ISSN:0975-9646

Security Issues in Wireless Sensor Networks – An Overview

Sujesh P. Lal
Research Scholar,
Faculty of Computer Science and Engineering
Sathyabama University, Chennai, India

Dr. Joe prathap P M
Professor, Department of Information Technology
RMD Engineering College,
Chennai, India

***Abstract*— A wireless sensor network (WSN) is a spatially distributed autonomous sensors to monitor and cooperatively report information about physical or environmental conditions, such as temperature, sound, pressure, etc. through the network to a server machine. WSNs are generally implemented for collecting information from insecure environment. Nearly all security protocols for WSN believe that the intruder can achieve entirely control over a sensor node by way of direct physical access. The appearance of sensor networks as one of the main technology in the future has posed various challenges to researchers. The challenges thrown by WSNs are unique given their delicate architecture and scant resources. Even though security for wireless networks has been a widely researched area for many decades, security for WSNs is still a major roadblock for their efficiency and performance.**

Keywords—wireless sensor networks; security; WSN; barrier coverage; intrusion detection system; IDS

I. INTRODUCTION

The security issues in wireless sensor network is due to the struggle of how much resources can be expended for security in proportion to the sensor application. The current security perspective for WSNs is on a per-attack basis, which creates an inflexible model resulting in poor efficiency and scalability. Creating a security framework offering high flexibility, good scalability and a redundancy-free security layer for the WSN protocol stack and is based on a resource perspective when deciding security solutions, where solutions are designed to secure each resource in the WSN environment, rather than defend against attacks.

A. Intrusion Detection System

There are many challenges to the security in wireless sensor network and it is due to some reasons like the nature of data transfer of wireless communication, limited resources of sensor nodes, unattended situations where sensor nodes might be susceptible to physical attack, etc. To enhance the security of wireless sensor networks authentication techniques, cryptography techniques can be used. These solutions alone can never prevent all possible attacks. So a second level of security is Intrusion Detection Systems (IDS) [4].

B. Secure localization in wireless sensor networks

Ad hoc wireless sensor networks (WSNs) have attracted a great deal of attention in recent years for their broad potential in both military and civilian operations. The proper operations of many WSNs rely on the knowledge of physical sensor locations. However, most existing localization algorithms developed for WSNs are vulnerable to attacks in hostile environments. As a result, adversaries can easily subvert the normal functionalities of location-dependent WSNs by exploiting the weakness of localization algorithms. In this paper, we first present a general secure localization scheme to protect localization from adversarial attacks. We then propose a mobility-assisted secure localization framework for WSNs.

II. INTRUSION DETECTION AND PRIVACY

Wireless sensor networks often have to be protected not only against an active attacker who tries to disrupt a network operation, but also against a passive attacker who tries to get sensitive information about the location of a certain node or about the movement of a tracked object. To address these issues, we can use an intrusion detection system and a privacy mechanism simultaneously. However, both of these often come with contradictory aims. A privacy mechanism typically tries to hide a relation between various events while an intrusion detection system (IDS) tries to link the events up. Here, we first explore several problems that may appear when both an intrusion detection system and a privacy mechanism are employed in the network. There are problems that might occur when both IDSs and privacy mechanisms are used simultaneously.

A. Problem causes to IDS

Privacy mechanisms usually intentionally hide the identity of nodes, assign multiple pseudonyms to a single node or use dynamically changing pseudonyms. Thus a single node may have different pseudonyms for communication with different neighbours and these pseudonyms may change in time. Packets sent by the node then contain identifiers that are understandable only to this node and the intended recipient. This may cause trouble to an ID since it is not able to link overheard packets with a particular sender or recipient. The IDS will also not be able to decide whether the claimed pseudonym of a node is true or not.

