Security Aspects for Wireless Sensor Network

Rohit Tiwari
Department of Computer Engineering, K. J. Institute of Engg. & Tech., Vadodara, India

Monika Kohli
Department of Information Technology, K. J. Institute of Engg. & Tech., Vadodara, India

Abstract

Wireless Sensor Networks (WSNs) made of hundreds and even thousands of very small sensor nodes, working unconventionally and mostly without access to renewable energy resources. Price limitations and the requirement for ubiquitous (pervasive) and unseen implementations will result in tiny and resource-compelled sensor nodes. Earlier WSNs were implemented having the security ignored. But as sensor network may deal with highly sensitive content and functions without much interaction with external stimuli. In this paper we emphasis on exploring the security issues and challenges in WSN.

1. Introduction

Sensor Network is defined as a combination of actuators and small sensors with general purpose computing elements. WSN contains various sensor node devices in a quite huge area. It is a blend of computing, distributed sensing and communication. We can say that Wireless Sensor Network=Wireless Sensing+Data Networking. WSNs are networks which are built of independent and dispersed, but working together small sensors. These sensors have sensing ability which is used for monitoring, tracking and detection of environmental as well as physical conditions at various locations like heat, trembling, force etc. Smart Environments use WSNs as one of the most crucial part for information collection. Only WSNs, which are fast and quite simple in installation as well as in maintenance, will sustain in the current scenario. Because of the less power wireless communications and accessibility of micro sensors, there are miscellaneous WSN applications domains are there. But there are many different security attacks and challenges, we have identified, for a Wireless Sensor Network implementation. In this paper, we emphasis on security attacks on Wireless Sensor Networks, as well as various challenges faced by WSN implementation process.

2. WSN Architecture

Architecture of a Wireless Sensor Network consists of the network components listed below-

i. **Sensor Nodes** –Sensor Nodes are small devices which generate a computable reaction to a variation in a physical or environmental condition.

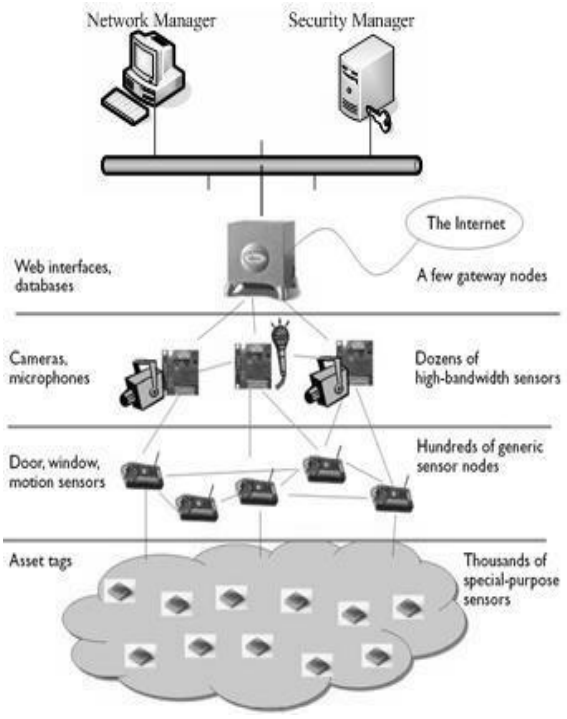

Fig.1 Typical Wireless Sensor Network Architecture.

These can be individually used to compute and to convert a physical or environmental amount into a signal which is read by a device or by an observer. Sensor Nodes are used for routing of packets for additional devices must be done by them only. The process or process apparatus is mostly characterized or controlled by them. There is a special type of field device, called as router, which does not have control apparatus or process sensor. Router has interface with the process itself.

ii. **Gateway or Access Points** – communication between field devices and host application is being provided by a Gateway.

iii. **Network Manager** – setting up communication among devices, routing table management, and observing and reporting the condition of the network and configuration of the network, are all Network Manager's accountability.

iv. **Security Manager** – Creation, stocking and managing of keys are facilitated by Security Manager.

