Wireless Sensor Networks: An Overview on its Security Threats

Kalpana Sharma
CSE Department,
SMIT, Sikkim, India

M K Ghose
CSE Department,
SMIT, Sikkim, India

ABSTRACT

Wireless sensor networks have become a growing area of research and development due to the tremendous number of applications that can greatly benefit from such systems and has lead to the development of tiny, cheap, disposable and self contained battery powered computers, known as sensor nodes or "motes", which can accept input from an attached sensor, process this input data and transmit the results wirelessly to the transit network. Despite making such sensor networks possible, the very wireless nature of the sensors presents a number of security threats when deployed for certain applications like military ,surveillances etc . The problem of security is due to the wireless nature of the sensor networks and constrained nature of resources on the wireless sensor nodes, which means that security architectures used for traditional wireless networks are not viable. Furthermore, wireless sensor networks have an additional vulnerability because nodes are often placed in a hostile or dangerous environment where they are not physically protected. In this paper we discuss some security threats and challenges faced by WSNs.

Keywords

Security, Wireless Sensor Networks (WSN), threats, Denial of Service (DoS)

1. INTRODUCTION

Sensor networks [5][6][7][9] are highly distributed networks of small, lightweight wireless nodes, deployed in large numbers to monitor the environment or system by the measurement of physical parameters such as temperature, pressure, or relative humidity. Building sensors have been made possible by the recent advances in micro-electromechanical systems (MEMS) technology. The sensor nodes are similar to that of a computer with a processing unit, limited computational power, limited memory, sensors, a communication device and a power source in form of a battery. In a typical application, a WSN is scattered in a region where it is meant to collect data through its sensor nodes. The applications of sensor networks are endless, limited only by the human imagination [5] [6] [7]. In this paper an overview on various WSN attacks are mentioned with a special mention on Denial of Service (DoS). Summery on the counterattacks and possible preventive measures are mentioned. It is to be mentioned that all the attacks are mentioned thoroughly as well as the preventive measures mentioned in this paper is also not exhaustive. The rest of the paper is as follows: Section 2 gives an overview on the applications of WSN followed by section 3 in which various types of attacks on WSN are highlighted. In section 4 countermeasures of the WSN security threats are discussed by the conclusion in section 5.

2. APPLICATIONS OF WSN

Wireless Sensor Networks (WSN) has off late, found applications in wide-ranging areas. In this section we list some of the prominent areas of applications of WSN. The list would be very lengthy if we exhaust all the areas of WSN applications. Therefore, in this paper only handful applications are provided.

2.1 The military applications of sensor nodes include battlefield surveillance and monitoring, guiding systems of intelligent missiles and detection of attack by weapons of mass destruction.

2.2 The Medical Application: Sensors can be extremely useful in patient diagnosis and monitoring [9]. Patients can wear small sensor devices that monitor their physiological data such as heart rate or blood pressure.

2.3 Environmental monitoring: It includes traffic, habitat, Wild fire etc.

2.4 Industrial Applications: It includes industrial sensing and diagnostics. For example appliances, factory, supply chains etc.

2.5 Infrastructure Protection Application: It includes power grids monitoring, water distribution monitoring etc.

2.6 Miscellaneous Applications: Sensors will soon find their way into a host of commercial applications at home and in industries. Smart sensor nodes can be built into appliances at home, such as ovens, refrigerators, and vacuum cleaners, which enable them to interact with each other and be remote-controlled.

3. TYPES OF ATTACKS ON WSN

Why is security necessary in WSN? The reasons are many. First of all Wireless networks are vulnerable to security attacks due to the broadcast nature of the transmission medium. Furthermore, wireless sensor networks have an additional vulnerability because nodes are often placed in a hostile or dangerous environment where they are not physically safe.

