ISSN:0975-9646
Alok Ranjan Prusty et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (3) , 2012,4028 - 4037

The Network and Security Analysis for Wireless Sensor Network : A Survey

Alok Ranjan Prusty

Computer Science & Engineering
Koustuv Institute Of Technology (KIT)
Biju Patnaik University of Technology (B.P.U.T), Odisha, India

***Abstract*— A wireless Sensor network(WSN) is a group of sensor nodes cooperating to form a network over a wireless link based on zero fixed network infrastructure. The main idea is to make sensor node cheap and easily deployed every where to create a omnipresent network with smart geographical distribution.WSN become demanding because of its service towards wide range of applications. But constraints are with WSN like ,low computation capability, small memory, limited energy, susceptible to physical capture , lack of infrastructure etc. However along with such constraints, due to operation of sensors round the clock in harsh uncontrolled environment make security as a critical issue and challenge. In this paper I survey the network, different types of attacks, security loop holes ,their consequences and discus the counter measures which will be beneficial for students and researchers in this area .**

***Keywords*— wireless sensor network, applications, protocol stack, security class, security challenges, security attacks, miscellaneous attacks.**

I. INTRODUCTION

The emergence of sensor network as one of the dominant technology in current and coming decade [1] has posed various unique challenges to the researchers .WSN comes to spot light because of its low cost solution for a variety of practical application and real time need. Originally , WSN technology was designed for military monitoring and surveillance with a objective of structuring a system that was cheap , quick to deploy and at the same time hard to destroy. Most common application frame work of WSN range from troop and tank detection at battle field, wild life monitoring, land slide detection, pollutant monitoring, green house monitoring, measuring traffic flow on road, industrial quality control, infrastructure health monitoring etc. Offering of better capability and higher flexibility at a low cost as compared to traditional infrastructure based wired network makes WSN an effective and alternative network solution for mankind.

The basic networked sensor devices in WSN are a radio, a power unit, sensor, embedded processor, memory etc. The ultimate aim of each sensors in WSN is to route collected data to high power sink/base station for user access through internet. The communication architecture and structure of an individual sensor node in WSN is shown in Figure 1. Sometimes, several WSN applications require only an aggregate value to be reported to the observer. In this case, sensors in different regions of the field can collaborate to aggregate their data and provide more accurate reports about
their local regions. For example, in a habitat monitoring application [15].

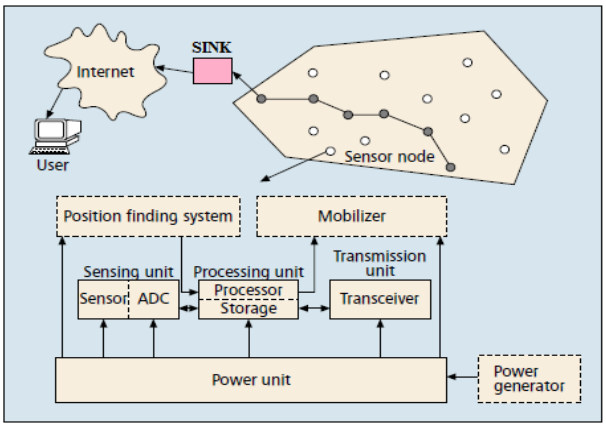


Figure 1:communication architecture of WSN and structure of a individual sensor node

In order to support data aggregation through efficient network organization, nodes can be sometimes partitioned into a number of small groups called clusters. Each cluster has a coordinator, called a cluster head, and a number of member nodes. Clustering results in a two-tier hierarchy in which cluster heads (CHs) form the higher tier while member nodes form the lower tier. Figure 2 illustrates architecture of a clustered sensor network. The member nodes report their data to the respective CHs. The CHs aggregate the data and send them to the Sink/base station directly or through other CHs.

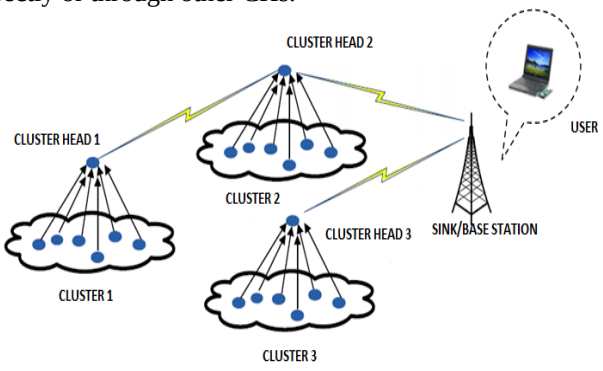


Figure 2: Architecture of a clustered wireless sensor network

Both the sink/base station and sensor nodes uses the protocol stack [2] for working smoothly in the network, the architecture is given in Figure 3. This protocol stack integrates power and routing awareness i.e., energy aware

routing, integrates data with networking protocols i.e., data aggregation or clustering, communicates efficiently through the wireless medium and promotes cooperative efforts of the sensor nodes for better task management . physical layer addresses the needs of a robust modulation, transmission and receiving techniques. The network layer takes care of routing the data supplied by the transport layer. The transport layer helps to maintain the flow of data if the wireless sensor network application requires it.

