A Survey on Wireless Sensor Network: Comparative Review

Puneet Kaur, Navpreet Kaur
Computer Science and Engineering, Punjabi University Regional Centre for IT and Management, Mohali, Punjab, India

DOI: 10.23956/ijarcsse/V7I7/0133

Abstract: Due to advanced features of wireless sensor devices, the usage of these devices are rises tremendously all over the world. Many researchers work on wireless devices for new enhancement in ad hoc network. WSN (Wireless Sensor Network) included small, low-cost and resource constrained nodes. In order to provide the unique communication protocols many researches have been done in the existing algorithms by introducing new methods and algorithms. In this study, some approaches to eliminate the Sinkhole Attack are introduced that happened in WSN. Apart from this, various routing protocols that can be used to improve the performance of network during transmission of data are discussed in this paper. The performance prediction of routing protocol is very tough task due to varying network scenarios. The performance of WSN is measured using various parameters like throughput, end to end delay are also discussed in this paper.

Keywords— WSN, sensors, attacks, protocols, performance.

I. INTRODUCTION

Wireless Sensor Network made up of small nodes that have the ability to sense and send that data to base station with limited processing and computing resources. [1] Wireless Sensor Networks provides low cost solution for data measurement and collection. Smart Sensor Nodes are low power equipment’s with some sensors, power supply, memory and radio. A number of mechanical, biological, thermal, optical, chemical and magnetic sensors attached to the node to measure various properties of the environment. The sensor nodes have less memory and deploy mainly in difficult-to-access locations; thus, a radio is implemented for transfer the data to base station like laptops, mobile phones or any access point to fixed infrastructures during wireless communication [2]. Battery is used as a power source in sensor nodes but additionally solar panels added to nodes according to environment conditions where sensors are deployed [3].

Fig. 1 Components of WSN

The above Fig. 1 describes the basic components of WSN. Sensor unit, processor, memory, power unit, transceiver are physical components of sensor in WSN. Some applications of WSN that commonly used now a day are military activities that are used to track the movement of enemy, providing health care, emergency disaster relief, surveillance, prevention of biological and chemical threats, critical infrastructure, gathering battlefield intelligence and many more [4].

II. CHALLENGES IN WSN

The main advantage of WSN is to easily self-configure the network by using some routing protocols. The WSN are used to be monitor infrastructure (like water distribution), thus it is necessary that integrity of WSN must be protected against malicious attacks. [5] Unfortunately, some of wireless network are used in unfriendly area and most of their routing protocols don’t consider the security aspects of them because of varying resource constraints. Some of constraints are lower in power supply, computational power, communication range and memory. Due to these constraints, the chance of routing attacks on wireless sensor network is increased. Routing attacks are potentially vulnerable by routing protocols that can stop the disrupt connectivity in the network. The classical cryptographic defenses protect the wired networks, while the wireless sensor nodes make resources intensive cryptography impractical [6]. A WSN is a network that have many constraints as compare to traditional computer network. Some of them are:
A. Wireless Medium: The WSN is less secure because eavesdropping is easy and simple because of its broadcast nature. The transmissions can be easily intercepted, replayed or altered by an adversary. Wireless medium allows any attacker to easily intercept packets and inject malicious ones.

B. Data Confidentiality: To remain the message private data confidentiality is used to conceal the data from the passive attacks. The main issue in network security is data confidentiality so that no one can read the private data of anyone. The nodes have not disclosed information of its neighbor nodes.

C. Ad-Hoc Deployment: There is not any particular structure defined in network deployment. The topology of network is always changed due to failure, addition and mobility of nodes. The network must support self-configuration because of nodes failure or replaced. Security is difficult to operate within this dynamic nature.

D. Network Scalability: The sensor nodes may be thousands or millions in any network. Thus scalability is the critical factor.

E. Hostile Environment: In this environment, the functioning of sensor nodes is performed. The possibility of destruction of nodes or capturing of nodes by attackers are faced in Hostile environment. The attackers can easily access the physical address of devices and extract the valuable information (like cryptographic keys) from it.

F. Fault Tolerance: The failure of nodes is occurred if some responsive situation are created during transmission of data. This dynamic behavior should be incorporated in designing and implementation.

G. Resource Scarcity: The extreme need of sensor devices poses considerable challenges for security mechanism. The algorithms basically depend upon bandwidth, memory and computational complexity. Energy and power are the basic resource for sensor networks. The communication is efficient if energy efficiency is high during security mechanism.

H. Unreliable Communication: Unreliable communication is another problem in security of sensor network. the security depends upon the protocols. (a) Unreliable Transfer is occurred in packet based routing of sensor network. The packet based routing is connectionless and unreliable. (b) Conflicts are occurred in network due to broadcast nature of WSN. Even the channel is reliable but communication is still unreliable. (c) Latency is occurred due to multi-hop routing, node progressing and network congestion. This synchronization is difficult to achieve in sensor nodes.

