A Survey on Attacks of WSN and their Security Mechanisms

Kanchan Kaushal
CTIEMT
Shahpur
Jalandhar, India

Taranvir Kaur
CTIEMT
Shahpur
Jalandhar, India

ABSTRACT

WSNs perform an important role in many applications, such as battlefields surveillance, patient health monitoring, home automation, traffic control, environmental observation and building intrusion surveillance. WSNs are convenient, cost effective, and give ease of integration with other networks and their components. However, wireless technology also creates new threats. Since WSNs communicate by using radio frequencies therefore the risk of interference is more than with wired networks. If the message to be passed is not in an encrypted form, or is encrypted by using a weak algorithm, the attacker can read it, and it is the compromise to the confidentiality. Security objectives include: protecting confidentiality, assuring integrity, providing authentication and supporting availability of the information and information systems. In this paper we describe the types of existing security threats and how existing techniques can be used to prevent or mitigate these attacks in WSNs.

General Terms

Network security, Attacks on WSN, Security mechanisms.

Keywords

Network security, Attacks on WSN, Security mechanisms, prevention of attacks from security threats.

1. INTRODUCTION

WSNs consist of multifunction and spatially distributed small sized sensor nodes communicate wirelessly over short distances. The sensor nodes integrate different properties for sensing the environment, as well as data processing and communication among other sensors. It monitors physical/environmental conditions like sound, temperature, pressure, vibration, humidity, motion or pollutants. WSNs perform an important role in many applications, such as battlefields surveillance, patient health monitoring, home automation, traffic control, environmental observation and building intrusion surveillance. The wireless networking has improved productivity through increased accessibility to information resources and easier, faster and less expensive network configuration. WSNs are convenient, cost effective, and give ease of integration with other networks and their components. However, wireless technology also creates new threats. Since WSNs communicate by using radio frequencies therefore the risk of interference is more than with wired networks.

If the message to be passed is not in an encrypted form, or is encrypted by using a weak algorithm, the attacker can read it, and it is the compromise to the confidentiality. Security objectives include: protecting confidentiality, assuring integrity, and supporting availability of the information and

information systems. WSNs present a handful of concerns for network managers. Unauthorized access points, unknown stations, captured nodes; spoofed acknowledgements are some of the problems given in WSN troubleshooting. Moreover, onsite maintenance for remotely deployed sensor nodes is infeasible, thus a thorough consideration of security solutions and troubleshooting tools must be available.

2. TYPES OF ATTACKS ON WSN

2.1 Node Capture Attack

One of the distinct attacks in WSNs is a node capture. In this attack, an attacker gains full control over a sensor node through a direct physical access. Then the attacker can easily extract cryptographic primitives and obtain unlimited access to the information stored on the memory chip of the captured node through a reverse engineering process with the potential to cause substantial damage to the entire WSN. Three main factors that can aid the attackers during a node capture attack:

- If sensor nodes within the WSN share a key or keys with neighboring nodes that is used to encrypt or decrypt data.
- A node capture attack has a great impact on the structure or topology of a WSN.
- The density of the WSN has a direct influence on node capture attacks, having a similar affect to the network structure.

2.2 Side Channel Attack

A side channel attack refers to any attack that is based on information gathered from the physical implementation of a cryptosystem, in contrast to vulnerabilities in the algorithm itself [1]. For example the attacker monitors the power consumption or the electromagnetic (EM) emanation from such cryptographic devices, and then analyzes the collected data to extract the associated crypto key.

Side channel attacks include:

- Simple power analysis (SPA) is a technique that involves directly interpreting power consumption measurements collected during cryptographic operations
- Simple electromagnetic analysis (SEMA) an adversary is able to extract compromising information from a single electromagnetic sample [4].
- In differential power analysis (DPA) an adversary monitors the power consumed by cryptographic devices, and then statistically analyzes the collected

data to extract a key in contrast to the simple power analysis.

- In differential electromagnetic analysis (DEMA), instead of monitoring the power consumption, an attacker monitors electromagnetic emanations from cryptographic devices, and then the same statistical analysis as that for the differential power analysis is performed on the collected electromagnetic data to extract secret parameters [4].

2.3 DoS Attacks

It occurs by the unintentional failure of nodes or malicious action. The simplest DoS attack tries to exhaust the resources available to the victim node, by sending extra unnecessary packets and thus prevents legitimate network users from accessing services or resources to which they are entitled. DoS attack is meant not only for the adversary's attempt to subvert, disrupt, or destroy a network, but also for any event that diminishes a network's capability to provide a service. In wireless sensor networks, several types of DoS attacks in different layers might be performed. At physical layer the DoS attacks could be jamming and tampering, at link layer, collision, exhaustion, unfairness, at network layer, neglect and greed, homing, misdirection, black holes and at transport layer this attack could be performed by malicious flooding and desynchronization.