3. Challenges

The major challenge is the Random deployment, where autonomous setup & regular maintenance is required. Because WSNs are generally Infrastructure-less networks, so they follow the concepts of distributed routing. In WSN, energy, the major constraint, is responsible in trading off network lifetime for fault tolerance or accuracy of results. Security solutions for WSN can be designed, but there are a few resource constraints which can't be ignored and should be specially taken care of. These resource constraints include Limited Energy, Limited Bandwidth, Limited Computing Power, Limited Communication Range & Limited Memory. The security mechanism relies on the limitations and proficiencies of sensor node networks and it is hosted on a sensor node platform. The communication process in Wireless Sensor Network is only through wireless medium such as radio. Due to this reason the security mechanism is unrealistic for a WSN. WSN always have dynamic topology and the sensor nodes are arranged in arbitrary manner. In sensor network implementation process large number of nodes is required due to unpredictable nature of this implementation. The implementation cost of WSN should likely to be less.

4. Attacks and Threats in Wireless Sensor Network

Attacks on WSN are mostly categorized into two different stages, first is the attack over the elementary mechanism (e.g. routing) and second is the attack over the security mechanism. Here we draw attention to few of the main attacks over Wireless Sensor Network. To make a Wireless Sensor Network secure, the network should support all security parameters like availability, confidentiality, authenticity and integrity.

The attacks over a Wireless Sensor Network are as described in brief here as under:

i. **Denial of Service (DOS)**

Denial of Service is produced by the unpremeditated failure of nodes. DOS attacks exhaust the resources of the target victim node by transferring unnecessary excessive packets, hence preventing the network from accessing services. Numerous DOS attacks might be executed in WSN in different layers [2].

ii. **Sybil**

In a Sybil attack, multiple identities are presented by the attacker for a single node, although many protocols presume that a single node presents a unique identity. The Sybil attack basically implies that the attacker can be present at more than one place concurrently [3]. The attacker will be selected as the next-hop in geographic forwarding by making false identities of nodes placed at the verge of communication area all around a target victim. The assurances made by a multipath routing scheme will be reduced by the attack.

iii. **Wormhole**

In the case of a wormhole attack, rivals work together to deliver a low latency side channel for communication [4]. It can be better understood with the scenario discussed here. Suppose there are two attackers, who may own an additional radio for communicating over a higher speed and a long range link.

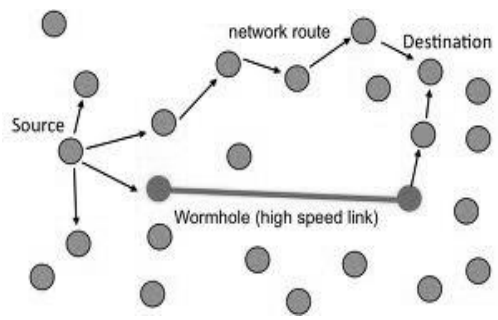

Fig. 2 Wormhole Attack

One attacker will relay the message received by him, to the other via the side channel. In this side channel, the messages are communicated as if these are only one node away from the original source. Because it minimizes the distance between two adjacent nodes, it might be the reason for adjacent nodes to favor the attacker for a wormhole attack. Services will not be denied, but the same will be improved provided that the side channel is present. Though, the network will enter and remain in an unpredictable state that requires re-initialization of some services to bring back into appropriate function, when the attacker moves or stops to tunnel messages.

iv. **Sinkhole (Black hole)**

In Sinkhole attacks, a compromised node is made to look exclusively attractive to its neighboring nodes regarding the routing algorithm and pull almost all of the traffic from a specific area via the compromised node this process creates a symbolic sinkhole with the adversary at the center [12]. As the nodes near or on the path of packet have countless opportunities to damage the application data, sinkhole attacks may empower various other threats e.g. selective forwarding.

