International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A Review on Sinkhole Attack in WSN

Priyanka[1] Arpit Bansal[2]
[1](Student, CSE department, Yadwindra Engineering College, Talwandi Sabo)
[2](Assistant Professor CSE department, Yadwindra Engineering College, Talwandi Sabo)

Abstract: ***Wireless Sensor Network (WSN) is being emerged as a prevailing technology in future due to its wide range of applications in military and civilian domains. These networks are easily prone to security attacks. Unattended installation of sensor nodes in the environment causes many security threats in the wireless sensor networks. There are many possible attacks on sensor Network such as selective forwarding, jamming, sinkhole, wormhole, Sybil and hello flood attacks. Sinkhole attack is among the most destructive routing attacks for these networks. It may cause the intruder to lure all or most of the data flow that has to be captured at the base station. Once sinkhole attack has been implemented and the adversary node has started to work as Network member in the data routing, it can apply some more threats such as black hole or gray hole. Ultimately this drop of some important data packets can disrupt the sensor networks completely. We have presented some countermeasures against the sinkhole attack.***

Keywords: Wireless sensor networks; ILEACH; fuzzy logic

I. INTRODUCTION

Wireless sensor network (WSN) is a collection of sensor nodes which are capable of sensing and processing data and send them to a base station. These sensor nodes are small in size. They are deployed in an unattended environment which is not physically protected. They are used for monitoring of that environment and send back the collected data to the Base Station (BS). WSN are light weighted and have limited power sources, limited memory storage, limited computational capability and transmission range. They are vulnerable to various security threats as they use the wireless medium for transmission of the data to the BS. There are several attacks in each layer of the sensor networks. The physical layer attacks are jamming, tampering, Data link layer attacks are Jamming and collision; Network layer attacks are selective forwarding attack, sinkhole attack, Sybil attack, black hole attack, wormhole attack; Transport layer attacks are flooding attack, de-synchronization attack. One of the most dangerous and very difficult to detect the attack is sinkhole attack because using this attack we can perform any type of attack in the WSN. Wireless sensor networks (WSNs) have gained worldwide attention in recent years. These sensors are small, with limited processing and computing resources, and they are inexpensive compared to traditional sensors. These sensor nodes can sense, measure, and gather information from the environment and based on some local decision process they can transmit the sensed data to the user. Smart sensor nodes are low power devices equipped with one or more sensors, a processor, memory, a power supply, and a radio. A variety of mechanical, thermal, biological, chemical, optical, and magnetic sensors may be attached to the sensor node to measure properties of the environment. Since the sensor nodes have limited memory and are typically deployed in difficult-to-access locations, a radio is implemented for wireless communication to transfer the data to a base station like a laptop, a personal handheld device, or an access point to a fixed infrastructure. Battery is the main power source in a sensor node. Secondary power supply that harvests power from the environment such as solar panels may be added to the node depending on the appropriateness of the environment where the sensor will be deployed. Some current applications of sensor networks include providing health care for the elderly, surveillance, emergency disaster relief, detection and prevention of chemical or biological threats, gathering battlefield intelligence, and critical infrastructure.

A. Wireless sensor networks have the following characteristics

1) All sensor nodes use the direct transmission or multi-hop transmission to communicate with the base station.

2) Sensor nodes sense conditions at different locations at a fixed rate and always have data to send to the base station.

3) The sensor nodes are organized into a group is called cluster. Cluster head performs data aggregation and BS receives compressed data.

4) The lifetime of wireless sensor network is the total amount of time before the first sensor node runs out of power.

5) Power consumption constraints for nodes using batteries or energy harvesting.

6) Ability to cope with node failures

7) Mobility of nodes.
8) Heterogeneity of nodes.
9) Scalability to large scale of deployment.
10) Ability to withstand harsh environmental conditions.

B. Applications of Wireless Sensor Networks

1) Military applications
2) National Security
3) Traffic surveillance
4) Medical application

C. Types of attacks

Active attack: Active attack is an attack which the attacked entity gets aware of when attacked. That is the interruption from the attacker is of such kind that he gets aware of the attack, hence called active attack. For example: trying to steal some info. These attacks on computers involve using information gathered during a passive attack, such as user IDs and passwords, or an outright attack using technological "blunt instruments." Such instruments include password crackers, denial-of-service attacks, email phishing attacks and other malware attacks. In an active attack, the attacker is out to bring a website down, steal information or even destroy computing equipment. As network administrators install defenses against existing attack tools, hackers develop more sophisticated tools and the game of technology leapfrog continues.

