Safety in Wireless Sensor Networks: Types of Attacks and Solutions

Héctor KASCHEL, José MARDONES, Gustavo QUEZADA

Departamento de Ingeniería Eléctrica, Facultad de Ingeniería, Universidad de Santiago de Chile,
Avenida Bdo. O'Higgins 3363, Estación Central, Santiago, Chile
hector.kaschel@usach.cl, jose.mardonesf@usach.cl, gustavo.quezada@usach.cl

Abstract: Wireless Sensor Networks (WSN) are highly vulnerable in their security. They are generally deployed in hostile environments to collect different kinds of data, so they are exposed to serious physical and software attacks. Therefore, developing methods to increase security becomes an essential aspect of the study of these networks. WSNs are used in military, medical and biological applications, among others. This paper analyzes the security requirements of WSNs, the main attacks, and their main characteristics; finally it reviews some security methods currently proposed or implemented in these networks, and identifies the possible types of security attacks that can affect the layers of the OSI Reference Model.

Keywords: Wireless Sensor Networks (WSN), Types of attacks.

1. Introduction

Wireless Sensor Networks are formed by a large number of small nodes, which consume low levels of energy and are low cost. These sensors are easy to deploy in an area designed for wireless networks performing specific functions. The fact that these networks are formed by a large number of nodes allows them to be used in industrial environments to carry out the control functions. Their configuration makes it possible for the sensors to be located abundantly, at all points of interest, and at a low cost. These kinds of networks also offer the same services and advantages as normal wireless networks. Because of the low cost of the nodes, it is possible to reconfigure them or adapt them to specific access points, providing access to a larger network such as, for example, the Internet.

Rapid technological advances cause products and services to vary constantly, forcing industry to satisfy those variable demands for the number and diversity of products. To fulfil those requirements, industry must develop two basic concepts: flexible manufacturing and processes. In this context, wireless networks can contribute process flexibility by offering mobility and control independent of the physical location of the process. They also offer control for processes in motion or for moving parts; they offer access to places that are inaccessible to wired networks, and provide safety with respect to broken wires. Figure 1 shows the main applications of wireless sensor networks.

On the other hand, industrial processes must offer high energy availability and efficiency so as to satisfy the associated production requirements. A lack of availability may mean great economic loss caused by stopping some highly important production line, or even worse, the whole production process. Also, the system must have a high level of security so that there is no change in information at any time.

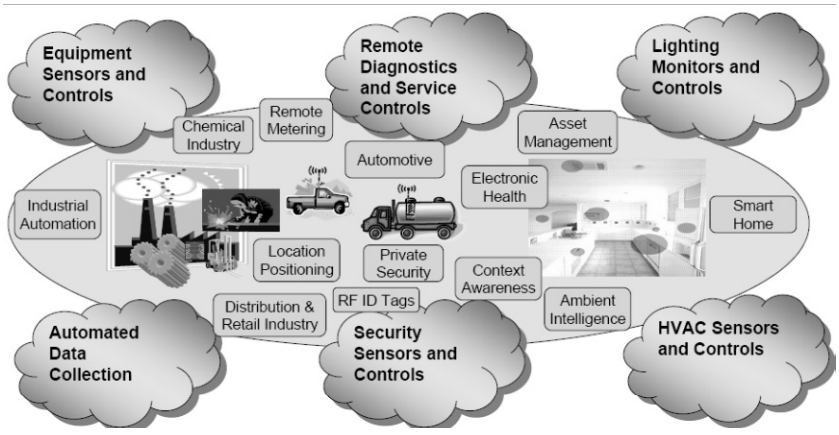

Figure 1. Application of Wireless Sensor Networks

Section 2 analyzes the security requirements; section 3 shows the different types of security attacks and their impact on the wireless sensors; section 4 describes some proposed designs and security solutions used for WSNs; section 5 provides a security approach based on the layers of the OSI Reference Model; and finally section 6 gives the conclusions of this research work.

2. Security Requirements

WSN networks were initially designed for military purposes, so their field of work was in hostile environments from the beginning. Each sensor node is constantly open so they are susceptible to attack. The information that travels through the node has a high probability of being stolen, decoded and used against it.

