ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 7, July 2013

SECURITY VULNERABILITY ISSUES IN WIRELESS SENSOR NETWORKS: A SHORT SURVEY

C K Marigowda[1], Manjunath Shingadi[2]

Associate Professor, Department of Information Science & Eng, Acharya Institute of Technology, Bangalore, India[1]

PG Student, Department of Information Science & Engineering, Acharya Institute of Technology, Bangalore, India[2]

Abstract: Wireless Sensor Networks are special kind of Ad-hoc networks, used in various applications like military and healthcare areas and characterized by severely constrained computational, memory and energy resources. When wireless sensor networks are deployed in an open or hostile environment security becomes extremely important, as they are prone to different types of malicious attacks. This paper includes the outline of the energy constraints, security requirements, and some of the security mechanisms to counter these attacks.

Keywords: wireless sensor networks, attacks, security Mechanisms, security, constraints

I. INTRODUCTION

Wireless Sensor Networks are special kind of Ad-hoc networks, consists of thousands of small devices each with sensing, processing, and communication capabilities to monitor the real-world environment and are used in a variety of applications such as military sensing and tracking, environmental monitoring, disaster management, etc.

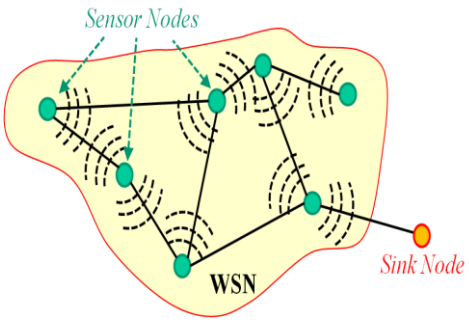

Figure 1.1 Scenario of Wireless sensor node deployment and data collection.

In these networks, a large number of sensor nodes are deployed to monitor a vast field, where the operational conditions are most often harsh or even hostile [7]. However, the nodes in WSNs have severe resource constraints due to their lack of processing power, limited memory and energy. Since these networks are usually deployed in remote places and left unattended, they should be equipped with security mechanisms to defend against attacks such as node capture, physical tampering, eavesdropping, denial of service, etc [7].

II. CONSTRAINTS IN WSNs

Sensor nodes in the WSNs are inherently resource constrained. These nodes have limited processing capability, very low storage capacity, and constrained communication bandwidth. Due to these constraints, it is difficult to directly employ the conventional security mechanisms in WSNs [7]. Some of the major constraints of a WSN are listed below [6,7].

***A. Energy constraints*:** Energy is the biggest constraint for a WSN. In general, energy consumption in sensor nodes can be categorized in three parts [6, 7]: (i) energy for the sensor transducer, (ii) energy for communication among sensor nodes, and (iii) energy for microprocessor computation.

B. Memory limitations: A sensor is a tiny device with only a small amount of memory and storage space. Memory in a sensor node usually includes flash memory and RAM. Flash memory is used for storing downloaded application code and RAM is used for storing application programs, sensor data, and intermediate results of computations. There is usually not enough space to run complicated algorithms after loading the OS and application code [6, 7].

C. Unreliable communication: This is another serious threat to sensor security. Normally the packet-based routing of sensor networks is based on connectionless protocols and thus inherently unreliable. Packets may get damaged due to channel errors or may get dropped at highly congested nodes. Furthermore, the unreliable wireless communication channel may also lead to damaged or corrupted packets. Higher error rate also mandates robust error handling schemes to be implemented leading to higher overhead. In certain situation even if the channel is reliable, the communication

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 7, July 2013

may not be so. This is due to the broadcast nature of wireless communication, as the packets may collide in transit and may need retransmission [7].

D. Higher latency in communication: In a WSN, multi-hop routing, network congestion and processing in the intermediate nodes may lead to higher latency in packet transmission. This makes synchronization very difficult to achieve. The synchronization issues may sometimes be very critical in security as some security mechanisms may rely on critical event reports and cryptographic key distribution [7].

