Security Attacks in Wireless Sensor Network

Prachi Bansal, Beenu Yadav, Sonika Gill, Harsh Verma

Abstract— Wireless Sensor Networks (WSNs) use small nodes with constrained capabilities to sense, collect, and disseminate information in many types of applications. One of the major challenges wireless sensor networks face today is security Wireless Sensor Networks (WSN) is an emerging technology and have great potential to be employed in critical situations like battlefields and commercial applications such as building, traffic surveillance, habitat monitoring and smart homes and many more scenarios. One of the major challenges wireless sensor networks face today is security. In this paper we present a introduction to wireless sensor networks, its usage in every environment followed by a brief overview of characteristics and requirements for deploying such a network. The different attacks on these networks are discussed. For each of these attacks, counter measures are presented if applicable.

Index Terms— Authentication, Confidentiality, DoS (Denial of Service), Routing, Security Goal, Security Attacks, WSN (Wireless Sensor Network).

I. Introduction

WSN are composed of a large set (hundreds to a few thousand) of homogeneous nodes with extreme resource constraints [1]. Each sensor node has wireless communication capability plus some level of intelligence for signal processing and data networking. These nodes are usually scattered over the area to be monitored to collect data, process it, and forward it to a central node for further processing. Military sensor networks might detect and gather information about enemy movements of people and equipment, or other phenomena of interest such as the presence of chemical, biological, nuclear, radiological, explosive materials. In almost every environment different kinds of sensors are in use. Sensors are used in buildings automation for controlling lights, access control, refrigeration control or HVAC control. Industrial automation uses different kinds of sensors such as sensors for temperature sensing and control, pressure sensing, level sensing and machinery monitoring. Power and utility automation use sensors for remote reading of residential meters or for power distribution diagnostics. Environmentalist uses them for environmental monitoring to measure air and water quality as well as seismic activity, health specialist uses them for tele-health monitoring and diagnostics where they significantly reduce overall medical costs by enabling home-based proactive monitoring and medical care, like personalized patient-based monitoring techniques for measuring the heart rate or respiration . sensors can also be used for maintaining the integrity and safety of buildings, industrial facilities, roadways, water supplies and other public infrastructure. In short – different kinds of sensors are used in our day to day environment to detect, monitor, collect data obtained in different environments.

Nowadays several different wire-based or actuators network products can be found in building automation, industrial automation, security systems or automotive systems. Wired sensors though of great use share some; namely are expensive to install, inflexible once installed, limited in size, in complexity, in functionality and are highly obtrusive in existing infrastructure. On the other hand wireless sensor networks are not restricted by these limitations.

Wireless sensor networks offer advantages in terms of scalability for multi-hop networks with ten to thousands of devices, robustness because of self reconfigurations and distributed intelligence, profitability through low installation costs and flexibility in terms of wireless data collections [1], [3]. The application of their operation includes building controls (fire alarms systems), thermo technology climate control systems, in military for tracking and monitoring borders and so on. This shows that the content of transmitted data covers a spectrum of applications from low security like thermo technology to the high security requirement for military purposes.

Depending on the kind of application it might be necessary to transmit information to other parties. Data collected by outside temperature sensors might be forwarded to a computing system which uses the information for weather forecast applications. The security system, which for example detects an alarm, might inform the owner directly by email or an SMS about the alarm in his house, besides contacting security facilities.

It must be ensured that a central unit is able to collect the data and information about the wireless sensor network. Therefore, a connection from the wireless sensor network to this central unit is required. Hence the challenge that lies with wireless sensor networks is the security of data transmission, reduce power consumption and cost reduction.

Figure I, shows the layout of a sensor networks where sensor nodes are used to collect the data which is passed through a transit network through multi –hops to reach the base station where the processing of data takes place and then it is forwarded to data service center for storage and analysis of the data collected takes place [4].

- *Prachi Bansal, Lecturer, Department of CSE, Teerthanker Mahaveer University, Moradabad, India, E-mail: enggprachi@gmail.com*
- *Beenu Yadav, Assisstant Professor, Department of CS, College of Professional Education, Meerut, India, E-mail: beenu_yadav@rediffmail.com*
- *Sonika Gill, Lecturer, Department of CSE, K N G D Modi Engg. College, Modinagar, India, E-mail: sonika.gill108@gmail.com*
- *Harsh Verma, Assisstant Professor,Trident Group Of Institutions, Gaziabad,India, E-mail: er.harsh86@gmail.com*