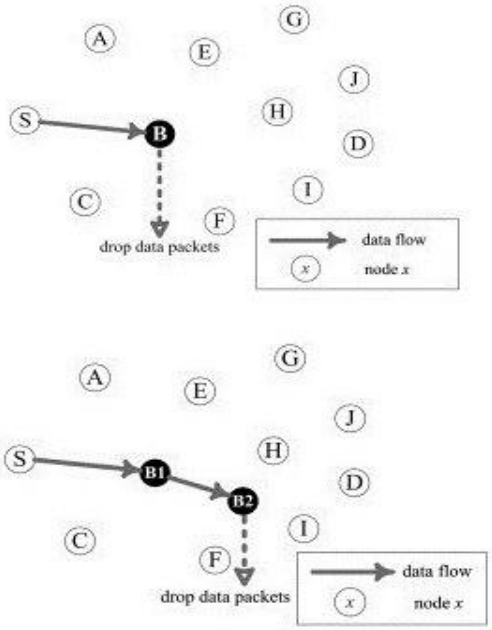

Fig. 3 Sinkhole Attack

v. **Selective Forwarding**

Wireless Sensor Networks generally rely on every node to take part in routing for its adjacent nodes if it can offer a desired forwarding path. Many selective forwarding attacks can exploit this dependence to cause Denial of Service via routing. A subverted sensor device can just discard to forward certain messages. A random dropping policy increases the local loss rates and may prompt costly end-to-end recovery mechanisms. An attacker may also drop messages to or from certain victims, such as base stations or other servers.

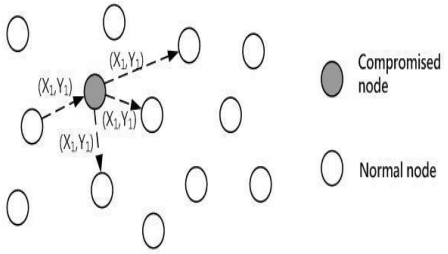

Fig. 4 Selective Forwarding Attack

vi. **Hello Flood**

In Hello flood attack, the hello packets are used as a weapon by the attacker to influence the sensor nodes. This is done by sending hello packets to many sensor nodes spread in a big area within a Wireless Sensor Network. Subsequently while transferring the information to the sink, the victim node tries to go through the attacks as they know that it is their neighbor and ultimately deceived by the attacks.

vii. **Traffic Analysis Attacks**

As we have already discussed that wireless sensor networks are usually built of several low-power sensors communicating with a few relatively robust and powerful base stations.

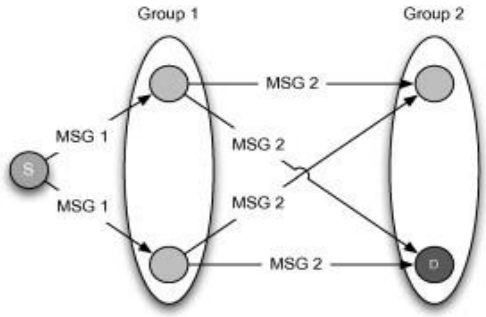

Fig.5.Traffic Analysis Attack

Hence, it is quite natural that data will be collected by each and every node and from where it will be eventually routed to the base station. The attacker can simply disable the base station often, to effectively render the network useless for an adversary [13]. As we can see in the Fig-5 that by associating message *MSG 1*, attackers recognize nodes in *Group 1* and then by associating message *MSG 2*, they can recognize the next group, *Group 2*.

viii. **Acknowledgement Spoofing**

Many of the routing algorithms for wireless sensor network depend on implicit or explicit link layer acknowledgements. An adversary can spoof link layer acknowledgments for overheard packets addressed to adjacent nodes, because of the inherent broadcast medium. Basically the aims of acknowledgement spoofing include making the sender believe that a weak link is strong or that a dead or disabled node is alive.

