IJCSMS International Journal of Computer Science and Management Studies, Vol. 12, Issue 03, Sept 2012
ISSN (Online): 2231-5268
www.ijcsms.com

Attacks on Wireless Sensor Network: A Survey

Dr. Yudhvir Singh[1], Dheer Dhwaj Barak[2], Vikas Siwach[3], Prabha Rani[4]

[1]Associare Professor, Department of CSE, U.I.E.T, M.D.U. Rohtak -124001 (INDIA)
dr.yudhvirs@gmail.com

[2]Assistant Professor, Department of CSE, HIT Asodha M.D.U. Rohtak -124001 (INDIA)
barakdheer410@gmail.com

[3]Assistant Professor, Department of CSE, U.I.E.T, M.D.U. Rohtak -124001 (INDIA)
singhvikash94@yahoo.com

[4]Department of CSE, U.I.E.T, M.D.U. Rohtak -124001 (INDIA)

Abstract

Security is a crucial service in wireless sensor networks that is becoming increasingly common in WSNs because wireless sensor nodes are typically deployed in an unattended environment, leaving them open to possible hostile network attack. Because wireless sensor nodes are limited in computing power, data storage and communication capabilities, any user authentication protocol must be designed to operate efficiently in a resource constrained environment. With a widespread growth in the potential applications of WSN, the need for reliable security mechanisms for them has increased manifold. Security protocols in WSNs, unlike the traditional mechanisms, need special efforts and issues to be addressed. The set of challenges in sensor networks are diverse, we focus on attacks on Wireless Sensor Network in this paper.

Keywords: *Wireless Sensor Network, WSN, Security, Attacks.*

1. Introduction

Wireless Sensor Networks (WSN) consist of small Devices—called sensor nodes—with RF radio, processor, memory, battery and sensor hardware. We use the term sensor network to refer to a heterogeneous system combining tiny sensors and actuators with general purpose computing elements. One can precisely monitor the environment with widespread deployment of these devices. Sensor nodes are resource-constrained in terms of the RF radio range, processor speed, memory size and power. Apart from this, sensor nodes are generally stationary. The traffic rate is very low and traffic is periodic as well. There may be long idle periods during which sensor nodes turn off their radio to save energy consumed by idle listening. Recharging or replacing batteries is expensive and may not even be feasible in some situations. Therefore, WSN applications need to be extremely energy-aware. WSNs are mostly unguarded. Hence capturing a node physically, altering its code and getting private information like cryptographic keys is easily possible for an attacker. Wireless medium is inherently broadcast in nature. This makes them vulnerable to attacks. These attacks can disrupt the operation of WSN and can even defeat the purpose of their deployment. An adversary can launch DoS attacks without much effort (e.g. even without cracking keys used for cryptography-based solutions). The Application domain of Wireless Sensor Network is diverse due to the availability of micro-sensors and low-power wireless communications. Unlike the traditional sensors, in the remote sensor network, a vast numbers of sensors are densely deployed. These sensor nodes will perform significant signal processing, computation, and network self-configuration to achieve scalable, robust and long-lived networks [3]. WSN's unique features, sensor networks are used in wide range of applications in areas like health, military, home and commercial industries in our day to day life [4] [5] [6].

In the near future, this wide range of application areas will make sensor networks an integral part of life [7]. WSN technology enables monitoring of vast and remote geographical region, in such a way that abnormal events can be quickly detected. The cost of sensor nodes varies from hundreds of dollars to a few cents, depending upon their size and complexity. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and transmission range [8].

2. Security Issues in WSN’s

Typical WSN has the various network components as *Sensor motes (Field devices)* – Field devices are mounted in the process and must be capable of routing packets on behalf of other devices. In most cases they characterize or control the process or process equipment. A router is a special type of field device that does not have process sensor or control equipment and as such does not interface with the process itself. *Gateway or Access points* – A Gateway enables communication between Host application and field devices. *Network manager* – A Network Manager is responsible for configuration of the network, scheduling communication between devices (i.e., configuring super frames), management of the routing tables and monitoring and reporting the health of the network. *Security manager* – The Security Manager is responsible for the generation, storage, and management of keys [1]. The security goals are classified as primary and secondary [2][9]. The primary goals are known as standard security goals such as Confidentiality, Integrity, Authentication and Availability. The secondary goals are Data Freshness, Self- Organization, Time Synchronization and Secure Localization. However, the security mechanisms devised for wireless ad hoc networks could not be applied directly for wireless sensor networks because of the architectural disparity of the two networks. While ad hoc networks are self-organizing, dynamic topology, peer to peer networks formed by a collection of mobile nodes and the centralized entity is absent [10]; the wireless sensor networks could have a command node or a base station (centralized entity, sometimes termed as sink). The architectural aspect of wireless sensor network could make the employment of a security schemes little bit easier as the base stations or the centralized entities could be used extensively in this case. Nevertheless, the major challenge is induced by the constraint of resources of the tiny sensors. In many cases, sensors are expected to be deployed arbitrarily in the enemy territory (especially in military reconnaissance scenario) or over dangerous or hazardous areas. Therefore, even if the base station (sink) resides in the friendly or safe area, the sensor nodes need to be protected from being compromised.

