IJCSE International Journal of Computer Sciences and Engineering Open Access

Review Paper Volume-4, Issue-5 E-ISSN: 2347-2693

# Attacks in Wireless Sensor Network- A Review

Amandeep Kaur[1*] and Sandeep Singh Kang[2]

[1,2]Department of Computer Science and Engineering
Global Institute of Management & Emerging Technologies, Amritsar (PUNJAB)

Available online at: www.ijcseonline.org

Received: Apr/17/2016 Revised: May/01/2016 Accepted: May/19/2016 Published: May/31/2016

**Abstract— In wireless multi-hop sensor networks, an intruder may launch some attacks due to packet dropping in order to disrupt the communication. To tolerate or mitigate such attacks, some of the schemes have been proposed. But very few can effectively and efficiently identify the intruders. The Packet Droppers and Modifiers are common attacks in wireless sensor networks. It is very difficult to identify such attacks and this attack interrupts the communication in wireless multi-hop sensor networks. Today wireless communication technique has become an essential tool in any application that requires communication between one or more sender(s) and multiple receivers. Since multiple users can use this technique simultaneously over a single channel, security has become a huge concern. Even though there are numerous ways to secure a wireless network and protect the network from numerous attacks, providing 100% security and maintaining confidentiality is a huge challenge in recent trends. This paper is all about various attacks that can affect WSN. Some attacks disturb nodes, some disturbs network, some drops packets, some theft information. Different remedies and precautions are taken to overcome different attacks.**

***Keywords*- WSN, Node, Routing, Attack.**

## I. INTRODUCTION

The Simplicity in Wireless Sensor Network with resource constrained nodes makes them extremely vulnerable to variety of attacks. In a Wireless sensor networks sensor nodes monitor the environment, detect events of interest, produce data and collaborate in forwarding the data towards to a sink, which could be a gateway, base station or storage node. Securing the Wireless Sensor Networks need to make the network support all security properties: confidentiality, integrity, authenticity and availability. A sensor network is often deployed in an unattended and hostile environment to perform the monitoring and data collection tasks. When it is deployed in such an environment, it lacks physical protection and is subject to node compromise. After compromising one or multiple sensor nodes, an adversary may launch various attacks to disrupt the in-network communication. Among these attacks, two common ones are dropping packets and modifying packets, i.e., compromised nodes drop or modify the packets that they are supposed to forward. Sensor networks consist of hundreds or thousands of sensor nodes as in Figure 1. Each node represents a potential point of attack, making it impractical to monitor and protect each individual sensor from either physical or logical attack. The networks may be dispersed over a large area, further exposing them to attackers who capture and reprogram individual sensor nodes. Attackers can also obtain their own commodity sensor nodes and induce the network to accept them as legitimate nodes, or they can claim multiple identities for an altered node. Once in control of a few nodes inside the network, the adversary can then mount a variety of attacks.