The security requirements of a wireless sensor network [1] can be classified as follows:

1. **Authentication:** Authentication of messages is fundamental for the different applications in WSNs, preventing an attacker from cloning a node or extracting password information to send malware to the network. Therefore, it is necessary to generate mechanisms that allow the nodes to authenticate the information received, which is possible by means of the validation of the identity of the transmitting node.
2. **Integrity:** This is the property that aims to keep the data free from unauthorized modifications. Integrity consists in keeping the accuracy of the information exactly as it was generated, without it being manipulated or altered by unauthorized persons or processes. Data Authentication can also provide Data Integrity.
3. **Confidentiality:** Data confidentiality refers to protection of the data as well as of the information exchanged between an emitting node and one or more addresses from third parties. Guaranteeing it requires a mechanism for communication enciphering and occultation. Digitally, the confidentiality of a document can be maintained through the use of asymmetric keys. The enciphering mechanisms guarantee the confidentiality during the time needed to decipher the message. For that reason it is necessary to determine how long the message must continue being confidential.
4. **Availability:** It encompasses the access to the information and to the systems by authorized persons at the time when they need it. The introduction of encryption algorithms in the wireless sensor networks makes them more costly. Whichever method is implemented, it increases processing time, which finally involves greater energy consumption, greatly threatening the availability of the network.
5. **Data Refreshing:** Although the confidentiality and the integrity of the data are ensured, guaranteed message updating is also required. Data refreshing implies that the data are up-to-date therefore it is important to ensure that an adversary node has not replaced the current message by an old one.

3. Types of Security Attacks on WSNs

Table 1 shows the types of attacks, and their main characteristics, that can invade a Wireless Sensor Network. Attacks on WSNs can be considered from two standpoints: one is the attack to the security mechanisms, and the other is an attack on the basic mechanisms (routing mechanisms) [2], [3], [4], [5], and [38] as indicated below:

As seen in Table 1, the attacks can be classified according to the different modes of action:

Attack techniques:

- The attacker can listen to the transmitted packets to analyze the traffic or the cryptography.
- The attacker can introduce false packets in the network to confuse the sensor network.
- The attacker can introduce malicious nodes to modify the packets received before resending them.

Node compromise:

- An attacker can capture a sensor node and extract all its secrets to use them in the security protocols.
- Often, the attacker is not interested in the content of the data, but rather in the interference of communications between the nodes.

Table 1. Main Attacks and their Characteristics.

Attacks	Characteristics
DoS (Denial of Service) [6] [7],[8]	- Produced by the unintentional action of nodes or the action of an attacker.
Attacks on the in transit information [9] [10]	- They alter, falsify and repeat the information in transit to the source. - They take control of one node and are capable of manufacturing new falsified packets. - Their scope can be over several sensor nodes at the same time.
Sybil attack [11] [13]	- An attacker takes the identical characteristics of another node to become involved in the network - This attack tries to degrade the integrity of the data, of the security and the use of the resources that the algorithm of is accessible through the stolen sensor. - Attacks the distributed storage, routing mechanisms and data aggregation. - When attacked, the network can fight back with strong protocols.
Backhole/Sinkhole Attack [14] [15]	- One node acts as a black hole to attract the whole group of sensor nodes. - When the malicious node intercepts the communication nodes, it can do anything with them.
Attack Hello Flood [16] [17]	- The attacker uses greetings packets to attract and convince the nodes. - The nodes are convinced that the attacker is its neighbor. - Once the nodes send the packet to the receiver, they must pass through the attacker, intercepting the packets and doing what they want it to do.
Wormhole Attack [18], [19]	- In this critical attack, the attacker saves the packets in a network address and the tunnels in another. - It is a significant threat, because it can occur at the beginning, when the sensor nodes are just finding out about the neighboring sensors.

– An attacker can interfere with the communication channel to deteriorate it, causing packet loss.

Passive vs. active:

– In the passive mode the attacker gets information without being discovered.

– In the active mode the attacker is more aggressive and launches various attacks to damage the network.

Internal vs. external:

– External attacks are limited and can be launched only from outside the networks application environment.

– Internal attacks compromise a network node or they implement malicious nodes.

As indicated in Table 1, in the face of the different types of attacks, it is indispensable to have security mechanisms for WSNs, since they are very prone to attacks, and as stated, there are many different kinds of attacks.

4. Security Methods for the Wireless Sensor Networks

In recent years, WSN security has attracted the attention of a large number of researchers all over the world.

