Various Attacks in Wireless Sensor Network: Survey

K.Venkatraman, J.Vijay Daniel, G.Murugaboopathi

Abstract-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 journal will present you a survey about the various threats to wireless networks, the various advancements in securing a network and the various challenges in implementing the same.

Keywords: wireless sensor networks, denial of service attacks, Sybil attacks, node replication attack, traffic analysis attack, secure routing protocols, trust management, intrusion detection.

I. INTRODUCTION

Group communications refers to either point-to multipoint (In which a packet is delivered from a group member to the other members) or multipoint-to multipoint communications (in which packets are sent from multiple members to other members simultaneously). The characteristics of different wireless networks - wireless infrastructure networks (WINs), ad hoc networks (AHNs), and wireless sensor networks (WSNs) - are vastly different in terms of group management, packet types, and resources. However, one common risk among these networks is that all members communicating through wireless channels are more insecure and susceptible to numerous attacks than wired networks.

1.1 Attacks in wireless networks

Here, we present some known attacks (intensively discussed in the references) that pose a significant threat to group communications over wireless networks, and categorize these attacks based on their impacts, including data integrity and confidentiality, power consumption, routing, identity, privacy, and service availability.

II. DATA INTEGRITY AND CONFIDENTIALITY-RELATED ATTACKS

In general, this type of attack attempts to reveal or compromise the integrity and confidentiality of data contained in the transmitted packets.

2.1 Denial of Service (DoS) Attack: Denial of Service attack is an attempt to make a network unavailable for its legitimate users. An attacker tampers with data before it is read by sensor nodes, thereby resulting in false readings and eventually leading to a wrong decision. A DoS attack generally targets physical layer applications in an environment where sensor nodes are located. One common method of such attack involves saturating the target machine with external communications requests so that it cannot respond to legitimate traffic, or responds slowly. Such attacks usually lead to a server overload. This attack is implemented by either forcing the targeted computer to reset, or consuming its resources so that it can no longer provide its intended service or obstructing the link between the intended users and the victim so that they can no longer communicate adequately. A typical DoS attack structure is explained in Fig 1. Denial-of-service attacks are considered violations of the IAB's Internet proper use policy, and also violate the acceptable use policies of virtually all Internet service providers.

2.2 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 [1]. 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.

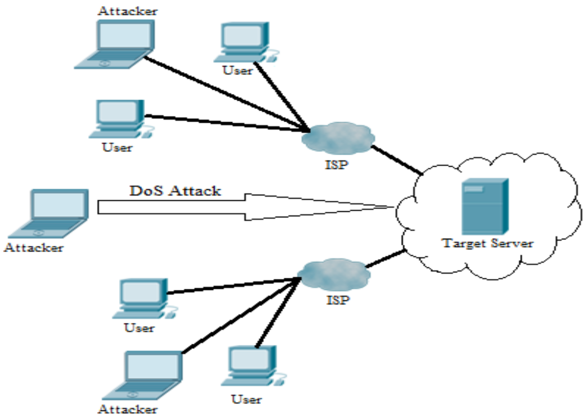

Fig 1 Denial of Service

Manuscript received March 2013

K. Venkatraman, Veltech MultiTech Dr.Rangrajan Dr.Sakunthala Engg. College , Chennai, India.
J. Vijay Daniel, Veltech MultiTech Dr.Rangrajan Dr.Sakunthala Engg. College , Chennai, India.
Dr. G.Murugaboopathi, Associate Professor Veltech MultiTech Dr.Rangrajan Dr.Sakunthala Engg. College, Chennai, India.

2.3 Eavesdropping attack: Eavesdropping is the process of gathering information from a network by snooping on transmitted data and to eavesdrop is to secretly overhear a private conversation over a confidential communication in an unauthorized way. The information remains the same but its privacy is compromised. An attacker eavesdrops secretly between any two nodes and may collect the necessary information regarding connection such as MAC address and cryptographic information. An attacker may also steal the User Id and password information as shown in Fig 2. Although this attack can be classified into other categories such as privacy-related attacks, we group it into this category since its consequences are severe in the sense that the collected cryptographic information may break the encryption keys such that the attacker can retrieve meaningful data. An example of eavesdropping is intercepting credit card numbers, using devices that interrupt wireless broadcast communications or tapping wire communications

III. POWER CONSUMPTION RELATED ATTACKS

One of the most valuable asset in wireless network is the power supply. In power consumption related attacks an attacker tries to exhaust the wireless device's power supply and it may degrade the lifetime of the network. A worst case scenario may even collapse the network communication.