E. Unattended operation of networks: As the sensors nodes are deployed in remote environment and left unattended. The likelihood that a sensor encounters a physical attack in such an environment is therefore, very high. Remote management of a WSN makes it virtually impossible to detect physical tampering. This makes security in WSNs a particularly difficult task [7].

III. SECURITY REQUIREMENTS IN WSNs

WSNs are special kind of Ad-hoc networks. Security services in WSNs are required to protect the information and resources from attacks and misbehavior. The security requirements [1] [3] [4] [6] [7] in WSNs include:

***A. Availability*:** Availability ensures that the desired network services are available even in the presence of denial-of-service attacks require configuring the initial duty cycle carefully [1].

B. Authorization: Authorization ensures that only authorized sensors can be involved in providing information to network services [1].

C. Privacy: Privacy prevents adversaries from obtaining information that may have private content [3].

D. Authentication: which ensures that the communication from one node to another node is genuine, that is, a malicious node cannot masquerade as a trusted network node [1].

E. Anonymity: Anonymity hides the source of the data. It is a service that can help with data confidentiality and privacy [3].

F. Resilience: Resilience sustains the network functionalities when a portion of nodes are compromised by the attacks.

G. Confidentiality: Confidentiality ensures that a given message cannot be understood by anyone other than the desired recipients [1].

H. Integrity: Integrity ensures that a message is not modified during the transmission.

I. Nonrepudiation: Nonrepudiation denotes that a node cannot deny sending a message it, has previously sent [1].

J. Self Organization: Wireless sensor networks are spatial kind of Ad-hoc networks in which every sensor node should be self healing and self organizing. The dynamic nature of a WSN makes it sometimes impossible to deploy any preinstalled shared key mechanism among the nodes and the base station [7].

K. Time Synchronization: Most sensor network applications rely on some form of time synchronization. Furthermore, sensors may wish to compute the end-to-end delay of a packet as it travels between two pair wise sensors. A more collaborative sensor network may require group synchronization for tracking applications [9, 10].

L. Secure Localization: In WSN each sensor node is required to locate itself in the network accurately and automatically to identify the location of the fault.

M. Flexibility: Sensor networks will be used in dynamic battlefield scenarios where environmental conditions, threat, and mission may change rapidly. Changing mission goals may require sensors to be removed from or added to an established sensor node. Furthermore, two or more sensor networks may be fused into one, or a single network may be split in two .Key establishment protocols must be flexible enough to provide keying for all potential scenarios a sensor network may encounter [10].

N. Freshness: Freshness implies that the data is recent and ensures that no adversary can replay old messages [1]. To make sure that no old messages replayed a timestamp can be added to the packet [7].

IV. COMMON ATTACKS IN WSNs

Attacks in sensor networks can be classified into the following categories [1, 7]:

A. Outsider versus insider attacks: outsider attacks are defined as attacks from nodes which do not belong to a WSN; insider attacks occur when legitimate nodes of a WSN behave in unintended or unauthorized ways.

B. Passive versus active attacks: passive attacks include eavesdropping on or monitoring packets exchanged within a WSN; active attacks involve some modifications of the data steam or the creation of a false stream.

C. Mote-class versus laptop-class attacks: in mote-class attacks, an adversary attacks a WSN by using a few nodes with similar capabilities to the network nodes; in laptop-class attacks, an adversary can use more powerful devices (e.g., a laptop) to attack a WSN. These devices have greater transmission range, processing power, and energy reserves than the network nodes.

WSNs are vulnerable to various types of attacks. According to the security requirements in WSNs, these attacks can be categorized as [1] [6] [7]:

A. Attacks on secrecy and authentication: Attacks include eavesdropping, packet replay attacks, and modification or spoofing of packets.

B. Attacks on network availability: attacks on availability are often referred to as denial-of-service (DoS) attacks. DoS attacks may target any layer of a sensor network.

