6ème Conférence Internationale en Automatique & Traitement de Signal (ATS-2021)
Proceedings Book Series –PBS- Vol 1, pp.74-79

Security in Wireless Sensor Networks communication protocols: challenges and solutions

Mohamed Boukhani[1], Abderrahmane Hajraoui[2]

Department of Physics, Communication and Detection Systems Team
University of Abdelmalek Essaâdi, Faculty of Sciences, Tetouan, Morocco
[1]bm.boukhani@gmail.com
[2]hajraouiabder@gmail.com

ABSTRACT- **Wireless Sensors Network (WSN) are a promising platform for emerging technologies like Internet of Things (IOT), energy optimisation, smart grid, vehicular sensor networks, cloud computing, water monitoring and many others [1]. Generally, sensors have limited resources in terms of energy and of treatment capacities. Despite the indicated limitation, WSN has to permit resolution of many complexes problems concerning Quality of Service (QoS), security, reliability and scalability. Today, WSN is vulnerable to security threats like conventional networks and presents many specific problems to provide security to new generation of internet services such as delay sensitive applications [2] … Providing security over WSN is much more challenging compared with security over wired networks. It is due to sensors mobility, links state and dynamic topology. In the present paper, we discuss the security objectives and requirements. We present some technics proposed in recent years to ensure security in WSN environment.**

KEYWORDS- **WSN, Quality of Service, security, attacks, routing protocol.**

I. INTRODUCTION

The WSN is a collection of mobile sensors self-organized in dynamic network topologies. These sensors are used to form networks and exchanges data with other nodes through radio links without any fixed infrastructure. This characteristic allows any WSN to be quickly deployable than the wired network. WSN applications continue to grow day by day in various fields.

In Fig.1, we present a WSN architecture consisting of sensors. Each node acts as a router and as a user terminal at the same time. It receives data transmitted by the other nodes and transmits the queued information to a given destination.

All sensors of WSN send data to the base station. Then, this sink node transmits it to the end user through a network structure.

Most military and civilian applications which use WSN, need a high level of security. Several extensions of the existing protocols have been designed to ensure the requested security and quality of service. Other techniques are used or combined with those protocols to be able to route data in the right conditions and overcome the limitations of standard protocols

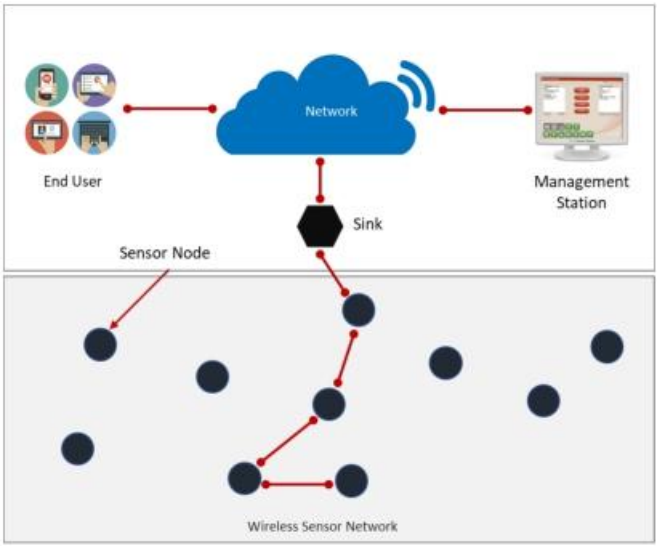

Fig. 1 Wireless sensor network (WSN) Architecture

Severe resource constraints are in WSN due to processing requirements, to energy consumption, to storage capacity, to major obstacles to the implementation of traditional security techniques. Due to this, the improvement of the security in WSN has been the active research area during the recent decades.

II. DESIGN CHALLENGES IN WSN

Compared to the traditional wired network, WSN has specials design challenges due to very limited energy, to limited memory and to processing capabilities.
Therefore, to implement useful security mechanisms it is necessary to know and understand these constraints [3], [4], [5]:

A. Energy contraints:

Any sensor node in WSN has generally a small dimension, it should rely on batteries to be able to move and communicate freely. The major problem in such environment is to maximize energy efficiency and to improve the network lifetime.

