International Journal of Advance Research in Engineering, Science & Technology(IJAREST),
ISSN(O):2393-9877, ISSN(P): 2394-2444,
Volume 2, Issue 7, July- 2015

Security Attacks in Wireless Sensor Networks

Ms. Kavita Joshi

Computer Science, Jodhpur National University, joshikavita171@gmail.com

Abstract

Wireless Sensor networks (WSN) is an emerging technology and have great potential to be employed in critical situations like battlefields and commercial applications such as building, traffic surveillance, habitat monitoring and smart homes and many more scenarios. Wireless communication technique has become an essential tool in any application that requires communication between one or more sender(s) and multiple receivers. Since multiple users can use this technique simultaneously over a single channel, security has become a huge concern. Even though there are numerous ways to secure a wireless network and protect the network from numerous attacks, providing 100% security and maintaining confidentiality is a huge challenge in recent trends. This paper discusses a wide variety of attacks in WSN and their classification mechanisms.

Keywords- *WSN (wireless sensor network), DoS (Denial of service), Desynchronization, Syn flooding, Attacks, Sybil, Sinkhole*

I. INTRODUCTION

A wireless sensor network (WSN) (sometimes called a wireless sensor and actor network[1] (WSAN)) are spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. A WSN typically has little or no infrastructure. It consists of a number of sensor nodes (few tens to thousands) working together to monitor a region to obtain data about the environment Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. There are two types of WSNs: structured and unstructured. An unstructured WSN is one that contains a dense collection of sensor nodes. Sensor nodes may be deployed in an ad hoc manner into the field. Once deployed, the network is left unattended to perform monitoring and reporting functions. In an unstructured WSN, network maintenance such as managing connectivity and detecting failures is difficult since there are so many nodes. In a structured WSN, all or some of the sensor nodes are deployed in a pre-planned manner.[2] The advantage of a structured network is that fewer nodes can be deployed with lower network maintenance and management cost. Fewer nodes can be deployed now since nodes are placed at specific locations to provide coverage while ad hoc deployment can have uncovered regions.

WSNs are usually sensibly (sometimes even orders of magnitude) larger than similar ad-hoc networks, and are often deployed in hostile environments and over wide geographic areas. Motes have limited computational power, memory and energy supply, which, together with the adverse working conditions, make them particularly prone to failures. Despite many energy harvesting solutions proposed so far, recharging is still considered hardly feasible, and motes are usually regarded as ‘‘disposable’’ devices. Due to the complexity of replacement and management operations, maximizing lifetime and productivity is of paramount importance. In essence, WSNs are ad-hoc networks with additional and more stringent constraints. They need to be more energy-efficient and scalable than other ad-hoc networks, which exacerbates the security challenges.

Initially, the development of WSNs was mainly motivated by military purposes, but nowadays WSNs are becoming pervasive systems, used in several fields, from home automation to border monitoring. However, military applications, together with automated medical systems, still represent the contexts where security aspects are more relevant. In both cases, the network handles critical information, hence to ensure data availability is crucial.

Further classified, military data and private patients health-status information, raise the concern for confidentiality and privacy.

WSN applications need to contrast most security issues communal to conventional networks, like message injection, eavesdropping, impersonation, etc. However, the design of a security infrastructure in WSNs must pervade any layer of the system, from the application layer to the physical layer (that is often considered secure in conventional settings). Further, mainly because of their limited resources, standard techniques such as tamper-proof hardware, secure routing, public-key cryptography, etc., do not suit WSNs. Specific solutions for WSNs are required, that must be conceived with these low-end devices in mind.

II. SECURITY REQUIREMENT IN WIRELESS SENSOR NETWORK

A sensor network is a special type of network. we can think of the requirements of a wireless sensor network as encompassing both the typical network requirements and the unique requirements suited solely to wireless sensor networks.

Data Confidentiality:

Data confidentiality is the most important issue in network security. Every network with any security focus will typically address this problem first.

•A sensor network should not leak sensor readings to its neighbors.