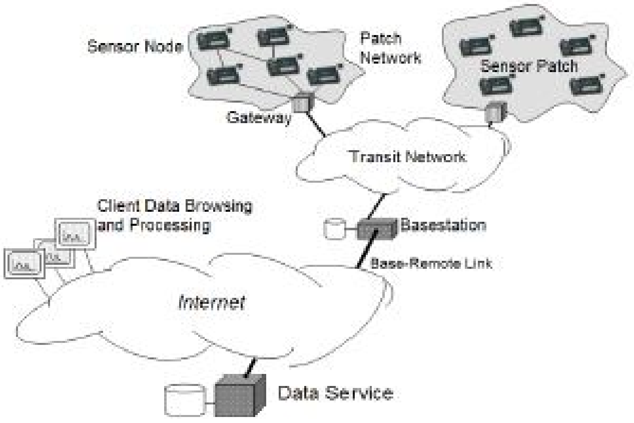

Fig. I: Layout of Wireless Sensor Networks [2]

A. Layout of Node

Figure II (a): shows a typical layout of a sensor node which comprises of a power unit which is the battery, a processing unit which consist of the memory and embedded processor (Tiny OS which is mostly used as a operating system) , a sensing unit the sensor and a communication unit that is the transceiver.

With the flow of information dictating the criticality of these applications, it is pertinent to secure these networks from malicious or destructive entities and threats.

This motivates the need of security for Sensor Networks. Therefore we look into various threats that could hamper the integrity of this network

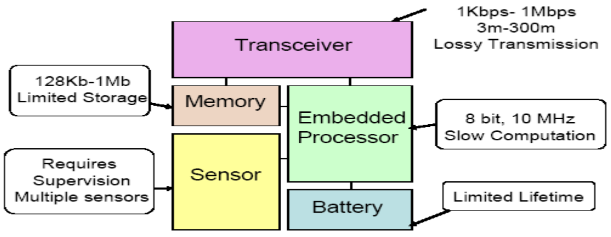

Figure II (a) : Layout of a node [3]

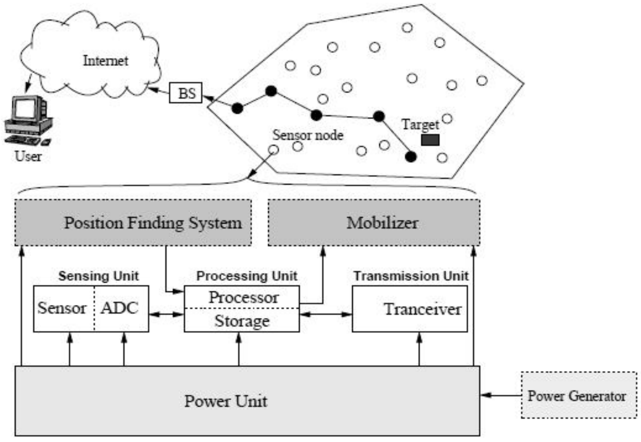

Figure II(b) : Components of a Sensor node

B. Characteristics and requirements

In this section, the different physical characteristics are discussed. Knowing these will help in understanding the difficulties in implement a truly secured solution in wireless sensor networks.

- *Small in size and low power consumption* [2]*:* Wireless sensors or nodes are small in size so that they can be placed in any environment such as to monitor fire alarms, road traffic, forests, oceans, etc. Being small adds to the ease of use and also brings up the issue of power consumption. These devices are made to utilize low power for computation, processing and data transfer to enable energy efficiency. As it is unfeasible to recharge thousands of nodes every month or in weeks.
- *Concurrency–intensive operation* [2]*:* The prime goal of wireless sensors is to allow data flow within the network with minimum amount of processing at each node. The communication is established by communicating through multi-hop in order for the data to reach the base station.
- *Diversity in design and usage* [2]*:* Networked sensors are devised to be application specific as opposed to general purpose, because of their size and function. Therefore minimum requirements are met at both hardware and software level.
- *Low cost* [2]*:* Each scenario whether it be for military purposes, or track weather conditions, hundreds and thousands of nodes are used in each case to form a network; hence the cost should be low for their deployment.
- *Security* [2], [7]*:* Secure networks need to be devised for maintaining the integrity of data. A lot of research is being carried out in this field to enable proper deployments of secure wireless sensor networks.

II. Security Goals for Sensor Networks

As the sensor networks can also operate in an adhoc manner the security goals cover both those of the traditional networks and goals suited to the unique constraints of adhoc sensor networks. The security goals are classified as primary and secondary . The primary goals are known as standard security goals such as Confidentiality, Integrity, Authentication and Availability (CIAA). The secondary goals are Data Freshness, Self-Organization, Time Synchronization and Secure Localization [7].