B. Limitation of bandwidth:

The Bandwidth is very limited due to the characteristics of the physical links and of mobility unpredictable. The most

ISSN: 2961-6611

challengeable problem is how to optimize the bandwidth for data transmission without any disruption or loss of information.

C. Limited Memory and Storage capacity:

The available installed memory and storage capacity in any node are generally too small. Besides, they are shared by the operating system and the data processing operations.

D. Dynamic topologies:

The nodes move frequently in the space with different speeds. The high vibration in the topology is due to the high degree of the nodes mobility.

E. Hostile deployment environment:

Due to its dynamic topology and hostile deployment environment, WSN will become the target of several malicious attacks. Security WSN is a challenging task and a very hard problem to solve; it permits to prevent malicious packets, denial-of-service attacks, snooping, and redirection of packets.

F. Scalability:

In case of the large network, the difficulty lies in update of the topology information. The latency and message overhead in any WSN, can be increased in proportion with its nodes number. Its routing protocol must be able to contract resource to accommodate the growth of network size.

G. Availability and reliability:

Any node in WSN may fail due to various reasons but the failure of node should not affect the performances. Availability and reliability are regarded as the capacity to ensure service continuity of the network due to node failure [6].

WSN is developed in the form of layers as show in Fig. 1 below[illegible]erent protc

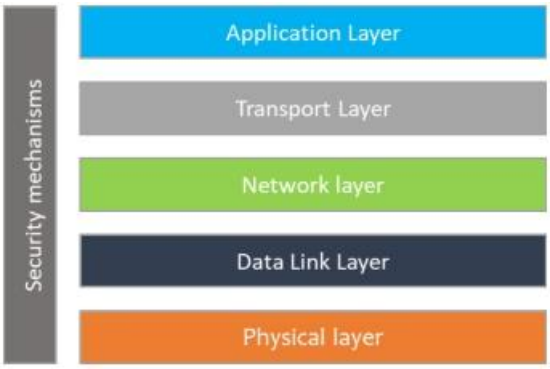

Fig. 2 WSN layered architecture

It becomes very necessary in WSN to overcome its limitations and to provide security and Quality of Service to support the growth of demand for the industrial Internet of things.

III. Security Principles

The main security objectives that should a Wireless Sensor provide, are in [7] and [8]:

A. Confidentiality:

Data confidentiality is the most important service in network security. It allows the network to ensure the secrecy of the data transmitted. For example, in military applications, WSN should establish a secure link to exchange sensitive data between sensor nodes.

B. Integrity:

Data integrity ensures that any transmitted data must not be changed during transmission. Malicious node in the network having access to the data may breach the integrity of the information.

This integrity service can be performed by the use of file permissions and by the user access controls.

C. Availability:

Data availability service ensures that data is available to the authorized user or application at any time.

Fig. 3 Security objectives

IV. Security Threats and Attacks in WSN

WSN applications are growing rapidly in various fields. Therefore, the security in WSN becomes a significant concern and should be updated as well.

WSNs possess additional vulnerabilities in comparison with traditional wired network. Owing to this, the traditional security technique cannot be directly applied.

The dynamic nature of WSNs makes it enormously complicated to ensure security and that's why the consistency of data transmission in this network cannot be guaranteed.

Data packets sent through any network may be dropped, compromised, modified or altered by attackers.

WSN security focuses on how to secure and protect the transmitted data against attacks.

V. Types of Attacks

Security attacks in WSN can be classified as [7], [9], [10], [11]:

ISSN: 2961-6611

A. External or physical attacks:

Attacker does not have the control of sensor nodes. It could overhear or eavesdrop on information in the network or disrupt physically, the service of a wireless network.

B. Internal or network attacks:

Attacker is able to capture the sensor nodes by injecting faulty data to control their activity. It uses the attacked nodes to disturb the network traffic.