Attacks on WSNs can be classified from two different levels of views:-

1. Attack against security mechanisms.

2. Attack against basic mechanisms (like routing mechanisms).

In many applications, the data obtained by the sensing nodes needs to be kept confidential and it has to be authentic [10]. In the absence of security a false or malicious node could intercept private information, or could send false messages to nodes in the network. The major attacks are: Denial of Service (DOS), Worm hole attack, Sinkhole attack, Sybil attack, Selective Forwarding attack, Passive information gathering, Node capturing, False or malicious node, Hello flood attack etc. In this section a brief overview on these attacks are presented.

3.1 Denial of Service (DoS)

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[1][2].

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 [2].

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.

3.2 The Wormhole attack

One node in the network (sender) sends a message to the another node in the network (receiver node)[10].Then the receiving node attempts to send the message to its neighbors. The neighboring nodes think the message was sent from the sender node(which is usually out of range), so they attempt to send the message to the originating node, but it never arrives since it is too far away.

Wormhole attack is a significant threat to wireless sensor networks, because, this sort of attack does not require compromising a sensor in the network rather, it could be performed even at the initial phase when the sensors start to discover neighboring information [12].

Wormhole attacks are difficult to counter because routing information supplied by a node is difficult to verify.

3.3 The Sybil attack

In this attack, a single node i.e. a malicious node will appear to be a set of nodes and will send incorrect information to a node in the network.

The incorrect information can be a variety of things [10], including position of nodes, signal strengths, making up nodes that do not exist.

Authentication and encryption techniques can prevent an outsider to launch a Sybil attack on the sensor network. However, an insider cannot be prevented from participating in the network, but he should only be able to do so using the identities of the nodes he has compromised.

Public key cryptography can prevent such an insider attack, but it is too expensive to be used in the resource constrained sensor networks.

3.4 Selective Forwarding attack

It is a situation when certain nodes do not forward many of the messages they receive. The sensor networks depend on repeated forwarding by broadcast for messages to propagate throughout the network.

3.5 Sinkhole attacks

In a sinkhole attack, the adversary's aim is to lure nearly all the traffic from a particular area through a compromised node, creating a metaphorical sinkhole with the adversary at the center [4]. Sinkhole attacks typically work by making a compromised node look especially attractive to surrounding nodes with respect to the routing algorithm.

Sinkhole attacks are difficult to counter because routing information supplied by a node is difficult to verify.

As an example, a laptop-class adversary has a strong power radio transmitter that allows it to provide a high-quality route by transmitting with enough power to reach a wide area of the network [4].

3.6 Passive Information Gathering

An intruder with an appropriately powerful receiver and well designed antenna can easily pick off the data stream.

Interception of the messages containing the physical locations of sensor nodes allows an attacker to locate the nodes and destroy them [7] [8]. Besides the locations of sensor nodes, an adversary can observe the application specific content of messages including message IDs, timestamps and other fields.

3.7 Node Capturing

A particular sensor might be captured, and information stored on it might be obtained by an adversary [7][8].

3.8 False or Malicious Node

Most of the attacks against security in wireless sensor networks are caused by the insertion of false information by the compromised nodes within the network [8].

3.9 Hello flood attacks

The Hello flood attacks can be caused by a node which broadcasts a Hello packet with very high power, so that a large number of nodes even far away in the network choose it as the parent [10]. All messages now need to be routed multi-hop to this parent, which increases delay.

4. DEFENSE MECHANISMS

This section highlights the preventive measures of all the attacks mentioned through 3.1 to 3.9.It is to be noted that the list would be very vast if we try to exhaustively list all the preventive measures. So the list is restricted to only a handful of the solutions.

4.1 DOS prevention

The mechanisms to prevent DoS attacks include payment for network resources, pushback, strong authentication and identification of traffic [1] [2]. One security technique uses authentication streams to secure the reprogramming process. This divides a program binary into a series of messages, each of which contains a hash of the next message. This mechanism ensures that an intruder can't hijack an ongoing program transmission, even if he or she knows the hashing mechanism. This is because it would be almost impossible to construct a message that matches the hash contained in the previous message. A digitally signed advertisement, which contains the program name, version number, and hash of the first message, ensures that the process is securely initiated [2].