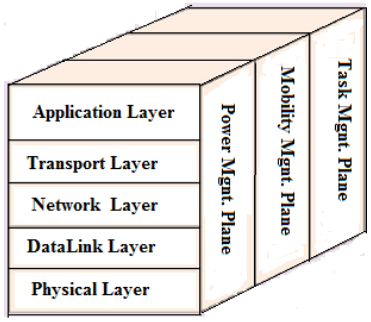


Figure 3: protocol stack architecture

In WSN, the sensing nodes are deployed densely in ad-hoc manner and each node has contact with several other nodes for data collection and communication .The ad-hoc nature of large scale network ,unreliable communication channel, broad cast nature and uncontrolled operation results a new class of network management, routing and security issues. While the deployment of sensor nodes in unattended hostile, physically unprotected environment make the network vulnerable to a variety of potential attack, the inherent power and memory limitation of sensor node makes the conventional security system infeasible .To achieve a secure system security must be integrated in to every components otherwise weak security makes WSN application field very small and limited. Hence for creating a suitable and powerful security system for WSN requires vast knowledge ,understanding and analysis of security threats and attacks .

Section II , deals with security class in WSN. I presented security challenges in WSN in section III. In section IV I have described about the security goals and requirements for WSN. Types of security attack in WSN is shown in section V. The broad view of Passive Attack and Active attack and others are reflected in section VI and VII respectively. Different Miscellaneous attacks counter techniques in WSN is given in section VIII and at last section IX contains the conclusion of this paper.

II. Security Class

Attacks on the computer system or network can be broadly classified [12] as Interruption , Interception., Modification and Fabrication. In normal condition of data communication in a network, the data generated sent by the source node is received by the designated receiver node as shown in Figure: 4. Interruption is an attack on the availability of the network, for example physical capturing of the nodes, message corruption, insertion of malicious code etc. (Figure:5). Interception is an attack on confidentiality. The sensor network can be compromised by an adversary to gain unauthorized access to sensor node or data stored within it (Figure:6). Modification is an attack on integrity. Modification means an unauthorized party not only accesses the data but tampers it, for example by modifying the data packets being transmitted or causing a denial of service attack such as flooding the network with bogus data, presented in Figure :7.

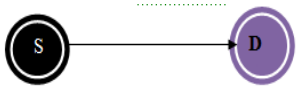


Figure 4 : Normal data communication

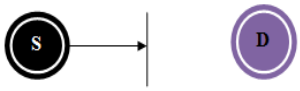


Figure 5 : Interruption

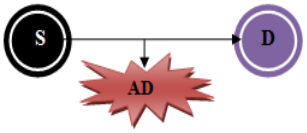


Figure 6 : Interception

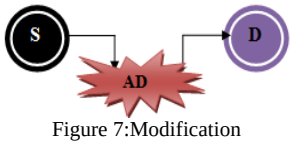


Figure 7:Modification

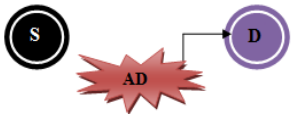


Figure 8 : Fabrication

Fabrication is an attack on authentication. In fabrication, an adversary injects false data and compromises the trust worthiness of the information relayed as shown in Figure:8.

III. Security Challenges In WSN

The networked nature of large, ad-hoc, wireless sensor networks raises new threats and significant challenges in designing security schemes. We are going to present four of the most common challenges in Wireless Sensor Network security.

A. Wireless Medium

The pervasive applications proposed for sensor networks necessitate vast wireless communication links. The wireless medium allows an attacker to easily intercept valid packets and easily inject malicious ones i.e. various forms of data into the network without joining the network .

B. Ad-hoc Deployment

The ad-hoc nature of sensor networks means no structure can be statically defined before hand. The network topology is always subject to changes due to node failure, addition, or mobility. Nodes may be deployed

randomly by air drop, so nothing is known about the topology prior to deployment. The ever changing nature of sensor networks requires more robust designs for security techniques to cope with such dynamics.

C. Hostile Environment

Hostile environment in which functioning of sensor node is a challenge . Depending on the application of the particular sensor network, the sensor nodes may be left unattended for long periods of time. Node compromise occurs when an attacker gains control of a node in the network after deployment. Since nodes may be in a hostile environment, attackers can easily gain physical access to the devices. Once in control of a node, the attacker can alter the node to listen to information in the network, input malicious data or perform a variety of attacks. The attacker may also disassemble the node and extract information vital to the network's security such as routing protocols, data, and cryptographic keys. Generally, compromise occurs once an attacker has found a node, and then directly connects the node to their computer via. a wired connection of some sort. Once connected, the attacker controls the node by extracting the data and/or putting new data or controls on that node.

D. Resource Scarcity

All security approaches require a certain amount of resources for the implementation, including data memory, code space, and energy to power the sensor etc. However, currently these resources are very limited in a tiny wireless sensor. Energy is the biggest constraint as well as most precious resource to wireless sensor capabilities. The extra power consumed by sensor nodes due to security is related to the processing required for security functions, the energy required to transmit and store the security related data/parameters. The radio is typically the largest energy consumer of the sensor node, both when sending and receiving. Minimizing the listening time, the number of packets and the size of each packet are important to preserve battery power.

IV. Security Goals And Requirements For WSN

The security goals are classified as primary and secondary [20]. The primary goals are known as standard security goals such as data confidentiality, data authentication. data integrity, data availability and the secondary goals are data freshness, self organization, time synchronization, secure localization etc.

A. Data Confidentiality

Confidentiality is the ability to conceal messages from a attacker so that any message communicated via. the sensor network remains confidential. Confidentiality protection ensure that an attacker cannot read data being transferred. The standard approach for keeping sensitive data secret is to encrypt the data with a secret key that only intended receivers possess.

