ISSN:0975-9646

Survey on different types of Security Threats on Wireless Sensor Networks

Genita Gautam, Biswaraj Sen

Computer Sc & Engineering, SMIT, SMU
Sikkim, India

Abstract: A Wireless Sensor Network (WSN) consists of spatially distributed autonomous sensors.WSNs are vulnerable to security attacks due to the broadcast nature of radio transmission.This paper provides a study of different types of security attacks in WSNs. The focus has been on the sleep deprivation torture (denial-of-sleep) attack which is a type of denial-of-service (DOS) attack. The sleep deprivation torture attack aims at preventing a sensor from sleeping thus draining its battery more quickly than it would be under normal usage. A brief study on related works carried out on this attack is also presented.

Keywords: Wireless Sensor Networks (WSNs), Denial-of-Service (DOS).

I. INTRODUCTION

A wireless sensor network is a group of specialized sensors with a communications infrastructure that uses radio to monitor and record physical or environmental condition such as temperature and pressure. As numerous sensors are connected to controllers and processing stations directly (example, Local Area Network), burgeoning number of sensors divulge the data collected wirelessly to a centralized processing unit. The potential of a sensor could differ as a sensor node is not only obligated to collect data, but also for in-network examination, correlation, and combination of its own sensor data and data from other sensor nodes. Unlike simple sensors, which monitor a single physical phenomenon, sophisticated devices combine numerous sensing techniques (example, acoustic, optical, magnetic). Also simple sensors may only collect and communicate information about the observed environment, more powerful devices may also perform extensive processing and aggregation functions.

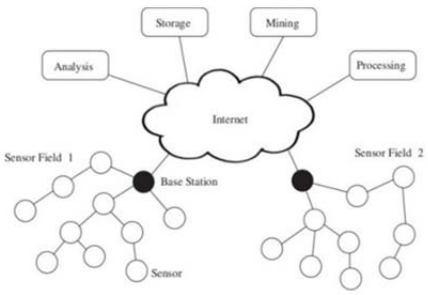

Fig 1: Wireless sensor networks [8]

A number of applications have been inspired by Wireless sensor networks. A large number of them are practically useful while many are futuristic. The diversity of applications in the latter category is remarkable – environment monitoring, target tracking, pipeline (water, oil, gas) monitoring, structural health monitoring, precision agriculture, health care, supply chain management, active volcano monitoring, transportation, human activity monitoring, and underground mining.

II. SECURITY IN WSN

Security and privacy are enormous challenges in all types of wired and wireless networks. These challenges are of even greater importance in wireless sensor networks, where the unique characteristics of these networks and the application purposes they serve make them attractive targets for intrusions and other attacks. In applications such as battlefield surveillance and assessment, target tracking, monitoring civil infrastructure such as bridges and tunnels, and assessment of disaster zones to guide emergency response activities, any breach of security, compromise of information, or disruption of correct application behaviour can have very serious consequences.

Sensor networks are frequently used in remote areas, left to operate unattended and therefore providing an easy target for physical attacks, unauthorized access, and tampering. Sensor nodes are typically very resource-constrained and operate in harsh environments, which further facilitate compromises and makes it often difficult to distinguish security breaches from node failures, varying link qualities, and other commonly found challenges in sensor networks.

III. SECURITY CHALLANGES IN WSNS

WSNs exhibit a variety of unique challenges that must be considered when addressing the security concerns. This is due to the below constraints:

A. Limited Resources

Many security mechanisms are computationally expensive or require communication with other nodes or "remote" devices (e.g., for authorization purposes), thereby leading to energy overheads. Small sensor devices are constrained in their available memory and storage capacities. A sensor is a tiny device with only a small amount of memory and storage space for the code. Therefore the traditional security algorithms that require a significant amount of memory and storage space are therefore infeasible for such kind of sensors.

B. Unreliable Communication

Unreliable communication is another threat to sensor security. This is due to the broadcast nature of the wireless sensor network. Packets in WSNs may be lost or corrupted due to a variety of reasons, including channel errors,

routing failures, and collisions. This may interfere with some security mechanisms or their ability to obtain critical event reports.

C. Unattended Operation

The first line of defence against security attacks is to provide controlled physical access to a sensor node. Many WSNs are left unattended, because they are operated in remote and hard-to-reach locations, deployed in environments open to public access, or so large that it would be infeasible to continuously monitor and protect sensor nodes from attacks. These challenges make it difficult to prevent unauthorized physical access and to detect tampering with the sensor devices, particularly since the low cost of many sensor nodes may prohibit advanced (and expensive) protective measures.