We can defeat many threats using existing encryption and authentication mechanisms, and other techniques (such as identifying jamming attacks) can alert network administrators of ongoing attacks or trigger techniques to conserve energy on affected devices [14].Summary of DoS attack is given in table 1.

Table 1: Sensor Network layers and Denial-of- Service defenses [1]

Network Layers	**Attacks**	**Defenses**
PHYSICAL	1.Jamming	Spread spectrum, priority messages, region mapping
	2.Tampering	Tamper proofing, Hiding
LINK	1.Collision	Error-correcting code
	2.Exhaustion	Rate limitation
	3.Unfairness	Small frames
NETWORK and ROUTING	1.Neglect and Greed	Redundancy, Probing
	2.Homing	Encryption
	3.Misdirection	Authorization, Monitoring
	4.Black holes	Authorization, Monitoring
TRANSPORT	1.Flooding	Client puzzles
	2.Desynchronization	Authentication

4.2 Wormhole attack prevention

The mechanism to combat the wormhole attack include, DAWWSEN [13] , 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. 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.

4.3 Sybil prevention

The mechanisms to prevent against Sybil attacks are to utilize identity certificates [11]. The basic idea is very simple. The setup server, before deployment, assigns each sensor node some unique information. The server then creates an identity certificate binding this node's identity to the assigned unique information, and downloads this information into the node. To securely demonstrate its identity, a node first presents its identity certificate, and then proves that it possesses or matches the associated unique information. This process requires the exchange of several messages. Merkle hash tree can be used as basic means of computing identity certificates [11]. The Merkle hash tree is a vertex-labeled binary tree, where the label of each non-leaf vertex is a hash of the concatenation of the labels of its two child vertexes. The primary path of a leaf vertex is the set of vertexes on the path from the leaf to the root of the tree. The authentication path consists of the siblings of the vertexes on this primary path. Given a vertex, its authentication path, and the hash function, the primary path can then be computed, up to and including the root of the tree. This computed value of the root can then be compared with a stored value, to verify the authenticity of the label of the leaf vertex.

4.4 Passive information gathering prevention

To minimize the threats of passive information gathering, strong encryption techniques need to be used.

4.5 Node capture prevention

If a node has been compromised then how to exclude that node and that node only, from the sensor network is at issue. This issue is solved by Localized Encryption and Authentication protocol (LEAP). LEAP (localized encryption and authentication protocol) is an efficient protocol for inter-node traffic authentication. This protocol relies on a key sharing approach that authorizes in-network processing, and at the same time mitigates a number of possible attacks.

4.6 False or Malicious Node prevention

This attack basically should be checked in the Routing layer itself. Details pertaining to the preventive measures for 'false node' attack are out of the scope of this paper.

4.7 Hello flood attacks prevention

This can be avoided by checking the bidirectional of a link, so that the nodes ensure that they can reach their parent within one hop. The table no.2 contains the summary of the various attacks of WSN and also in short summarizes the defense mechanism.

Table 2: WSNs threats in layers & defense mechanisms

Attacks	**Layers involved**	**Defenses**
Denial of Service	Physical, Link, Network, Transport layers	Priority messages, hiding, monitoring, authorization,redundancy, encryption[14]
Wormhole attack	Link layer, Network layer	Dawwsen proactive routing rotocol[13]suspicious node detection by signal strength,[10]
Sybil attack	Network layer, Application layer	Identity certificates[11]
Hello flood attack	Network layer	Suspicious node detection by signal strength[10]
Sink hole attack	Link layer, Network layer	Detection on MintRoute[4]

4.8 Selective Forwarding attack prevention

Multipath routing can be used to counter these types of selective forwarding attacks. Messages routed over paths whose nodes are completely disjoint are completely protected against selective forwarding attacks involving at most compromised 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 [16].

4.9 Sinkhole attacks prevention

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 [15].