B. Data Authentication

Authentication ensures the reliability of the message by identifying its origin. Authenticity protection tells that the source of the data is possible to trace. Attacks in sensor networks do not just involve the alteration of packets, adversaries can also inject additional false packets [24]. Data authentication verifies the identity of the genuine senders and receivers. Data authentication is achieved through symmetric or asymmetric mechanisms where sending and receiving nodes share secret keys

C. Data Integrity

Data integrity ensures and confirms that a message sent from one node to another is not tampered, altered or modified by malicious intermediate nodes.

The integrity of the network will be in trouble when:

1) A malicious node present in the network injects false data.

2) Unstable conditions due to wireless channel cause damage or loss of data.

D. Data Availability

Data 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/sink or cluster head’s availability will eventually threaten the entire sensor network. Thus availability is of primary essential for maintaining an operational sensor network.

E. Data Freshness

Data freshness ensure that the data being transferred has not been sent before. Even if confidentiality and data integrity are assured, there is a need to ensure the freshness of each message. Freshness protection prevents replay attacks, where an attacker captures and later resends a packet with correct authenticity and integrity codes. To solve this problem a time related freshness counter, can be added into the packets.

F. Self Organization

There is no fixed infrastructure available for the purpose of network management in a sensor network. A wireless sensor network[24] is a typically an densely deployed ad hoc network, which requires every sensor node be independent and flexible enough to be self-organizing and self-healing according to different situations. 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 pair wise sensors. Most sensor network applications rely on some form of time synchronization. In order to conserve power, an individual sensor’s radio may

be turned off for periods of time. A more collaborative sensor network may require group synchronization [23] for tracking applications. The authors in [20] propose a set of secure synchronization protocols for sender and receiver in WSN.

H. Secure Localization

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 pin point the location of a fault. Unfortunately, an attacker can easily manipulate non secured location information by reporting false signal strengths and replaying signals.

In addition, WSNs have following specific security objects ,like:

1) *Forward secrecy*: Preventing a node from decrypting/able to read any future secret messages after it leaves the network

2) *Backward secrecy*: Preventing a joining node from decrypting any previously transmitted secret message

3) *Survivability*: Providing a certain level of service in the presence of failures or attacks.

V. Types Of Security Attack

Security attacks can be classified into two major categories, according to the interruption of communication act , namely Passive attacks and Active attacks. Figure:9 shows the classification of attacks under general categories.

A. Passive Attacks

The monitoring and listening of the communication channel by unauthorized attackers are known as passive attack. The Attacks against privacy is passive in nature. To a passive attack it is said that the attacker obtain data exchanged in the network without interrupting the communication.

B. Active Attacks

The unauthorized attacker monitors, listens to and modifies the data stream in the communication channel are known as active attack. Meaning is when it is referred to an active attack it can be affirmed that the attack implies the disruption of the normal functionality of the network by information interruption and modification etc.

Other categories of attacks can be, *Outsider attacks* where attacks from nodes which do not belong to home WSN. *Insider attacks* occur when legitimate nodes of a WSN behave in unintended or unauthorized ways. 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 may be a laptop to attack a WSN. These devices have greater transmission range, processing power, and energy reserves than the network nodes.

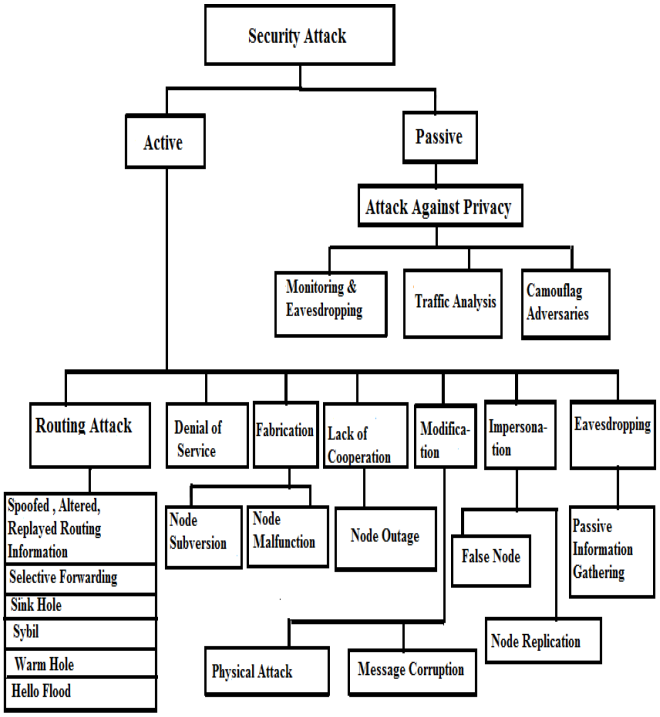


Figure 9: The classification of attacks under general categories.

VI. Passive Attack Type

A. Attack Against Privacy

Sensor networks intensify the privacy problem because they make large volumes of information easily available through remote access. Hence, adversaries need not be physically present to maintain surveillance. They can gather information at low risk in anonymous manner. Some of the more common attacks[23] against sensor privacy are,

1) *Monitor and Eavesdropping:* This is the most common attack to privacy where intercepting and reading of messages and conversations by unintended receivers occurs. By snooping to the data, the adversary could easily discover and read the communication contents.