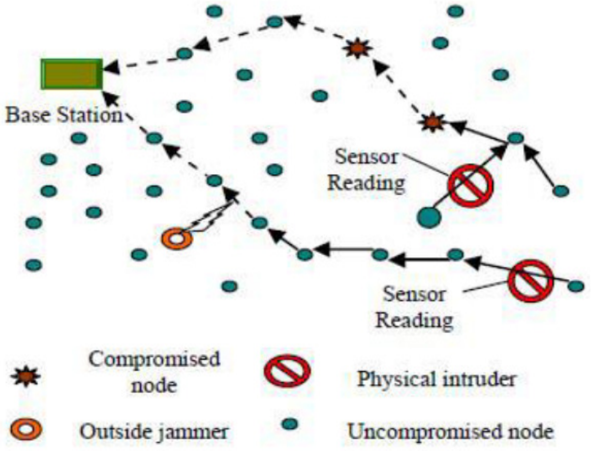

Figure 1- Sensor Network

## II. SOLUTION AND IMPACT OF ATTACKS SOURCE LOCATION PRIVACY

### *A.* Fake Node and Dummy packets

First technique uses fake source with that node sending fake event packets to confuse the adversary. Fake event is basically a dummy message that message is created by another node than a source location. Fake node is sent message request at real node to capture credential information. Sometime adversary does not know which real packet to follow. Fake source node is injecting fake message into network and thus diffuse the source of message. It is using flooding protocol to generate more fake packet in network. Fake node has been created fake node identity and packet does not mention any source and destination identity. It is randomly transmitted any direction in sensor area. content privacy threats generate due to the ability of the adversary to observe and manipulate the content of packet being sent over the wireless sensor network .It is efficiently create fake source and define the optimal message generation rate. Flooding technique is energy consuming and there is the possibility of adversary backtracking to the source node. Real node can use cryptography technique for source location privacy.

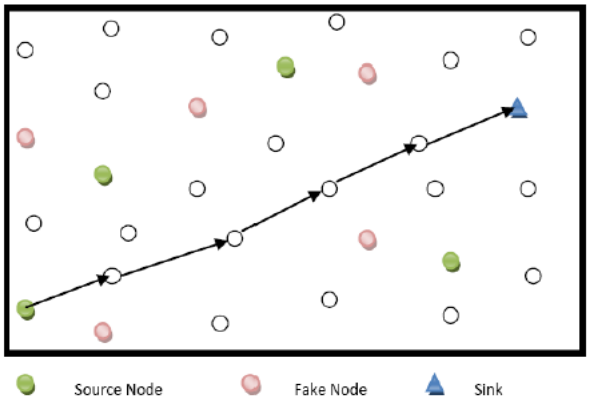

Figure 2- Fake node and Packet

### *B.* Cluster Based Anonymization

It is used for to hide real identity for source node and packet over network. It gives random identity for each and every source node in sensor area. Adversary finds out the source ID by reading the header information, but adversary cannot find real identity .It gets to know only the pseudo identity number which is not linked with source location. Adversary cannot distinguish a source in the observed area. There are divided in different category namely packet anonymization, cluster based anonymity, hash based randomization, cryptographic technique anonymity. Source location anonymity have own identity to represent divert for adversary.

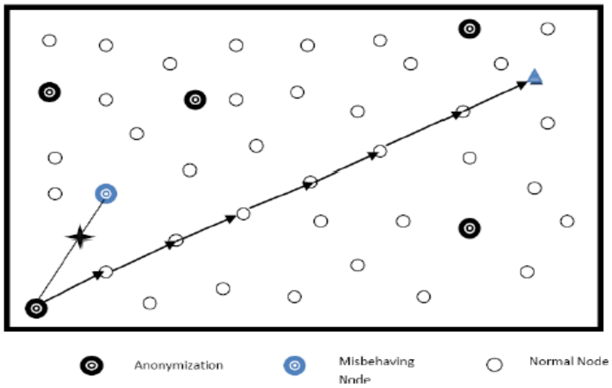

Figure 3- Cluster Based Anonymization

### *C.* Routing based source location privacy

It develops a model to quantitatively measure source location credential information leakage for routing based source location privacy schema. The main idea is to protect the adversaries from tracing back to the source location through traffic monitoring and analysis. Routing based protocol is the phantom routing protocol. It is used two phase routing schema to protect routing based source location information. Message is selected random path forward to actual destination node. Direction information must be stored in the messages header. Intermediate node is selected random path to transfer next forward node on the routing path along the same direction. Adversary can trace message on network mixing ring using fake packet. It possible for adversary to monitor and link all message from the same source node which may help the adversary to identify the source location, ID is corresponding to the grid location.