This Section has discussed the security challenges that are mostly available in wireless sensor networks and the next section describes about the attacks that commonly occur on wireless sensor networks.

### III. LITERATURE SURVEY

Many scholars have been working on sensor network field to offer security mechanism that suits the resources constrained because of large requests of applications in sensitive area. There are some techniques introduced by many researchers to detect and identify the sinkhole attacks in WSN [17]. In 2007[15], Krontiri et al. introduced rule based technique to prevent sinkhole attacks in network. In the proposed solution, they scratched their IDs to detect attacks that resulted in succeed in intrusion detection system and with increase in network density the false negative rates decrease. The robust and secure network is developed during this process. The main limitation of this technique is node imperfection and network overhead. In 2009[16], Choi et al. introduced Anomaly based technique that used LQI (link quality indicator) to detect sinkhole attack. With increase in detection nodes the probability of detection rate is increased and false positive rate only depends upon extent to tolerant value. The main advantage is that detector nodes communicate via exclusive channel and limitation is that the sensor nodes have no mobility, detection of sinkhole is occurred only when node is between the sinkhole node and base station, the energy of detector node is high as compare to source node. In 2007[17], Coppolino et al. introduced the Hybrid base in which intrusion detection system protect the critical data from direct attacks. It results in 95-97% detection rate and 3% false positive rate. The advantages of this approach are that it satisfied the available resources and use anomaly or misuse method. In 2009[19], Papadimitriou et al introduce a key management approach that introduce a RESIST protocol that increases the resilience to attacks and prevents the malicious nodes from changing distance above one node. But the RESIST is very expensive because it requires two additional message packets. In 2011[18], Sheela D et al. introduce a non- cryptographic method that uses mobile agents to defend attacks. The probability to defend Sinkhole attack is decreased when Number of nodes are more and energy decreases with time goes up. The limitation of this method, exact number of mobile agents are not specified and matrix method is complex of available resources. The above techniques describe how to detect and prevent sinkhole attack in WSN. All the approaches that managed to identify, detect and provided resistance to sinkhole attacks. The major disadvantages produce by these approaches including high memory and network overhead, creates high false positive rate or many more not able to work on mobile WSN. In next sections, various attacks that occurred in WSN instead of sinkhole are explained and various protocols that used to improve the performance of sensor network while data is transmitted from source to base station.

### IV. ATTACKS ON SENSOR NETWORK

Due to broadcast nature of communication medium, WSN is vulnerable to network attacks[7]. WSN have more problems because nodes are not protected in the hostile environment. Classification of the attacks in Figure1.
The above Fig. 2 describes the various attacks by some unauthorized medium on the network. Attacks are basically classified as passive and active attacks.

A. Passive Attacks: The communication channel has been monitor and accessed by unauthorized attacker during passive attack[8]. These attacks affect the privacy of data. Main data is stealing from sensor network or through direct site surveillance. Other attacks against privacy of sensor network are:

1) By snooping, the adversary easily collect the information regarding to communication contents.
2) Eavesdropping occurred when the traffic send the control information (detailed information) regarding to the sensor network configuration.
3) Traffic analysis: Encrypted message still have high possibility analysis of communication patterns during transferred in network. Thus, sensor nodes can easily reveal enough information to an adversary that can cause malicious harm to network.
4) Camouflage Adversaries: The nodes are inserted for hiding the network, that causes in misroute of packets. The misroute is occurred because network nodes are copy as normal nodes for attracting the packets.

B. Active Attacks: The data stream of communication channel has been monitor, accessed and modifies [9]. The following are some active attacks:

1) Routing Attacks in Sensor Networks: The attacks that can act on the network layer are known as routing attacks. The basic attacks that happen during the routing of message are:
   - Routing Information is spoofed, altered or replayed
   - Generate false error messages
   - Create routing loops
   - Increase end-to-end latency
   Selective Forwarding: A malicious node have been drop certain packets. These attacks are effective if combined with certain attacks that gather much traffic. Generally, node forward the received messages but the compromised node might refuse to forward the message or neighbors start choosing another route.

2) Sinkhole Attack: The traffic is attracted to the specific node in sink hole attack. The main goal of this attack is to attract all the nearby traffic from a particular area by a compromised node.

3) Sybil Attacks: During Sybil attack one node is duplicated to multiple locations. A single node is visualized at multiple locations in sensor network. The fault tolerant schemes are main target of Sybil attacks.

4) HELLO flood attacks: An attacker send and replay the HELLO packets of routing protocol from one node to another node with large amount of energy. In WSN these attacks follow HELLO packets as weapon to convince the sensors. An attacker with high processing power and radio transmission range sends the HELLO packets to various sensor nodes that are isolated in WSN. While sending message to base station, the victim nodes sometimes go through spoofed node by attacker.