C. Passive Attacks:

Passive Attacks are executed to gather and analyse information about the environment. The attacks do not have generally, any significant direct impact on the environment. The purpose of collecting information is to use it, to execute active attacks. The objectives of passive attacks are:

- Eavesdropping.
- Monitoring.
- Knowledge of confidential information.
- Traffic analysis.

D. Active Attacks:

Active Attacks use the information gathered to control or alter the network resources or activities such as routing protocol. Attacker can delete, modify the information and can change the information by injecting faulty data in the network. The objectives of active attacks are:

- Packet modification.
- Overloading.
- Energy degradation.
- Reducing traffic.
- Increasing data loss.

VI. NETWORK LAYER ATTACKS

WSN layered architectures are vulnerable to the different types of attacks. We describe briefly in the following some active attacks performed in WSNs network layer [7]:

A. Blackhole:

In blackhole attack [4], [7], a malicious node changes the routing table to forces the neighbor nodes to route the information through it. Then, the malicious node drops any data packets received including its own data. This attack can reduce traffic and increase data loss.

B. Sinkhole:

In sinkhole attack [7], [19], a malicious node advertises false information to create a center of attraction for other nodes. The result is that the neighbor nodes choose the malicious node as the next-hop node to route their information. This type of attack increases data loss, compromise transmission quality.

C. Sybil attack:

In this type of attack [19], a single malicious node presents multiple identities to other nodes in the network. This malicious node can have a strong influence on fault tolerant schemes such as multipath routing, distributed data storage systems, data aggregation.

D. Wormhole:

In wormhole attack [20], [21] called also the tunnelling attack; two or more malicious nodes create a low-latency link tunnel in different parts of the network. When a normal node sends packet to a destination then one malicious node tunnels the messages to another malicious node. The other malicious node receives this packet and replays it in its neighborhood. In this way, the malicious nodes convince the normal nodes to use them as a shortest path to route messages. This attack can disrupt the routing protocol operations. Wormhole attacks is potentially difficult to discover if it is used in combination with other type of attacks like selective forwarding, Sybil attack or eavesdropping,

E. Hello flood:

Some routing protocol use HELLO messages to allow nodes to discover their neighbors and establish or refresh the routing table. In a HELLO Flood attack, an attacker broadcasts messages with high transmission power to overload the network and to waste nodes' energy.

F. Selective forwarding:

In this attack [7], [20], a malicious node in the network can forward some of the received messages and selectively drops others. This attack is easy to detect if the attacker drops all the received packets (Blackhole) but is complicated if it forwards them selectively. This type of attack can result in reducing traffic and increasing data loss.

G. Denial of Service:

Denial of Service (DOS) attack can be performed at different layers: at physical layer this attack could be performed by jamming, tampering, at data link layer by collision, exhaustion, at network layer by attacking the routing protocol., SYN flooding, black holes, at transport layer it can be caused by de-synchronization and flooding. DOS attack could include several other attacks happening simultaneously it seeks to eliminate network's capacity to perform its expected function.

H. Spoofed, altered, information:

In this type of attack [7], [21], an attacker can disrupt traffic in the network. These disruptions include attracting/repelling network traffic, creating routing loops, generating non-existent information or fake error messages. This attack will cause network partitioning and increasing end-to-end delay.

I. Replication attack:

In a node replication attack, an attacker creates replicas of captured sensor nodes in an attempt to control information that is reaching the base station or, more generally, compromise the functionality of the network [16]. A node replicated can potentially cause severe disruption in message communication.

ISSN: 2961-6611

VII. PROPOSED SECURITY SCHEMES

WSN security has attracted the attentions of a significant number of researchers around the world in the past few years. In this section, we present a various security schemes, as shown in Table 1, proposed to prevent attacks and reduce network vulnerabilities.

Z. Sun, Y. Xu, G. Liang and Z. Zhou [12] proposed an intrusion detection model named as WSN-NSA based on an improved V-detector algorithm for WSN. The main tasks of Intrusion Detection Model is to secure the WSN from the routing attacks.