3.1 Denial of Sleep Attack: In a wireless network when there is no radio transmission, the MAC layer protocol reduce 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.

3.2 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.

3.3 De-Synchronisation 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.

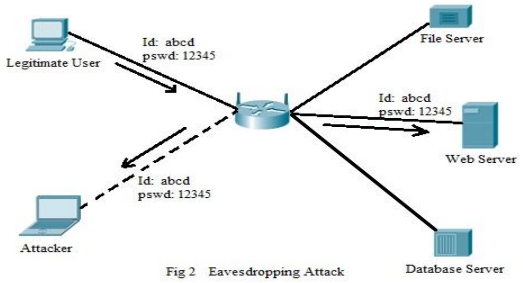

Fig 2 Eavesdropping Attack

IV. SERVICE AVAILABILITY AND BANDWIDTH CONSUMPTION RELATED ATTACKS

These attacks mainly aim to devastate the forwarding capability of forwarding nodes or consume meagerly available bandwidth; they are more likely related to availability of service and bandwidth consumption. These attacks can also be categorized as power consumption-related attacks. If these attacks result in a denial of service to legitimate members, they can also be referred to as a variant of denial-of-service (DoS) attacks.

4.1 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.

4.2 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.

4.3 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.

4.4 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 behaviour causes a **DoS attack** for that particular node or a group of nodes as shown in Fig 3. 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.

V. ROUTING RELATED ATTACKS

In general, these attacks attempt to change routing information, and to manipulate and benefit from such a change in various ways.

- Spoofed, altered and replayed routing Information.
- 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.
- Create routing loops.
- Extend or shorten service routes.
- Generate false error messages.
- Increase end-to-end latency.

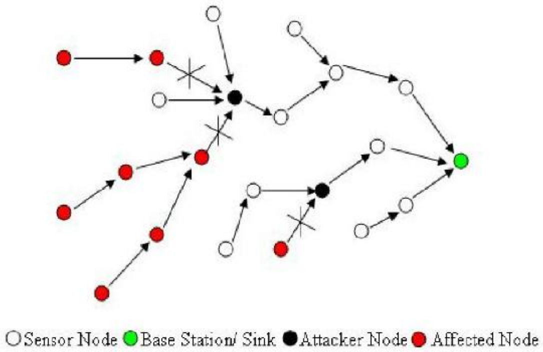
○Sensor Node ●Base Station/ Sink ●Attacker Node ●Affected Node

Fig 3 Selective Forwarding Attack

5.1 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.

5.2 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.

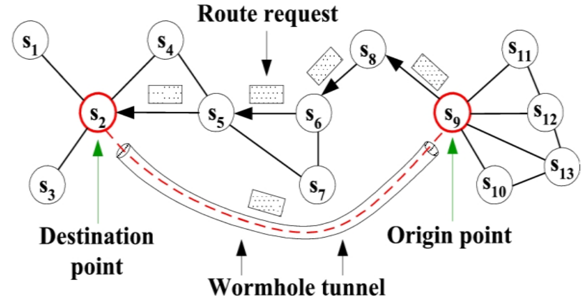

Fig 4 Wormhole Attack

5.3 Spoofing Attack: In spoofing attack attacker complicates the network by creating routing loop, attracting or replaying the routing information.

5.4 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 shown in Fig 5. 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.

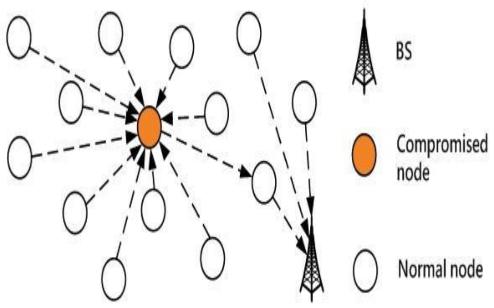

Fig 5 Sinkhole Attack

VI. IDENTITY RELATED ATTACKS

In general, these attacks cooperate with eavesdropping attacks or other network-sniffing software to obtain vulnerable MAC and network addresses. They target the authentication entity.

6.1 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. As illustrated in Fig. 6 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.

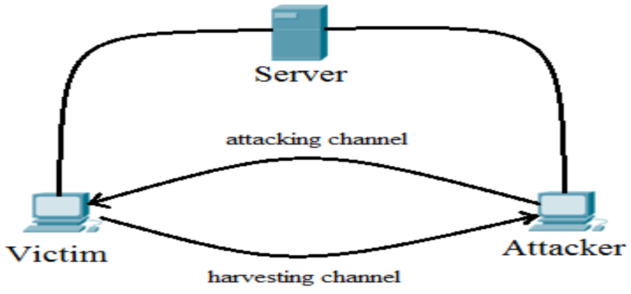

Fig 6 Impersonate Attack

6.2 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.

