Sinkhole Attack: a Security Vulnerability in Wireless Sensor Networks

Amulya D (*Author*)
Department of ISE
The National Institute of Engineering
Mysuru, India

C.N Chinnaswamy (*Author, Associate Professor*)
Department of ISE
The National Institute of Engineering
Mysuru, India

Abstract

Wireless Sensor Networks(WSN) have found a wide range of applicability in our day-to-day life and also a bright future of interest because of its salient features such as lesser power consumption, low cost, and easier implementation, etc. This wide range of popularity and usability of these networks makes the security threats and their prevention as the hot topics for research. The security challenges and the various security vulnerabilities that occur in the wireless sensor networks have been surveyed and documented in this paper. One such vulnerability, Sinkhole attack is viewed in detail. The challenges in the detection of the attack, the approaches used to detect and prevent sinkhole attack have been briefed in this paper. Finally, a conclusion over the attacks and the work being carried out is stated.

Keywords— *Wireless Sensor Network (WSN), Sinkhole attack, Base station, Denial of Service (DoS)*

I. INTRODUCTION

Wireless Sensor Network (WSN) is a network of autonomous sensors that are spatially distributed over a physical region in order to monitor physical or environmental conditions, such as pressure, temperature, sound, etc. and that data is circulated through the network in a coordinative manner to a main location called as the Base station where the actual data evaluation or validation is achieved. The modern implementation of wireless sensor network supports bi-directional communications enabled with control of sensor activity. WSNs are deployed in various fields such as military applications like battle field surveillance to track the existence of enemies, to monitor environmental conditions such as fire detection and in health monitoring applications such as cardiac-monitoring and etc. WSN can be classified into two types: Structured and Unstructured. An Unstructured WSN consists of dense collection of sensor nodes, which are homogeneous by their nature both physically and architecturally. Structured WSN consists of some or all the nodes being implemented in a pre-planned manner. The low cost for maintenance and management of the network are the advantages of the structured WSN. However, the deployment of WSN happens in an unfriendly area being unnoticed. The resource constraints such as low memory, low communication range, low computational power, low power supply etc. make the routing protocols used in the deployment not to consider the security aspect. This constraint provides opportunities for various attackers to attack the WSN. Various attacks that can be implemented are jamming attack, DoS, Sinkhole attack, Wormhole attack and etc. Most commonly implemented attack is Sinkhole attack where an intruder compromises a node to become a malicious node that tries to attract all the traffic towards it with the intention of preventing the base station from receiving correct sensing and complete data from the other nodes of the network. The attack is launched by the attacker by inserting a malicious node which will be relatively close to the base station of the network. The malicious node advertises fake routing information regarding the quality of the link which is used by the routing protocols to choose the optimal route for data transmission resulting in the entire traffic being passed through it from the neighbor nodes to the base station. The sinkhole attack is used as a spring board for other attacks such as knowledge spoofing attack, selective forwarding attack and altered routing information attack. Various kinds of possible security attacks in the WSN are discussed in brief and a detailed view on the detection and countering against the Sinkhole attack has been surveyed and documented in this paper.

II. GOALS OF NETWORK SECURITY

The main goal of the security services is to protect the computer system or the network against unauthorised access or unintended usage. Thus, the security component must be well encompassed with the services, policies and mechanisms that provide the three main services namely confidentiality, integrity and availability. The security goals can be broadly classified into primary and secondary goals.

A. *Primary Goals*

The security goals that deal with providing confidentiality, integrity and availability services are categorised under primary goals.

1) *Confidentiality:* It deals with the security mechanisms which ensure that only intended recipients is capable to interpret and analyze the correct message and also avoids the unauthorized access and usage of data.
2) *Integrity:* These mechanisms are concerned with restricting the modification of data under communication by intruder.
3) *Availability:* These mechanisms provide the conformance that the system or the network and its associated application are available at any point of time and are able to do their tasks without interruption.

B. *Secondary Goals*

These goals are concerned with the data freshness, organization and synchronization among the nodes in the network.