It is often infeasible to have a central point of control in sensor networks, for example, because of their large scale, resource constraints, and network dynamics. Therefore, security solutions should be decentralized and nodes must collaborate to achieve security.

IV. SECURITY REQUIREMENTS

Computer and network security is the collection of all policies, mechanisms, and services that afford a computer system or network the required protection from unauthorized access or unintended uses. Most security mechanisms are built to address three well-known services in the CIA security model:

A. Confidentiality

Security mechanisms must ensure that only the intended receiver can correctly interpret a message and that unauthorized access and usage is prevented. For example, confidentiality ensures that sensitive information such as a person's social security number or credit card information are not obtained by an unauthorized individual. A threat to such kind of service is Eavesdropping which refers to the reception of a message by an unauthorized individual.

B. Integrity

Security mechanisms must ensure that a message cannot be modified as it propagates from the sender to the receiver, that is, unauthorized individuals should not be able to destroy or alter the contents of sensitive information. A threat to such kind of service is man-in-the-middle attack which refers to a situation where an unauthorized individual or system positions itself between the sender and receiver such that the sender's messages are intercepted, modified, and retransmitted to the receiver (where the receiver believes the received message came directly from the original sender).

C. Availability

Availability is a measure which is defined as the probability of a component/system is functioning at time *t*. This requirement ensures that the services of a WSN should always be available. A threat to such kind of service is denial-of-service attack refers to an adversary's attempt to disrupt the transmission or service provided by the sender. For example, the adversary can overload the sender with requests and tasks such that the sender is not able to transmit its message (in a timely fashion) to the receiver.

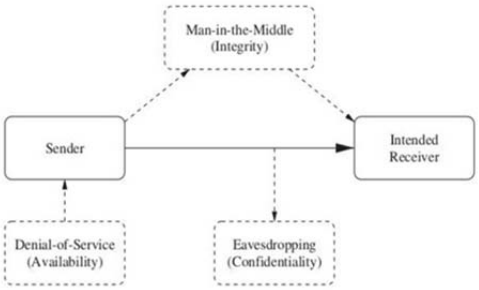

Fig 2: Attacks on CIA model [8]

V. ATTACKS ON WSN

Sensor networks are vulnerable to a variety of attacks that attempt to compromise the network's operation and the data the sensor nodes generate. Specifically when sensor networks serve application purposes such as battlefield assessments and monitoring of civil infrastructure, they require protection from unauthorized access and tampering.

A. Classification of attacks based on interruption

Attacks can be classified into two major categories according the interruption of communication act, namely passive attacks and active attacks.

1) Passive attacks: It is an attack in which fake data is received from the attacker without interrupting the communication. Examples of this type of attack are eavesdropping, traffic analysis, and traffic monitoring.

2) Active attacks: It is an attack in which fake data is received from the attacker disrupts the entire network. Examples of active attacks include jamming, impersonating, modification, denial of service (DoS), and message replay.

B. Types of Denial of Service attacks

1) Jamming Attack

A standard attack on wireless sensor networks is simply to jam a node or set of nodes. A jamming attack occurs when an adversary interferes with the radio frequencies of a WSN. If well positioned, a few attacking nodes can disable an entire network, even if the number of attacking nodes is much smaller than the number of nodes in the network. Even a single attacking node could disable an entire network if it is positioned close to a "critical" node (e.g., a gateway, therefore preventing any sensor data from leaving the sensor network) or its transmission power is large such that all nodes in a network may be prevented from correctly receiving any meaningful data. There are two types of jamming:

Constant jamming: It jams the entire network. No messages are able to be sent or received.

Intermittent jamming: the nodes exchange messages periodically, but not consistently. This may also impact on the sensor network as the messages can be time sensitive.

2) Sleep Deprivation Torture Attack

This type of attack is on the link layer. This is the most dangerous type of attack. Here, the target of the attacker is to minimize the lifetime of the sensor nodes by increasing power consumption. In this paper only concern is with this type of attack. The main concern in this paper is this type of attack.

3) Flooding

The transport layer is also susceptible to attack, as in the case of flooding. The flooding attack exploits the fact that many transport protocols (such as TCP) maintain state information and are therefore vulnerable to memory exhaustion. For example, an attacker may repeatedly make new connection requests, each adding more state information at the affected node and potentially leading to the node refusing further connections due to resource exhaustion. This in turn prevents connection requests from legitimate nodes from succeeding.

C. Other types of Attacks

1) Sybil Attack

The Sybil attack is defined as a "multiple identities taken illegitimately by malicious device". When attacker claims to have several identities in network, then it occurs. Similarly, in location-based routing protocols, an attacker claims to be at several locations simultaneously. If many nodes believe that this malicious node is their neighbour, there is a good chance that they will choose this node as forwarding node for their network traffic.