The primary goals are:

A. Data Confidentiality

Confidentiality is the ability to conceal messages from a passive attacker so that any message communicated via the sensor network remains confidential. This is the most important issue in network security. A sensor node should not reveal its data to the neighbors.

B. Data Authentication

Authentication ensures the reliability of the message by identifying its origin. Attacks in sensor networks do not just involve the alteration of packets; adversaries can also inject additional false packets. Data authentication verifies the identity of the senders and receivers. Data authentication is achieved through symmetric or asymmetric mechanisms where sending and receiving nodes share secret keys. Due to the wireless nature of the media and the unattended nature of sensor networks, it is extremely challenging to ensure authentication.

C. Data Integrity

Data integrity in sensor networks is needed to ensure the reliability of the data and refers to the ability to confirm that a message has not been tampered with, altered or changed. Even if the network has confidentiality measures, there is still a possibility that the data integrity has been compromised by alterations. The integrity of the network will be in trouble when:

- A malicious node present in the network injects false data.
- Unstable conditions due to wireless channel cause damage or loss of data.

D. Data Availability

Availability determines whether a node has the ability to use the resources and whether the network is available for the messages to communicate. However, failure of the base station or cluster leader’s availability will eventually threaten the entire sensor network. Thus availability is of primary importance for maintaining an operational network.

The Secondary goals are:

E. Data Freshness

Even if confidentiality and data integrity are assured, there is a need to ensure the freshness of each message. Informally, data freshness suggests that the data is recent, and it ensures that no old messages have been replayed. To solve this problem a nonce, or another time related counter, can be added into the packet to ensure data freshness.

F. Self-Organization

A wireless sensor network is a typically an ad hoc network, which requires every sensor node be independent and flexible enough to be self-organizing and self-healing according to different situations. There is no fixed infrastructure available for the purpose of network management in a sensor network. This inherent feature brings a great challenge to wireless sensor network security. If self-organization is lacking in a sensor network, the damage resulting from an attack or even the risky environment may be devastating.

G. 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 pairwise sensors. A more collaborative sensor network may require group synchronization for tracking applications.

H. Secure Localization

Often, the utility of a sensor network will rely on its ability to accurately and automatically locate each sensor in the network. A sensor network designed to locate faults will need accurate location information in order to pinpoint the location of a fault. Unfortunately, an attacker can easily manipulate non-secured location information by reporting false signal strengths, replaying signals.

This Section has discussed about the security goals that are widely available for wireless sensor networks and the next section explains about the attacks that commonly occur on wireless sensor networks.

III. Security Attacks

In this section, the different security attacks of the wireless sensor network are discussed. We begin by investigating the denial of service attacks that are usually implemented on the physical layers. Then, various different tactics that are target at the routing mechanism of WSNs are discussed. Some of these attacks also applies to general ad-hoc wireless networks.

A. Denial of Service Attacks

Due to the importance of functionality of sensors in WSNs (Wireless Sensor Networks), it is imperative that the resources of the network be available in order for these sensors to perform their functions. Denying service to these sensors by any means will severely debilitate the functioning of not only the sensors, but also the effected areas of the network. This issue is not only limited to denial of resources, but also extends to flooding of resources in the network to render it useless during the period of the attack.

Sensor networks could be vulnerable to these types of attacks at different layers of the protocol stack.

1) Physical Layer DoS Attacks

The physical layer of sensor networks comprises of a wireless medium which is universally accessible without requirement of any physical connectivity. This renders these networks more susceptible to attacks like jamming of medium and tampering of physical nodes causing denial of service.

- *Jamming.* An adversary can jam radio frequencies used by sensor nodes. This could affect part or the entire sensor network depending on how wide the attack is. Though jamming can be easily sensed by the network, counter measures are often resource heavy resulting in effecting the functioning of the network [5]. Effective counter measures include use of spread-spectrum communication, switching to lower duty cycles to conserve power, isolating jammed region to circumvent communications, etc.
- *Tampering.* Tampering of nodes involves physically interrogating nodes to obtain valuable data or information like cryptographic keys in order to be used to gain access to higher level communications [5]. Though may not be feasible to limit access to hundreds of nodes in a network, they can be built tamper-resistant to some extent. Nodes should react to illegal

interrogation in ways such as auto-erasing critical information so as to not compromise the same.

2) Link Layer DoS Attacks

Denial of service attacks at the link layer could include creating collisions, or exhausting nodes using very minimal resources.