1) *Data Freshness:* This mechanism identifies the recent data being transmitted and received among the nodes in order to prevent replay attack. Data freshness can be of two types: Weak freshness that is applicable for measuring sensors and gives partial message ordering without considering any delay information and Strong freshness which gives the delay estimation and total ordering of the message and is being implemented in time synchronization in the network.
2) *Self-Organization:* The sensor nodes in the WSNs are not implemented with any fixed infrastructure and hence are random in nature. Thus, the capability of being self-organizable must be provided for the sensor nodes so that they can adapt and organize to the environment and situation accordingly.
3) *Time Synchronization:* The randomly implemented sensor nodes must be synchronized with respect to time through some or the mechanism so that the end-to-end delay of the packet during the time of communication between a pair of nodes can be computed and optimized.
4) *Secure Organization:* The efficient utilization of the sensor network depends on the capability of the network to locate each sensor, automatically and accurately in the network.

III. Challenges in Network Security

Various challenges have to be faced in order to provide security to the wireless sensor applications. Some of them are listed below.

A. *Resource Constraints*

The limited set of resources make the adoption of traditional security mechanisms difficult since they involve high overheads.

B. *Lack of Central Control*

Due to larger network size, limited set of resources, and dynamic nature of the network it is infeasible in order to have a central common control point in the network.

C. *Error-Prone Communication*

The packet based routing of sensor networks are based on connectionless protocols, hence are inherently unreliable. The errors in the channel may cause damage to the packets and the packets may even be dropped at the nodes which are highly congested. The implementation of robust error handling schemes due to higher error rate will lead to higher overhead. Due to the broadcast nature of wireless communication results in collision among the packets in transit and needs retransmission making the communication to be error prone even if the communication channel is reliable.

IV. Security Vulnerabilities in Wireless Sensor Networks

Security vulnerabilities are nothing but the exploitation of the security of the network by introducing some sort of attack in order to disturb the normal functionality of the network components. Such attacks can be classified based on the capability of the attacker, attacks based on the information in transit, host based and network based attacks and the attacks performed based on the protocol stack of the network. Among these a brief analysis on the active and passive attacks which are achieved based on the capability of the attacker, are identified and specified in this paper.

A. *Active Attacks*

It is the mode of attack where the unauthorized intruder or the attacker tampers the data in transit. The attacker launches the attack by monitoring, listening and modifying the data packets in transit by performing routing attacks, eavesdropping and false stream creation etc. Impersonation, introduction of faulty data into the WSN, modification of the packets are the various activities being performed by the attacker. The different active attacks are,

1) Routing Attack: The attacks that are implemented at the network layer are known as "Routing attacks". The attack results in advertising false routing information which is chosen by the routing metrics while routing the messages resulting in data loss, over delay etc.

2) Spoofed and Altered Routing Information Attack: In this attack the malicious node disturbs the traffic in the network either by altering or spoofing false routing information in the network.

3) Selective Forwarding: The attack results in the loss of messages because the malicious node selectively forwards only certain messages to other nodes in the network and discards the other messages.

4) Sybil Attack: The fault tolerant mechanisms such as multipath routing, distributed storage and topology maintenance are the targets of Sybil attack.

5) Wormhole Attack: In this attack the packets of data under transmission are collected by the attacker at a particular location and are being transferred to some other location and are finally retransmitted into the network thus resulting in delay.

6) HELLO Flood Attack: The HELLO packets used by the routing protocols are flooded from one to another, throughout the network by the malicious node with an abnormal very high transmission power.

7) Sinkhole Attack: The adversary node advertises a false optimal path with sufficient available bandwidth and power and thus attracts the entire traffic towards it from a particular region. The two possible attackers to launch the sinkhole attack are the malicious insider and resourceful outsider.

8) Blackhole Attack: It is the attack in which during the path finding process the routing metric chooses wrong path as good path to the destination based on the false advertisement advertised by the malicious node.

9) Denial of Service Attack: This kind of attack is launched by making multiple false service requests to a node in the network and preventing an authorised node to obtain the actual service. It may also be caused by sudden failure of nodes within the network due to some malicious activity.

10) Node Replication Attack: The attacker introduces a malicious node into the network with the same node-id as that of a normal authorised node of the wireless sensor network.

B. Passive Attacks

The unauthorized users or attackers within the WSN monitor and tamper the data packets being exchanged among the nodes that are legitimate in the network and this attack is known as "Passive attack". The passive attacker collects the information from the WSN by acting as a normal node within the network. Examples of Passive attacks are as follows,

1) Monitor and Eavesdropping: The attacker gains the control over the data under communication through snooping and easily finds the contents of communication.