2) Node Replication Attacks

Conceptually, a node replication attack is quite simple: an attacker seeks to add a node to an existing sensor network by copying (replicating) the node ID of an existing sensor node [2]. A node replicated in this fashion can severely disrupt a sensor network's performance. A scheme known as distributed wake-up scheduling scheme for data collection in a sensor networks that achieves both energy conservation and low reporting latency, i.e. in a multihop wireless network, a simple and efficient way of defining interference neighbours is to prohibit a node from using the same slot0code as those of its 1-hop and 2-hop neighbours. Power saving and latency are improved to prolong network lifetime and freshness of data. Herein this scenario, since not all nodes are involved in the communication and communication directions are always toward the sink, a node only need to consider a tighter set of interference neighbours and other drawback is that this scheme cannot handle the multiple tasks at a same time. Packets can be corrupted or even misrouted. This can result in a disconnected network, false sensor readings, etc. An attacker can get physical access to the entire network and replicate the sensor and insert the replicated nodes at strategic points in the network. [2]. The attacker can easily manipulate a network by inserting the replicated nodes and perhaps by disconnecting it all together**.**

3) Attacks against Privacy

The main concern perhaps is not that the sensor networks facilitate data collection. In fact, much information from sensor networks could probably be collected through direct site surveillance. Further, the privacy problem could exacerbate because huge volumes of information becomes vulnerable and readily available through remote access. The different types [3] of privacy attacks are:

- Monitor and Eavesdropping: This is the most obvious attack to privacy. The adversary could easily find the communication contents by listening to it. The sensor network contains potentially more detailed information than accessible through the location server. The control can effectively act against privacy protection only if the traffic carries the control data about the sensor network.
- Traffic Analysis: Traffic analysis combines monitoring and eavesdropping. The sensor can be signalled that a particular sensor has a registered activity when there is an increase in the number of transmitted packets between certain nodes. The sensors with special roles and activities can effectively identify through an analysis.
- Camouflage: Adversaries can insert their node or compromise the nodes to hide in the sensor network. After that these nodes can masquerade as a normal node to attract the packets, then misroute the packets, e.g. forward the packets to the nodes conducting the privacy analysis.

4) Attacks on Data Aggregation

Data aggregation and data fusion are often used to combine multiple sensor data and to eliminate redundant information. Aggregation can often have beneficial effects on the resource requirements of sensor flows, for example, by reducing the frequency of transmissions or the packet sizes. Even simple aggregation functions can easily be influenced by an attacker such that a network's behaviour can be altered (Wagner 2004). For example, the average function $f(x_1, \ldots, x_n) = (x_1 + \cdots + x_n)/n$ is insecure even in the presence of a single malicious node. By replacing one real measurement x_1 with a fake reading $x1*$, the average is changed from $y = f(x_1, ..., x_n)$ to $y* = f(x_1*, x_2, ..., x_n) = y + (x_1* - x_1)/n$. An attacker can freely choose the value of x_1* and, therefore, can control the outcome of the aggregation.

Similarly, the sum, minimum, and maximum functions are also insecure. The sum $f(x_1,..., x_n) = x1 + \cdots + x_n$ can be modified at will by maliciously replacing a real measurement x1 with a fake reading x1 . The minimum function $f(x_1, ..., x_n) = \min(x_1, ..., x_n)$ is also insecure, even though replacing a real measurement with a fake value does not always affect the function's outcome. That is, replacing x_1 with $x_1 *$ only raises the minimum if x_1 is the unique smallest sensor reading among all x_i .However; an attacker can modify the computed minimum by choosing x_1 to be very small compared to all correct readings. By symmetry, the maximum function is also insecure, since an attacker can raise the maximum value by hijacking a single sensor reading.

VI. SLEEP DEPRIVATION TORTURE ATTACK

Sleep deprivation torture (also known as denial-of-sleep) attack render a device inoperable by draining the battery more quickly than it would be under normal usage. In a typical mobile computer, the battery is expected to give a certain battery life under a set of usage conditions where the user is actively using the device for a small fraction of the time, and device is idle the rest of the time. When the device is idle, power management software puts the device into low power standby and sleep modes, extending the device's battery life. If an attacker can prevent the device from entering low power modes by keeping it active, the

battery life can be drastically shortened [3].Such an attack is called the sleep deprivation torture attack.