VII. PRIVACY RELATED ATTACKS

In general, this type of attack uncovers the anonymity and privacy of communications and, in the worst case can cause false accusations of an innocent victim.

7.1 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.

VIII. CONCLUSION

We have identified the threats and vulnerabilities to WSNs and we have summarized the various categories of such attacks. 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.

ACKNOWLEDGEMENT

The Authors sincerely thank the chairman of VelTech group of institution Col. Prof. Dr.Vel Sri.R.Rangarajan, Chairperson and Managing Trustee, Director for their encouragement to prepare this review. They further extends sincere thanks to Principal and Head of the Department of Information Technology of Vel Tech Multi Tech Dr.Rangarajan Dr.Sakunthala Engineering College for their constant support at every stage to complete this review.

REFERENCES

[1] Tamara Bonaci, Linda Bushnell and Radha Poovendran "Node Capture Attacks in Wireless Sensor Networks: A System Theoretic Approach"

[2] Pitipatana Sarkarindr and Nirwan Ansari, New Jersey Institute of Technology "Security Services In Group Communications Over Wireless Infrastructure, Mobile Ad hoc, and wireless Sensor Networks"

[3] Fadi Farhat *University of Windsor* "Eavesdropping attack over Wi-Fi"

[4] Sachin Dev Kanawat and Pankaj Singh Parihar "Attacks in Wireless Networks" IJSSAN 2011

[5] Prateek Suraksha Bhushan, Abhishek Pandey, and R.C. Tripathi of IIT Allahabad "A Scheme for Prevention of Flooding Attack in Wireless Sensor Network" ISSN: 2047-0037 (IJRRWSN)

[6] Alejandro Proano, Loukas Lazos of University of Arizona, "Selective Jamming Attacks in Wireless Networks"

[7] Wazir Zada Khan, Yang Xiang, Mohammed Y Aalsalem, Quratulain Arshad "Comprehensive Study of Selective Forwarding Attack in Wireless Sensor Networks" published on February 2011 in MECS.

[8] Yih-Chun Hu, Adrian Perrig *and* David B. Johnson, Members, IEEE "Wormhole Attacks in Wireless Networks"

[9] Ioannis Krontiris, Thanassis Giannetsos, Tassos Dimitriou "Launching a Sinkhole Attack in Wireless Sensor Networks; t he Intruder Side"

[10] James Newsome, Elaine Shi, Dawn Song and Adrian Perrig of Carnegie Mellon University "The Sybil Attack in Sensor Networks: Analysis & Defenses"

AUTHORS PROFILE

Mr. J. Vijay Daniel is currently a student of Veltech Multitech Dr. Rangarajan Dr.Sakunthala Engineering college, Chennai and he is doing his Masters in "Network Engineering". He received his Bachelors degree in "Electronics and Communication" from SMK Fomra Inst of Tech, Chennai in 2011. His research interests include network and system security, sensor networks, wireless and ad hoc networks. His subjects of interest include Sensor Networks, Wireless Networks, Network Security.

Mr. K. VenkatRaman, is a student of Veltech Multitech Dr. Rangarajan Dr. Sakunthala Engineering college, Chennai and he is doing his Masters in "Network Engineering". He received his Bachelors degree in "Electronics and Communication" from SMK Fomra Inst of Tech, Chennai in 2011. He received his diploma in "Electronics and Communication" from Thiru Seven Hills Polytechnic in 2008. His areas of intrest include Wireless networks, Network Security and.Ad-Hoc.Networks.

G.Murugaboopathi, received the Undergraduate Degree in Computer Science and Engineering from Madurai Kamaraj University, in 2000, the Post Graduate degree in Digital Communication and Network from Madurai Kamaraj University, in 2002 and Ph.D in Computer Science and Engineering at Bharath University, Chennai. He has more than 20 publications in National, International Conference and International Journal proceedings. He has more than 11 years of teaching experience. His areas of interest include Wireless Sensor Networks, Mobile Communication, Mobile Computing, Mobile Adhoc Networks, Computer Networks, Network Security, High Speed Networks, Network and Data Security, Cryptography and Network security, DBMS and etc., He is currently working as an Head R & D and Associate Professor in the Department of Information Technology at Vel Tech Multi Tech Dr.Rangarajan Dr.Sakunthala Engineering College Chennai, India.