- *Collision.* Collisions can be created by subverted nodes using minimal amount of energy [5]. These attacks could cause the networks involvement in expensive back offs resulting in failure to perform functions. Error correcting codes could provide a counter measure against these attacks; however, they need the full cooperation of all nodes in the network.
- *Exhaustion.* A subverted node could continually invoke requests to communicate with other nodes are provoke responses, thereby exhausting the limited power resources of the node [5]. Rate limiting could effectively work around these types of attacks.

3) Network Layer DoS Attacks

The network layer plays a critical role in sensor networks. In the absence of routing infrastructure in these networks, all nodes are expected to route vital information at some point or the other. Attacks on protocols in this layer can severely debilitate the functioning of the networks. Some of the vulnerabilities are discussed below [5]:

- *Neglect and Greed.* Subverted or malicious nodes could participate in exchange of some data / information between neighbors but choose to drop important information, not routing it to its intended destination. On the other hand, a malicious node could broadcast itself as the shortest route to the destination, thereby attracting all traffic creating congestion around it. Counter measures include using multiple routing paths and / or redundant messages.
- *Homing.* This involves targeting nodes that have special responsibilities in a locality. As these nodes provide critical services, they are likely candidates for attack. Once subverted, location and presence of critical resources is divulged.
- *Misdirection.* This is a more active attack in which malicious nodes can misdirect traffic along wrong paths by advertising wrong routes. Only authorized nodes exchanging routing information can be an effective counter measure against this type of attack.
- *Black Holes.* Malicious nodes in networks using distance vector routing protocols can advertising zero-cost routes to other nodes. This results in all nodes directing traffic to this adversary node, thereby exhausting resources of the neighboring nodes creating a black hole. Again, authorized exchange of routing information can be a deterrent to this type of attack.

4) Transport Layer DoS Attacks

Attacks on protocols in this layer aim at disrupting reliable communication between two sensors. Types of DoS attack could be [5]:

- *Flooding.* Adversaries can send several connection establishment requests, thereby causing sensors to allocate memory to maintain the connections. A counter measure against this attack is solving client puzzles.
- *De-synchronization.* Malicious nodes can disrupt reliable communication between two nodes by forging messages to the sender and / or receiver, thereby rendering their communication useless. Authentication of each message could counter this attack.

B. Spoofed, Altered or Replayed Routing Information

Routing information exchanged between sensors can be falsified or altered by malicious nodes to attract traffic towards itself. The same can also be done to ward traffic off important routes. Also, routing information can be replayed to loop information in circles amongst the same nodes exhausting their vital energy resources.

Counter measures against these types of attacks is authentication amongst nodes that route traffic during exchange of routing information. This would prevent malicious nodes from establishing themselves within the network and inadvertently getting neighboring nodes to route information to them [6].

C. Selective Forwarding

Routing in sensor networks relies on cooperation of each intermediate node to dedicatedly route all information directed towards it to the next hop. Adversaries can exploit this situation by subverting a node on a path of major data flow and selectively forward only some messages to the next hop.

A counter measure to this is to use redundant routes (multi-path routing) to pass on information. In case one route is compromised due to an adversary, redundant messages can reach the destination and pass on messages.

D. Sinkhole Attacks

Compromised nodes are made attractive to other nodes in the region by advertising incorrect routing information or high quality routes. This prompts most nodes in the area to route their traffic through this subverted node. This malicious node has now created a ‘sink’ in the region and is now handling a lot of traffic crucial to the network.

Now that the subverted node has created a ‘sphere of influence’ attracting traffic to be routed through it, it can perform different types of actions like selective suppression of packets or data modification on information sent from any node in the region.

Notice that sinkhole attacks are particularly of interest in these types of networks as all data is routed to one final destination [6].

Counter Measure

One way to overcome this issue is to implement a hierarchical system of routing information where each region has a leader node and the leader nodes forward information to the base station. If the different nodes switch performing the role of leaders in their regions, it would prevent subversion for a prolonged duration of time.

Another way to work around this attack is to use geographic routing protocols. These protocols use local routing information and dynamically establish routes to the base station. Hence, attraction towards sink holes is minimal.

E. Sybil Attack

In a Sybil Attack, an adversary node assumes multiple identities, thus presenting itself to the network as multiple nodes [6]. This could cause ineffectiveness in a network, especially the ones that implement fault tolerant schemes and ones that uses geographic routing protocols.

Counter Measure

A protocol can be created to counter Sybil attacks. In such protocol, each node is assigned one or more “verified” neighbors. The base station also sets the number of neighbors a node is allowed to have. A node is allowed to route its data through anyone of its neighbors (verified or not). However, the base station keeps track of how many neighbors each node has. If a node has more than the specified upper limit (an indication of a possible Sybil attack), an error message is sent to that node, and it is then only allowed to communicate through its verified neighbors. Neighbor verification can be implemented through digital certificates or any public key crypto system.