C. Stealthy attacks against service integrity: In a stealthy attack, the goal of the attacker is to make the

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 7, July 2013

network accept a false data value. For example, an attacker compromises.

WSN attacks categorized at different layers:

A. Physical layer: Attacks at the physical layer include jamming and tampering. These two attacks are discussed in this subsection.

***1. Jamming*:** Jamming is a type of attack which interferes with the radio frequencies that a network's nodes are using [6] [7]. An attacker sends some radio waves at the same frequency that it is used by wireless sensor networks [2]. A jamming source may either be powerful enough to disrupt the entire network or less powerful and only able to disrupt a smaller portion of the network.

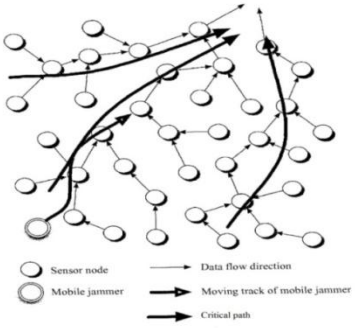

Figure 4.1 A Radio jamming attack

2. Tampering: Another physical layer attack is tampering [6]. Given physical access to a node, an attacker can extract sensitive information such as cryptographic keys or other data on the node. The node may also be altered or replaced to create a compromised node which the attacker controls.

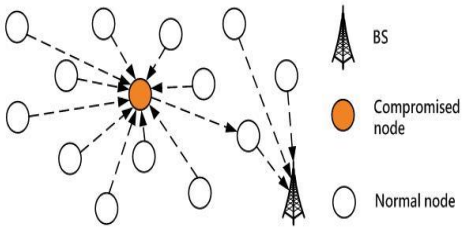

Figure 4.2 A Tampering attack

B. Data link layer: Attacks at the link layer include collisions, resource exhaustion, and unfairness. This subsection looks at each of these three link-layer attack categories.

1. *Collisions:* A collision results when two nodes trying to send data on same frequency. When packets collide, a change will likely occur in the data portion, causing a checksum mismatch at the receiving end. The packet will then be discarded as invalid. An adversary may strategically cause collisions in specific packets such as ACK control messages. A possible result of such collisions is the costly exponential back-off. The adversary may simply violate the communication protocol and continuously transmit messages in an attempt to generate collisions [7].

2. *Exhaustion:* Repeated collisions can also be used by an attacker to cause resource exhaustion [6], 7]. For example, a naive link-layer implementation may continuously attempt to retransmit the corrupted packets. Unless these hopeless retransmissions are discovered or prevented, the energy reserves of the transmitting node and those surrounding it will be quickly depleted [6, 7].

3. *Unfairness:* Unfairness can be considered a weak form of a DoS attack. An attacker may cause unfairness in a network by intermittently using the above link-layer attacks. Instead of preventing access to a service outright, an attacker can degrade it in order to gain an advantage such as causing other nodes in a real-time MAC protocol to miss their transmission deadline [6, 7].

C. Network layer: The network and routing layer of sensor networks is usually designed according to the following principles [6].

- Power efficiency is an important consideration.
- Sensor networks are mostly data-centric.
- An ideal sensor network has attribute-based addressing and location awareness.

The attacks in the network layer include the following.

1. Spoofed, Altered, or Replayed Routing Information: The most direct attack against a routing protocol in any network is to target the routing information itself while it is being exchanged between nodes. An attacker may spoof, alter, or replay routing information in order to disrupt traffic in the network [6] [7]. These disruptions include the creation of routing loops, attracting or repelling network traffic from select nodes, extending and shortening source routes, generating fake error messages, partitioning the network, and increasing end-to-end latency.