A. Types of denial-of-sleep attack

There three main forms of sleep deprivation attacks on general purpose mobile computers: Service request attacks, benign power attacks, and malignant power attacks. The goal of each type of attack is to maximize the power consumption of the target, thereby decreasing its battery life. The attacks achieve this by keeping the target device busy, and preventing it from going into low power sleep modes. However, the mechanism for each attack is different:

1) Service request power attacks

Attackers repeatedly make valid network service requests, such as telnet, ssh and web server requests, for the purpose of using up the device under attack's (DUA) battery capacity. This type of attack keeps the DUA busy authenticating/servicing the requests.

2) Benign power attacks

The DUA is made to execute a valid but energy-hungry task indefinitely, such as displaying a hidden animated gif or executing a hidden Java script; though invisible to the user, the task secretly drains the energy source. The essential feature of the benign power attack is that the attacker provides data to a valid program that causes the program to execute in such a way that it consumes a pathological amount of power.

3) Malignant power attack

The attacker maliciously penetrates the system and alters operating system kernel or application binary code such that more energy is needed to execute them; the altered binaries may or may not be functionally correct. These attacks will thus be either viruses or Trojan horses.

Using existing techniques, in this case, some of the attacks can be precluded. For example, using virus-scanning software malignant power attack can be prevented. But in other cases, for example, the benign power attacks, detecting the attacks using existing techniques will be difficult. There is a chance that the security techniques could themselves be used to mount a sleep deprivation attack: An attacker could send a virus that he knows will be caught by the target system's virus-scanning software, but the energy consumed by the virus- scanning software may exhaust the battery if the attacker causes it to run repeatedly.

B. Impact of denial-of-sleep attack

A successful attack will maximize power consumption while presenting to the user the appearance that the system is behaving normally, with the possible exception of the battery status indicator. Side effects that one would expect to see of these attacks if they are not implemented subtly include the CPU fan turning on while the user is performing some action that does not normally cause the fan to come on, the system becoming less interactive than usual, and the hard drive spinning up immediately after a spin down. A successful attack will likely cause the user to believe that the battery has become defective and will no longer keep a charge.

A successful attack can use the subsystems which have largest difference between idle or sleep state consumption of power and state of power consumption is activated. To illustrate the potential of these attacks, assume that the device uses power P active while active and power P sleep while sleeping, that PFR = P active /P sleep , and that the device has a usage duty factor of D (fraction of time that the device is active) [5]. Then the battery life, normalized to being asleep 100% of the time (D=0), is equal to $1/(1-D + PFR \times D)$. Since *P*FR is much greater than 1, in order to minimize battery life, one should increase D, increase PFR, or both. Typically D is very small; 0.0035 was the value reported in [5], which is equal to using a device 10 times a day for about 30 seconds each time.

The motive of the intruder is to keep the device as busy as possible, to make D=1. Assuming that in normal usage D is very small, and then the battery life when under attack will be reduced by a factor of approximately PFR. Given the range of values for PFR from above, an attacker could reduce the battery life of currently available sensor by a factor of 30 to 280.

C. Related works on denial-of-sleep attack

1) Brownfield et al. [4] proposed new MAC protocol which overcomes many of the effects of denial of sleep attacks by centralizing cluster management. MAC has several energy saving features which not only extend the network lifetime, but the centralized architecture makes the network lifetime more resistant to denial of sleep attacks. Other than single period and synchronization message, it has two contention period and different networks for sending the message within the clusters and outside the cluster through the gateway node. The MAC protocol Performance Results show that G-MAC performs significantly better than other protocols in every traffic situations. The empty network case shows the protocol overhead and idle listening effects determined by the effective duty cycle-MAC has .95% duty cycle is weighted average of duty cycle of gateway node and other nodes. Attacker can gain access to network through gateway node. But attacker can only affect one node at a time because nodes alternate the gate way responsibilities based upon incremental increase in battery levels.

2) David R. Raymond et al. [5] classifies sensor network denial-of-sleep attacks in terms of an attacker’s knowledge of the medium access control (MAC) layer protocol and ability to bypass authentication and encryption protocols. Attacks from each classification are then modelled to show the impacts on four sensor MAC protocols S-MAC,T-MAC,B-MAC and G-MAC. Implementations of selected attacks on MAC, T-MAC, and B-MAC are described and analysed in detail to validate their effectiveness and analyse their efficiency. And it shows that the most efficient attack on S-MAC can keep a cluster of nodes awake 100% of the time by an attacker that sleeps 99% of the time. Attacks on T-MAC can keep victims awake 00% of the time while the attacker sleeps 92% of the time. With knowledge of protocol because of differences exist in packet structure and timing between WSN MAC protocols, and even without

ability to penetrate encryption; all wireless sensor network MAC protocols are susceptible to a full domination attack, which reduces the network lifetime to the minimum possible by maximizing the power consumption of the nodes' radio subsystem. Even without the ability to penetrate encryption, subtle attacks can be launched, which reduce the network lifetime by orders of magnitude. If sensor networks are to meet current expectations, they must be robust in the face of network attacks to include denial-of-sleep. This approach also increases the network overhead.