F. Wormhole Attack

A wormhole attack is one in which an adversary node tunnels messages from one part of the network to another, usually through a low latency link [6]. This attack is usually performed using two powerful adversary nodes, located at different side of the network, in order to attract traffic. This attack is usually used in conjunction with selective forwarding or eavesdropping.

Counter Measure

Wormhole attacks are hard to detect, simply because in most cases, the communication medium or protocol between the two adversary nodes are unknown. The only way to detect or counter wormhole attacks is to somehow control and verify the hop counts for each message received by the base station. However, this scheme severely limits the self-organizing criteria of an ad-hoc network. Also, it is possible for the adversary nodes to mimic hop counts by altering the routed messages.

Wormhole attack takes advantage of the fact a route is calculated based on hop counts. Hence, one can design a protocol that doesn’t use hop counts, thus deeming the attack meaningless. For example, in a geographic routing protocol, a route is created based on the coordinates of the sending node and intermediate nodes. Unless an adversary node can mimic its location, it is hard for it to attract traffic.

G. HELLO Flood Attack

In many protocols, when a new sensor node is introduced into the network, it broadcasts a HELLO message. Any nodes that can hear the message will reply. Through this mechanism, the new node identifies its neighbors, and also let the neighbors know of its existences. If the new node provides a better route to the base station, its neighbors will change their existing routes such that data is now routed through the new node.

In a HELLO flood attack, a powerful adversary node whose transmission range is farther than a typical node is placed in the network [6]. It broadcasts the HELLO message, advertising a very high quality base station link. Any nodes receiving this message will reply, thinking that a better route can be created through this adversary node. Additionally, due to the high power transmission of the message, it also reaches the nodes that are outside the normal range of a typical node. The target nodes attempt to reply to the adversary node. However, the replies are sent in vain – the target nodes are not able to send messages strong enough to reach their destination.

Counter Measure

The solution for this attack is quite simple. The HELLO protocol can be extended to a three-way handshake [6]. In this protocol, the new node broadcasts a HELLO message. Any receiving nodes that can hear the message send a nonce to new node. The new node must resend the nonce back to each receiving node. The receiving nodes verify the reply with the original nonce to confirm the link. Hence, this protocol guarantees the bi-directionality of a link before any meaningful messages can be sent through it, thus countering the HELLO flood attack.

H. Acknowledgement Spoofing

In most sensor network (and any network for that matter), an acknowledgment is sent by the receiver back to the sender to confirm the safe arrival of the data. However, due to the broadcast medium used by most sensor networks, an adversary node can easily intercept message sent between two parties.

An acknowledgement spoofing attack is one in which an adversary node spoofs an acknowledgement to the sender, even through the message might not be properly received [6]. The goal of this attack is to convince the sender that a weak link is strong or a dead or disabled one is still active.

IV. Conclusion

Due to their communication layers and routing topologies, wireless sensor networks are vulnerable to many different kinds of attacks, many of these are applicable also to general ad-hoc network. Unlike ad-hoc networks, these attacks are complicated by the physical limitations of wireless sensors. Finding suitable solutions for each of these attacks is indeed a very challenging task. However, it is very important that these security problems be solved, knowing that this type of network will soon be applied to military, defense and biological surveillance applications.

REFERENCES

[1] Vierira, Marcos and Silva, Diogenes. "Survey on Wireless Sensor Network Devices". Technical report *IEEE-0-7803-7937/03, Federal University of Minas Gerais,* 2003

[2] Hill, Jason and Culler, David. "System Architecture Directions for Networked Sensors". Technical report ACM 0-89791-88-6 / 97 / 05, University of California, Berkeley, 2004

[3] Archana Bharathidasan, Vijay Anand Sai Ponduru. "Sensor Networks: An Overview". University of California, Davis.

[4] Culpepper, B.J., Dung, L., Moh, M., "Design and Analysis of Hybrid Indirect Transmissions (HIT) for Data Gathering in Wireless Microsensor Networks". *ACM Mobile Computing and Communications Review* (Mc2R), Jan / Feb 2004.

[5] Wood, D. Anthony and Stankovic, A. John. "Denial of Service in Sensor Networks". Technical Report *IEEE-0018-9162/02, University of Virginia,* 2002.

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

[7] P.K. Goel, V.K. Sharma,,"Wireless Sensor Network: Security Model", *International Journal of Science Technology and Management, IJSTM* Vol. 2, Issue 2, ISSN: 2229-6646 (online) , pp 100-107.