3. Attacks in WSNs

WSN pose unique challenges and because of this traditional security threats that the other entire wireless network face cannot assume for WSN. In a large-scale sensor network individual sensors are subject to security compromise. Where the nature of communication is broadcast and hence an attacker can overhear messages posted by any sensor node, security is an important issue here. Wireless Sensor Networks (WSNs) are comprised of many small and resource constrained sensor nodes that are deployed in an environment to gather sensed data and forward that data to interested legal users. Attacks against wireless sensor networks could be broadly considered from two different levels of views. One is the attack against the *Security Mechanisms* and another is against the *Routing Mechanisms*.

The major attacks in wireless sensor networks are as follows:

- *Denial of Service (DoS)*
- *Selective forwarding attack*
- *Sinkhole attack*
- *Sybil attack*
- *Wormholes attack*
- *HELLO flood attack*
- *Acknowledgement spoofing and sniffing*
- *Energy drain attack*
-

Denial of Service Attack

Denial of service attack may also occur at physical layer by jamming (by broadcasting mechanism) and/or tampering (modification or fabrication) of the packet. In Link Layer it is by producing collision data, exhaustion of resources and unfairness in use of networks. In network layer, it occurs by way of neglecting and the greediness of packets resulting into path failure. In transport layer, DOS attack occurs due to flooding and de-synchronization. DoS is produced by the unintentional failure of nodes or malicious action. DoS attack is meant not only for the adversary’s attempt to subvert, disrupt, or destroy a network, but also for any event that diminishes a network’s capability to provide a service. In wireless sensor networks, several types of DoS attacks in different layers might be performed. At physical layer the DoS attacks could be jamming and tampering, at link layer, collision, exhaustion and unfairness, at network layer, neglect and greed, homing, misdirection, black holes and at transport layer this attack could be performed by malicious flooding and de-synchronization. The mechanisms to prevent DoS attacks include payment for network resources, pushback, strong authentication and identification of traffic.[11]. An attacker can damage and replace a node, for example, by stealing or replacing information or cryptographic keys. At the link layer the attacker can generate collisions and exhaustion may be caused from protocols that attempt retransmission repeatedly, even when triggered by an unusual and suspicious collision. Additionally unfairness threats may occur when the attacker seeks to abuse a cooperative MAC-layer priority scheme. This threat may not result a total DoS, but it could downgrade the service which others experience.

Selective Forwarding Attack

WSNs are usually multi-hop networks and hence based on the assumption that the participating nodes will forward the messages faithfully. Malicious or attacking nodes can however may refuse to forward certain messages and simply drop them, ensuring that they are not propagated any further. If they drop all the packets through them, then it is called a Black Hole Attack. However if they selectively forward the packets, then it is called selective forwarding. These attacks are typically most effective when the attacker is explicitly included on the path of a data flow. However, an attacker may also be able to jam the network by simply causing collisions of packets of interest. To include himself on the path of the data flow, the adversary can use two major strategies which correspond to the Sink Hole Attacks and the Sybil Attacks.

Eavesdropping Attack

It aims to obtain some confidential information that should be kept secret during the communication. The information may include the location, public key, private key or even passwords of the nodes.

Sybil Attack

In Sybil attack [13], the attacker/malicious node show multiple identities. Since each actual node in a sensor network has a single identity, hence numerous threats can be observed. For example, in case of multi-hop transmission, the malicious node may get an identity which is the same as that of the next-hop of a neighboring node, hence getting access to all of its data. Serious threats are also possible in case of the multi-path routing. Since adversary has multiple identities, the innocent nodes may be routing multi-path data through the same malicious node.