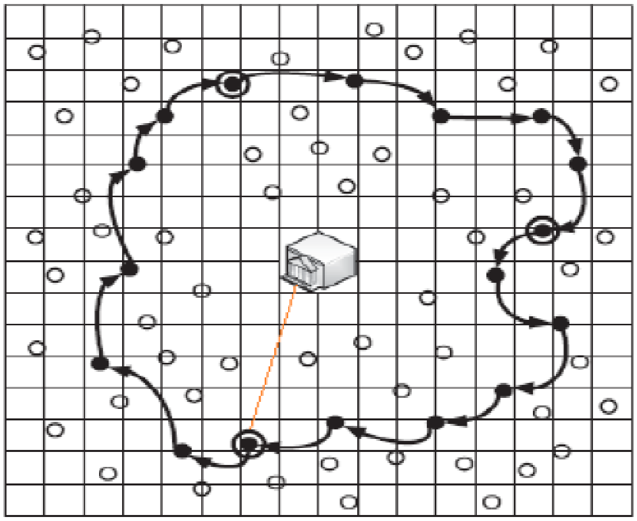

Fig. 4- Grid Information

### *D.* Flooding based techniques

Flooding based routing is handled various packet flow in Sensor environment. It posed various security problems in sensor network for example link failure, collision, network jamming and packet loss ratio increases. Techniques are usually easy to implement since simplifies the routing protocol. The communication cost of message flooding might be prohibitively expensive in WSNs. for flooding based approach it should be generate fake packet traffic to confuse for local and global adversary.

### *E.* Single path routing

It mentions criteria to quantitatively measure source location message leakage in single routing based source location privacy schemes for WSN's. It is energy efficient routing techniques allow a node to forward packets only to one of its neighbors. Single-path routing techniques usually require either extra hardware support or a pre-configuration phase. It's nearest neighbors and the destination to calculate a greedy single routing path. There are number following technique to maintain flow and source privacy: trajectory based routing, directed diffusion.

## III. TYPES OF ATTACKS AND ITS IMPACT IN SOURCE LOCATION PRIVACY

Different attack happens on wireless sensor network to provide source location privacy. In Some condition various attacks reduce network performance but fake nodes are protected real data from those attacks. There are following attack show various impact on network namely: adversary, eavesdropper, compromise nodes, packet spoofing, and Black hole attack.

### *A.* Adversary attack

Adversary can drop number of packets in simulation time. It can insert its own packets into the network. Internal adversary can compromise a node within the sensor area. Whereas an external adversary cannot do that .internal adversary has access to components and an external adversary does not have permission to access. The active attacks of the adversary comprise injecting false packet into the dropping actual packet network traffic. Passive attack is eavesdropping in which adversary listens to the traffic and tries to capture the content that is exchange between at node. A semi honest adversary follows the protocol within the WSN to ensure that it remain unidentified as an adversary while a dishonest adversary does not comply with the protocol within the sensor network. Semi honest is compliant with the protocol and dishonest is not compliant.

### *B.* Eavesdropping

The Eavesdropping attack is a serious security threat to a sensor network. Conventional sensor area consist of wireless nodes equipped with Omni-directional antennas, which broadcast radio signals in all directions and are consequently prone to the eavesdropping attacks. For Passive Eavesdropping in which the malicious nodes detect the information by listening to the message transmission in the broadcasting wireless medium. For Active eavesdropping where the malicious nodes actively grab the information via sending queries to transmitters by disguising themselves as friendly nodes. For eavesdropping attacks they are using cluster based anonymization techniques to protect from those attacks.