• it is extremely important to build a secure channel in a wireless sensor network.

The standard approach for keeping sensitive data secret is to encrypt the data with a secret key that only intended receivers possess, thus achieving confidentiality.

Data Integrity:
With the implementation of confidentiality, an adversary may be unable to steal information. However, this doesn't mean the data is safe. The adversary can change the data, so as to send the sensor network into disarray. Data integrity ensures that any received data has not been altered in transit.

Data Freshness:
Even if confidentiality and data integrity are assured, we also need to ensure the freshness of each message. Informally, data freshness suggests that the data is recent, and it ensures that no old messages have been replayed.

Availability:
The services provided by the network must be always available (often in a timely manner), despite of any malfunctioning of the system. Resource depletion attacks are the main class of attacks aiming at subverting this property. Resistance to such attacks is therefore of primary importance.

Self-Organization:
A wireless sensor network is a typically an ad hoc network, which requires every sensor node be independent and flexible enough to be self-organizing and self-healing according to different situations. There is no fixed infrastructure available for the purpose of network management in a sensor network. This inherent feature brings a great challenge to wireless sensor network security as well.

Time Synchronization:
Most sensor network applications rely on some form of time synchronization. In order to conserve power, an individual sensor's radio may be turned off for periods of time. Furthermore, sensors may wish to compute the end-to- end delay of a packet as it travels between two pairwise sensors. A more collaborative sensor network may require group synchronization for tracking applications, etc.

Secure Localization:
Often, the utility of a sensor network will rely on its ability to accurately and automatically locate each sensor in the network. A sensor network designed to locate faults will need accurate location information in order to pinpoint the location of a fault. Unfortunately, an attacker can easily manipulate non- secured location information by reporting false signal strengths, replaying signals, etc.

Authentication:
An adversary is not just limited to modifying the data packet. It can change the whole packet stream by injecting additional packets. So the receiver needs to ensure that the data used in any decision-making process originates from the correct source. On the other hand, when constructing the sensor network, authentication is necessary for many administrative tasks (e.g. network reprogramming or controlling sensor node duty cycle). From the above, we can see that message authentication is important for many applications in sensor networks.

III. ATTACKS TO WIRELESS SENSOR NETWORKS

At a high level, attacks against wireless ad-hoc networks can be classified based on the status of the attacker, on its behavior, and on the purpose of the attack.

3.1. Status:

The first classification is based on whether the attacker is an outsider or an insider. Outsider attackers are entities that do not belong to the network but want to disrupt the provided service. Insider attackers are legitimate nodes behaving in a malicious way.

3.2. Behaviour:

The second classification distinguishes between passive and active attacks.

Passive Attack:
A passive attack monitors unencrypted traffic and looks for clear -text passwords and sensitive information that can be used in other types of attacks. Passive attacks include traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic, and capturing authentication information such as passwords. Passive interception of network operations enables adversaries to see upcoming actions. Passive attacks result in the disclosure of information or data files to an attacker without the consent or knowledge of the user.

Active Attack:
In an active attack, the attacker tries to bypass or break into secured systems. This can be done through stealth, viruses, worms, or Trojan horses. Active attacks include attempts to circumvent or break protection features, to introduce malicious code, and to steal or modify information.

3.3. Purpose:

The third categorization depends on the purpose of the attack.

3.3.1. Attacks against network availability and service integrity.

Attacks on network availability and service integrity, aim at disrupting the services provided by the network. Many denial-of-service, routing and physical attacks fall within this category. Attacks against network availability and service integrity are often referred to as denial-of-service (DoS) attacks: an adversary attempts to disrupt, subvert or destroy the services provided by the network. DoS attacks can have as a target any layer of the sensor network. Indeed, known attacks perform on the physical, the data link, the network and the transport layers. In this section, we will analyze existing DoS attacks layer by layer.

Physical layer attacks: Five types of Attacks in physical layer are Jamming, Sniffing, interruption and Tampering.