Sinkhole (Black hole) Attack

In this type of attack, attacker places himself in a network with high capability resources (high processing power and high band width) by which it always creates shortest path. As a result, all data passes through attacker‟s node (compromise node). A compromised node which is placed at the centre of some area creates a large "Sphere of influence", attracting all traffic destined for a base station from the sensor nodes. Some routing protocols try to verify the bidirectional reliability of a route with end to end acknowledgements which contain information regarding the reliability or latency information. When we consider the laptop-class adversaries with a powerful transmitter which can actually provide a high quality link between a node and the base station, then the adversary can easily dupe the other nodes. The adversary creates a large sphere of influence, which will attract all traffic destined for the base station from nodes which may be several hops away from the compromised node. The attacker targets a place to create sinkhole where it can attract the most traffic, possibly closer to the base station so that the malicious node could be perceived as a base station. The main reason for the sensor networks susceptible to sinkhole attacks is due to their specialized communication pattern. It may be extremely difficult for an adversary to launch such an attack in a network where every pair of neighboring nodes uses a unique key to initialize frequency hopping or spread spectrum communication.

Wormhole Attack

The attacker connects two different parts of the ad hoc network using an extra communication channel as a tunnel. As a result two distant nodes assume they are neighbors and send data using the tunnel. The attacker has the possibility of conducting a traffic analysis or selective forwarding attack. In the wormhole attack [12], an adversary tunnels messages received in one part of the network over a low-latency link and replays them in a different part. Specifically, packets transmitted through the wormhole should have lower latency than those packets sent between the same pair of nodes over normal multihop routing. The simplest instance of this attack is a single node situated between two other nodes forwarding messages between the two of them. An adversary situated close to a base station may be able to completely disrupt routing by creating a well-placed wormhole. An adversary could convince nodes who would normally be multiple hops from a base station that they are only one or two hops away via the wormhole. This can create a sinkhole: since the adversary on the other side of the wormhole can artificially provide a high quality route to the base station, potentially all traffic in the surrounding area will be drawn through her if alternate routes are significantly less attractive. This will most likely always be the case when the endpoint of the wormhole is relatively far from a base station. Wormholes can be used to exploit routing race conditions. A routing race condition typically arises when a node takes some action based on the first instance of a message it receives and subsequently ignores later instances of that message. In this case, an adversary may be able to exert some influence on the resulting topology if it can cause a nodes to receive certain routing information before it would normally reach them though multihop routing. Wormholes are a way to do this, and are effective even if routing information is authenticated or encrypted. Wormholes can also be used simply to convince two distant nodes that they are neighbors by relaying packets between the two of them. Wormhole attacks would likely be used in combination with selective forwarding or eavesdropping.

HELLO Flood Attack

Many protocols require nodes to broadcast HELLO packets for neighbor discovery, and a node receiving such a packet may assume that it is within (normal) radio range of the sender. So an attacker with greater range of transmission may send many neighbors. Hello messages to a large number of nodes in a big area of the network. These nodes are then convinced that the attacker is their neighbor, so that all the nodes will respond to the HELLO message and waste their energy. Consequently the network is left in a state of confusion. The result of a HELLO flood that every node thinks the attacker is within one-hop radio communication range. If the attacker subsequently advertises low-cost routes, nodes will attempt to forward their messages to the attacker. Protocols which depend on localized information exchange between neighboring nodes for topology maintenance or flow control are also subject to this attack. HELLO floods can also be thought of as one-way, broadcast wormholes.

Acknowledgement Spoofing/Sniffing Attack

The inherent broadcast medium, an adversary can spoof link layer acknowledgments for “overheard” packets addressed to neighboring nodes. Protocols that choose the next hop based on reliability issues are susceptible to acknowledgments spoofing. These results in packets being lost when travelling along such links, the goal includes convincing the sender that a weak link is strong or that a dead or disabled node is alive. Since packets sent along weak or dead links are lost, an adversary can effectively mount a selective forwarding attack using acknowledgement spoofing by encouraging the target node to transmit packets on those links.

Energy Drain Attack

WSN is battery powered and dynamically organized. It is difficult or impossible to replace/recharge sensor node batteries. Because there is a limited amount of energy available, attackers may use compromised nodes to inject fabricated reports into the network or generate large amount of traffic in the network. Fabricated reports will cause false alarms that waste real world response efforts, and drain the finite amount of energy in a battery powered network. However the attack is possible only if the intruder’s node has enough energy to transmit packets at a constant rate. The aim of this attack is to destroy the sensor nodes in the network, degrade performance of the network and ultimately split the network grid and consequently take control of part of the sensor network by inserting a new Sink node.