- An IDS concludes that a particular node is malicious. However, it may not be able to mark the node as malicious since it has no suitable identifier of the node that could be unambiguously understood by other nodes. Thus it will have trouble providing other nodes with the information that the certain node is malicious. An usual way to cope with this problem is to use the physical location of the malicious node. However, the nodes may only have some information on the radio signal strength of the received packets, not on the accurate sender location

- An IDS may not be able to detect a Sybil attack since it is legitimate for every node to have multiple identities. An IDS without additional information is not able to distinguish between a true identity and a malicious identity either fabricated or stolen.
- Detection accuracy of an IDS may decrease if it does not know the identities of its neighbours. For example, in order to detect a selective forwarding attack an IDS monitors (Node A in the figure 2.1) packets in its communication range. If the IDS overhears a packet (from the node X), it may want to check whether the packet is properly forwarded by the recipient (the node Y). If the IDS assumes that the recipient is in its communication range, while it in fact is not, false positives might occur. On the contrary, if the IDS assumes the recipient is out of reach and it is not true, false negatives might occur.

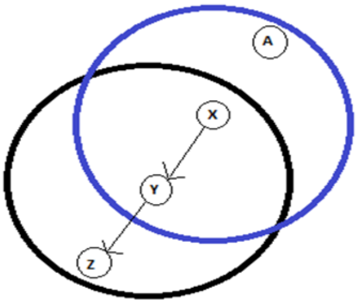

Figure 2.1 Communication range of nodes X and Y

- An IDS may not be able to detect a selective forwarding (jamming) attack in case a forwarding (jamming) node has multiple identities and the IDS does not know that these identities belong to that node. Then the IDS cannot link two dropping (sending) events that look innocent when separated and would be recognized as an attack when linked together. Furthermore, the IDS has to maintain larger tables in the memory due to a higher number of identities monitored.

B. *Non-interfering privacy mechanisms*

The simplest way to avoid all of the aforementioned problems is to run protocols that do not cause these problems. However, the likely cost for this evasion will be a decrease in performance (security functionality) of either IDSs, privacy mechanisms or both. Another impact can be an increase in protocol complexity. For example, the IDS may use a node behaviour to identify the node instead of the node identifier. Such behaviour may be represented by hashes of messages sent by the node recently. This information can be understood by all nodes in the communication range of the malicious one.

Privacy mechanisms make a mess in a network by hiding identities of nodes, introducing new traffic, etc. Privacy mechanisms might share some (secret) information with an IDS, in particular should this sharing help the IDS to organize the mess" and successfully detect active attackers. A problem to solve is that a certain IDS node may accumulate a lot of secret information, becoming a sweet spot for an attacker. The following approaches to sharing can be taken.

1. Pre-shared secret: Privacy mechanisms employ a trapdoor function for pseudonym generation, content protection or dummy traffic identification. The trapdoor information is pre-shared between a privacy mechanism and an IDS, thus the IDS knows all the information necessary to run properly. No further cooperation is needed. However, the IDS knowing the trapdoor information is tempting for an attacker. The impact of an IDS compromise can be minimized by sharing only partial information or information that is valid only for a certain time.
2. Delayed information disclosure: Certain information is retrospectively revealed by privacy mechanisms, especially if this information helps the IDS to understand audit data recorded in the past. This approach assumes that an attacker needs the information immediately and delayed disclosure is not helpful for her. This approach can be used, for example, to retrospectively differentiate dummy and real traffic.
3. Information is revealed on demand: The information necessary to cancel the effect of privacy mechanisms' protective actions can be obtained by an IDS on demand, if the IDS executes an additional protocol and a privacy mechanism cooperates. The key characteristics are that IDSs cannot obtain the information without cooperation of privacy mechanisms and the obtained information is limited to cancelling effects of privacy mechanism protective actions only for a certain subject or time period (one message, one identity, etc.).
4. Threshold scheme for information availability: Information available to an IDS running on a particular node is intentionally limited to provide additional resilience against the node compromise. To obtain full information required, multiple nodes with an IDS/privacy mechanism must cooperate, potentially with the support of a suitable cryptographic threshold scheme.

C. *IDS Leverage*

Co-existence of IDSs and privacy mechanisms may benefit both when used properly. If an IDS has several identities, it can, for example, send a probing message (using one identity) that should be forwarded back to itself (represented by another identity). These probing messages increase the amount of traffic and may play the role of dummy traffic. This also makes the traffic analysis harder and helps the privacy mechanism. Another benefit is that an attacker cannot easily avoid an IDS by selecting one (static) path without IDSs if a privacy mechanism ensures that multiple routes or randomly chosen routes are used.