Jamming is one of many exploits used compromise the wireless environment. It works by denying service to authorized users as legitimate traffic is jammed by the overwhelming frequencies of illegitimate traffic. Depending on its transmission power, the jammer may disturb the entire network or a smaller portion of it. Jamming can be classified as follows: [3]

Spot jamming is the simplest jamming technique. The attacker directs all its compromising power against a single frequency. It is usually effective, but it may be avoided by changing the frequency used.

Sweep jamming targets multiple frequencies in quick succession, by rapidly shifting the target frequency. Since the activity of the attacker is not continuous, the effectiveness of
this type of attack is limited. However, in WSNs it can force many retransmissions due to packet loss.

Barrage jamming concurrently targets a range of frequencies. However, as the attacked range grows, the output power of jamming is reduced proportionally.

Deceptive jamming consists in fabricating or replaying valid signals on the channel incessantly, thereby occupying the available bandwidth and trying to destroy the network service. It can be applied to a single frequency or a set of frequencies.

Tampering A wide range of active attacks, generally carried out by outsiders, all rely on a communal approach: gaining physical access to a subset of sensors by tampering with their hardware. DoS attacks are only one of the possible ways an adversary can leverage tampering. More generally, the purpose may be to modify the behaviour of the nodes, to replace them with malicious sensors under the control of the attacker, or to steal confidential data and cryptographic material.[4]

Sniffing is a type of software attack where an attacker tries to gain access to private communications, using a utility such as Dsniff or Network Monitor, in order to steal the content of the communication itself or to obtain user names and passwords for future software attacks, such as a takeover attack.

Interruption attacks are attacks against the availability of the network. These attacks can take the form of overloading a server host so that it cannot respond. And blocking access to a service by overloading an intermediate network or network device.

Link layer attack: The Mobile Ad Hoc Network (MANET) is an open multipoint peer-to-peer network architecture. Specifically, one-hop connectivity among neighbours is maintained by the link layer protocols, and the network layer protocols extend the connectivity to other nodes in the network. Attacks may target the link layer by disrupting the cooperation of the layer's protocols. All such attacks share two main objectives: (i) depleting the energetic resources of the sensors, relying on the fact that most energy consumption in WSNs is due to communication, and (ii) degrading the timeliness of the service

Link Layer Collision: This attack is very similar to jamming in the physical layer. It occurs when an attacker uses his radio to identify the frequency used by the WSN, and, as soon as he hears the start of a legitimate message transmission, he sends a signal for as little as one octet (or byte) in order to corrupt the entire message[5]. The only evidence of the attack is the reception of an incorrect message, which is detected when a link layer frame fails a cyclic redundancy code (CRC) check. In that case, the link layer automatically discards the entire packet, thereby causing energy and bandwidth waste.

Link Layer Exhaustion: This attack occurs when the attacker manipulates protocol efficiency measures and causes nodes to expend additional energy. Providing a rate limitation by allowing nodes to ignore excessive network requests from a node is an effective countermeasure against this attack.

WEP Weakness : When people do use WEP, they forget to change their keys periodically. Having many clients in a wireless network potentially sharing the identical key for long periods of time.

Unfairness: In an unfairness attack, the adversary transmits a large number of packets when the medium is free, to prevent honest sensors from transmitting legitimate packets. As a result, the quality of service degrades and real-time deadlines are possibly missed.

Sleep Deprivation Torture: In WSNs, a sleep mechanism is used by the nodes to adjust their operation mode and extend their lifetime. At full power, a sensor can run for approximately two weeks before exhausting its power resources. To the contrary, if nodes remain in sleep mode and activate as little as possible (e.g., around 1% of the time), their batteries can last even more than a year. As the name suggests, the ''Sleep Deprivation Torture'' or ''denial-of-sleep'' attack, firstly introduced in [6], aims at preventing a sensor from sleeping.

