Security and Attacks in Wireless Sensor Networks

Messai Mohamed Lamine
Doctoral school in computer science, UAMB, Bejaia
messai.amine@gmail.com

Rezigue hamza
Automatic department, UFAS, Sétif
rezig.hamza@gmail.com

Abstract

Security in a wireless environment is an important issue which has been investigated by researchers for few years. Recently, the advancements in the miniaturization of the electromechanical systems (MEMS) allowed the appearance of a new type of wireless networks: wireless networks of sensors. Like a type of ad hoc networks, wireless sensor networks (WSNs) are useful in a variety of domains; military applications, health monitoring, places monitoring, smart environment, etc. Generally sensors are deployed in hostile environment prone to different types of attacks. Attacker now, has a physical access to sensor node, what is new in securing networks. So security becomes extremely important. Limitations of sensors (computation capability, memory storage, and limited battery energy) make security solutions proposed in wired networks inadequate.

In this paper, we present challenges of security, and the different possible attacks in WSNs, discuss the problems of security in each layer of network OSI model. Finally, we conclude the paper with three key questions to address for securing WSNs.

Keywords: *attacks, security, wireless sensor networks.*

1. Introduction

Current technologies realizations of electronic components, and in particular, of microprocessors, make possible to develop equipment with low cost and low power, of size and weights increasingly reduced. WSNs are a particular type of ad hoc networks, comprised mainly of large number (hundred or thousand) deployed sensor nodes[1] with limited resources and one or more base stations (BSs) or sink (Figure 1), typically serve as the access point for the user or as a gateway to another network. Nodes can collect and transmit (with wireless links) environmental data (temperature, pressure, humidity, noise levels, etc) in autonomous manner. The node in WSN plays tow roles: collect data and route data back to the base station.

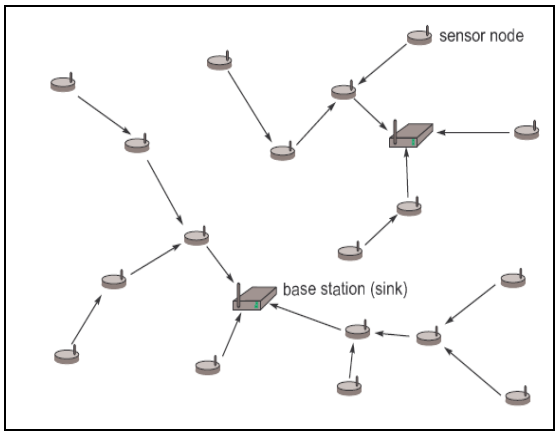

Figure 1. A WSN.

Typically, sensor node consists of five components, as shown in figure 2: power unit (battery), memory, transmitter/receiver, embedded processor, and sensing unit.

Additional components can be implanted in a sensor node: location finding system: allow the node to find its position, a power generator: used for recharging battery node and prolong its lifetime, and a mobilizer: make nodes move [8]. Sensing units are usually composed of two subunits: sensor and analog-to-digital converter (ADC). When an event was produced (analog data) node sense analog signal observed convert it to digital signals by the ADC unit, and then treat it with the processing unit. A transceiver unit connects the node to the network. One of the most important components of a sensor node is the power unit (battery); it is the fuel of the node. For detailed stat of the art see [8, 15].

For example, SmartDust node have only 8 bit processor, an 8 KB instruction flash memory, and a bandwidth of 10 Kbps (Kilo bit per second) [12].

[1] In our paper, sensor node, sensor, node (called mote in some other papers) means the same signification.

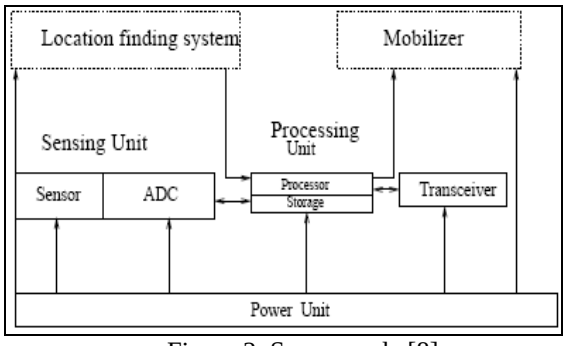

Figure 2. Sensor node [8].

