International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org, editorijaiem@gmail.com
Volume 2, Issue 2, February 2013 ISSN 2319 - 4847

Detecting Sinkhole Attack in Wireless Sensor Network

Vinay Soni[1], Pratik Modi[2], Vishvash Chaudhri[2]

[1,2] Department of Computer Engineering,
LDRP -ITR, Gujarat Technological University,

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 network, Security attack, Adversary node, legitimate node.

1. INTRODUCTION

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 (e.g., 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 typical example of a sensor node, sometimes called a mote, is the IMote2, which has a 32-bit processor running at 13 MHz, with 256 KB SRAM, 32 MB flash memory, and 32 MB SDRAM. The radio has an integrated 802.15.4 radio and an external 2.4 GHz antenna.

2. SECURITY GOALS

When dealing with security in WSNs, we mainly focus on the problem of achieving some of all of the following security contributes or services:

Confidentiality: Confidentiality refers to data in transit to be kept secret from eavesdroppers. Here symmetric key ciphers preferred for their low power consumption.

Integrity: Integrity measures that the received data is not altered in transit by an adversary.

Authentication: Authentication enables a node to ensure the identity of the peer with which it is communicating.

Availability: The service should be available all the time.

Data Freshness: It suggests that the data is recent, and it ensures that no old messages have been replayed.

Non-repudiation: It denotes that a node cannot deny sending a message it has previously sent.

Authorization: It ensures that only authorized nodes can be accessed to network services or resources.

These goals are not ensured by traditional cryptographic techniques. So some new cryptographic measures are needed for sensor network.

3. ATTACKS ON WIRELESS SENSOR NETWORKS

The Sensor networks are self-organizing networks which, once deployed, are expected to run autonomously and without human attendance. Major attacks on sensor networks are as follow:

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.

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.

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.

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.

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.

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.

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.

4. THE SINKHOLE ATTACK

In a sinkhole attack, the adversary's aim is to lure nearly all the traffic from a particular area through a compromised node, creating a metaphorical sinkhole with the adversary at the center. Sinkhole attacks typically work by making a compromised node look especially attractive to surrounding nodes with respect to the routing algorithm. Sinkhole attacks are difficult to counter because routing information supplied by a node is difficult to verify. As an example, a laptop-class adversary has a strong power radio transmitter that allows it to provide a high-quality route by transmitting with enough power to reach a wide area of the network.

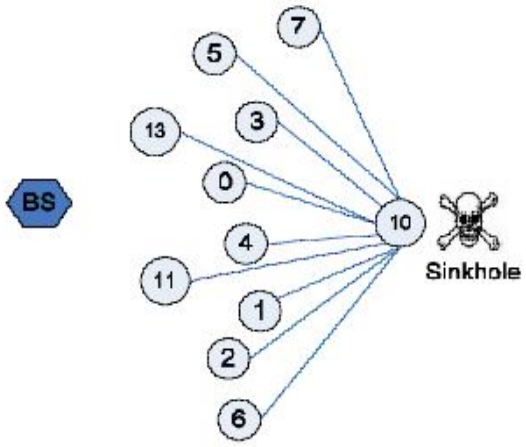

Figure 1: Demonstration of a sinkhole attack

As shown in fig. 2 a compromised node attracts all the traffic from its neighbors by telling its neighbor that it has shortest route to reach to the base station. This route is artificial high quality route.

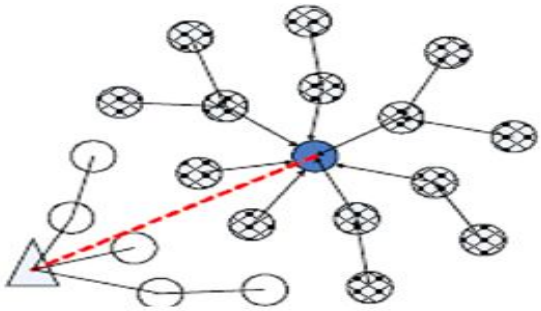

Fig 2 Sinkhole using an artificial high quality route

Fig. 3 denotes how sinkhole is created using wormhole. As shown in figure, one malicious node attracts all the traffic and make a tunnel with another malicious node to reach to the base station.

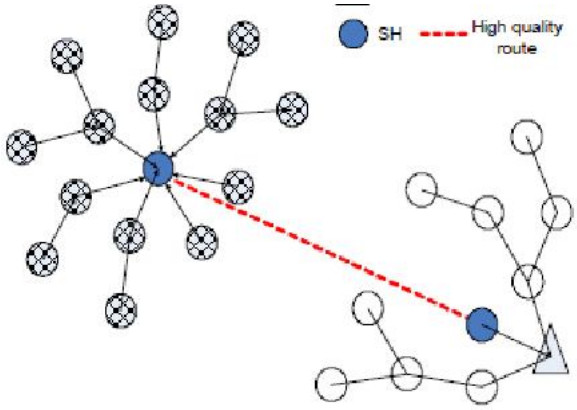

Fig 3 Sinkhole using a wormhole

5. COUNTERMEASURES AGAINST SINKHOLE ATTACK

Data Consistency & Network Flow Information Approach

The approach presented in [1] involves the base station in the detection process, resulting in a high communication cost for the protocol. The base station floods the network with a request message containing the IDs of the affected nodes. The affected nodes reply to the base station with a message containing their IDs, ID of the next hop and the associated cost. The received information is then used from the base station to construct a network flow graph for identifying the sinkhole. The algorithm is also robust to deal with cooperative malicious nodes that attempt to hide the real intruder. The performance of the proposed algorithm has been examined through both numerical analysis and simulations. The results have demonstrated the effectiveness and accuracy of the algorithm. They also suggest that its communication and computation overheads are reasonably low for wireless sensor networks.