4. DEFENSE TECHNIQUES IN WSNs

Table 1 shows the summary of various attacks in wireless sensor networks and defense techniques these attacks.

Table 1: Attacks on WSNs & Defense Techniques

Treat	Layer	Defense Technique
Jamming	Physical	Spread Spectrum
Tempering		Temper Proofing
Exhausting	Link	Rate Limitation
Collision		ErrorCorrecting Code
Route Inform Manipulating	Network	Authenticatin, Encryption
Selective Forwarding		Redundancy, Probing
Sybil Attack		Authenticatin
Sinkhole		Monitoring, Redundancy
Wormhole		Flexible Routing
Hello flood		Two Way Authenticatio
Flooding	Transport	Limiting connection numbers
Clone attack	Application	Unique pair wise Keys

5. Conclusions

This paper outlined different security issues and attacks in wireless sensor network in general and made an extensive study of different attacks associated with WSNs. As these protocols are not designed taking security issues into account, most of them are prone to different types of attacks. 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. These attacks are described in this paper.

ACKNOWLEDGEMENT

Grant received from University Grant Commission, New Delhi to Dr. Yudhvir Singh (PI) under Major Research Project is duly acknowledged.

References

[1] Hemanta Kumar Kalita1, and Avijit Kar, WIRELESS SENSOR NETWORK SECURITY ANALYSIS, International Journal of Next-Generation Networks (IJNGN),Vol.1, No.1, December 2009

[2] Prabhudutta Mohanty1, Sangram panigrahii2, Nityananda Sarma3 and Siddhartha Sankar Satapathy4 SECURITY ISSUES IN WIRELESS SENSOR NETWORK DATA GATHERING PROTOCOLS: A SURVEY, Journal of Theoretical and Applied Information Technology © 2005 – 2010, JATIT.

[3] Y. Zou, K. Chakrabarty, "Sensor deployment and target localization based on virtual forces", INFOCOM 2003. Twenty- Second Annual Joint Conferences of the IEEE Computer and Communications Societies. IEEE, Volume: 2, Pages: 1293 - 1303, April 2003.

[4] Lin, R., Wang, Z. & Sun, Y., (2004) “Wireless Sensor Networks Solutions for Real Time Monitoring of Nuclear Power Plant in”, *The Proceedings of the 5’ World Congress on intelligent Control and Automation*, Hangzhou, P.R. China.

[5] Römer, K., Mattern, F. & Zurich, E., (2004) “The Design Space of Wireless Sensor Networks”, *IEEE Wireless Communications*.

[6] Yoneki, E. & Bacon, J., (2005) “A survey of Wireless Sensor Network technologies: research trends and middleware’s role”, technical report. *Http://www.cl.cam.ac.uk/techreports,* ISSN 1476-2986.

[7] . J. Kahn, R. Katz, and K. Pister, “Next century challenges: Mobile networking for smart dust”, In 5th ACM/IEEE Annual International Conference on Mobile Computing (MOBICOM1999), pages 271-278, 1999.

[8] Luis E. Palafox, J. Antonio Garcia-Macias,(2008) Security in Wireless Sensor Networks, IGI Global, Chapter 34.

[9] John Paul Walters, Zhengqiang Liang, Weisong Shi, Vipin Chaudhary, “Wireless Sensor Network Security: A Survey”, Security in Distributed, Grid and Pervasive Computing Yang Xiao (Eds), Page3-5, 10-15, year 2006

[10] Pathan, A-S. K., Alam, M., Monowar, M., and Rabbi, F., “An Efficient Routing Protocol for

Mobile Ad Hoc Networks with Neighbor Awareness and Multicasting", Proc. IEEE E-Tech, Karachi, 31 July, 2004, pp. 97-100.

[11] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong, "Security in Wireless Sensor Networks: Issues and Challenges**",** International conference on Advanced Computing Technologies**,** Page1043-1045, year 2006

[12] Y.-C. Hu, A. Perrig, D.B. Johnson, Packet leashes: a defense against wormhole attacks in wireless networks, in: IEEE Infocom, 2003.

[13] D.Dallas,C.Leckie, and K. Ramamohanarao, "Hop-count monitoring:Detecting sinkhole attacks in wireless sensor networks," inicon '07:Proceedings of the 15th IEEE International Conference on Network Adelaide, SA, 2007, pp. 176–181.