2.4 Software Attacks

In Software-based attacks on WSNs, an attacker may try to modify the software code in memory or exploit known vulnerabilities in the software code. A well-known example of such an attack is a buffer overflow attack. In this type of attack a process tries to store data beyond the limits of a fixed length buffer, thus, resulting in the extra data overwriting the adjacent memory locations.

2.5 Routing Attacks

As described earlier, every node acts as a router in a WSN. Routing and data forwarding are an important task for sensor nodes. Routing protocols have to be energy and memory efficient, but at the same time they have to be robust against attacks and node failures. There have been many power-efficient routing protocols proposed for WSNs. However, most of them suffer from security vulnerabilities of one sort or another. In the real world, a secure routing protocol should guarantee the integrity, authenticity and availability of messages in the existence of adversaries of arbitrary power. Every authorized receiver should receive all messages proposed for it and should be capable of proving the integrity of every message and also the identity of the sender.

Some of the routing protocol attacks are the following [10]:

- Black hole attacks or packet drop attack;
- Spoofed, altered, or replayed attack;
- Wormholes attack;
- Selective forwarding attack;
- Sinkhole attack;
- HELLO flood attack;
- Acknowledgement spoofing.

2.6 Traffic Analysis Attacks

All communication in WSNs is moving toward a base station in many-to-one or many-to-few patterns. An attacker is able to

gather much information on the topology of the network as well as the location of the base station and other strategic nodes by observing traffic volumes and pattern. There are two types of traffic analysis attacks in WSNs: a rate monitoring attack and a time correlation attack. In a rate monitoring attack an attacker monitors the packet sending rate of nodes near the attacker and moves closer to the nodes that have a higher packet sending rate. In a time correlation attack an attacker observes the correlation in sending time between a node and its neighbor node that is assumed to be forwarding the same packet and deduces the path by following the sound for each forwarding operation as the packet propagates towards the base station [3].

2.7 Sybil Attacks

The Sybil attack is defined as a malicious device illegitimately taking on multiple identities. For example, a malicious node can claim false identities, or impersonate other legitimate nodes in the network [1][2]. The Sybil attack can affect a number of different protocols such as the following:

- Distributed storage protocols;
- Routing protocols;
- Data aggregation (used in query protocols);
- Voting (used in many trust schemes);
- Fair resource allocation protocols;
- Misbehavior detection protocols.

2.8 Attacks on In-Network Processing

Data aggregation or in-network processing is very useful in terms of reducing the communication overhead. However there can be different types of attack on in-network processing:

- Compromise a node physically to affect aggregated results [12];
- Attack aggregator nodes using different attacks;
- Send false information to affect the aggregation results.

2.9 Attacks on Time Synchronization Protocols

Time synchronization protocols provide a mechanism for synchronizing the local clocks of nodes in a sensor network. Three of the most prominent protocols are the reference broadcast synchronization (RBS) protocol, TPSN (Timing-sync Protocol for Sensor Networks) and FTSP (Flooding Time Synchronization Protocol). Since most of the time synchronization protocols do not consider security, an attacker can physically capture a fraction of the nodes and injecting them with faulty time synchronization message updates easily. This event can make the nodes in the entire network out-of-sync with each other.

2.10 Replication Attacks

There are two ways to launch replication attacks in WSNs. First, an attacker can eavesdrop on communications and resend old packets again multiple times in order to waste its neighboring sensor nodes' energy. Then, an attacker can insert additional replicated hostile sensor nodes into the WSN after obtaining some secret information from captured sensor nodes or through infiltration.

3. Security Mechanisms

In transport protocols, reliability is delivering each segment successfully that is generated at source to the eventual destination. Reliability could be attained by detecting the dropped packets and retransmit packets to significant sources.

3.1 Preventing DoS Attacks

Wireless communications are also vulnerable to denial-of-service (DoS) attacks. Organizations can take several steps to reduce the risk of such unintentional DoS attacks. Careful site surveys can identify locations where signals from other devices exist; the results of such surveys should be used when deciding where to locate wireless access points. Regular periodic audits of wireless networking activity and performance can identify problem areas; appropriate remedial actions may include removal of the offending devices or measures to increase signal strength and coverage within the problem area.

3.2 Preventing Sybil Attacks

Proposed solutions to the Sybil attack include the following:

- radio resource testing which relies on the assumption that each physical device has only one radio;
- random key pre-distribution which associates the identity of each node to the keys assigned to it and
- validates the keys to establish whether the node is really who it claims to be;
- registration of the node identities at a central base station; and
- Position verification which makes the assumption that the WSN topology is static.

3.3 Preventing Software Attacks

The following countermeasure can be considered to secure the WSN software and be protected from being exploited by malicious users:

- Software authentication and validation, e.g., remote software-based attestation for sensor networks;
- Defining accurate trust boundaries for different components and users;
- Using a restricted environment such as the Java Virtual Machine;
- Dynamic run-time encryption/decryption for software. This is similar to encryption/decryption of data
- Except that the code running on the device is encrypted. This can prevent a malicious user from exploiting the software;
- Hardware attestation. The trusted computing group platform and next generation secure computing base provide this type of attestation. A similar model could be used in sensor networks.