Interrogation: constantly request-to-send

Network and routing layer: At the network layer, many attacks can disrupt the network availability. The network layer of WSNs is vulnerable to the different types of attacks such as: Wormhole, Sinkhole, Black hole, hello Flooding. Direct Attacks on Routing Information A direct attack against the routing layer can try to spoof, alter, or replay routing information. By subverting this information the adversary can change to his favour the data flow.

Hello Flooding: Hello messages are often used to discover neighbouring nodes and automatically create a network. Many protocols which use this mechanism make the naive assumption that the sender is within radio range. However, an adversary with a high powered transmitter can corrupt a sensor and make other sensors believe that such a malicious node is in their neighbourhood. Data packets routed to the malicious sensor will be indeed sent into oblivion[7], causing both data loss and energy wasting.

Wormhole attack: In a wormhole attack, an attacker receives packets at one point in the network, "tunnels" them to another point in the network, and then replays them into the network from that point. An attacker intrudes communications originated by the sender, copies a portion or a whole packet, and speeds up sending the copied packet through a specific wormhole tunnel in such a way that the copied packet arrives at the destination before the original packet which traverses through the usual routes. Such a tunnel can be created by several means, such as by sending the copied packet through a wired network and at the end of the tunnel transmitting over a wireless channel, using a boosting long-distance antenna, sending through a low-latency route, or using any out-of bound channel.

Sinkhole attack: The sinkhole attack is a particularly severe attack that prevents the base station from obtaining complete and correct sensing data, thus forming a serious threat to higher-layer applications. In a Sinkhole attack, a compromised node tries to draw all or as much traffic as possible from a particular area, by making itself look attractive to the surrounding nodes with respect to the routing metric. As a result, the adversary manages to attract all traffic that is destined to the base station by advertising as having a higher trust level and as a node in the shortest distance or short delay path to a base station.

Selective Forwarding: When a malicious node does not follow the routing protocol, but acts as a filter forwarding certain messages and dropping others, we face a selective forwarding attack[7].The black hole attack can be seen as a special case of selective forwarding,where all the packets are dropped.

Sybil attack: A single node presents itself to other nodes with multiple spoofed identifications (either MAC or network addresses). The attacker can impersonate other nodes identities or simply create multiple arbitrary identities in the MAC and/or network layer. Then the attack poses threats to other protocol layers; for examples, packets traversed on a route consisting of fake identities are selectively dropped or modified; or a threshold-based signature mechanism that relies on a specified number of nodes is corrupted.

Transport layer attacks: All transport layer protocols can be classified into those that provide congestion control mechanisms, and those that provide reliability [8] of the data transfer. The latter are the most relevant, and their main purpose is to guarantee that every packet loss is detected, and that lost packets are retransmitted until they reach their destination. A reliable transport layer protocol can only detect packet losses if there is some kind of feedback in the system. A scheme can use two types of acknowledgments (ACKs): explicit, when a node sends back a confirmation for any packet received, or implicit, when each node verifies the delivery of a packet to a neighbor by overhearing that that neighbor is forwarding the packet. Further, a protocol can use negative acknowledgments (NACKs) if nodes are somehow able to realize the non-reception of a packet, and they explicitly send a request for retransmission. we will analyze the following type of attacks to the transport layer [9]: flooding, desynchronization , Session hijacking, Syn flooding.

Flooding: Flooding attacks exhaust the memory resources of a sensor, by sending many connection establishment requests to the victim, which consequently allocates resources that maintain state for those connections.

Desynchronization: In a desynchronization attack, the adversary forges messages containing bogus sequence numbers or control flags to disrupt an existing connection between two end-points. By continuously causing retransmission requests, this attack can eventually prevent the end-points from exchanging any useful information, other than quickly drain all the power resources of the attacked nodes.

Session hijacking: It is the exploitation of a valid computer session—sometimes also called a session key to gain unauthorized access to information or services in a computer system. In particular, it is used to refer to the theft of a magic cookie used to authenticate a user to a remote server.

Syn flooding: This attack is denial of service attack. An attacker may repeatedly make new connection request until the resources required by each connection are exhausted or reach a maximum limit. It produces severe resource constraints for legitimate nodes.