Passive Attack: when the attacked entity is unaware of the attack, hence called PASSIVE like the attacker is just trying to listen. This attack involves someone listening in on telecommunications exchanges or passively recording computer activity. An example of the former is an attacker sniffing network traffic using a protocol analyzer or some other packet capturing software. The attacker finds a way to plug into the network and begins capturing traffic for later analysis. Other attackers rely on key loggers, usually as a Trojan horse record keystrokes such as user IDs and passwords. The goal is just to listen and record the data passing through. The passive attack itself is not harmful but the information gathered during the session could be extremely damaging.

D. Attacks on Wireless Sensor Networks

1) *Jamming:* Jamming interferes with the radio frequencies of the sensor nodes. Only a few jamming nodes can put a considerable amount of the nodes out of order. If the adversary can block the entire network then that constitutes complete DoS.
2) *Tampering:* A tampering attacker may damage a sensor node, replace the entire node or part of its hardware or even electronically interrogate the nodes to gain access to sensitive information, such as shared cryptographic keys and how to access higher communication layers.
3) *Spoofed, altered or replayed routing information:* This is the most direct attack. By spoofing, altering or replaying routing information the attacker can complicate the network and create routing loops, attracting or repelling traffic, generating false error messages, shortening or extending source routes or partitioning the network.
4) *Selective forwarding:* In such an attack the adversary includes itself in a data flow path of interest. Then the attacker may choose not to forward certain packets and drop them causing a sort of black hole.
5) *The Sybil Attack:* A malicious node present multiple identities to the network is called Sybil attack. This attack is especially confusing to geographic routing protocols as the adversary appears to be in multiple locations at once.
6) *Wormholes:* In these attacks the adversary tunnels messages received in one part of the network over a low latency link, to another part of the network where the messages are then replayed. Wormholes often convince distant nodes that they are neighbors, leading to quick exhaustion of their energy resources. An attacker close to the base station can completely disrupt routing by creating well positioned wormholes that convince nodes multiple hops from the base station that they are only a couple of hops away through the wormhole.
7) *Hello flood attacks:* In many routing protocols, nodes broadcast hello messages to announce their presence to their neighbors. A node receiving such a message can assume that the node that sent the message is within its range. An attacker with a high powered antenna can convince every node in the network that it is their neighbor.
8) *Sinkhole Attack:* WSNs are susceptible to a wide class of attacks among which sinkhole attack has been identified as one of the serious threats. In this type of attack, a malicious node advertises itself as a best possible route to the base-station which

deceives its neighbors to use the route more frequently. Thus, the malicious node has the opportunity to tamper with the data, damage the regular operation or even conduct many further challenges to the security of the network. The main deception of the attack is that a malicious node attracts the traffic of its neighbors by pretending that it has the shortest path to the base-station. The attack may jeopardize many important security measures. The sinkhole may launch a variety of attacks against the data traffic, such as selectively dropping the data packets, tampering data aggregation algorithms or interfering with clustering protocols. Two types of attackers may establish sinkhole attacks; a malicious insider or a resourceful outsider. In the former case, an adversary utilizes a compromised node to launch the attack in which a route is advertised to deceive neighbors. In the latter case, a laptop-class adversary equipped with high performance computation and communication capabilities conducts a single-hop route from its surrounding region to the base-station which convinces the neighbors to forward all the traffic through such route. Furthermore, the high quality route not only attracts the neighbors of sinkhole but also it attracts almost all the nodes that are closer to the sinkhole than to the base-station which amplifies the threat. The sinkhole also can be conducted using wormhole attack. In this type of attacks, a malicious node first captures a routing packet from one of its neighbors and utilizes a secret tunnel to send the packet to another colluded node. The colluded node eventually delivers the message to the base-station. Even though the two ends of the tunnel may be at a longer distance compared with other routes, it can prevent the source from discovering other legitimate routes greater than two hops away from the destination and thus disrupts network functionality.