2) Traffic Analysis: It is a kind of attack where the attacker analyses the traffic within the network during data transmission in order to predict the complexity of the content being transmitted.

3) Camouflage Adversaries: The intruder injects a malicious node or compromises a normal node to become a malicious node. The malicious node behaves itself as a normal node ant attracts the packets towards it.

V. SINKHOLE ATTACK

Sinkhole attack is an active and intruder attack where an attacker or intruder launches the attack either by introducing a malicious node or by compromising an existing node in the network to act as malicious node. The malicious node attracts the network traffic from all its neighbor nodes towards it by advertising a false optimal path information regarding the reachability to the base station through the malicious node and this routing information used by the routing metric in order to choose the best path by the implemented routing protocols leads to the launch of the sinkhole attack successfully in the network. Thus, the malicious node successfully avoids the base station from receiving the complete and the correct messages from the other nodes in the network. The many to one communication pattern where each individual node sends data to the base station makes the WSN vulnerable to the sinkhole attack [5]. Sinkhole attack can be launched by introducing a malicious node that does not necessarily target all the nodes in the network but intendedly targets those nodes which are close to the base station. Sinkhole attack in a network is demonstrated with a simple example as shown below. The network structure in Figure 1 shows the organization of nodes without any sinkhole attack.

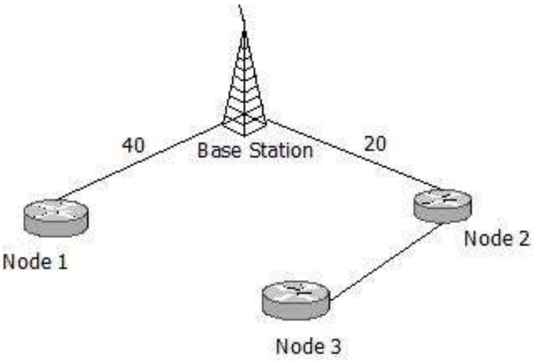

Figure 1

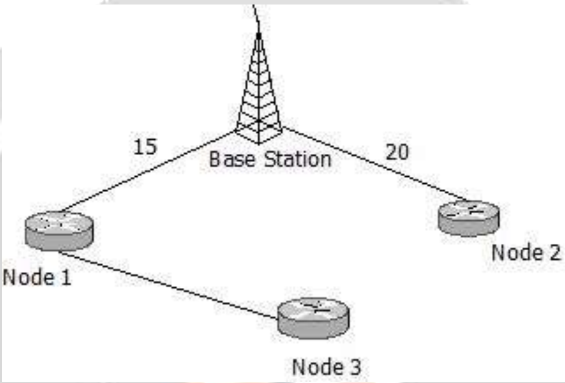

Figure 2

In this structure, node 3 communicates with the base station via node 2 since node 2 has the shortest reachability to base station than node 1. Similarly, the structure in Figure 2 shows the network organization with node 1 being the malicious node for the sinkhole attack. In this scenario node 3 communicates with the base station via node 1 because of the false advertisement of shortest reachability made by node 1.

VI. Challenges in Detecting Sinkhole Attack in Wireless Sensor Networks

The review through literature surveys on sinkhole attack has provided the basis to identify the challenges in the detection of sinkhole attacks in the wireless sensor networks. The main challenges are as follows,

A. *Communication Patterns in WSNs:* The many to one communication pattern of the wireless sensor network provides the opportunity for the sinkhole attack because the messages delivered to the base station from all the sensor nodes are directed via other nodes in the routing path selected by the routing metrics. Thus, the intruder can launch the attack based on the communication pattern by compromising the nodes that are close to the base station. Hence the design and maintenance of the communication pattern poses a challenge for detecting the sinkhole attack.

B. *Dynamic Nature of WSN:* The mobility of the sensor nodes in the WSN with the routing pattern built as sensors and base station makes the location identification of the sensor node a different task. This provides an opportunity for the intruder to launch the attack by introducing a malicious node randomly at some region near to the base station. Thus, the detailed tracking and maintenance of dynamicity information of the nodes is a challenge to detect the attack.