3) Chen C. et al. [7] describe a scheme is proposed employing fake schedule switch with RSSI measurement aid. Here we focus on previous attack and introduce fake schedule. The sensor nodes can reduce and weaken the harm from exhaustion attack and on the contrary make the attackers lose their energy quickly so as to die. Simulation results show that at a bit price of energy and delay, network health can be guaranteed and packets drop ratio has been decreased compare with original scenario without our scheme. Here in this paper we consider only S-MAC protocol with duty cycle 10%. If packet loss is not caused by the attack, then fake schedule switch is harmful. Due to which RSSI is used as a value assigned to each node and node having attacker one hop away has larger RSSI value.

4) Tapalina Bhattasali et al. [9] proposed a hierarchical framework which is based upon distributed collaborative mechanism for detecting sleep deprivation torture in wireless sensor network efficiently. n heterogeneous sensor field, sensor nodes are categorized into various roles such as sink gateway (SG), sector monitor(SM), Sector-in – charge (SIC) and leaf node (LN) depending on their battery capacity. To sense the data leaf node is used here, SIC is used to collect the data and SM detects whether the data is valid data or invalid data. Other networks are accessed using Sink Gateway. Here if leaf nodes are directly affected by intruder, node cannot detect it. As a result battery of affected node may be low or exhausted completely. This can affect data transmission for network due to which it is done in authenticated way.

5) Fang-Jing wu et al. [1] stated a scheme known as distributed wake-up scheduling scheme for data collection in a sensor networks that achieves both energy conservation and low reporting latency, i.e. in a multihop wireless network, a simple and efficient way of defining interference neighbours is to prohibit a node from using the same slot0code as those of its 1-hop and 2-hop neighbours. Power saving and latency are improved to prolong network lifetime and freshness of data. Herein this scenario, since not all nodes are involved in the communication and communication directions are always toward the sink, a node only need to consider a tighter set of interference neighbours and other drawback is that this scheme cannot handle the multiple tasks at a same time.

VII. CONCLUSION

This paper provides a brief study of WSN and the various types of security threats in WSN. The focus has been laid on a type of denial-of-service attack called denial-of-sleep attack. This attack is a clever attack that keeps the sensor nodes radio ON that drain the battery in only few days.

REFERENCES

[1] Jianliang Zheng and Myung J. Lee,"A Comprehensive Performance Study of IEEE 802.15.4",IEEE, Aug. 1999.

[2] Wireless Sensor Network(2005): A Networking Perspective by Jun Zheng and Abbas Jamalipour, Kenneth Moore,Director of IEEE Book and Information Services (BIS)Jeanne Audino, Project Editor.

[3] Manju.V.C (2005): "Analysis of Denial of Sleep Attack in WSN", International conference on Recent Development in Engineering and technology.., pp. 224-229.

[4] Michael Brownfield, Yatharth Gupta, Mem and Nathaniel Davis IV (2005):" Wireless Sensor Network Denial of sleep attack" published by IEEE 2005

[5] Raymond D. R., Midkiff S. F (2007), "Clustered Adaptive Rate Limiting: Defeating Denial-Of-Sleep Attacks In Wireless Sensor Networks", Military Communications Conference, 2007, MILCOM 2007, IEEE, pp. 1-7.

[6] David R. Raymond, Randy C. Marchany, Michael I. Brownfield, and Scott F. Midkiff, (2008): "Effect of Denial of sleep attacks on wireless sensor network MAC protocols" published by IEEE.

[7] Chen C., Hui L., Pei Q., Ning L., Qingquan P. (2009) , "An Effective Scheme for Defending Denial-of-Sleep Attack in Wireless Sensor Networks", Proceedings of the 2009 Fifth International Conference on Information Assurance and Security, Vol. 02, IEEE CS, Washington DC, USA.

[8] Waltenegus Dargie and Christian Poellabauer," FUNDAMENTALS OF WIRELESS SENSOR NETWORKS", John Wiley & Sons, Ltd, pp.25-30, 2010.

[9] Tapalina Bhattasali, Rituparna Chaki, Sugata sanyal (2012): "Sleep deprivation Attack Detection in WirelessSensor network", International Journal of Computer Applications, February 2012.