9) Different Reviews

Huabiao Qin, “Balanced Energy Consumption and Cluster-Based Routing Protocol” purpose a balanced energy consumption and cluster-based routing protocol (BECCRP) as an improvement on LEACH protocol in order to monitor large-scale environment longer and stably. Gateways will construct a multi-hops path to transmit packet, Cluster heads are just responsible for gathering and aggregating data from cluster members. By setting gateway, the task of data transmission is separated from cluster heads. Therefore, they success in sharing the communication energy consumption at each node equally, enhancing the system efficiency, extending the lifetime of the network.

Prashant Krishan, “A Study on Dynamic and Static Clustering Based Routing Schemes for Wireless Sensor Networks” presents a comprehensive survey of Dynamic and static Clustering based routing techniques in wireless sensor networks. They have the common objective of trying to extend the lifetime of the sensor network while not compromising data delivery.

Chutima, P. and Sujitra, M, “Optimal WSN Design for Efficient Energy Utilization” states energy efficiency in WSN by installing the new fewer nodes as Relay Nodes (RN). These relay nodes may be equipped with more sophisticated energy sources such as solar cells with larger batteries. The SNs will transmit the sensing information to the suitable RN. The proposed model aims at determining routes for transmitting this information so that the resulting network can guarantee the required network lifetime and ensure the radio communication between SNs so that network can guarantee packet delivery from SNs to base station.

Vidya K S and Arun Anoop M, “Lifetime Enhanced Cluster Based Routing in Wireless Sensor Networks” propose a cluster based routing method with a power saving mechanism for enhancing the lifetime. The overlapping coverage area of the randomly deployed nodes forms the basis of the power saving scheme. The routing node selection is based on residual energy which makes the routing procedure energy efficient. The nodes consume a small amount of power during sleep period and hence the lifetime of entire network is enhanced.

Hairong Zhao, Wuneng Zhou, Yan Gao, “Energy Efficient and Cluster Based Routing Protocol for WSN” propose an improved-LEACH protocol in order to save node energy, which is divided into two aspects: Cluster head election and Data transmission. The improved algorithm still uses the concept of "round”. A round is divided into clusters establish phase and stable data transmission phase. Stable data transmission phase must be longer than the cluster establish phase in order to make full use of energy. Thus improved-LEACH protocol can reduce energy consumption and prolong the network lifetime.

II. CONCLUSION

In contrast to traditional networks, Wireless Sensor networks (WSN) are more vulnerable to attacks. Among all major attacks on sensor networks, sinkhole attack is the most destructive routing attacks for these networks. Now we have surveyed various countermeasure techniques for sinkhole attack.

REFERENCES

[1] Huabiao Qin, "Balanced Energy Consumption and Cluster-Based Routing Protocol", IEEE International Conference on Control and Automation (ICCA),2011
[2] Prashant krishan , "A Study on Dynamic and Static Clustering Based Routing Schemes for Wireless Sensor Networks", International Journal of Modern Engineering Research (IJMER), www.ijmer.com Vol.3, Issue.2, pp-1100-1104, 2013.
[3] Chutima, P. and Sujitra, M. "Optimal WSN Design for Efficient Energy Utilization", Advanced Information Networking and Applications, IEEE Workshops of International Conference, pp. 814-819, Singapore, 2011.
[4] Vidya K S and Arun Anoop M, "Lifetime Enhanced Cluster Based Routing in Wireless Sensor Networks" International Journal of Engineering Science Invention, ISSN, www.ijesi.org Vol.2, Issue 7, pp-69-72,2013.
[5] Hairong Zhao, Wuneng Zhou, Yan Gao, "Energy Efficient and Cluster Based Routing Protocol for WSN" Eighth International Conference on Computational Intelligence and Security, 2012.
[6] I.Krontiris, T.Dimitriou, T.Giannetsos, M.Mpasoukos, Intrusion detection of sinkhole attacks in wireless sensor networks, in: Algorithmic Aspects of Wireless Sensor Networks, 2008, pp.150–161.
[7] E.Ngai, J.Liu, M.Lyu, An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks, Computer Communications 30 (11) (2007) 2353–2364.

.