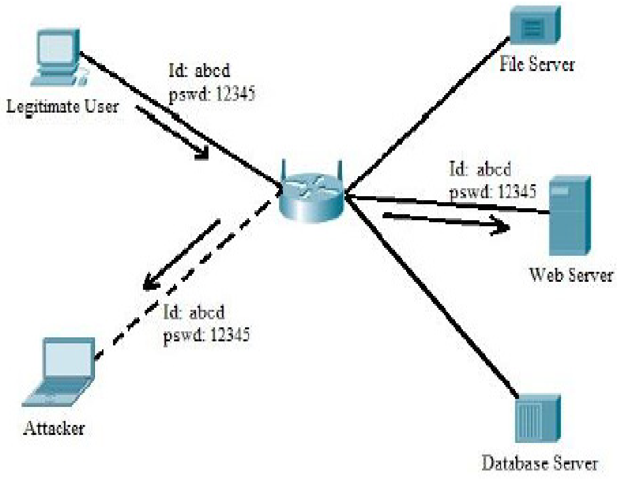

Figure 5- Eavesdropping attack

### *C.* Compromise node

Adversary uses a compromised node to influence the protocol or to detect other node .adversary can also destroy a node in this case. Adversary uses a compromised node to get information such as the identity of a node, the information received and sent by node and encrypt keys of a node. Compromise node can send packet to real node to access data unauthorized way. On that node they can access data from different node. Fake node used for to confuse compromise node packet attack in sensor area.

### *D.* Black hole attack

A packet drop attack or black hole attack is a type of denial of service attack accomplished by dropping packets. A black hole attack is an attack that is mounted by an external adversary on a subset of the sensor nodes in the network. When the source select the path including the attacker node, the traffic starts passing through the adversary node and this nodes starts continuous dropping the packets selectively or in whole. Reprogrammed nodes are termed as black hole nodes and the region containing the black-hole nodes are black hole region. Black hole region is the entry point to a large number of harmful attacks.

### *E.* Node Capture Attack

In Node Capture Attack an attacker physically captures sensor nodes and compromises them so that sensor readings sensed by compromised nodes are inaccurate or manipulated. The attacker may also attempt to extract essential cryptographic keys like a group key from wireless nodes that are used to protect communications in most wireless networks. Node capture not only enables to get a hold of cryptographic keys and protocol states, but also to clone and redeploy malicious nodes in the network. Several methods to identify such cloned nodes in the network are described in. But still the lack of a common analytical framework prevents any discussion about the degree of an attack, the network's resilience against an attack and the stability of WSNs, all of which are required to guarantee secure and reliable WSNs.

### *F.* Denial of Sleep Attack

In a wireless network when there is no radio transmission, the MAC layer protocol reduces the node's power consumption by regulating the node's radio communications. An attacker may use this scenario and try to drain a wireless device's limited power supply (especially sensor devices) so that the node's lifetime is significantly shortened. Thus, the attacker attacks the MAC layer protocol to shorten or disable the sleep period. If the number of power drained nodes is large enough, the whole sensor network can be severely disrupted. Even with power management tools in place, unless a MAC protocol can create opportunities to sleep for long durations, the platform cannot achieve extended network lifetimes.

### *G.* Collision Attack

In collision attack, attacker tries to corrupt the octet of transmitted packets. If attacker succeeds in doing so; then, at the receiving end; the packets will be discarded due to checksum mismatch. The retransmission of packets could cause exhaustion of necessary resources i.e. energy of the sensor nodes.

### *H.* De-Synchronization Attack

In de-Synchronization Attacks, attacker forges messages between endpoints. Modification in control flags or sequence numbers are usually made. If the attacker is lucky and got the control at right timing, then he might prevent the endpoints from ever exchanging messages as they will be, by continuously requesting retransmission of lost message. This attack leads to an infinite retransmission cycle that exhausts lot of energy.

### *I.* Flooding Attack

There are various kinds of denial of service attacks which are planned in different manner and decreases network lifetime in different ways. One among them is the flooding kind of Denial of Service attack. An attacker using this kind of attack normally sends a large number of packets to the victim or to an access point to prevent the victim or the entire network from establishing or continuing communications. This process is analogous to TCP SYN attacks where, attacker sends many connection establishment requests, forcing the victim to store the state of each connection request. The primary aim of flooding attacks is to cause exhaustion of resources on victim system.