C. *Unpredictable Nature of Sinkhole Attack:* The communication in the WSN happens through the packet transmission via the path selected by the routing metrics used by the routing protocols. Thus, the attack will be launched by the compromised node which is specific to the routing metric used by the protocol of the network under threat. Hence, the sinkhole attack remains unpredictable to be detected with common mechanism in all the networks.

D. *Insider Attack:* Sinkhole attack can be launched as an Insider attack. In this technique, the attacker or the intruder comprises one of the legitimate nodes of the network to become the malicious node by node tampering or through the weakness in the system software of the node. Once the node is compromised the attacker disrupts the network by modifying the routing packets. The compromised node contains sufficient knowledge pertaining to the topology of the network and will also have adequate access privileges in the network. Hence this situation creates additional challenges in the detection of sinkhole attack.

E. Resource Constraints limit detection methods: The resource constraints such as limited power supply, lower communication range, low capacity for memory and limited computational ability of the sensor nodes hinder the implementation of stronger security mechanisms. Low computational power and limited memory capacity makes the implementation of strong cryptographic methods infeasible in WSN. Thus, the adaptations of weaker security mechanisms that are compatible with the available resources provide an opportunity to launch attack.

F. Physical Attack Vulnerability: The deployment of WSN in a hostile environment and being unattended provides an opportunity for the intruder to attack the node physically and gains the necessary information with respect to the network structure and communication pattern.

VII. EXISTING APPROACHES TO PREVENT AND DETECT SINKHOLE ATTACK

Due to wide popularity and adaptability of the wireless sensor networks the requirement to provide security mechanisms that suits the resource constraint challenge has given a wide platform for the researchers. Based on such research works, different approaches to detect and prevent the sinkhole attacks have been identified and listed as mentioned in our paper. The approaches are classified as rule based, anomaly based, statistical method, hybrid based and prevention based. The following subsections give a brief description of these approaches.

A. Rule Based: This approach deals with the designing and defining the rules based on the technique and behaviors used by the attackers to launch the sinkhole attack. The defined rules are implemented in the intrusion detection system that is adapted and being executed by each sensor node in the WSN. The packets under transmission in the network are analyzed with respect to the defined rules. The node which violates these defined rules is considered to be adversary and compromised and hence it will be isolated from the network.

The existing approach proposed by Krontiris et al [4] used the distributed rule based intrusion detection system in order to detect the sinkhole attack in the network.

B. Anomaly Based: It a detection based approach where a differentiation between the normal user behavior and an anomalous activity in the network is defined and implemented in the intrusion detection system. Hence the detection of the attack in the network is achieved by considering intrusion as an anomalous activity since it will be abnormal with respect to the normal behavior of the legitimate user. Rule based and statistical methods form a subset under this category of detection approach.

The detection approach proposed by Tumrongwittayapak and Varakulsiripunth [9] which uses the RSSI (Received Signal Strength Indicator) value which is received by the EM (Extra Monitor) nodes to detect the sinkhole attack based on the calculation of VGM (Visual Geographical Map) makes use of the anomaly based detection approach.

C. Statistical Method: The analysis of the data associated with the nodes in the network with respect to certain activities is performed and recorded. This information is used by the statistical method to detect the attack in the network. For example, the monitoring of the normal packets in the network and their transmission patterns between the nodes is analyzed. The detection of the adversary is done by comparing the threshold value used as a reference with the actual behavior of the node, the node is considered as an intruder if its value exceeds than the threshold value.

Chen and et al [1] have proposed technique Statistical GRSh-(GirshickRubinShyriaev)-based algorithm for the detection of malicious nodes based on the value calculated by the base station as a difference of actual CPU usage of each node and the monitored value of CPU usage in a fixed interval of time. The node is concluded to be malicious by the base station if the difference exceeds the predefined threshold value.

D. Hybrid Based: Anomaly based and Cryptographic approaches are implemented in combination with each other in order to detect and prevent the sinkhole attack in the network, respectively. The combination of these two approaches forms the Hybrid approach. The usage of hybrid approach reduces the false positive rate that is produced by the anomaly based approach individually. The detection of malicious node can be achieved by defining the signature of the legitimate nodes in the database and the one whose signature being not defined is caught as to be an intruder; this provides an advantage to the system.