III. ATTACKS ON SENSOR NETWORKS

Wireless sensor networks are not limited to simply denial of service attacks, but rather encompass a variety of techniques including node takeovers, attacks on the routing protocols, and attacks on a node's physical security. In this section, we first address some common denial of service attacks [4].

A. Types of Denial of Service attacks

The transmission of a radio signal that interferes with the radio frequencies being used by the sensor network is called jamming [5].Jamming may come in two forms: constant jamming, and intermittent jamming. Constant jamming implies the jamming of the entire network. While in the case of intermittent jamming, the sensor nodes are able to exchange messages periodically. At the link layer, one possibility is that an attacker may simply intentionally violate the communication protocol, e.g., ZigBee [17] or IEEE 802.11b protocol, and continually transmit messages in an attempt to generate collisions. Such collisions would require the retransmission of any packet lost by the collision. At the routing layer, a node may take advantage of a multi-hop network by simply refusing to route messages. With the net result being that any neighbor who routes through the malicious node will be unable to exchange messages with the part of the network. The transport layer is also vulnerable to attack, as in the case of flooding[18]. Flooding means sending many connection requests to a malicious node. In this case, resources must be allocated to handle the connection request. Eventually a node's resources will be exhausted, thus rendering the node useless.

B. The Sybil attack

Reference [7] defines Sybil attack as a malicious node illegitimately taking on multiple identities. It was originally
described as an attack able to defeat the redundancy mechanisms of distributed data storage systems in peer-to-peer networks.

C. Traffic Analysis Attacks

Often, for an attacker to effectively render the network in useless state, the attacker can simply disable the base station. To make matters worse, Authors in [8] demonstrate two attacks that can identify the base station in a network without even understanding the contents of the packets. A rate monitoring attack posits that nodes close to the base station tend to forward more packets than those farther away from the base station. While in a time correlation attack, an attacker generates events and monitors to whom a node sends its packets.

D. Node Replication Attacks

By copying the node ID of an existing node an attacker can add a node to an existing sensor network. A replicated node can severely disrupt a sensor network's performance; packets can be corrupted or even misrouted. This can result in a disconnected network and false sensor readings [9].

E. Physical Attacks

Indeed, in hostile outdoor environments, the small form factor of the nodes, coupled with the unattended and distributed nature of their deployment makes them vulnerable to physical attacks [10,16].Physical attacks ruin sensors permanently, so the losses are irreversible. For instance, attackers can access cryptographic secrets, tamper with the associated circuitry, spoofing / modifying programming in the nodes, and/or replace them with malicious nodes all of these within the control of the attacker.

IV. COUNTER MEASURES IN WSN

This section describes the countermeasures for satisfying the security requirements and protecting the sensor network from attacks. Table I below summarizes the attacks and counter-measures in a layering model in WSNs

Layers	Attack Type	Counter Measures
Application Layer	Subversion and Malicious Nodes	Malicious Node Detection and Isolation
Network Layer	Sinkholes, wormholes, Sybil, Routing Loop	Key Management, Secure Routing
Data Link Layer	Link Layer Jamming	Link Layer encryption
Physical Layer	DoS and Node capture attack	Adaptive antennas, Spread Spectrum

A. Defending Against DoS Attacks

One strategy in defending against the jamming attack is to identify the jammed part of the sensor network and effectively route around the unavailable portion. To handle jamming at the MAC layer[13], nodes might utilize a MAC admission control that is rate limiting. This would allow the network to ignore those requests designed to exhaust the power reserves of a node. This, however, is not fool-proof as the network must be able to handle any legitimately large traffic volumes.