### *J.* Jamming (Radio Interference) Attack

Jamming is one of many activities used to compromise the wireless environment. One of the fundamental ways for degrading the network performance is by jamming wireless transmissions. In the simplest form of jamming, the attacker corrupts the transmitted messages by causing electromagnetic interference in the network's operational frequencies, and in proximity to the targeted receivers. An attacker can commendably cut off the link among nodes by communicating continuous radio signals so that other sanctioned users are not allowed to access a particular frequency channel. The attacker can also send jamming radio signals which intentionally collide with legitimate signals originated by target nodes.

### *K.* Replay Attack

A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an attacker who intercepts the data and retransmits it, possibly as part of a masquerade attack by IP packet substitution (such as stream cipher attack). An attacker copies a forwarded packet and later sends out the copies repeatedly and continuously to the victim in order to exhaust the victim's buffers or power supplies, or to base stations and access points in order to degrade network performance. In addition, the replayed packets can crash poorly designed applications or exploit vulnerable holes in poor system designs.

### *L.* Selective forwarding attack

This attack is sometimes called Gray Hole attack. In a simple form of selective forwarding attack, malicious nodes try to stop the packets in the network by refusing to forward or drop the messages passing through them. There are different forms of selective forwarding attack. In one form of the selective forwarding attack, the malicious node can selectively drops the packets coming from a particular node or a group of nodes. This behavior causes a DoS attack for that particular node or a group of nodes. A forwarding node selectively drops packets that have been originated or forwarded by certain nodes, and forwards other irrelevant packets instead. They also behave like a Black hole in which it refuses to forward every packet. The malicious node may forward the messages to the wrong path, creating unfaithful routing information in the network.

### *M.* Unauthorized routing update attack

An attacker attempts to update routing information maintained by routing hosts, such as base stations, access points, or data aggregation nodes, to exploit the routing protocols, to fabricate the routing update messages, and to falsely update the routing table. This attack can lead to several incidents, including: some nodes are isolated from base stations; a network is partitioned; messages are routed in a loop and dropped after the time to live (TTL) expires; messages are perversely forwarded to unauthorized attackers; a black-hole route in which messages are maliciously discarded is created; and a previous key is still being used by current members because the rekeying messages destined to members are misrouted or delayed by false routings.

### *N.* Wormhole attack

In a wormhole attack, an attacker receives packets at one point in the network, "tunnels" them to another point in the network, and then replays them into the network from that point. An attacker intrudes communications originated by the sender, copies a portion or a whole packet, and speeds up sending the copied packet through a specific wormhole tunnel in such a way that the copied packet arrives at the destination before the original packet which traverses through the usual routes. Such a tunnel can be created by several means, such as by sending the copied packet through a wired network and at the end of the tunnel transmitting over a wireless channel, using a boosting long-distance antenna, sending through a low-latency route, or using any out-of bound channel. The wormhole attack poses many threats, especially to routing protocols and other protocols that heavily rely on geographic location and proximity, and many subsequent attacks (e.g., selectively forwarding, sinkhole) can be launched after the wormhole path has attracted a large amount of traversing packets.

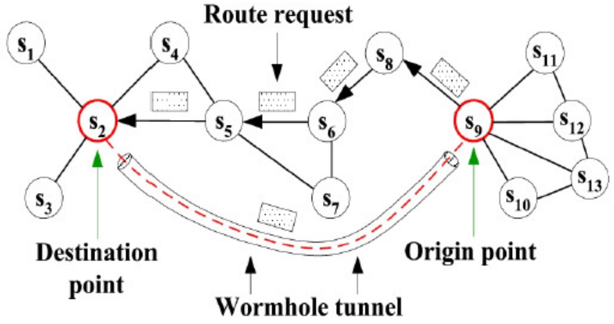

Figure 6- Wormhole Attack

### *O.* Sinkhole attack

The sinkhole attack is a particularly severe attack that prevents the 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. As a result, the adversary manages to attract all traffic that is destined to the base station by advertising as having a higher trust level and as a node in the shortest distance or short delay path to 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.