Application layers attacks: The different type of application layers attack is Overwhelm, BS Path DoS, Repudiation, Data Corruption and Malicious Code.

Overwhelm: In this attack, an attacker might overwhelm network nodes, causing network to forward large volumes of traffic to a base station. This attack consumes network bandwidth and drains node energy.

BS Path DoS : In a PDoS attack, an adversary overwhelms sensor nodes a long distance away by flooding a multihop end-to-end communication path with either replayed packets or injected spurious packets.

Repudiation Attacks: This makes data or information to appear to be invalid or misleading (Which can even be worse). For example, someone might access your email server and inflammatory information to others under the guise of one of your top managers. This information might prove embarrassing to your company and possibly do irreparable harm. This type of attack is fairly easy to accomplish because most email systems don't check outbound email for validity. Repudiation attacks like modification attacks usually begin as access attacks.

Data corruption refers to errors in computer data that occur during writing, reading, storage, transmission, or processing, which introduce unintended changes to the original data. Computer storage and transmission systems use a number of measures to provide data integrity, or lack of errors.

Malicious Code: Viruses and worms are related classes of malicious code; as a result they are often confused. Both share the primary objective of replication. However, they are distinctly different with respect to the techniques they use and their host system requirements. This distinction is due to the disjoint sets of host systems they attack. Viruses have been almost exclusively restricted to personal computers, while worms have attacked only multi-user systems.

Multi-layer attacks: Some security attacks can be launched from multiple layers instead of a particular layer. Examples of multilayer attacks are denial of service (DoS), man-in-the middle, and impersonation attacks [10].

Denial of service: Denial of service (DoS) attacks could be launched from several layers. An attacker can employ signal jamming at the physical layer, which disrupts normal communications. At the link layer, malicious nodes can occupy channels through the capture effect, which takes advantage of the binary exponential scheme in MAC protocols and prevents other nodes from channel access. At the network layer, the routing process can be interrupted through routing control packet modification, selective dropping, table overflow, or poisoning. At the transport and application layers, SYN flooding, session hijacking, and malicious programs can cause DoS attacks.

Impersonation attacks: Impersonation attacks are launched by using other node's identity, such as MAC or IP address. Impersonation attacks sometimes are the first step for most attacks, and are used to launch further, more sophisticated attacks.

Man-in-the-middle attacks: An attacker sits between the sender and the receiver and sniffs any information being sent between two ends. In some cases the attacker may impersonate the sender to communicate with the receiver, or impersonate the receiver to reply to the sender.

3.3.2. Attacks against confidentiality and privacy.

The more WSNs become pervasive, the more confidentiality and privacy represent two primary concerns. Data confidentiality needs to be enforced through access control policies, to prevent misuse of information by unintended parties. Privacy must be addressed when sensors are not property of the central authority, or in general every time data gathering may involve contextual information which monitored entities do not want to share with the network authority. Confidentiality and privacy issues involve even ethical or legal aspects.

Eavesdropping: This is the most common attack to privacy. If end-to-end communications are not protected, anyone is able to discover the communication content by simply eavesdropping on the network's radio frequency range. By snooping to the data, the adversary could easily discover the communication contents. When the traffic conveys the control information about the sensor network configuration, which contains potentially more detailed information than accessible through the location server, the eavesdropping can act effectively against the privacy protection.

Traffic Analysis Even when the messages transferred are encrypted, it still leaves a high possibility analysis of the communication patterns. Sensor activities can potentially reveal enough information to enable an adversary to cause malicious harm to the sensor network.

Camouflage Adversaries: One can insert their node or compromise the nodes to hide in the sensor network. After that these nodes can copy as a normal node to attract the packets, then misroute the packets, conducting the privacy analysis.

3.3.3. Attacks against data integrity.

Data integrity is violated when the adversary corrupts records, and the sink is not able to restore the original sensed data, or at least to detect that data have been manipulated.