Reference [13] proposed a trust mechanism which evaluates communication trust and Data trust for WSNs. Based on simulation study, TWSN model successfully mitigates the attacks on WSNs.

Noor Alsaedi, Fazirulhisyam Hashim, A. Sali, Fakhrul and Z. Rokhani [14] proposed an Energy Trust System (ETS) for clustered WSNs to effectively detect Sybil attacks. The simulation results show that the proposed system is effective and robust in detecting Sybil attacks in terms of the true and false positive rates.

In [15] the authors propose a lightweight anonymous authentication protocol for WSN-based real-time applications to deal with DoS attacks without compromising any anonymity support.

T. Dimitriou, E. A. Alrashed, M. H. Karaata and A. Hamdan [16] proposed a fully distributed and completely decentralized solutions to detect replication attacks in mobile sensor network. Through extensive simulations, this approach demonstrates the practicality to mitigate the node replication attack.

In [17] the authors propose a method based on RTT (Round Trip Time) mechanism using AOMDV protocol to detect and prevent the wormhole attacks in WSN.

Reference [18] proposed a detection strategy using coordinator nodes to detect the nodes causing Hello flood attack. The performance of algorithm was tested using the NS-2 simulator.

TABLE I
SECURITY SCHEMES FOR WSN

Proposed security schemes	**Treated attacks**	**Network Architecture**	**Features**
Intrusion Detection Model for Wireless Sensor Networks [12]	Routing attacks	Traditional wireless sensor network	Reduces the data storage space and computation. Ensures high detection accuracy. Reduces the memory consumption and the computation consumption of nodes.
Data Trust for Wireless Sensor Networks TWSN [13]	Forwarding/modification attacks, bad mouthing attacks, collusion attacks and on-off attacks	Traditional wireless sensor network	Mitigates packet modification/dropping attack, bad mouthing attack, collusion attack and on-off attack. Identifies malicious sensor data.
Energy Trust System (ETS) [14]	Sybil attacks	Clustered wireless sensor network	Detects the Sybil attacks. Reduce communication overhead, memory overhead, and energy consumption.
Anonymous User Authentication Protocol for Wireless Sensor Networks [15]	DoS attacks	Traditional wireless sensor networks	Protects the network from DoS attacks. Reduce the wastage amount of computational and communication overhead during resynchronization process.
Imposter detection for replication attack s in mobile sensor networks [16]	Replication attack	Mobile wireless sensor networks	Mitigates the node replication attack. Detects imposters in MWSNs.
Wormhole detection and prevention mechanism in WSNs using AOMDV protocol [17]	Wormhole Attack	Traditional wireless sensor networks	Detects and prevents the wormhole attacks.
Detection strategy using coordinator nodes prevent Hello flood attack [18]	Hello Flood Attack	Clustered wireless sensor network	Detects and prevents the Hello Flood attacks.

ISSN: 2961-6611

VIII. CONCLUSION

In this paper we have highlighted the security design challenges and the security principals in WSNs. We have tried to address a classification of security attacks. Therefore, we have briefly presented the active network attacks on communication protocols and their major consequences on network's performance.

We also have provided a summary of various security schemes proposed by active researches to detect, prevent and mitigate the security attacks.

The proposed works provide additional features to enhance the existing routing protocols and to ensure security requirements.

So, we will try to improve the existent security mechanisms or to develop new security schemes for the most popular WSN communication protocols.

REFERENCES

[1] Rehmani, M. (Ed.), Pathan, A. (Ed.). (2016). Emerging Communication Technologies Based on Wireless Sensor Networks. Boca Raton: CRC Press.

[2] Ali, A., Y. Ming, et al. (2017). "A Comprehensive Survey on Real-Time Applications of WSN." Future Internet 9(4): 77.

[3] Oreku, G. S. and T. Pazynyuk (2016). QoS as Means of Providing WSN Security. Security in Wireless Sensor Networks. Cham, Springer International Publishing: 25-40.