As much of technology, the development of WSNs was caused by military needs. Indeed, the armies discreetly wish to be in measurement of espionner their enemies. SOSUS (the SOund SUrveillance System) used during the cold war to detect Soviet submarines [13, 14], other applications are: environmental monitoring, health monitoring of patients, habitat monitoring, disaster recovery, smart environment.

Sensor nodes are deployed in hostile and inaccessible area (e.g. military use to enemy surveillance), and it is impossible (in general) to know the position of the node after deployment, so nodes can be physically captured or destroyed by attackers. Provide security is a very important problem in WSNs.

Traditional security techniques used in traditional networks can not be applied directly, because of extremely constrained resources like energy, bandwidth and capabilities of processing and storing data of nodes in WSNs. The tiny hardware of sensor node is not capable of performing complex security protocols, so security should be reconsidered and new ideas in security researches are needed.

In this paper, we aim to give an overview of security problem in WSNs, present different attacks, and classify these attacks in the OSI model. The reminder of this paper is organized as follows: in section 2, OSI model of these networks is briefly presented. Sections 3-6 discuss constraints and limitation of sensor nodes and security goals. Sections 7-9 give definitions of attacks, attackers, and impact of attacks toward each layer of OSI model. Finally, we conclude in section 10.

2. The OSI model

The role of this model (Opening System Interconnect) consists in standardizing the communication between the participants so that various manufacturers can develop compatible products (software or hardware).

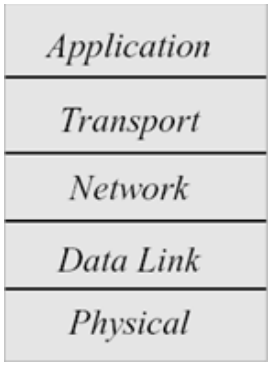

Figure 3. OSI model in WSNs.

Each layer of the model communicates with an adjacent layer (that of the top or that of the lower part). Each layer uses the services of the sub-bases and provides some to that of higher level.

3. Vulnerability analysis

The physical vulnerability is the fact that sensors are scattered in insecure place like public places, the natural environments (mountainous region) as well as the buildings, smart houses and museums (smart environment), so attacker have the physical access to the node, and with appropriate tools, he can read the secret information (like keys, programs, etc) stored in the node memory.

Other vulnerability is related to wireless technology. Unlike the traditional wired networks, the attackers could easily capture the data packet because the data transmissions are all in the air. Whoever having the adequate receiver can potentially listen to or disturb the exchanged messages.

Sensor nodes are themselves routers. Packets pass through different nodes in multi-hops routes to arrive at their destination. Due to the possible of violation of such nodes, this feature presents a serious vulnerability.

Sensor nodes are prone to failure, witch make topology dynamic. Dynamic network topology can be caused also by the mobility of nodes and addition of new nodes.

4. Constraints influencing on security in WSNs

Constraints that make traditional security impractical in WSNs are:

- Low energy power: The energy of the nodes is limited (limited battery lifetime), and generally irreplaceable and no-recharging battery. Protocols of WSNs must concentrate mainly on the conservation of energy.

- Limited memory and computation capacity: In the majority of WSNs, nodes are not able to memorize keys of significant size, or to carry out complex protocols cryptographic [1].

Therefore, new security measures are needed to address constraints of WSNs.

5. Energy for security

Lifetime node is generally limited by the lifetime of a tiny battery, so energy is the fundamental resource constraint.

The additional power consumed by nodes of sensor due to security is dependent on:

- Calculation necessary for the functions of security, such as ciphering, deciphering, verification of the signature.
- Energy necessary for the transmission and management of security material (keys, etc).
- Energy necessary for the storage of the keys.