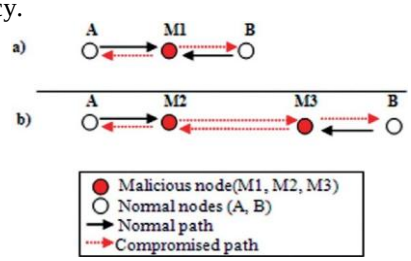

Figure 4.3 A Replay attack

2. Selective Forwarding: A significant assumption made in multihop networks is that all nodes in the network will accurately forward received messages. An attacker may create malicious nodes which selectively forward only certain messages and simply drop others [6] [7]. One form of this attack is Black hole [2]. A simple approach is

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 7, July 2013

that malicious nodes refuse to forward any packets through it, which is like a black hole attack [8].

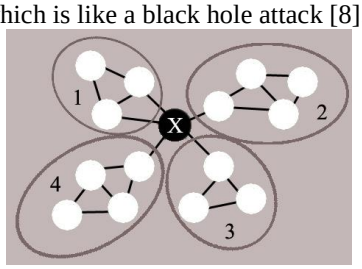

Figure 4.4 An example of black hole attack in a clustering network [2]

3. Sinkhole: In a sinkhole attack, an attacker makes a compromised node look more attractive to surrounding nodes by forging routing information [6] [7]. The end result is that surrounding nodes will choose the compromised node as the next node to route their data through. This type of attack makes selective forwarding very simple, as all traffic from a large area in the network will flow through the adversary's node.

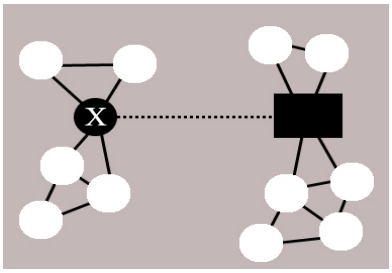

Figure4.5 A sinkhole attack [2]

4. Sybil: The Sybil attack is a case where one node presents more than one identity to the network [6]. It was originally described as an attack intended to defeat the objective of redundancy mechanisms in distributed data storage systems in peer-to-peer networks [7]. A Sybil attack is attack in which an attacker destabilizes the reputation scheme of a peer-to-peer network by creating a huge number of pseudonymous entities, using them to gain a disproportionately big influence [4].

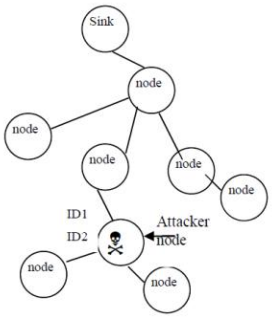

Figure 4.6 A sybil attack [11]

5. Wormhole attack: Wormhole attack needs to insert at least two malicious nodes in the network and these nodes are connected by a powerful connection [2]. A wormhole is low latency link between two portions of a network over which an attacker replays network messages [6] [7]. This link may be established either by a single node forwarding messages between two adjacent but otherwise non-neighboring nodes or by a pair of nodes in different parts of the network communicating with each other.

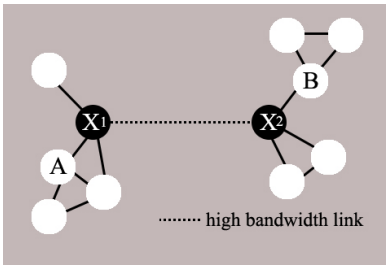

Figure 4.7A Wormhole attack [2]

6. Hello Flood Attacks: An attacker sends or replays a routing protocol's HELLO packets from one node to another with more energy. This attack uses HELLO packets as a weapon to convince the sensors in WSN. In this type of attack an attacker with a high radio transmission range and processing power sends HELLO packets to a number of sensor nodes that are isolated in a large area within a WSN. The sensors are thus influenced that the adversary is their neighbor. As a result, while sending the information to the base station, the victim nodes try to go through the attacker as they know that it is their neighbor and are ultimately spoofed by the attacker. [9]

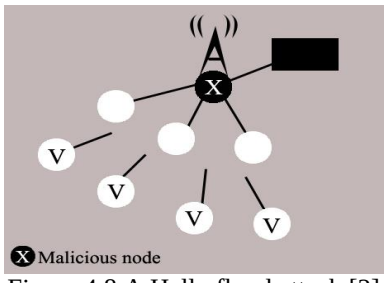

Figure 4.8 A Hello flood attack [2]

7. Acknowledgment Spoofing: Routing algorithms used in sensor networks sometimes require acknowledgments to be used [6] [7]. Attacking node spoof the routing information and send false information to the receiving node. An example of such false information is claiming that a node is alive when in fact it is dead [6].