2) *Traffic Analysis:* Data gathered by the individual nodes ultimately routed to the base station. In [17] traffic analysis attack classified as two types, A rate monitoring attack simply makes use of the idea that nodes closest to the base station tend to forward more packets than those farther away from the base station. An attacker need only monitor which nodes are sending packets and follow those nodes that are sending the most packets. In time correlation attack where an adversary simply generates events and monitors to whom a node sends its packets.

3) *Camouflage Adversaries:* Here, one can insert their node or compromise the nodes to hide in the sensor network. After that these nodes can copy as a normal node to attract the packets, then misroute the packets, conducting the privacy analysis etc.

VII. ACTIVE ATTACK TYPE

There are several active class of attacks that may affect the healthy wireless sensor network. Generally, most of the active attacks are routing attacks types which occurs in the network layer of protocol stack in WSN. The following are the attacks that happen while routing the messages.

A. *Spoofed, Altered And Replayed Routing Information*

Spoofing means pretending to be something you are not. An attacker may spoof, alter, or replay routing information in order to disrupt traffic in the network [7].Due to the open nature of the wireless medium, it is easy for adversaries(AD) to monitor communications to find Media Access Control (MAC) addresses of the other entities.MAC address is typically used as a unique identifier for all the nodes on the network. Further, for most commodity wireless devices, attackers can easily forge their MAC address in order to masquerade as another transmitter. As a result, these attackers appear to the network as if they are a different device. Such spoofing attacks can have a serious impact on the network performance as well as facilitate many forms of security weaknesses, such as attacks on access control mechanisms in access points [13], and denial-of-service through a de authentication attack [14]. An unprotected ad-hoc routing is vulnerable to these types of attacks, as every node acts as a router, and can therefore directly affect routing information by following,(Figure:10)

1) *Create routing loops*
2) *Extend or shorten service routes*
3) *Generate false error messages*
4) *Increase end-to-end latency* [2]

Adversaries may be able to create routing loops, attract or repel network traffic, extend or shorten source routes, generate false error messages, partition the network, and increase end-to-end latency.

The standard solution to address potential spoofing attacks, is the conventional authentication check approach. However, the application of authentication requires reliable key distribution, management, and maintenance mechanisms. It is not always desirable to apply authentication because of its infrastructural, computational, and management overhead.

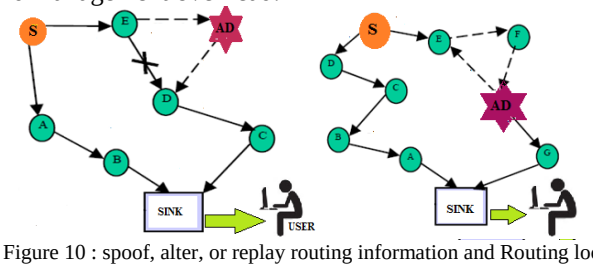
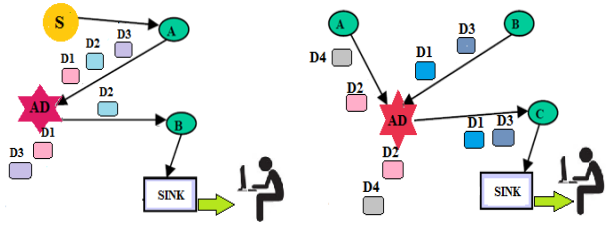


Figure 10 : spoof, alter, or replay routing information and Routing loop

Further, cryptographic methods are susceptible to node compromise, a serious concern as most wireless nodes are easily accessible i.e. allowing their memory to be easily scanned.

B. *Selective Forwarding*

A malicious node can selectively drop only certain packets. Especially effective if combined with an attack that gathers much traffic via. the node. In sensor networks it is assumed that nodes faithfully forward received messages. But some compromised node might refuse to forward packets, however neighbours might start using another route.[8]. A significant assumption made in multi hop networks is that all nodes in the network will accurately forward received messages[7].Multi-hop mode of communication is commonly preferred in wireless sensor network data gathering protocols. Multi-hop networks assume that participating nodes will faithfully forward and receive messages. However a malicious node may refuse to forward certain messages and simply drop them, ensuring that they are not propagated any further. This attack can be detected if packet sequence numbers are checked properly and continuously in a conjunction free network. Addition of data packet sequence number in packet header can reduce this attack. Figure 11(i), source node 'S' forwards its data packet D1, D2, D3 to node 'A' and node 'A' forward these received packets to node 'B'. In other hand an adversary node AD selectively forwards packets D2 while dropping packet D1 and D3. In another scenario shown in Figure.11(ii), an adversary may selectively drop packets originated from one source and forward that of others. One defence against selective forwarding attacks is using multiple paths to send data [7]. A second defence is to detect the malicious node or assume it has failed and seek an alternative route.



(i) (ii)

Figure 11: selective forwarding (i) and (ii)

C. *Sinkhole Attack*

The sinkhole attack is a particularly severe attack that prevents the sink/base station from obtaining complete and correct sensing data, thus forming a serious threat to higher-layer applications. In a Sinkhole attack , a compromised node tries to draw all or as much traffic as possible from a particular area, by making itself look attractive to the surrounding nodes with respect to the routing metric. The end result is that surrounding nodes will choose the compromised node as the next node to route their data through to the sink. The attacker always 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. By taking part in the routing process, it can then launch more severe attacks, like selective forwarding, modifying or even dropping the packets coming through. 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 neighbouring nodes uses a unique key to initialize frequency hopping or spread spectrum communication. Sinkholes are difficult to defend in protocols that use advertised information such as remaining energy or an estimate of end-to-end reliability to construct a routing topology because this information is hard to verify. The Figure 12 is showing the sinkhole attack where 'SH' is a sinkhole. This sinkhole attracts traffic from nearly all the nodes to rout through it.