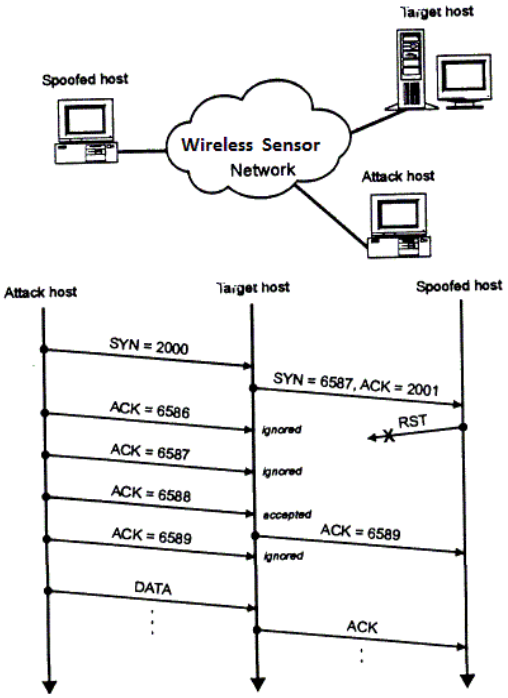

Fig. 6 Acknowledgement Spoofing Attack

ix. **Insider Attacks**

It is also known as Mote Class attack. In insider attacks, the attackers have an authenticated contestant in the sensor network [6]. These attacks are generally invoked via either corrupted sensor node running infected code or adversary who have snatched the key material, code, and data from authentic nodes, and who then uses one or more laptop class gadgets to attack the network. In this class of attack, the attacker can't access more than a few sensor nodes having same abilities to our own.

x. **Outsider Attacks**

It is also known as Laptop Class attack. The attackers of this class have no exceptional access to the sensor network, but almost all of them can access more powerful gadgets, such as tablet PCs, notebooks etc., which replace the authentic nodes when installed for action. And these gadgets have more battery power, a sensitive antenna, a processor with better proficiencies and a stronger transmitter. The attackers might be capable of blocking the whole sensor network using its more power radio transmitter. An entire network can be collapsed just by the attack of a single attacker

of this class. The attackers generally have a greater bandwidth and communications channel with less delay which actually helping these attackers to synchronize their efforts.

xi. **Impersonation**
In this kind of attack, by duplicating the node ID of a current sensor node, an attacker tries to augment a node to an existing sensor network. Such kind of attacks might occur if an adversary copies the node ID of a node in the network. In this way the packets could be violated, misguided or removed, and also if the adversary is able to execute such replication then there are possibilities that it might cause the cryptographic keys to be unveiled. Such attacks are known as Multiple ID or Node Duplication too.

xii. **Eavesdropping**
Fundamentally it is observing and eavesdropping and known as confidentiality too. The attacker in this kind of attack can effortlessly determine the communication contents only via listening to the data. Sensor network traffic is quite susceptible to observing and eavesdropping. Although a robust security protocol is used, but observing might invoke other attacks such as wormhole and black hole attacks.

5. Proposed Protection Mechanisms

5.1 Denial of Service Attack Protection

Protection from the denial of service attacks can be achieved via various mechanisms; the list consists of payment for network resources, identification of traffic, pushback and strong authentication and identification of traffic [10]. One of the security mechanisms is using the authentication streams for securing the reprogramming procedure. In this approach a program binary is split into a chain of messages, each having a hash of a next message. This technique provides assurance that even if an intruder is aware of the hashing technique he or she cannot take over a currently running program transmission. This technique works on the concept that it will be almost impossible to create a message that matches the hash present in the previous message[11]. Using present encryption and authentication techniques, we can get protection against so many attacks, and there are some other techniques which can be used to alert network managers about present attacks or trigger techniques to preserve energy on affected devices.

5.2 Wormhole Attack Protection

To fight against the wormhole attack one can use a proactive routing protocol known as DAWWSEN [9]. This protocol is built upon the construction of a hierarchical tree in which the root node acts as the base station, and the sensor nodes are represented as the leaf (internal) nodes of the tree. Usage of DAWWSEN provides a huge benefit that it does not need any physical information of the sensor nodes and does not take the time stamp of the packet as a method to detect a wormhole attack, though it is quite significant for the resource constrained nature of the sensor nodes.

5.3 Sybil Protection

The Sybil attack protection mechanism is based on the utilization of ID certificates. It is basically quite a simple approach in which, the setup server allocates every sensor node certain unique information, before deployment. Then it creates an ID certificate joining this ID of node to the allocated unique information, and transfers this information into the node. To exhibit its ID securely, a node presents its ID certificate first, and then proves that it possesses or matches the associated unique information. The complete process involves the receiving and transferring of numerous messages. Merkle has proposed a hash tree which is used quite often as elementary resource for ID certificates computation [11]. The proposed hash tree is a vertex-labeled binary tree, where each non-leaf vertex label is a hash of the combination of the labels of its two child vertexes. The set of vertexes on the path from the leaf to the root of the tree is the primary path of a leaf vertex. The authentication path has the siblings of the vertexes on this primary path. One can compute the primary path up to and including the root of the tree, if provided with a vertex, its authentication path, and the hash function. And then, to verify the legitimacy of the label of the leaf vertex this computed value of the root can be compared with a stored value.