Table 2. Summary of different Security Methods applied to Wireless Sensor Networks

Security method	**Attacks**	**Network architecture**	**Main characteristics**
JAM [20], [21]	DoS attack	Traditional wireless sensor networks.	Uses linked neighbouring nodes to prevent avoidance of the jammed region.
Based on Wormhole [18], [19]	DoS attack	Hybrid sensor network (wireless and wired).	Uses Wormholes to avoid jamming.
Random key pre-distribution, radio resource testing, etc. [12], [13]	Sybil attack.	Large number of sensors. Highly dense wireless sensor network.	Uses radio resources, random key pre-distribution, registration procedure, verification of position, and code testing for detecting Sybil entity.
Two-directional verification, multi-base station routing, multirouting [16], [22]	Hello flood attack.	Traditional wireless sensor networks.	Adopts a secret, probabilistic, sharing compartment. Also uses two-directional verification and multiple-base station routing and multirouting.
Based on communication security [23]	Information or data spoofing.	Traditional wireless sensor networks.	Efficient use of the resources. Protects the network even if part of the network is compromised.
TIK[19]	Wormhole attack, information or data spoofing.	Traditional wireless sensor networks.	Based on symmetric cryptography, requires synchronization between all communicating parties, implements temporary leashes.
Pre-distribution of random key [24][25]	Data and information spoofing. Attacks information in transit.	Traditional wireless sensor networks.	Provides resilience in the network, protects the network, even if part of the network is compromised, provides authentication measures for sensor nodes.
Eschenauer & Gligor, [26]	Data and information spoofing.	Distributed sensor network, large scale of wireless sensor network with a dynamic nature.	Allowed for a large number of wireless sensors that make it possible to add and remove sensors. Resilient to the capture of a sensor node.
REWARD [27]	Blackhole attacks.	Traditional wireless sensor networks.	Uses geographic routing, takes advantage of being the sender to see the neighbour's transmission and detects blackhole attacks.
TinySec [28][29]	Data and information spoofing, the messages repeat the attacks.	Traditional passive wireless sensor networks.	Centred on providing message authenticity, integrity and confidentiality messages-works in the link layer.
SNEP y µTESLA [30][31]	Data and information spoofing, the messages repeat the attacks.	Traditional passive wireless sensor networks.	Replay protection, semantic security, data authentication, low communication overhead.

Table 2 shows a revision of various proposed or implemented security methods based on the type of WSN attack [5], and their main characteristics.

The main idea followed by the Wireless Sensor Networks in the matter of security is to have an integral approach, so as to improve the performance of the networks with respect to security, longevity and interconnectivity under the changing environmental conditions.

5. Security Approach based on The Layers of the OSI Reference Model

It is important to carry out a holistic approach to security in which the OSI Reference Model layers participate to guarantee the network's overall security. Therefore we have that:

- **In the application layer:** The data are collected and administered in the application layer; it is important to ensure the reliability of the data and to transmit them to the lower levels. One of the problems that can arise is a security attack on the desynchronization of the data transfer.
- **In the network layer:** It is in charge of identifying the existing routing between one or more networks. The objective of this layer is to make the data arrive from their origin to their destination, even when both are not directly connected. Its aim is to find the best route, making use of efficient routing algorithms. The kinds of attacks that can occur in this layer are often Wormhole, Sinkhole, Sybil and Hello Flood.
- **In the data link layer:** This layer is in charge of physical addressing of the network's topology, access to the medium, error detection and/or correction, ordered mesh distribution, and flow control. This layer is vulnerable to Jamming and Collisions attacks that cause collision of packets and therefore shorter useful life of the battery by having to retransmit the packets, generating confusion in the neighbouring nodes.
- **In the physical layer:** It is in charge of providing the data transmission service over the medium and also controlling the radiofrequency transceptor, the signal's energy consumption, and the selection of access channels. Its objective is to increase reliability, while subsequently reducing loss. The most frequent types of attacks are DoS.

Table 3 presents a synthesis of the possible attacks that can appear in the different layers of the OSI Reference Model of a Wireless Sensor Network [1], [32], [33]:

Table 3. Possible attacks on the WSN layers.