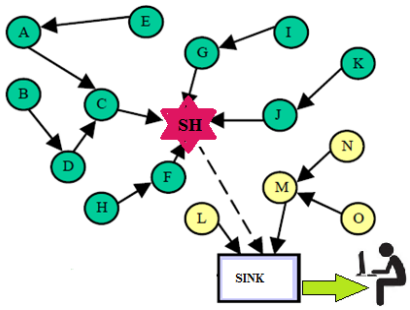


Figure 12: sink hole attack

D. Sybil Attacks

Sybil attack is defined as a malicious device illegitimately taking on multiple identities[19]. In a Sybil attack, a single node presents multiple identities to other nodes in the network. This attack can occur in a distributed system that operates without a central authority to verify the identities of each communicating entity [10]. Each entity is only aware of others through messages over a communication channel, it was originally described as an attack able to defeat the redundancy mechanisms of distributed data storage systems in peer-to-peer networks [18].A Sybil attacker can assume many different identities by sending messages with different identifiers. An entity in the system can attempt to determine if some set of entities are distinct by testing their resource limits, but this is not so easy task. If a single Sybil attacker pretends to be multiple entities, it may not have the same computational, storage, and bandwidth capabilities as multiple independent entities. However, testing based on such an assumption requires an accurate model of the attacker's resources.

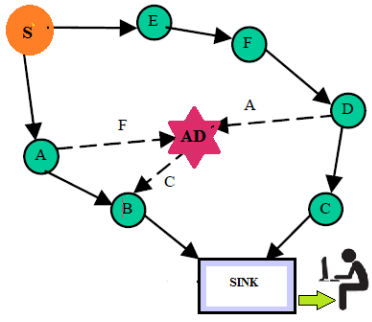


Figure 13: sybil attack

A Sybil attacker that has more resources than expected can impersonate a number of entities proportional to the amount of its resources are under estimated. Similarly, a set of entities that are more resource constrained than expected may fail to prove their independence. The testing entity might also attempt to verify identity and independence indirectly by asking entities to vouch for each other. This strategy is prone to the Sybil attack because multiple entities can be the multiple identities of one or more Sybil attackers. Sybil attacks can pose a significant threat to geographic routing protocols. Location aware routing often requires nodes to exchange coordinate information with their neighbours to construct the network. So it expects nodes to be present with a single set of coordinates, but by using the Sybil attack an adversary can ''be in more than one place at once''. Since identity fraud leads to the Sybil attack, proper authentication and encryption techniques can prevent an outsider to launch a Sybil attack on the sensor network.. The Figure 13 tells about the Sybil attack where an adversary node 'AD' is present with multiple identities. 'AD' appears as node 'F' for 'A', 'C' for 'B' and 'A' as to 'D' so when 'A' wants to communicate with 'F' it sends the message to 'AD'.

E. Wormholes Attacks

A wormhole is a low latency link between two portions of the network over which an attacker replays network messages.In the wormhole attack, an attacker records packets (or bits) at one location in the network, tunnels them to another location, and retransmits them into the network. Here, an adversary (AD) receives packets at one location in the network and tunnels them (possibly selectively) to another location in the network, where the packets are resent into the network. The link through the tunnel may be established either by a single node forwarding messages between two adjacent but otherwise non neighbouring nodes or by a pair of nodes in different parts of the network communicating with each other. Thus the high speed off-channel false route established through tunnel would shorten the hop distance between any two non malicious nodes. Wormhole attackers can make far apart nodes believe they are immediate neighbours, and force all communications between affected nodes to go though them. A wormhole attack is equally dangerous for both proactive and on-demand protocols[9]. A wormhole link is simply unreliable, as there is no way to protect what the attackers can do and when.

Wormholes are effective even if routing information is authenticated or encrypted. This attack can be launched by insiders and outsiders. 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 it if alternate routes are significantly less attractive. When this attack is coupled with selective forwarding and the Sybil attack it is very difficult to detect. Figure 14 demonstrates Wormhole attack where 'WH' is the adversary node which creates a tunnel between nodes 'E' and 'I'. These two nodes are present at most distance from each other. Moreover, 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.

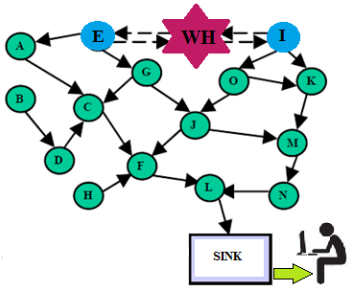


Figure 14: wormhole attack

This can be prevented by avoiding routing race conditions. The solution requires clock synchronization and accurate location verification, which may limit its applicability to WSNs.