The hybrid Intrusion Detection system proposed by Coppolino and Spagnuolo [2] makes use of detection agent to identify the sinkhole attack. The hybrid intrusion detection mechanism is deployed in each node and based on the anomalous behavior of the nodes they are blacklisted. The central node receives the list of blacklisted nodes and makes the final decision based on the defined feature of the attack patterns.

E. Prevention Based: The cryptographic techniques such as the encryption and decryption keys are used to maintain the integrity and authenticity of the packets under transmission in the network. The packet is transmit is encrypted with the help of encryption key such that the access to the message can be obtained only with the availability of the decryption key and also helps in the identification of any small changes in the data during transmission. The authenticity mechanism provides the verification about the origin of the message from the base station and the legitimate nodes in the network.

Cryptographic approach proposed by Papadimitriou et al [6] addresses the sinkhole attack in routing protocols. Each node is provided with a key which is used to authenticate the origin of the message from the base station. The pairs of public and private keys were also used to provide authentication and integration through signed data messages. This approach avoided the hiding of node IDs and the packet forgeries between the nodes in the network. Thus this method provides resistance to sinkhole attack rather than detecting and mitigating it.

VIII. CONCLUSION

The level of security required for the deployment of the Wireless Sensor Network in an application domain must be determined. According to our analysis and opinion, the increased number potential security issues are a result of the vulnerabilities caused due to deployment of the WSN in a hostile environment and being unattended, makes the security mechanisms as mandatory requirement. As a parallel constraint the resource availability make the deployment of stronger security mechanisms infeasible. From our studies, the system architects are recommended to decide the required level of security and the value of data under transmission and processing. The resource constraints can be taken into consideration by analyzing the computational resources that are required to transmit individual packets between the nodes. Cryptographic security mechanisms such as two way authentication, encryption will cost the resources. If the mapping between the data value and resource consumption for providing security can be achieved by the architect, a better decision making approach can be achieved.

REFERENCES

[1] Chen, C., Song, M. and Hsieh, G. (2010). Intrusion Detection sinkhole attack in large scale wireless sensor network, In Wireless Communication, Networking and Information Security (WCNIS), 2010 IEEE Interational Conference on (pp. 711-716). IEEE.

[2] Coppolino, L., D'Antonio, S., Romano, L., and Spagnuolo, G.(2010). An intrusion detection system for critical information infrastructures using WSN technologies. In Critical Infrastructure (CRIS), 2010 5th International Conference on (pp. 1-8). IEEE

[3] Jaydip Sen. (2009). A Survey on Wireless Sensor Network Security, International Journal of Communication Networks & Information Security, 1(2).

[4] Krontiris,I., Dimitriou,T., Giannetsos,T. and Mpasoukos, M. (2008). Intrusion Detection Sinkhole Attacks in Wireless Sensor Network. In Networking and Communications, 2008. WIMOB'08. IEEE Interational Conference on Wireless and Mobile Computing, (pp. 526-531). IEEE.

[5] Ngai, E., Liu, J and Lyu, M. (2007) An efficient intruder detection algorithm against sinkhole attack in wireless sensor network. Computer Communications, 30(11), 2353-2364.

[6] Papadimitriou, A., Fessant, L. F. and Sengul, C. (2009). Cryptographic protocols to fight sinkhole attacks on tree based routing in WSN. In Secure Network Protocols, 2009. NPSec 2009. 5th IEEE Workshop on (pp.43-48). IEEE

[7] Pathan, K., AI-S. (2011) Security of Self-Organizing Networks-MANET, WSN, VANET, WMN. ISB N-13:978-1-4398-1920-3. Taylor and Francis Group.

[8] Suman Deb Roy, Sneha Aman Singh, Subhrabrata Choudhury, and N. C. Debnath. (2008). Countering Sinkhole and Black hole Attacks on Sensor Networks using Dynamic Trust Management", In computers and Communications, 2008. ISCC 2008. IEEE Symposium on (pp.537-542). IEEE.

[9] Tumrongwittaya and Varakulsiripunth. (2009). Detection of Sinkhole attack in Wireless Sensor Networks, In ICCAS-SICE, 2009 (pp. 1966-1971). IEEE..

[10] Suparna Biswas and Subhajit Adhikari (2015). A Survey of Security Attacks, Defenses and Security Mechanisms in Wireless Sensor Network, In International Journal Of Computer Applications.