Hop Count Monitoring Scheme

A novel intrusion detection system that detects the presence of a sinkhole attack is proposed in [2]. The scheme is based on hop count monitoring. Since the hop-count feature is easily obtained from routing tables, the ADS (Anomaly Detection System) is simple to implement with a small footprint. Moreover, the proposed ADS is applicable to any routing protocol that dynamically maintains a hop-count parameter as a measure of distance between source and destination nodes. The scheme can detect attacks with 96% accuracy and no false alarms using a single detection system in a simulated network.

RSSI Based Scheme

A new approach of robust and lightweight solution for detecting the sinkhole attack based on Received Signal Strength Indicator (RSSI) readings of messages is proposed in [3]. The proposed solution needs collaboration of some Extra Monitor (EM) nodes apart from the ordinary nodes. It uses values of RSSI from four EM nodes to determine the position of all sensor nodes where the Base Station (BS) is located at origin position (0, 0). This information is used as weight from the BS in order to detect Sinkhole attack. The simulation results show that the proposed mechanism is lightweight due to the monitor nodes were not loaded with any ordinary nodes or BS. The proposed mechanism does not cause the communication overhead.

Monitoring node's CPU usage

A novel algorithm for detecting sinkhole attacks for large scale wireless sensor networks is discussed in [4]. The detection problem is formulated as a change-point detection problem. The CPU usage of each sensor node is monitored and analyzes the consistency of the CPU usage. By monitoring the CPU usage of each node in fixed time interval, the base station calculates the difference of CPU usage of each node. After comparing the difference with a threshold, the base station would identify whether a node is malicious or not. Thus, the proposed algorithm is able to differentiate between the malicious and the legitimate nodes.

Mobile Agent Based Approach

The scheme to defend against sinkhole attacks using mobile agents is proposed in [5]. Mobile agent is a program segment which is self controlling. They navigate from node to node not only transmitting data but also doing computation. A routing algorithm with multiple constraints is proposed based on mobile agents. It uses mobile agents to collect information of all mobile sensor nodes to make every node aware of the entire network so that a valid node will not listen the cheating information from malicious or compromised node which leads to sinkhole attack. It does not need any encryption or decryption mechanism to detect the sinkhole attack. This mechanism does not require more energy than normal routing protocols.

Using Message Digest Algorithm

Detection of sinkhole attack in wireless sensor networks using message digest algorithms is proposed in [6]. The main goal of the protocol is to detect the exact sink hole using the one-way hash chains. In the proposed method destination detects the attack only when the digest obtained from the trustable forward path and the digest obtained through the trustable node to the destination are different. It also ensures the data integrity of the messages transferred using the trustable path. The algorithm is also robust to deal with cooperative malicious nodes that attempt to hide the real intruder. The functionality of the proposed algorithm is tested in MAT lab.

6. 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. In this paper, we have surveyed various countermeasure techniques for sinkhole attack.

REFERENCES

[1.] Edith C. H. Ngai, Jiangchuan Liu and Michael R. Lyu; "On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks" IEEE International Conference on Communications, 2006, Volume 8, pp. 3383-3389.

[2.] Daniel Dallas, Christopher Leckie, Kotagiri Ramamohanarao; "Hop-Count Monitoring: Detecting Sinkhole Attacks in Wireless Sensor Networks" 15th IEEE International Conference on Networks, 2007, ICON 2007, pp. 176-181.

[3.] Chanatip Tumrongwittayapak and Ruttikorn Varakulsiripunth; "Detecting Sinkhole Attacks in Wireless Sensor Networks" ICROS-SICE International Joint Conference 2009, pp. 1966-1971.

[4.] Changlong Chen, Min Song, and George Hsieh; "Intrusion Detection of Sinkhole Attacks In Large-scale Wireless Sensor Networks" IEEE International Conference on Wireless Communications, Networking and Information Security (WCNIS), 2010, pp. 711-716.

[5.] D.Sheela, Naveen kumar. C and Dr. G.Mahadevan; "A Non Cryptographic Method of Sinkhole Attack Detection in Wireless Sensor Networks" IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011, pp. 527-532

[6.] S.Sharmila and Dr G Umamaheswari; "Detection of sinkhole Attack in Wireless Sensor Networks using Message Digest Algorithms" International Conference on Process Automation, Control and Computing (PACC) 2011, pp. 1-6