B. Defending Against Attacks on Routing Protocols

There is a great need for both secure and energy efficient routing protocols in WSNs against attacks such as the sinkhole, wormhole and Sybil attacks. Authors in [15] describe an intrusion tolerant routing protocol, INSENS, which is designed to limit the scope of an intruder ruining and rout information within network intrusion. They posit utilizing the base station to compute routing tables on behalf of the individual sensor nodes[11]. This is done in three phases. The forwarding tables will include the redundancy information used for the redundant message transmission[18]. Attacks that can be made on the routing protocol during each of the three phases above are: First, sensor node might fool the base station by sending a bogus request message. Second, a compromised node might also include a bogus path(s) when forwarding the requested message to its neighbors. Finally, it may not even forward the requested message at all.

C. Combating Traffic Analysis Attacks

Authors in [8] use a random walk forwarding mechanism that occasionally forwards a packet to a node other than the sensor's parent node. This would make it difficult to discern a clear path from the sender node to the base station BS and would help to mitigate the rate monitoring attack, but would still be susceptible to the time correlation attack. To strive against the time correlation attack[14], it suggests a fractal propagation strategy[15]. In this mechanism a node will generate a forged packet when its neighbor is forwarding a packet to the base station. The forged packet is sent randomly to another neighbor who may also generate a forged packet. These packets essentially use a time-to-live to decide when the packet should discard. This effectively hides BS from time correlation attacks.

D. Key Management and Protocols

Sensor nodes may be deployed in a hostile environment; however, security becomes extremely important, as they are prone to variant types of malicious attacks. The open problem is how to set up pair-wise secret key between communicating nodes. In one of the recently presented secure schemes [1,7], the authors describe security as important as performance and energy efficiency for many applications. Key pre-distribution is a good idea to solve the key agreement problems in wireless sensor network, but in this case, the attacker might reveals it after compromising the node. Based on the Key-Insulated Encryption[18] (KIE)-WSNs, authors have proposed a new key pre-distribution scheme. They achieved both semantically security and optimal KIE-(N-1, N) safety, which means that even if N-1 nodes are compromised, there are no security threat to the remaining network.

E. Secure Broadcasting and Multicasting

The major communication pattern of wireless sensor networks is broadcasting and multicasting, e.g., 1-to-Y, Y-to-1, and X-to-Y, in contrast to the traditional point-to-point communication on the Internet network.

1) Secure Multicasting Pattern: Reference [6] proposes a directed diffusion based multicast technique for wireless sensor networks considering also the advantage of a logical key hierarchy. The key distribution center is the root of the key hierarchy while individual sensor nodes make up the leaves. By utilizing this technique, they modify the logical key hierarchy to build a directed diffusion based logical key hierarchy. This technique provides mechanisms for sensor nodes joining and leaving groups where the key hierarchy is used to effectively re-key all nodes within the leaving node's hierarchy.

2) Secure Broadcasting Pattern: Reference [7] suggests a routing-aware based tree where the leaf nodes are assigned keys *based* on all relay nodes above them. This technique takes advantage of routing information and is more energy efficient than mechanisms that arbitrarily arrange sensor nodes into the routing tree.

V. CONCLUSIONS

WSNs have became promising technology to many applications. In the absence of adequate security, deployment of sensor networks is vulnerable to variety of attacks. In this paper we have outlined the four main aspects of wireless sensor network security: obstacles, requirements, attacks, and defenses. Within each of those categories we have also sub-categorized the major topics including routing, key management, denial of service, and so on. Our aim is to provide a general overview of the rather broad area of wireless sensor network, security issues, and threat models give the main citations such that further review of the relevant literature can be completed by the interested researcher.

As wireless sensor networks continue to grow and become more common need for security in WSN applications will grow even further. We also expect that the current and future work in privacy and trust will make wireless sensor networks a more attractive option in a variety of new arenas. On the basis of our observation we motivate the need of a security framework to provide countermeasures against attacks in WSNs.

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “A survey on sensor networks,” IEEE Communications Magazine, vol. 40, no. 8, pp.102-114, August 2002.

[2] D. W. Carman, P. S. Krus, and B. J. Matt, “Constraints and approaches for distributed sensor network security,” Technical Report 00-010, NAI Labs, Network Associates, Inc., Glenwood, MD, 2000.