5.4 Selective Forwarding Attack Protection

To protect against selective forwarding attacks, there is a mechanism available known as multipath routing. If the Messages are transmitted over paths having entirely split sensor nodes, then these messages are totally protected from selective forwarding attacks [8]. And also if the sensor nodes are allowed to randomly choose the next hop of a packet possibly out of a set of potential candidates then it will reduce the possibilities of an attacker getting total control of a data stream in future.

5.5 Sinkhole Attacks Protection

Although it is quite tough to provide protection against sinkhole attacks, but there is a protocol class known as geographic routing protocols, which is resilient enough

to deal with such attacks [7]. These protocols build a network structure as per the demand and that to only with applying local interactions and information. From the base station, these protocols do not require any initiation.

5.6 Hello Flood Attacks Protection

One can get protection against hello flood attacks just via inspecting the link's bidirectional, as with this the nodes get an assurance that they should reach to their parent inside one hop.

6. Conclusion

The wireless sensor networks are having an extraordinary growth nowadays because of its huge number of sensor network applications in various fields. But to send and receive sensitive data within the wireless sensor networks without compromising its security is a critical job. In other words, the industry will only adopt a WSN based application, when it guarantees full security for all aspects. Although there are possibilities that upcoming research over confidentiality and authenticity in WSN will make it a smart choice in various new fields. Recently offered security mechanisms are centered on particular network structures, hence it is less efficient to provide a complete solution for the security in wireless sensor networks. In this paper, we deeply analyzed security attacks for wireless sensor networks & proposed their preventions.

7. Acknowledgements

The authors would thanks the reviewers for their help in improving the document.

References

[1] Hiren Kumar Dev Sharma, Ajit Kumar, Sikkim Manipal Institute of Technology "Security Threats in Wireless Sensor Networks", IEEE 2006.

[2] Md. Aniur Rehmam & Mitu Kumar Debnath, "Energy Efficient Data Security System for Wireless Sensor Network", Sixth International Conference on Computer and Information Technology, 2008.

[3] John R. Douceur, "The Sybil attack", In IPTPS, pages 251-260, 2002.

[4] Yih-Chun Hu, Adrian Perrig, and David B. Johnson, "Packet leashes: A Defence against Wormhole Attacks in Wireless Networks", In Proceedings of IEEE Infocom 2003, April 2003.

[5] Anthony D. Wood, John A. Stankovic, "A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks", Department of Computer Science, University of Virginia.

[6] Chris Karlof, David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", University of California at Berkeley.

[7] M. Zorzi, R. R. Rao, "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.

[8] D. Ganesan, R. Govindan, S. Shenker, D. Estrin, "Highly-Resilient, Energy-Efficient Multipath Routing in Wireless Sensor Networks", Mobile Computing and Communications Review, Vol. 4, No. 5, October 2001.

[9] Rouba El Kaissi, Ayman Kayssi, Ali Chehab, Zaher Dawy, "DAWWSEN: A Defence Mechanism against Wormhole Attack in Wireless Sensor Network", Proceedings of the Second International Conference on Innovations in Information Technology (IIT, 2005).

[10] A.D. Wood, J.A. Stankovic, "Denial of Service in Sensor Networks," Computer, Vol. 35, No. 10, 2002, pp. 54– 62.

[11] David R. Raymond, Scott F. Midkiff, "Denial-of-Service in Wireless Sensor Networks: Attacks and Defences," IEEE Pervasive Computing, Vol. 7, No. 1, 2008, pp. 74-81.

[12] Hemanta Kumar Kalita, Avijit Kar, "Wireless Sensor Network Security Analysis", International Journal of Next-Generation Networks (IJNGN), Vol.1, No.1, December 2009.

[13] J. Deng, R. Han, S. Mishra, "Countermeasures against Traffic Analysis in Wireless Sensor Networks", Technical Report CU-CS-987-04, University of Colorado at Boulder, 2004.