F. HELLO Flood Attacks

Many routing protocols in WSN require nodes to broadcast hello messages to announce themselves to their neighbours. A node which receives such a message may assume that it is within a radio range of the sender. However in some cases this assumption may be false; sometimes a attacker broadcasting routing or other information with large enough transmission power could convince every other node in the network that the attacker is its neighbour. Like, an adversary advertising a very high quality route to the base station could cause a large number of nodes in the network to attempt to use this route. But those nodes which are sufficiently far away from the adversary would be sending the packets into oblivion. Hence the network is left in a state of confusion. Protocols which depend on localized information exchange between neighbouring nodes for topology maintenance or flow control are mainly affected by this type of attack. [10] An attacker does not necessarily need to construct legitimate traffic in order to use the hello flood attack. 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 neighbour. 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 neighbour and are ultimately spoofed by the attacker.[8]. HELLO floods can also be thought of as one-way, broadcast wormholes. The Figure 15(iii) depicts how an adversary node 'AD' broadcast hello packets to convince nodes in the network as neighbour of 'AD'. Though some node like I,H,F are far away from 'AD' they think 'AD' as their neighbour and try to forward packets through it which results in wastage of energy and data loss. This attack can be defended by verifying the bi directionality of local links before using them is effective if the attacker possesses the same reception capabilities as the sensor devices. Another way by using Authenticated broadcast protocols

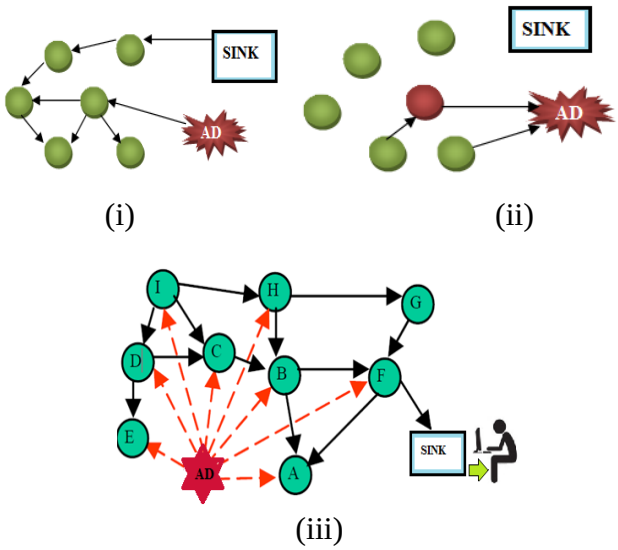


Figure 15: HELLO Flood attack

G. Denial of Service

Denial of Service attacks were first used to "have fun", get some kind of revenge from system operators or make complex attacks possible, With time and as the networking gets more required in communication system, hacktivism and Denial of Service gradually become a extortion. A Denial-of service attack (DoS attack) or distributed denial-of service attack (DDoS attack) is basically an attempt to make a computer resource unavailable to its intended users. 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 temporarily or indefinitely to provide a service. Perpetrators of DoS attacks typically target sites or services hosted on high profile web servers such as banks, credit card payment gateways, and even root name servers.

In WSN Denial of Service (DoS) is produced by the unintentional failure of nodes or malicious action. A small example is a sensor network designed to alert building occupants in the event of a fire could be highly susceptible to a denial of service attack. Even worse, such an attack could result in the deaths of building occupants due to the non-operational fire detection network. In WSN, 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.

H. Node Subversion

Capture of a node may reveal its information including disclosure of cryptographic keys and thus compromise the whole sensor network. A particular sensor might be captured, and information (key) stored on it might be obtained by an adversary[6].

I. Node Malfunction

A malfunctioning node will generate inaccurate data that could expose the integrity of sensor network especially if it is a data aggregating node such as a cluster leader [3].

J. Node Outage

Node outage is the situation that occurs when a node stops its function. In the case where a cluster leader stops functioning, the sensor network protocols should be robust enough to mitigate the effects of node outages by providing an alternate route [3].

K. Physical Attacks

Sensor networks typically operate in hostile outdoor environments. In such environments, the small form factor of the sensors, coupled with the unattended and distributed nature of their deployment make them highly susceptible to physical attacks, i.e., threats due to physical node destructions. Unlike many other attacks mentioned above, physical attacks destroy sensors permanently, so the losses are irreversible. For instance, attackers can extract cryptographic secrets, tamper with the associated circuitry, modify programming in the sensors, or replace them with malicious sensors under the control of the attacker.

L. Message Corruption

Any modification of the content of a message by an attacker compromises its integrity.[21]

M. False Node

A false node involves the addition of a node by an adversary and causes the injection of malicious data. An intruder might add a node to the system that feeds false data or prevents the passage of true data. Insertion of malicious node is one of the most dangerous attacks that can occur. Malicious code injected in the network could spread to all nodes, potentially destroying the whole network, or even worse, taking over the network on behalf of an adversary.[21]

N. Node Replication Attacks

This is an attack where attacker tries to mount several nodes with same identity at different places of the existing network. There are two methods for mounting this attack. In first method the attacker captures one node from the network and creates clone of a captured node and mounts in different places of the network. In second method attacker may generate a false identification of a node then makes clone out of this node and mounts in different places of the network. These mounted clone nodes tries to generates false data to disrupt the network. Node replication attack is different form Sybil attack. In Sybil attack a single node exists with multiple identities but in node replication attack multiple nodes present with same identity. Therefore in sybil attack an attacker can succeed by mounting only a single node where as node replication attack requires more node to be mounted throughout the network this increases the chance of detection. This attack can be avoided if we centrally compute the data gathering path by the BS then multiple place occurrence of the node can be detected. The other way to detect the attack is verifying the identities (authentication) of nodes by a trustworthy node. In the Figure:16, N is the identity of cloned nodes which are mounted in multiple places in the network to bias the entire network. The node replication approach can severely disrupt a sensor network's performance. Packets can be corrupted or even misrouted. This can result in a disconnected network, false sensor readings, etc.