3.4 Preventing Selective Forwarding Attacks

To prevent attacks like selective forwarding, multipath routing can be used. Messages routed over paths whose nodes are completely disjoint are completely protected against selective forwarding attacks involving at most compromised nodes. Allowing nodes to dynamically choose a packet's next hop probabilistically from a set of possible candidates can further reduce the chances of an adversary gaining complete control of a data flow.[6]

3.5 Preventing Sink Hole Attacks

Such attacks are very difficult to defend against. One class of protocols resistant to these attacks is geographic routing protocols. Geographic protocols construct a topology on demand using only localized interactions and information and without initiation from the base station.

3.6 Preventing Warm Hole Attacks

The mechanism to combat the wormhole attack include, DAWWSEN, a proactive routing protocol based on the construction of a hierarchical tree where the base station is the root node, and the sensor nodes are the internal or the leaf nodes of the tree [6]. A great advantage of DAWWSEN is that it doesn't require any geographical information about the sensor nodes, and doesn't take the time stamp of the packet as an approach for detecting a wormhole attack, which is very important for the resource constrained nature of the sensor nodes.

4. CONCLUSION

In this paper, we have presented a study of some existing security threats of WSN and their security mechanisms.

Our main concern is about security objectives include: protecting confidentiality, assuring integrity, providing authentication and supporting availability of the information and information systems. The main categories are the introduction to WSN, security threats of WSN and their security mechanisms. Within each of those categories we have also sub categorized the major topics including routing attacks, Sybil attacks, DoS attacks etc. Our aim is to provide both a general overview of the rather broad area of wireless sensor network security. As wireless sensor networks continue to grow and become more common, we expect that further expectations of security will be required of these wireless sensor network applications.

5. ACKNOWLEDGMENTS

The authors wish to thank the faculty from the computer science department at CTIEMT, Jalandhar for their continued support and feedback.

6. REFERENCES

- [1] T. Roosta, S. Shieh, S. Sastry, "Taxonomy of Security Attacks in Sensor Networks", 1st IEEE Int. Conference on System Integration and Reliability Improvements, , Hanoi (2006) pp. 13–15, 2006..
- [2] A. Perrig, J. Newsome, E. Shi, D. Song, "The Sybil Attack in Sensor Networks: Analysis and Defences", 3rd Int. Symposium on Information Processing in Sensor Networks, (ACM Press, New York, USA 2004) pp. 259–268, 2004.
- [3] J. Deng, R. Han, S. Mishra "Countermeasures Against Traffic Analysis Attacks in Wireless Sensor Networks", First IEEE/Cerata Net Conference on Security and Privacy in Communication Networks (SecureComm), Athens (2005) pp. 113–124, 2005.
- [4] K. Gandol, C. Mourtel, F. Olivier, "Electromagnetic Analysis: Concrete Results", Published in C. Koç, D. Naccache, and C. Paar, Eds Cryptographic Hardware and Embedded Systems { CHES 2001, vol. 2162 of Lecture Notes in Computer Science, pp. 251{261, Springer-Verlag, 2001.
- [5] Jennifer Yick, Biswanath Mukherjee, and Deepak Ghosal, "Wireless sensor network survey," Computer Networks, vol. 52, pp. 2292-2330, Elsevier, April 2008.

- [6] Kalpana Sharma, M K Ghose, “Wireless Sensor Networks: An Overview on its Security Threats”, IJCA Special Issue on “Mobile Ad-hoc Networks” MANETs, 2010.
- [7] Ahmad Abed, Alhameed Alkhatib, and Gurbinder Singh Baicher “Wireless Sensor Network Architecture,” International Conference on Computer Networks and Communication Systems, IPCSIT, vol. 35, 2012.
- [8] Vikash Kumar, Anshu Jain and P N Barwal, “Wireless Sensor Networks: Security Issues, Challenges and Solutions”, International Journal of Information & Computation Technology, ISSN 0974-2239 Vol 4, No 8, pp. 859-868, 2014.
- [9] Anthony D. Wood and John A. Stankovic, “A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks”, Unpublished.
- [10] Y.-C. Hu, A. Perrig, D.B. Johnson: Adriane: A Secure On-Demand Routing Protocol for Ad Hoc Networks, Annual ACM Int. Conference on Mobile Computing and Networking (MobiCom) 2002.
- [11] Ju young Kim, Ronnie D. Caytiles, Kyung Jung Kim, “A Review of the Vulnerabilities and Attacks for Wireless Sensor Networks”, Journal of Security Engineering.
- [12] K. Kifayat, M. Merabti, Q. Shi, D. Llewellyn-Jones: Group-based secure communication for large scale wireless sensor networks, J. Information Assurance Security. Vol 2, 139–147, 2007.