WSN Layer	Types of attacks
Physical	Denial of Service (DoS)
Data link	Jamming Collision
Network	Denial of Service (DoS) Wormhole Sinkhole Sybil Hello flood
Application	Malicious node Desynchronization

6. Conclusions

Most security attacks in WSNs are caused by the insertion of false data by the compromised nodes within the network. This paper presents the requirements, the different types of security attacks, a review of state-of-the-art main security methods proposed or implemented in Wireless Sensor Networks, and a security approach based on the layers of the OSI Reference Model, in Wireless Sensor Networks.

Acknowledgements

This research was done with the financial contribution of project DICYT USACH Code 061213KC “Design and implementation of an IWSN (Industrial Wireless Sensor Network) Tolerant to Faults, Energy Efficient, and with High Security.”

REFERENCES

1. JAIN, A., K. K. KANT, M. R. TRIPATHY, **Security Solutions for Wireless Sensor Networks**, Second International Conference on Advanced Computing & Communication Technologies (ACCT), 2012, pp. 430-433.
2. MODARES, H., R. SALLEH, A. MORAVEJOSHARIEH, **Overview of Security Issues in Wireless Sensor Networks**, Third International Conference on Computational Intelligence, Modelling and Simulation (CIMSiM), 2011, pp. 308-311.
3. SHARMA K., M. K. GHOSE, D. KUMAR, R. PEEYUSH KUMAR, SINGH, V. KUMAR PANDEY, **A Comparative Study of Various Security Approaches Used in Wireless Sensor Networks**. In IJAST, vol. 7, April 2010.
4. JAYDP, S., **A Survey on Wireless Sensor Network Security**, Technical Report 55-77, International Journal of Communication Networks and Information Security (IJCNIS) Vol. 1, Nº2 August 2009.
5. PATHAN, A. S. K. H.-W. LEE, C. S. HONG, **Security in Wireless Sensor Networks: Issues and Challenges**, The 8th International Conference on Advanced Communication Technology, ICACT 2006, vol. 2, 2006, pp. 1043-1048.
6. DAOJING, H., C. CHEN; CHAN, S. JIAJUN BU, DICODE, **DoS-Resistant and Distributed Code Dissemination in Wireless Sensor Networks**, IEEE Transactions on Wireless Communications, vol. 11, Issue 5, 2012, pp. 1946-1956.
7. OUYANG, X., T. BIN, L. QI, Z. JIAN-YI, H. ZHENG-MING, X. YANG, **A Novel Framework of Defence System Against DoS Attacks in Wireless Sensor Networks**, 7th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM), 2011, pp. 1-5.
8. WANG, B-T. H. SCHULZRINNE, **An IP traceback mechanism for reflective DoS attacks**, Canadian Conference on Electrical and Computer Engineering, Volume 2, 2-5 May 2004, pp. 901-904.
9. JIA, G., F. JIAN'AN, X. CHEN, **Survey on Secure Data Aggregation for Wireless Sensor Networks**, IEEE International Conference on Service Operations, Logistics and Informatics (SOLI), 2011, pp.138-143.
10. PFLEEGER, C. P. S. L. PFLEEGER, **Security in Computing**, 3rd edition, Prentice Hall 2003.
11. CHEN, S., G. YANG, S. CHEN, **A Security Routing Mechanism Against Sybil Attack for Wireless Sensor Networks**, International Conference on Communications and Mobile Computing (CMC), Vol. 1, 2010, pp. 142-146.
12. YI, S., C. YONGFENG, T. LIANGRUI, **A Multi-phase Key Pre-distribution Scheme based on Hash Chain**, 9th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD), 2012, pp. 2061-2064.
13. NEWSOME, J., E. SHI, D. SONG, A. PERRIG, **The Sybil Attack in Sensor Networks: Analysis & Defences**, Proceedings of the Third International Symposium on Information Processing in Sensor Networks, ACM, 2004, pp. 259-268.
14. SHARMILA, S., G. UMAMAHESWARI, **Detection of Sinkhole Attack in Wireless Sensor Networks Using Message Digest Algorithms**, International Conference on Process Automation, Control and Computing (PACC), 2011, pp. 1-6.
15. CULPEPPER, B. J. H. C. TSENG, **Sinkhole Intrusion Indicators in DSR MANETs**, Proceedings of the First International Conference on Broadband Networks, 2004, pp. 681-688.
16. WANG, W., J. XU, J. WANG, **Detection and Location of Malicious Nodes based on Source Coding and Multi-path Transmission in WSN**, 11th IEEE International Conference on High Performance Computing and Communications, 2009, pp. 458-463.
17. KARLOF, C., D. WAGNER, **Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures**, Elsevier's Ad Hoc Network Journal, Special Issue on Sensor Network Applications and Protocols, September 2003, pp. 293-315.