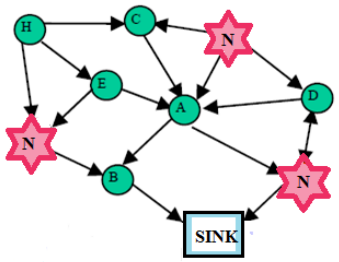


Figure 16: Node replication attack

If an attacker can gain physical access to the entire network he can copy cryptographic keys to the replicated sensor nodes. By inserting the replicated nodes at specific network points, the attacker could easily manipulate a specific segment of the network, perhaps by disconnecting it altogether.

O. Passive Information Gathering

An adversary with powerful resources can collect information from the sensor networks if it is not encrypted. An intruder with an appropriately powerful receiver and well designed antenna can easily pick off the data stream. Interception of the messages containing the physical locations of sensor nodes allows an attacker to locate the nodes and destroy them. Besides the locations of sensor nodes, an adversary can observe the application specific content of messages including message IDs, timestamps and other fields. To minimize the threats of passive information gathering, strong encryption techniques needs to be used.[34].

P. Flooding Attack

According to [4] and [12], at Transport layer, a protocol is required to maintain state at either end of a connection. An adversaries can exploit the protocols that maintain state at either end of the connection. For example, adversary sends many connection establishment requests to the victim node to exhaust its resources causing the Flooding attack. One solution against this attack is to limit the number of connections that a node can make. But, this can prevent legitimate nodes to connect to the victim node. Another solution is based on the client puzzles idea described in [22]. According to this idea, if a node wants to connect with other node, it at first must solve a puzzle. An attacker does not likely have infinite resources and it is not possible for him to make connections fast enough to exhaust a serving node. Though solving puzzle includes processing overhead, it is more desirable than excessive communication.

Q. De synchronization Attack

De-synchronization refers to the disruption of an existing connection [5]. An attacker repeatedly forges messages to one or both end points of an active connection with fake sequence number or control flag. Thus attackers desynchronize the end points so that sensor nodes retransmit messages and waste their energy. One countermeasure against this attack is to authenticate all the packets exchanged between sensor nodes along with all the control fields in transport header. The adversary cannot spoof the packets and header and thus this attack can be prevented.

VIII. MISCELLANEOUS ATTACK IN WSN

A. 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. To minimize the damage caused by this attack fabricated reports should be dropped en-route as early as possible.

B. Data Integrity Attack

Data integrity attacks compromise the data travelling among the nodes in WSN by changing the data contained within the packets or injecting false data. The attacker node must have more processing, memory and energy than the sensor nodes. The goals of this attack are to falsify sensor data and by doing so compromise the victim's research. It also falsifies routing data in order to disrupt the sensor network's normal operation, possibly making it useless. This is considered to be a type of denial of service attack. This attack can be defended by adapting asymmetric key system that is used for encryption or we can use digital signatures, but this requires a lot of additional overhead and is difficult to adapt in WSN.

C. Sniffing attack

Sniffing attack is a good example of interception or listen in channel attack. In this attack an adversary node is placed in the proximity of the sensor grid to capture data. The collected data is transferred to the intruder by some means for further processing. This type of attack will not affect the normal functioning of the protocol. An outside attacker can lunch this attack for gather valuable data from the sensors. Often this attack is related to military or industrial secrets. The attack is based on the inherit vulnerability of the wireless networks of having unsecured and shared medium. Sniffing attacks can be prevented by using proper encryption techniques for communication.

D. Interference and Jamming

Radio signals can be jammed or interfered with, which causes the message to be corrupted or lost. If the attacker has a powerful transmitter, a signal can be generated that will be strong enough to overwhelm the targeted signals and disrupt communications. The most common types of this form of signal jamming are random noise and pulse. Jamming equipment is readily available. In addition, jamming attacks can be mounted from a location remote to the target networks.

E. Rushing attack

Two colluded attackers use the tunnel procedure to form a wormhole. If a fast transmission path (e.g. a dedicated channel shared by attackers) exists between the two ends of the wormhole, the tunnelled packets can propagate faster than those through a normal multi-hop route. This forms the rushing attack. The rushing attack can act as an effective denial of service attack against all currently proposed on demand WSN routing protocols, including protocols that were designed to be secure.

F. Resource consumption attack

This is also known as the sleep deprivation attack. An attacker or a compromised node can attempt to consume battery life by requesting excessive route discovery, or by forwarding unnecessary packets to the victim node. Energy drain attack is an example of such attack.

G. Location disclosure attack

An attacker reveals information regarding the location of nodes or the structure of the network. It gathers the node location information, such as a route map, and then plans further attack scenarios. Traffic analysis, one of the subtlest security attacks against WSN, is unsolved. Adversaries try to figure out the identities of communication parties and analyse traffic to learn the network traffic pattern and track changes in the traffic pattern. The leakage of such information is devastating in security sensitive scenarios.

H. Malicious code attacks

Malicious code, such as viruses, worms, spywares, and Trojan Horses, can attack both operating systems and user applications. These malicious programs usually can spread themselves through the network and cause the computer system and networks to slow down or even damaged.

I. Repudiation attacks

Repudiation refers to a denial of participation in all or part of the communication.

Table I shows the layer wise attacks, security threats and defence mechanism required.