5) Denial of Service Denial of Service (DoS) Any malicious action or unintentional failure of nodes occurred during DoS. Network is subverting, disturbed and destroy by adversary or any event that diminished the network capability to provide services[10].
Table 1. Attacks on various layer in WSN

<table>
<thead>
<tr>
<th>Layer</th>
<th>Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Layer</td>
<td>Jamming, Tampering</td>
</tr>
<tr>
<td>Link Layer</td>
<td>Collision, Exhaustion, Unfairness</td>
</tr>
<tr>
<td>Network Layer</td>
<td>Neglect, Greed, Homing, Misdirection, Black Holes</td>
</tr>
<tr>
<td>Transport Layer</td>
<td>Malicious Flooding, Desynchronization</td>
</tr>
</tbody>
</table>

6) Node Supervision: Capture of node mainly reveal the main information like disclosure of cryptographic keys. A single sensor may be taken and info together with key might be attained by adversary.

7) Node Malfunction: A malfunctioning of node will generate some inaccurate data that might expose the integrity of WSN especially when node is data-aggregating such as cluster leader.

8) Node Outage: Any situation in which node stops its function is Node Outage. In the case when the cluster leader stops its functioning and by providing an alternate route the protocols of sensor network robust to mitigate the effects of node outages.

9) Physical Attacks: Sensor node established in the hostile environment. Physical attacks destroy the sensors permanently and their losses are irreversible. For instance, adversary can get cryptographic secrets, temper the associated circuitry, modify the programming in the sensors and replace with malicious sensors.

10) Message Corruption: the message is corrupted when any modification is done in the content of the message. The attacker compromises the integrity of message.

11) False Node: It includes the extra node via adversary and roots the dose of malicious information. An attacker add node to network that would feed some false information or prevents transmission of true data. The insertion of malicious node is most dangerous attacks occurred in WSN that could potentially destroying the network.

V. ROUTING PROTOCOLS IN SENSOR NETWORKS

Routing protocols determine a few policies that often governs end to end communication in network [11]. Routing protocols are required to send data between sensor nodes and base station. Lots of routing algorithms are developed by researchers. Routing protocols are basically unicast, broadcast and multicast. In this network, various routing protocols are introduced which is based on various network conditions as shown in Figure 3.

![Routing Protocols in Sensor Network](image)

Figure 3. Routing Protocols in Sensor Network

A. Proactive Routing Protocol

The proactive protocol provides efficient flooding of messages through Sensor network using some selected nodes known as MRPs. MRPs are Multipoint Relays that are selected by every node and used to control forward message [12]. A node simply maintains routes for all destinations in network, that’s why this protocol is suitable for random traffic patterns. Proactive is more suitable for Sensor network where large number of nodes are communicated with another set of large number of nodes. There are many proactive routing protocols like WRP, OLSR, DSDV etc.

B. Reactive routing protocol

The reactive routing protocol are also introduced as on demand routing protocol. The route is only established when a source node needs to transmit the data packets [13]. During this process, if a route is not available it broadcasts a RREQ packets. RREQ packets involve IP address of source and destination, request ID and hop count. If line breakage in any route occurred then RERR message is send to source node.

C. Hybrid routing protocol

There is a trade-off among proactive and reactive protocols. Hybrid Protocol use the properties of proactive protocol that makes use of table maintenance system and particular route breakthrough system of reactive protocol. Hybrid protocol perform better for large number of nodes present in network. There are many hybrid routing protocols like ZRP, SHARP [14].
In lore the protocols widely used to handle those attacks. The Sinkhole attack in wireless sensor networks are inherently different from traditional wired networks as well as wireless ad-hoc networks. Security is an important feature for the deployment of Wireless Sensor Networks. This paper reviews the main challenges in WSN and attacks that effects the parameters. An attempt has been made to explore the protocols widely used to handle those attacks. The challenges of Wireless Sensor Networks are also briefly discussed. This review will confidently inspire upcoming scholars to initiate up with smarter and robust security devices and make network safer.

### VII. CONCLUSION

The network becomes vulnerable when sensors nodes are deployed in an unattended environment. Wireless sensor network is normally used in various fields like military, health and commercial applications. Sensor networks are inherently different from traditional wired networks as well as wireless ad-hoc networks. Security is an important feature for the deployment of Wireless Sensor Networks. This paper reviews the main challenges in WSN and attacks that effects the parameters. An attempt has been made to explore the protocols widely used to handle those attacks. The challenges of Wireless Sensor Networks are also briefly discussed. This review will confidently inspire upcoming scholars to initiate up with smarter and robust security devices and make network safer.

### REFERENCES