[4] T. Azzabi, H. Farhat and N. Sahli, "A survey on wireless sensor networks security issues and military specificities," *2017 International Conference on Advanced Systems and Electric Technologies (IC_ASET)*, Hammamet, 2017, pp. 66-72.

[5] Shabbir, N. and S. R. Hassan (2017). Routing Protocols for Wireless Sensor Networks (WSNs). Wireless Sensor Networks - Insights and Innovations. P. Sallis. Rijeka, InTech**:** Ch. 02.

[6] A. Taherkordi, M. A. Taleghan and M. Sharifi, "Achieving availability and reliability in wireless sensor networks applications," *First International Conference on Availability, Reliability and Security (ARES'06)*, 2006, pp. 7 pp

[7] Tomić and J. A. McCann, "A Survey of Potential Security Issues in Existing Wireless Sensor Network Protocols," in *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1910-1923, Dec. 2017**.**

[8] Oreku G.S., Pazynyuk T. (2016) Introduction and Overview. In: Security in Wireless Sensor Networks. Risk Engineering. Springer, Cham.

[9] Y. Pinar, A. Zuhair, A. Hamad, A. Resit, K. Shiva and A. Omar, "Wireless Sensor Networks (WSNs)," 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT), Farmingdale, NY, 2016, pp. 1-8.

[10] A. Sen and S. Madria, "Risk Assessment in a Sensor Cloud Framework Using Attack Graphs," in IEEE Transactions on Services Computing, vol. 10, no. 6, pp. 942-955, Nov.-Dec. 1 2017.

[11] Mohan V. Pawar, J. Anuradha, Network Security and Types of Attacks in Network, Procedia Computer Science, Volume 48,2015, Pages 503-506.

[12] Z. Sun, Y. Xu, G. Liang and Z. Zhou, "An Intrusion Detection Model for Wireless Sensor Networks With an Improved V-Detector Algorithm," in IEEE Sensors Journal, vol. 18, no. 5, pp. 1971-1984, March1, 1 2018.

[13] V. Busi Reddy, S. Venkataraman and A. Negi, "Communication and Data Trust for Wireless Sensor Networks Using D–S Theory," in IEEE Sensors Journal, vol. 17, no. 12, pp. 3921-3929, June15, 15 2017.

[14] Noor Alsaedi, Fazirulhisyam Hashim, A. Sali, Fakhrul Z. Rokhani, Detecting sybil attacks in clustered wireless sensor networks based on energy trust system (ETS), Computer Communications, Volume 110, 2017, Pages 75-82.

[15] P. Gope, J. Lee and T. Q. S. Quek, "Resilience of DoS Attacks in Designing Anonymous User Authentication Protocol for Wireless Sensor Networks," in IEEE Sensors Journal, vol. 17, no. 2, pp. 498-503, Jan.15, 15 2017.

[16] T. Dimitriou, E. A. Alrashed, M. H. Karaata and A. Hamdan, "Imposter detection for replication attacks in mobile sensor networks," 2015 7th International Conference on New Technologies, Mobility and Security (NTMS), Paris, 2015, pp. 1-5.

[17] Parmar Amish, V.B. Vaghela, Detection and Prevention of Wormhole Attack in Wireless Sensor Network using AOMDV Protocol, Procedia Computer Science, Volume 79, 2016, Pages 700-707.

[18] Kaur, Reenkamal & Sachdeva, Monika. (2018). Detection of Hello Flood Attack on LEACH in Wireless Sensor Networks. 377-387. 10.1007/978-981-10-6005-2_40.

[19] Sen, J. (2009). "A Survey on Wireless Sensor Network Security." IJCNIS 1(2).

[20] Grover, Jitender & Sharma, Shikha. (2016). Security issues in Wireless Sensor Network A review. 397-404. 10.1109/ICRITO.2016.7784988.

[21] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications, 2003, pp. 113-127.

ISSN: 2961-6611