[3] HBE-Zigbex. Ubiquitous sensor network. Zigbex Manual. [Online].Available: http://www.hanback.co.kr.

[4] Y. Xiao, “Security in distributed, grid, and pervasive computing,” (Eds.) Chapt.17, in Wireless sensor network security: A Survey, J. P. Walters, Z. Liang,W. Shi, and V. Chaudhary, Auerbach Publications, CRC Press, 2006.

[5] A. D. Wood and J. A. Stankovic, “Denial of Service in Sensor Networks,” Computer, vol. 35, no. 10, pp. 54-62, 2002

[6] L. K. Bysani and A. K. Turuk, “A Survey on Selective Forwarding Attack in Wireless Sensor Networks,” in 2011 International Conference on Devices and Communications (ICDeCom), Feb., pp. 1–5.

[7] L. Lazos and R. Poovendran, “Secure broadcast in energy-aware wireless sensor networks,” in Proc. IEEE International Symposium on Advances in Wireless Communications (ISWC 02), BC Canada, 2002.

[8] J. Deng, R. Han, and S. Mishra, “Countermeasures against traffic analysis in wireless sensor networks,” Technical ReportCU-CS-987-04, University of Colorado at Boulder, 2004.

[9] B. Parno, A. Perrig, and V. Gligor, “Distributed detection of node replication attacks in sensor networks,” in Proc. IEEE Symposium on Security and Privacy (SSP 05), May 2005, pp. 49-63.

[10] V. Maty_a_s and J. K_ur. Conicts between intrusion detection and privacy mechanisms for wireless sensor networks. IEEE Security and Privacy, 11(5):73-76, 2013.

[11] S. Misra and G. Xue. E_cient anonymity schemes for clustered wireless sensor networks. International Journal of Sensor Networks, 1(1-2):50-63, 2006.

[12] D. Niculescu. Communication paradigms for sensor networks. IEEE Communications Magazine, 43(3):116-122, 2005.

[13] C. Karlof and D.Wagner. Secure routing in wireless sensor networks: attacks and countermeasures. In Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications, pages 113-127, 2003.

[14] V. Maty_a_s and J. K_ur. Conicts between intrusion detection and privacy mechanisms for wireless sensor networks. IEEE Security and Privacy, 11(5):73-76, 2013.

[15] F. Liu, X. Cheng, and D. Chen. Insider attacker detection in wireless sensor networks. In Proceedings of the 26th IEEE International Conference on Computer Communications, pages 1937{1945, 2007.

[16] A. Stetsko, L. Folkman, and V. Matyas. Neighbor-based intrusion detection for wireless sensor networks. Technical Report FIMU-RS-2010-04, Faculty of Informatics, Masaryk University, May 2010.

[17] Wireless Ad Hoc and Sensor Networks. [Online]. Available: http://www.zigbee.org/ 2005.

[18] Sujesh P Lal, Prof. H R Viswakarma. QoS Based Bandwidth Allocation for Networks. Volume-2, Number-2, December 2009. Pages 111-119.

[19] M. Cinque, A. Coronato, A. Testa, and C. Di Martino, “A Survey on Resiliency Assessment Techniques for Wireless sensor Networks,” in Proceedings of the 11th ACM International Symposium on Mobility Management and Wireless Access, New York, NY, USA, 2013, pp. 73–80.

Authors

Sujesh P Lal is a research scholar in Sathyabama University, Chennai, and an assistant professor in Federal Institute of Science and Technology (FISAT), Ernakulam. Completed his MCA Degree from Bharatiar University, India, in 2003 and MTech Degree in Computer Science and Engineering from VIT University, India, in 2010. Qualified UGC-NET in 2013. His research interests are Wireless Sensor Networks, Security in Networks, Mobile Sensor Networks.

Dr. Joe Prathap P M is a Professor in the Department of Information Technology, RMD Engineering college, Chennai. He received his BE degree from MS University, India in 2003, He received ME (computer science and information technology.)from Anna University, Chennai, India in 2005 and Ph.D in 2011(computer science and information technology). His research interests are networking, security, wireless sensors, routing techniques, etc.