The challenge is to minimize the consumption of the energy with maximizing the performances of security.

Energy is an important factor to consider when designing security measures for WSNs. Conserving node energy to extend his lifetime, and prolong network functionalities.

6. Security goals

Sensor networks with limited processing power, storage, bandwidth, and energy require special security approaches. The hardware and energy constraints of the sensors add difficulty to the security requirements of ad hoc networks concerning availability, integrity, confidentiality, freshness, authentication, access control, and nonrepudiation [2].

Availability: the availability gives insurance over the reactivity and time of response of the system to transmit information of one source to the good destination. It also means that the services of network are available to the authorized parts if necessary and ensures the services of network in spite of denies of service attack (DoS).

Integrity: İt is a service which guarantees that data are not be modified during the transmission. Integrity protects the network against the injection or the modification of messages.

Confidentiality: is the guarantee that the information of a node is not available or revealed only with its recipient.

Freshness: WSNs provide some measurements in time; we must ensure that each message is fresh. The freshness of data implies that the data are recent, and it ensures that no adversary replay the old messages.

Authentication: an adversary is not simply limited to modify the message. He can inject additional messages. Thus the receiver must make sure that the data used come from the correct source. In addition, by constructing WSNs, the authentication is necessary for many tasks.

Access control: gives to the legitimate participants a means to detect the messages coming from external sources of the network.

Nonrepudiation: ensures that the origin of a message cannot deny having sent the message [2].

7. Attacks in WSNs

A variety of attacks against WSNs is documented in the literature. To face these attacks, various against measurements were proposed. We present in the continuation the principal types of attacks, and in section 9 we assign these attacks to the layers concerned of the OSI model.

A classification of the attacks consists in distinguishing the passive attacks from the active attacks.

The passive attack (eavesdropping) is limited to listening and analyzes exchanged traffic. This type of attacks is easier to realize (it is enough to have the adequate receiver), and it is difficult to detect. Since, the attacker does not make any modification on exchanged information. The intention of the attacker can be the knowledge of confidential information or the knowledge of the significant nodes in the network (cluster head node), by analyzing routing information, to prepare an active attack.

In the active attacks, an attacker tries to remove or modify the messages transmitted on the network. He can also inject his own traffic or replay of old messages to disturb the operation of the network or to cause a denial of service. Among the most known active attacks, we can quote:

Tampering: it is the result of physical access to the node by an attacker; the purpose will be to recover cryptographic material like the keys used for ciphering [3].

Black hole: a node falsifies routing information to force the passage of the data by itself, later on; its only mission is then, nothing to transfer, creating a sink or black hole in the network [1].

Selective forwarding: as mentioned above, a node play the role of router, in a selective forwarding attack, malicious nodes may refuse to forward certain messages and simply drop them.

Sybil attack: Newsome et al. [5] definite this attack by:"malevolent device, taking multiple identities in an illegitimate way ", attacker can use the identities of the others nodes in order to take part in distributed algorithms such as the election.

HELLO flood attack: many routing protocols use "HELLO" packet to discover neighboring nodes and thus to establish a topology of the network. The simplest attack for an attacker consists in sending a flood of such messages to flood the network and to prevent other messages from being exchanged.

Jamming: a well-known attack on wireless communication, it consists in disturbing the radio channel by sending useless information on the

frequency band used. This jamming can be temporary, intermittent or permanent [6].

Blackmail attack: a malicious node makes announce that another legitimate node is malicious to eliminate this last from the network. If the malicious node manages to tackle a significant number of nodes, it will be able to disturb the operation of the network.

Exhaustion: is to consume all the resources energy of the victim node, by obliging it to do calculations or to receive or transmit unnecessarily data [7].

Wormhole attack: attackers here are strategically placed at different ends of a network. They can receive messages and replays them in different parts by means of a tunnel [9].