18. HARBIN, J., P. MITCHELL, D. PEARCE, **Wireless Sensor Network Wormhole Avoidance using Reputation-based Routing**, 7th International Symposium on Wireless Communication Systems (ISWCS), 2010, pp. 521-525.

19. TRIKI, B., S. REKHIS, N. BOUDRIGA, **Digital Investigation of Wormhole Attacks in Wireless Sensor Networks**. Eighth IEEE International Symposium on Network Computing and Applications, 2009, pp. 179-186.

20. XUAN, Y., Y. SHEN. N. P. NGUYEN, M. T. THAI, **A Trigger Identification Service for Defending Reactive Jammers in WSN**, IEEE Transactions on Mobile Computing, vol. 11, Issue 5, 2012, pp. 793-806.

21. MAHMOOD, A. R., H. H. ALY, M. N. EL-DERINI, **Defending Against Energy Efficient Link Layer Jamming Denial of Service Attack in Wireless Sensor Networks,** 9th IEEE/ACS International Conference on Computer Systems and Applications (AICCSA), 2011, pp. 38-45.

22. HAMID, M. A., M.-O. RASHID, C. S. HONG, **Routing Security in Sensor Network: Hello Flood Attack and Defence,** to appear in IEEE ICNEWS 2006, 2-4 January, Dhaka.

23. SLIJEPCEVIC, S., M. POTKONJAK, V. TSIATSIS, S. ZIMBECK, M. B. SRIVASTAVA, **On Communication Security in Wireless Ad-hoc Sensor Networks**, 11th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, 10-12 June 2002, pp.139-144.

24. DU, W., J. DENG, Y. S. HAN, P. K. VARSHNEY, **A Pairwise Key Pre-distribution Scheme for Wireless Sensor Networks**, Proceedings of the 10th ACM Conference on Computer and Communications Security, 2003, pp. 42-51.

25. CHAN, H, A. PERRIG, D. SONG, **Random Key Predistribution Schemes for Sensor Networks**, In IEEE Symposium on Security and Privacy, Berkeley, California, May 11-14 2003, pp. 197-213.

26. ESCHENAUER, L., V. D. GLIGOR, **A Key-management Scheme for Distributed Sensor Networks**, Proceedings of ACM CCS'02, 18-22 November 2002, pp. 41-47.

27. KARAKEHAYOV, Z., **Using REWARD to Detect Team Black-hole Attacks in Wireless Sensor Networks**, in Workshop on Real-World Wireless Sensor Networks (REALWSN'05), 20-21 June, 2005, Stockholm, Sweden.

28. MOON, M., D. S. KIM, JONG SOU PARK, **Toward Modelling Sensor Node Security Using Task-Role Based Access Control with TinySec**, Conference on Computational Intelligence and Security, vol. 2, 2006, pp. 1109-1112.

29. KARLOF, C., N. SASTRY, D. WAGNER, **TinySec: A Link Layer Security Architecture for Wireless Sensor Networks**, 2º International Conference on Embedded Networked Sensor Systems, Baltimore, MD, USA, 2004, pp. 162-175.

30. LI, Y., F. LIU, L. DING, **Research about Security Mechanism in Wireless Sensor Network**, International Conference on Image Analysis and Signal Processing (IASP), 2011, pp. 447-451.

31. YEO, D.-G., H.-Y. YOUM, **An µTESLA Protocols with Multi-senders Based on a 2-Level XOR Chain with Data-Loss**, 10th International Symposium on Tolerance Applications and the Internet (SAINT), 2010, pp. 269-272.

32. PANDEY, A., R. C. TRIPATHI, **A Survey on Wireless Sensor Networks Security**, International Journal of Computer Applications, Vol. 3, Nº 2, June 2010, pp. 43-49.

33. KASCHEL, H., Y. B. L. SANCHEZ, J. MARDONES, G. QUEZADA, **Modelling Sensor Node Security Using Task-Role based Access Control with TinySec**, Studies in Informatics and Control Journal. Vol. 20, N° 3, September 2011, pp. 285-292.