Node Replication: Conceptually, a node replication attack is quite simple; an attacker seeks to add a node to an existing sensor network by copying the nodeID of an existing sensor node. A node replicated in this approach can severely disrupt a sensor network's performance. Packets can be corrupted or even misrouted. This can result in a disconnected network, false sensor readings, etc. If an attacker can gain physical access to the entire network he can copy cryptographic keys to the replicated sensor nodes. By inserting the replicated nodes at specific network points, the attacker could easily manipulate a specific segment of the network, perhaps by disconnecting it altogether.

Packet Injection, Replication and Alteration: To modify data gathered by the network, the adversary has three main alternatives: inject completely false data, replicate previously captured packets, or intercept messages and alter their content. All these attacks can be easily run by insiders, but if the adversary is an outsider they require to break the authentication mechanisms to varying degrees. Injection requires forging from scratch a message that must be indistinguishable from legitimate ones. Replication uses already authenticated massages, but counters or timestamps used to avoid replay attacks need to be counterfeited. Alteration is in general as difficult as injection, but it can result sensibly easier when homomorphic encryption/ authentication is used.

IV. CONCLUSION:

The deployment of sensor nodes in an unattended environment makes the networks vulnerable. Wireless sensor networks are increasingly being used in military, environmental, health and commercial applications. Sensor networks are inherently different from traditional wired networks as well as wireless ad-hoc networks. Security is an important feature for the deployment of Wireless Sensor Networks. In this section, we discussed the main security threats and countermeasures in WSNs, classifying attacks according to their target. Depending on the service provided, secure WSNs need defensive mechanisms to protect (i) network availability and service integrity, (ii) data

confidentiality and privacy, and/or (iii) data integrity. When dealing with network and service reliability, Security mechanisms must perform at each layer, from the physical, to the link, the network, and the transport layer.

REFERENCES

[1] F. Akyildiz and I.H. Kasimoglu, "Wireless Sensor and Actor Networks: Research Challenges,"; Ad Hoc Networks, vol. 2, no. 4, pp. 351-367, Oct. 2004.

[2] J. Yick, B. Mukherjee, D. Ghosal, Analysis of a Prediction-based Mobility Adaptive Tracking Algorithm, in: Proceedings of the IEEE Second International Conference on Broadband Networks (BROADNETS), Boston, 2005.

[3] A. Mpitziopoulos, D. Gavalas, A survey on jamming attacks and countermeasures in WSNs, Surv. Tutor. 11 (4) (2009) 42–56,http:// dx.doi.org/10.1109/SURV.2009.090404

[4] O. Kommerling, M. Kuhn, Design principles for tamper-resistant smartcard processors, in: Of the USENIX Workshop on Smartcard, USENIX Association, Chicago, Illinois, 1999, pp. 9–20

[5] Y. Law, P. Hartel, J. den Hartog, P. Havinga, Link-layer jamming attacks on SMAC, in: Proceeedings of the Second European Workshop on Wireless Sensor Networks, 2005, IEEE, 2004, pp. 217–225, http://dx.doi.org/10.1109/EWSN.2005.1462013

[6] F. Stajano, R.J. Anderson, The resurrecting duckling: security issues for ad-hoc wireless networks, in: Proceedings of the 7th International Workshop on Security Protocols, Springer-Verlag, London, UK, 2000, pp. 172–194

[7] C. Karlof, D. Wagner, Secure routing in wireless sensor networks: attacks and countermeasures, in: Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications, Elsevier, 2003, pp. 113–127, http://dx.doi.org/10.1016/S1570-8705(03)00008-8.

[8] C. Wang, K. Sohraby, B. Li, M. Daneshmand, Y. Hu, A survey of transport protocols for wireless sensor networks, IEEE Netw. 20 (3) (2006) 34–40

[9] A.D. Wood, J.A. Stankovic, Denial of service in sensor networks, Computer 35 (2002) 54-62,http://dx.doi.org/10.1109/MC.2002.1039518

[10] Ehab Al-Shaer, "Network Security Attacks I: DDOS", DePaul University, 2007.