, 1(2), 293-315.

[5] D. G. Padmavathi, & M. Shanmugapriya, (2009). A survey of attacks, security mechanisms and challenges in wireless sensor networks. arXiv preprint arXiv:0909.0576.

[6] D. N. Sushma & V. Nandal, (2011). Security Threats in Wireless Sensor Networks. IJCSMS International Journal of Computer Science & Management Studies, 11(01).

[7] Federation of EA Professional Organizations. (2013): Common Perspectives on Enterprise Architecture,Architecture and Governance Magazine, Issue 9-4.

[8] H. M .BadrAbady, S.S. Mousavi. (2008): The Role of Information Technology in Organizational Procedures ' Improvement with Knowledge Based Approach-A Study of the Iranian Taxation Affairs Organization, World Applied Sciences Journal 3 Supple 2, pp. 55-56.

[9] I. Krontiris, T.Giannetsos, & T. Dimitriou, (2008, October). Launching a sinkhole attack in wireless sensor networks; the intruder side. In Networking and Communications, 2008. WIMOB'08. IEEE International Conference on Wireless and Mobile Computing, (pp. 526-531). IEEE.

[10] J. Lloret, M. Garcia, D. Bri, & S. Sendra, (2009). A wireless sensor network deployment for rural and forest fire detection and verification. sensors, 9(11), 8722-8747.

[11] J. Newsome, E. Shi, D. Song, & A. Perrig, (2004, April). The sybil attack in sensor networks: analysis & defenses. *In Proceedings of the 3rd international symposium on Information processing in sensor networks* (pp. 259-268). ACM.

[12] K.,Sharma, & M. K. Ghose, (2010). Wireless sensor networks: An overview on its security threats. *IJCA, Special Issue on "Mobile Ad-hoc Networks" MANETs*.

[13] L. Da Xu (2011). Enterprise systems: state-of-the-art and future trends, *IEEE Transactions on Industrial Informatics*, 7(4), 630-640.

[14] M. A. Mahmood, & Seah,(2012). Reliability in Wireless Sensor Networks: Survey and Challenges Ahead. *School of Engineering and Computer Science*, Victoria University of Wellington.

[15] M. Thoma, K. Sperner, T. Braun, & C. Magerkurth, (2013, November). Integration of WSNs into enterprise systems based on semantic physical business entities. In Wireless Days (WD), 2013 IFIP (pp. 1-8). *IEEE*.

[16] N. Shekhawat, & M. Ghosh, (2014). Enhancement the security of WSN using ALARM protocol to Prevention from Reply Attack. *Control Theory and Informatics, 4(4)*, 1-4.

[17] O.Abroun, A. Tahiri, N. Aknin, & K. E. El Kadiri,(May 2014), A Novel Intelligent Model For Enterprise Information System Based On Wireless Sensor Network, *International Journal of Engineering Science and Technology*.

[18] P. C. Shahare, & N. A Chavhan, (2014). Secure and Efficient Sink Node Location Privacy Technique in WSN. Traffic, 3(3).

[19] S. L. Ele , M. R. Kothari & D. N. N. Kota, (2014). 6LoWPAN Based Wireless Sensor Network to Monitor Temperature. *International Journal of Advanced Electronics and Communication Engineering*, 1(1), pp-1.

[20] S. S. Basha & N. M. Sultana, (2013) Secure Routing in Wireless Sensor Networks using WEAP Protocol.

[21] S. U. Rehman, M. Bilal, B. Ahmad, K. M. Yahya, A. Ullah, & O. U. Rehman,(2012). Comparison Based Analysis of Different Cryptographic and Encryption Techniques Using Message Authentication Code (MAC) in Wireless Sensor Networks (WSN). *International Journal of Computer Science Issues (IJCSI)*, 9(1).

[22] S. Wilkins. (2011 November 9), WLAN Authentication and Encryption, Retrieved from http://blog.pluralsight.com/wireless-encryption-authentication

[23] Y. C. Hu, A. Perrig, & D. B. Johnson. (2002). Wormhole detection in wireless ad hoc networks. Department of Computer Science, Rice University, Tech. Rep. TR01-384.

[24] Y. Yang, & Y. Sun, (2006). Energy-efficient Reliable Transmission Protocol with Outsourcing in WSNs. In *GLOBECOM*.