Identity replication attack: attacker can clone nodes, and place it in different part of the network in order to collect majority of information traffic. Unlike the Sybil attack, the identity replication attack [10] is based upon giving the same identity to different physical nods. This attack can be mounted because in a WSN there is no way to know that a wireless sensor node is compromised.

8. Attacker model

The goal of an attacker (adversary) is to illegally obtain keys stored in nodes by vulnerabilities exploitation.

Strong attacker: The adversary is considered as present before and after deployment of nodes. It can supervise all the communications, anywhere, and at any moment.

A realistic attacker model: The attacker is able to supervise a fixed percentage of communication channels after deployment [4].

"The hostile surveillance is not ubiquitous during the deployment phase of the network and only fraction of the established link keys can be obtained by the attacker" [4].

9. Problems of security in each layer

In this section, we provide a layer based classification of defined attacks on the OSI model described above.

9.1. Physical layer

Deal with the specification of the frequencies bands. This layer must ensure of the techniques of emission, reception and modulation of data in a robust way.

The attacks associated in the physical layer are very few but, at the same time, can be most difficult to prevent: jamming on the same frequency that the network uses, and the physical attack of a node.

One standard defense against jamming employs spread-spectrum communication [7]. Node capture is the more upsetting problem in the security of WSNs. The use of resistant hardware against capture attack (tamperproof node) can solve this problem, but increase the node cost.

9.2. MAC layer

This layer manages the access to the radio channel (MAC layer), and control errors. The adversary can only induce collision in a one byte of a transmission to disturb the entire data packet. So obligate the victim node to retransmit the data packet and cause a death of this node by consuming its energy (exhaustion attack).

The prevention of these attacks can be limited to impose the use of small packets, use techniques of correction to ask for the retransmission of packet.

9.3. Network layer

WSNs use a communication multi-hops for routing the packets towards the destination, the attacks in this layer are:

- Black hole
- Selective forwarding
- Sybil attack
- HELLO flood attack
- Wormhole
- Identity replication attack

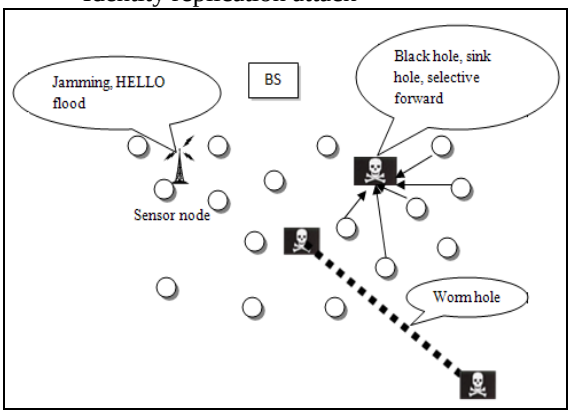

Figure 3. Routing layer attacks in WSNs.

The prevention of this kind of attacks invites to authenticate all messages. In a hierarchical network of sensors, the parents' nodes can check the identity of the source of a packet in transit.

Monitoring is a strategy to make safe the routing and to detect the abnormal behaviors of the nodes [11]. In this approach, the nodes act as "a watchdogs" to supervise the next transmission of the packet. If the misbehavior would be detected, the nodes will update the information of routing to avoid the compromised node.

Probing is another proactive defense against the malevolent nodes in WSNs [11]. This method periodically sends packets of probing through the network to detect areas of breakdown. Since the geographical protocols of routing have the knowledge of the topology of the network, probing is particularly well adapted to their use. The probing

packets must seem to be the normal traffic, in order to detect the compromised nodes.

Redundancy another approach suggested in [11] consists in sending the package several times on different paths; at least a path delivers the packet to the destination. It is clear that this method does not preserve energy but it increases the difficulty for an attacker of stopping the traffic.