5. CONCLUSION

All of the previously mentioned security threats, the Hello flood attack, wormhole attack, Sybil attack, sinkhole attack, serve one common purpose that is to compromise the integrity of the network they attack. Also In the past, focus has not been on the security of WSNs, but with the various threats arising and the importance of data confidentiality, security has become a major issue. Although some solutions have already been proposed, there is no single solution to protect against every threat. In our paper we mainly focus on the security threats in WSN. We've presented the summery of the WSNs threats affecting different layers along with their defense mechanism. We conclude that the defense mechanism presented just gives guidelines about the WSN security threats; the exact solution depends on the type of application the WSN is deployed for. There're many security mechanisms which are used in 'layer-by-layer' basis as a security tool. Recently researchers are going for integrated system for security mechanism instead of concentrating on different layers independently. Through this paper we've tried to present the most common security threats in various layers and their most probable solution.

6. REFERENCES

[1] A.D. Wood and J.A. Stankovic, (2002) "Denial of Service in Sensor Networks," Computer, vol. 35, no. 10, 2002, pp. 54–62.

[2] David R. Raymond and Scott F. Midkiff,(2008) "Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses," IEEE Pervasive Computing, vol. 7, no. 1, 2008, pp. 74-81.

[3] Chris Karlof, Naveen Sastry, David Wagner, (2004)Tiny Sec:a link layer security architecture for wireless sensor networks, Proceedings of the 2nd international conference on Embedded networked sensor systems , Nov 03-05,2004,Baltimore,MD,USA.

[4] E. C. H. Ngai, J. Liu, and M. R. Lyu, (2006)"On the intruder detection for sinkhole attack in wireless sensor networks," in Proceedings of the IEEE International Conference on Communications (ICC '06), Istanbul,Turkey..

[5] Jamal N. Al-Karaki & Ahmed E. Kamal, (2004) "Routing Techniques in Sensor Networks: A survey", IEEE communications, Volume 11, No. 6, Dec. 2004, pp. 6-28.

[6] M. Tubaishat, S. Madria, (2003) "Sensor Networks : An Overview ", IEEE Potentials, April/May 2003

[7] Al-Sakib khan Pathan et.al,(2006) "Security in wireless sensor networks: Issues and challenges" in feb.20-22,2006,ICACT2006,ISBN 89-5519-129-4 pp(1043-1048)

[8] C. Karlof and D. Wagner, (2003). "Secure routing in wireless sensor networks:Attacks and countermeasures," AdHoc Networks Journal, vol. 1, no. 2–3,pp. 293–315, September

[9] Feng Zhao,Leonidas Guibas,,"Wireless Sensor Networks", Morgan Kaufmann Publications.

[10] Adrian Perrig, John Stankovic, and David Wagner, (2004) "Security in wireless sensor networks", Commun.ACM,47(6):53-57.

[11] J. R. Douceur,(2002) "The Sybil Attack," in 1st International Workshop on Peer-to-Peer Systems (IPTPS '02).

[12] Zaw Tun and Aung Htein Maw,(2008)," Worm hole Attack Detection in Wireless Sensor networks", proceedings of world Academy of Science, Engineering and Technology Volume 36, December 2008, ISSN 2070-3740.

[13] Rouba El Kaissi, Ayman Kayssi, Ali Chehab and Zaher Dawy, (2005)" DAWWSEN: A Defense Mechanism against Wormhole ttack In Wireless Sensor Network",Proceedings of the Second International Conference on Innovations in Information Technology (IIT'05).

[14] A. D. Wood and J. A. Stankovic,(2002) "Denial of service in sensor networks",Computer, 35(10):54–62, 2002.

[15] M. Zorzi and R. R. Rao, (2003) "Geographic Random Forwarding (GeRaF) for Ad Hoc and Sensor Networks: Multihop Performance," IEEE Transactions on Mobile Computing, vol. 2, no. 4, pp. 337-348, 2003.

[16] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, "Highly-resilient, energy-efficient multipath routing in wireless sensor networks,"Mobil Computing and Communications Review, vol. 4, no. 5, October 2001.