D. Transport layer: Two possible attacks in this layer, flooding and desynchronization, are discussed in this subsection.

1. ***Flooding:*** Whenever a protocol is required to maintain state at either end of a connection it becomes vulnerable to memory exhaustion through flooding [6] [7]. An attacker may repeatedly make new connection requests until the resources required by each connection are exhausted or reach a maximum limit. In either case, further legitimate requests will be ignored.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 7, July 2013

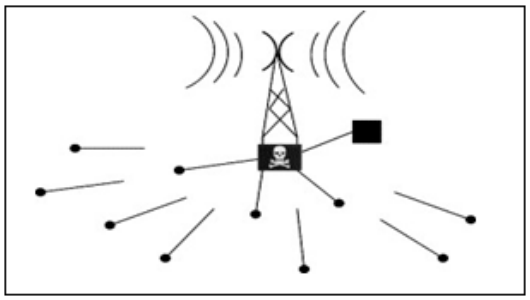

Figure 4.9 A Flooding attack

2. ***Desynchronization:*** Desynchronization refers to the disruption of an existing connection [6] [7]. An attacker may, for example, repeatedly spoof messages to an end host, causing that host to request the retransmission of missed frames. If timed correctly, an attacker may degrade or even prevent the ability of the end hosts to successfully exchange data, thus causing them to instead waste energy by attempting to recover from errors which never really existed.

V. SECURITY MECHANISMS

A. ***Shared Keys:*** This mechanism prevents attacks from outsider attacks. One security feature that receives a great deal of concentration in wireless sensor networks is the area of key management [4]. Wireless sensor networks are unique in this characteristic due to their size, mobility and power constraints. Traditionally, key establishment is completed using one of many public-key protocols. A usual method of protecting any network against outsider attacks is to just apply a simple key infrastructure [4].

B. ***Encryption:*** This mechanism provides security against passive attacks like eavesdropping. Sensor network mostly run in public or wild area over inherently unconfident wireless channels. It is therefore insignificant for a device to eavesdrop or even add messages into the network. The traditional key to this problem has been to espouse techniques such as message authentication codes, symmetric key encryption schemes and public key cryptography. [4]

C. ***Secure Data Aggregation:*** Sensor networks and data aggregation techniques are vulnerable to a range of attacks including denial of service attacks. As the data transfer increases, data traffic is the most important trouble in networks. So in order to decrease overhead cost and network traffic, sensor node aggregates measurements before sending them to the base station. Such data is particularly enticing to an attacker. An adversary with control over an aggregating node can chose to ignore report or produce false report, affecting the creditability of the generated data and hence the network as a whole must be considered. [4]

D. ***SPINS: Security Protocols for Sensor Networks:*** SPIN offers many security properties like Semantic security, Data authentication, Replay protection, Data freshness, and Low communication overhead and it is optimized for resource constrained and wireless communication [4]. SPIN which is a three-part approach providing for an authentication routing protocol as well as a three-part approach providing authenticated streaming broadcasts as well as two-party data authentication, data confidentiality, and freshness [5].

E. ***TinySec:*** *Link Layer Security Architecture:* TinySec provides authentication service and it is lightweight security package. It is included into the official TinyOS release. TinySec supports two special security options: authenticated encryption (TinySecAE) and authentication only (TinySecAuth) [4].

F. ***Defending against DoS Attacks:*** One strategy in defending against the classic jamming attack is to identify the jammed part of the sensor network and effectively route around the unavailable portion. To overcome the transport layer flooding denial of service attack, server should always force a client to commit more resources up front than the server. This strategy would likely be effective as long as the client has computational resources comparable to those of the server [10].