TABLE I
LAYER WISE ATTACK AND DEFENCE MECHANISM

THREAT	LAYER	DEFENCE MECHANISM
Jamming	Physical	Spread spectrum , Lower duty cycle, Tamper proof, key management scheme. effective ,key management scheme. 13 mm (0.51 in)
Tampering		
Exhausting	Link	Rate limitation
Collision		Error correcting code
Route information manipulating	Network	Authentication Encryption
Selective forwarding		Redundancy Probing
Sybil		Authentication
Sink hole		Authentication, Monitoring, Redundancy
Warm hole		Flexible Routing, Monitoring
Hello flood		Two way authentication, Three way handshaking.
Flooding De-synchronization	Transport	Limiting connection number, Client puzzle
Clone Attack	Application	Unique pair wise key

IX. CONCLUSION

The deployment of sensor node in a unprotected harsh environment creates different security loop holes in the network. But the wide application field of WSN encourage and motivate the researchers to make WSN more and more secure. This paper summarizes the understanding of wireless sensor network concepts, challenges, different security threats, network attacks, attack classification and counter measures for those security lapses. This survey will definitely create interest among the students and future researchers to dream about a reliable, robust and safer wireless sensor network .

ACKNOWLEDGEMENT

I like to thank my parents and my elder brother Er. Nilamani Prusty (Aircraft Engineer, AIRBUS) for continuous encouragement and support.

REFERENCES

[1]. Adrian Perrig, John Stankovic, David Wagner, "Security in Wireless Sensor Networks" Communications of the ACM, Page53-57, year 2004.
[2]. Avancha, S. et al. "Wireless Sensor Networks," Kluwer Academic/Springer Verlag Publishers, 2003 .
[3]. A.K.S Pathan,; Hyung-Woo Lee; Choong Seon Hong, "Security in wireless sensor networks: issues and challenges" Advanced Communication Technology (ICACT), Page(s):6, year 2006.
[4]. A. Wood and J. Stankovic. Denial of service in sensor networks. In Computer, volume 35, page 54U˝ 62, 2002.
[5]. A.D. Wood and J.A. Stankovic, "Denial of service in sensor networks", IEEE Computer, Vol. 35, No. 10, pp. 54-62, 2002.
[6]. Bo-Cang Peng, Chiu-Kuo Liang, (2006), Prevention Techniques for Flooding Attacks in Ad Hoc Networks, IEEE.
[7]. C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Proc. First IEEE Int'l. Wksp. Sensor Network Protocols and Applications, May 2003,pp. 113–27.
[8]. C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," in Proc. of 1st IEEE International Workshop on Sensor Network Protocols and Applications, May 2003.
[9]. D. Agrawal N. Shrivastava, C. Buragohain and S. Suri. Medians and beyond: new aggregation techniques for sensor networks. Proceedings of the 2nd inter- national conference on Embedded networked sensor systems, pages 239{249, 2004. ACM Press.
[10]. Dr. Moh. Osama K., (2007),Hello flood counter measure for wireless sensor network, International Journal of Computer Science and Security, volume (2) issue (3).
[11]. D. Agrawal N. Shrivastava, C. Buragohain and S. Suri. Medians and beyond: new aggregation techniques for sensor networks. Proceedings of the 2nd inter- national conference on Embedded networked sensor systems, pages 239{249, 2004. ACM Press.
[12]. D. R. Raymond and S. F. Midkiff. Denial-of-service in wireless sensor networks: Attacks and defenses. In IEEE Pervasive Computing, volume 7, pages 74–81, 2008.
[13]. F. Zhao and L. Guibas, Wireless Sensor Networks, Elsevier, 2004, pp.1-20.
[14]. Guo Bin,Li Zhe, "United voting dynamic cluster routing algorithm based on residual energy in wireless sensor networks". Journal of Electronics & Information Technology. 2007,29(12).pp:3006-3010
[15]. "Habitat Monitoring on Great Duck Island," http://www.greatduck island.net/, 2006.
[16]. 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.
[17]. J. Deng, R. Han, and S. Mishra. Countermeasuers against traffic analysis in wireless sensor networks. Technical Report CU-CS-987-04, University of Colorado at Boulder, 2004.
[18]. J. Douceur. The sybil attack. In Proc. of the 1st International Workshop on Peer-to-Peer Systems (IPTPS'02), February 2002.
[19]. J. Newsome, E. Shi, D. Song, and A. Perrig. The sybil attack in sensor networks: analysis & defenses. In Proceedings of the third international symposium on Information processing in sensor networks, pages 259–268. ACM Press, 2004.
[20]. S. Ganeriwal, S. ˇCapkun, C.-C. Han, and M. B. Srivastava. Secure time synchronization service for sensor networks. In WiSe '05: Proceedings of the 4th ACM workshop on Wireless security, pages 97–106, New York, NY, USA, 2005. ACM Press.
[21]. T.Zia; A. Zomaya, "Security Issues in Wireless Sensor Networks", Systems and Networks Communications (ICSNC) Page(s):40 – 40, year 2006 .
[22]. T. Aura, P. Nikander, and J. Leiwo. Dos-resistant authentication with client puzzles. pages 170 177. 2001.
[23]. Undercoffer, J., Avancha, S., Joshi, A. and Pinkston, J. "Security for sensor networks". In Proceedings of the CADIP Research Symposium, University of Maryland, Baltimore County, USA, year 2002 http://www.cs.sfu.ca/~angiez/personal/paper/sensor-ids.pdf.
[24]. Y. Wang, G. Attebury, and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks," IEEE Commun. Surveys Tutorials, vol. 8, pp. 2–23, year 2006.