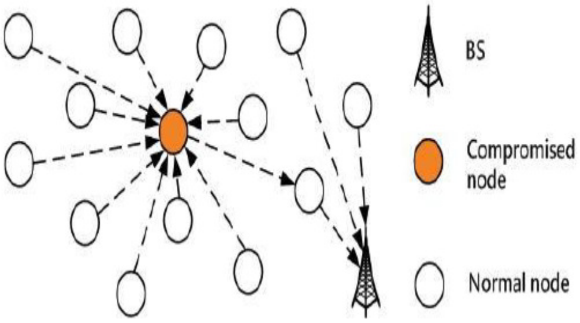

Figure 7- Sinkhole attack

### *P.* Impersonate attack

An attacker impersonates another node's identity (either MAC or IP address) to establish a connection with or launch other attacks on a victim; the attacker may also use the victim's identity to establish a connection with other nodes or launch other attacks on behalf of the victim. An attacker illegitimately uses the victim's credentials to access the Server. There are several software's capable of reprogramming the devices to forge the MAC and network addresses.

### *Q.* Sybil attack

A single node presents itself to other nodes with multiple spoofed identifications (either MAC or network addresses). The attacker can impersonate other nodes identities or simply create multiple arbitrary identities in the MAC and/or network layer. Then the attack poses threats to other protocol layers; for examples, packets traversed on a route consisting of fake identities are selectively dropped or modified; or a threshold-based signature mechanism that relies on a specified number of nodes is corrupted.

### *R.* Traffic analysis attack

An attacker attempts to gain knowledge of the network, traffic, and nodes behaviors. The traffic analysis may include examining the message length, message pattern or coding, and duration the message stayed in the router. In addition, the attacker can correlate all incoming and outgoing packets at any router or member. Such an attack violates privacy and can harm members for being linked with messages (e.g., religious-related opinions that are deemed provocative in some communities). The attacker can also perversely link any two members with any unrelated connections. If a group of attackers collude to launch any type of attacks, it is referred to as a collusion attack. For example, the colluding group of attackers orchestrates to collect information to significantly exploit the system, masquerade a legitimate member and send out fault messages on behalf of that member, conjointly mount attacks against other members or network entities, or falsely accuse a legitimate member as an attacker.

## CONCLUSION

Many threats and vulnerabilities to WSNs have been identified and many of such attacks have summarized. These threats could even prone to collapse the entire systems and networks, hence adding security in a resource constrained wireless sensor network with minimum overhead provides significant challenges, and is an ongoing area of research.

## REFERENCES

[1] Er. Satish Kumar, "A Study of Wireless Sensor Networks- A Review", International Journal of Computer Sciences and Engineering, Volume-04, Issue-03, Page No (23-27), Mar -2016

[2] Shamneesh Sharma, Dinesh Kumar and Keshav Kishore, "Wireless Sensor Networks- A Review on Topologies and Node Architecture", International Journal of Computer Sciences and Engineering, Volume-01, Issue-02, Page No (19-25), Oct -2013

[3] Sonam Jai, Deepak Singh Tomar and Rachana Kamble, "Survey of Attacks and Security Schemes in Wireless Sensor Network", International Journal of Computer Sciences and Engineering, Volume-03, Issue-05, Page No (122-128), May -2015

[4] N.Vanitha1, G.Jenifa, “Detection of Packet Droppers in Wireless Sensor Networks Using Node Categorization Algorithm”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 3, March 2013

[5] A. Babu Karuppiah1* and S. Rajaram, “False Misbehavior Elimination of Packet Dropping Attackers during Military Surveillance using WSN”, Advances in Military Technology, Vol. 9, No. 1, June 2014

[6] S.Ranjitha and D. Prabakar and S. Karthik, "A Study on Security issues in Wireless Sensor Networks", International Journal of Computer Sciences and Engineering, Volume-03, Issue-09, Page No (50-53), Sep -2015

[7] Devdatt Nadre, Balaso N. Jagdale, “Security for Source Node Privacy in Wireless Sensor Network”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 2, February 2015