10. Conclusion

Securing WSNs is a subject of active work. There are three issues to underwrite security in WSNs; (i) key management: to use encryption, the parties involved have to hold the right cryptographic keys. Key management schemes are essentials for every system to provide confidentiality, integrity, authentication, and the other security goals. It is the technique of establishment and maintenance of keys between legitimate nodes, and allows the updating, revocation and destruction of keys. Due to the resource limitation, providing efficient key management in WSNs is a challenge. (ii) Securing routing is the next issue to address. There are two kinds of threats to the routing protocols: external attackers, compromised interns' nodes, which are very difficult to detect because the compromised node can generate valid packets. Existents routing protocols for WSNs offer little or no security features [1]. (iii) Prevention of denial-of-service is the third issue, DoS can be defined as any event which decreases or eliminates the capacity of the network to carry out the functions envisaged. Breakdowns of hardware, programming errors, exhaustion of resource, environmental conditions, or any complicated interaction between these factors can cause DoS. DoS attacks prevent or reduce the use of computer or resources, interrupt or delay services, making network become unavailable, isolate legitimate users from a network.

Now, popularity of WSNs increases, and takes attention of many researchers.

This paper treats security in WSNs, which differ from the ad hoc networks with more severe restrictions in terms of energy, computation capabilities and communications. Consequently, the solutions of security must thus be adapted.

References

[1] Fei Hu and Neeraj K. Sharma, "Security considerations in ad hoc sensor networks", *Ad Hoc Networks*, Published by Elsevier Science, 2005, pp. 69–89.

[2] Rajeev Shorey, Akkihebbal L. Ananda, Mun Choon Chan, and Wei Tsang Ooi, "*Mobile, Wireless, and Sensor Networks: Technology, Applications, and Future Directions*",John Wiley & Sons, Inc, 2006.

[3] David Boyle, Thomas Newe. "Securing Wireless Sensor Networks: Security Architectures", *Journal of networks*, Volume 3, No. 1, 2008.

[4] Daniel Cvrcek, Petr Svenda, "Smart Dust Security – Key Infection Revisited", *Electronic Notes in Theoretical Computer Science 157*, Elsevier, 2006, pp. 11–25.

[5] John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary, "Wireless Sensor Network Security: A Survey", *Security in Distributed, Grid, and Pervasive Computing*, Auerbach Publications, CRC Press 2006.

[6] Farooq ANJUM and Saswati SARKAR, "MOBILE, WIRELESS, AND SENSOR NETWORKS TECHNOLOGY, APPLICATIONS, AND FUTURE DIRECTIONS", IEEE Press 2006.

[7] Perrig, Adrian, John Stankovic, and David Wagner. "Security in Wireless Sensor Networks", *Communications of the ACM*, Volume 47, 2004, pp. 53-57.

[8] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. l. Cayirci. "A survey on sensor networks", *IEEE Communications Magazine*, Vol. 40, No. 8, 2002, pp. 102-116.

[9] Chris Karlof, David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", *In First IEEE International Workshop on Sensor Network Protocols and Applications*, May 2003.

[10] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: analysis & defenses," in *IPSN '04: Proceedings of the third international symposium on Information processing in sensor networks*. ACM Press, 2004, pp. 259–268.

[11] Wood, A.D. and J.A. Stankovic. "Denial of Service in Sensor Networks". IEEE Computer, Volume: 35, Issue: 10, Oct. 2002, pp.48-56.

[12] Ning Hu, Randy K. Smith, Phillip G. Bradford, "Security for Fixed Sensor Networks", *ACMSE '04,* ACM, 2004, pp. 212-213.

[13] I. Khemapech, I. Duncan and A. Miller. "A survey of wireless sensor networks technology", *In PGNET, Proceedings of the 6th Annual PostGraduate Symposium on the Convergence of Telecommunications*, Networking & Broadcasting, June 2005.

[14] http://www.globalsecurity.org/intell/systems/sosus.htm

[15] Jennifer Yick, Biswanath Mukherjee, Dipak Ghosal. "Wireless sensor network survey". *Computer Networks*, Published by Elsevier Science, 2008, pp. 2292–2330.