G. **Defending against Attacks on Routing Protocols:** To prevent against attacks like sinkhole, wormhole and Sybil attacks, Tanachaiwiwat, *et al.* presents a novel technique named TRANS (Trust Routing for Location Aware Sensor Networks). The TRANS routing protocol is designed for use in data centric networks [10].

VI. CONCLUSION

Wireless Sensor Networks often operate in a resource constrained environment. Optimal resource utilization is main objective of WSN. But Wireless Sensor Networks are equally vulnerable to security attacks. Ensuring security in a hostile operational environment of WSN is a hurricane task. The idea of this paper is to provide comprehensive information on types of attacks WSN is exposed to and possible methods of countering such attacks effectively. The motto here is to help novice researchers with objective to work on security challenges in Wireless Sensor Network environment.

ACKNOWLEDGEMENT

We sincerely acknowledge all the cited authors for giving us base papers with strong fundamental concepts, We would like to thank Dr. Thriveni J, Department of Computer Science, UVCE, Bangalore for reviewing and providing invaluable minute details on organization of the paper and we thank all the members of Department of Information Science and Engineering, Acharya Institute of Technology for providing valuable advises and special thanks to Mr. Ravichandra M, of Acharya Institute of Technology for providing suggestions for a better structuring of the paper.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 7, July 2013

REFERENCES

[1] Yan-Xiao Li, Lian-Qin and Qian-Liang ,"Research On Wireless Sensor Network Security" 2010 International Conference on Computational Intelligence and Security
[2] David Martins and Hervé Guyennet, "Wireless Sensor Network Attacks and Security Mechanisms: A Short Survey" 2010 13th International Conference on Network-Based Information Systems
[3] Asmae BLILAT, Anas BOUAYAD, Nour el houda CHAOUI, Mohammed EL GHAZI, "Wireless Sensor Network: Security challenges" IEEE 2012
[4] Abhishek Jain, Kamal Kant and M. R. Tripathy ,"Security Solutions for Wireless Sensor Networks" 2012 Second International Conference on Advanced Computing & Communication Technologies
[5] Daniel E. Burgner , Luay A, "Wahsheh "Security of Wireless Sensor Networks" 2011 Eighth International Conference on Information Technology: New Generations
[6] Yong Wang, Garhan Attebury, and Byrav Ramamurthy "A survey of security issues in wireless sensor networks" 2nd quarter 2006, volume 8, NO. 2 IEEE communication surveys
[7] Jaydip Sen "A survey on wireless sensor networks security" International Journal of Communication Networks and Information Security (IJCNIS) Vol. 1, No. 2, August 2009
[8] Yuling li "Research about security mechanisms in wireless sensor networks" IEEE 2011
[9] Dr. G. Padmavathi, Mrs. D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks" (IJCSIS) International Journal of Computer Science and Information Security,Vol. 4, No. 1 & 2, 2009
[10] Mona Sharifnejad, Mohsen Sharifi, Mansoureh Ghiasabadi and Sareh Beheshti "A Survey on Wireless Sensor Networks Security" SETIT 2007 4th International Conference: **S**ciences of **E**lectronic, Technologies of **I**nformation and **T**elecommunications March 25-29, 2007 – TUNISIA
[11] Abhishek Pandey, R.G.Tripathy " A survey on wireless sensor network security" International journal of computer applications (0975-8887) volume 3-No. 2, June 2010.

BIOGRAPHY

Mr. C K Mari Gowda, Currently working as Associate Professor, Department of Information Science and Engineering, Acharya Institute of Technology, Bangalore, Karnataka, India. And Pursuing Ph.D. in VTU Research Resource Centre, Belgaum. In the field of Security issues in WSN.

Mr. Manjunath Shingadi, pursuing Master of Technology in Computer Network and Engineering, Department of Information Science and Engineering, Acharya Institute of Technology, Bangalore, Karnataka, India.