A REVIEW ON SINKHOLE ATTACKS IN WIRELESS SENSOR NETWORKS

Dharshini Y N[1], Chinnaswamy C N[2]

[1]PG student, Department of ISE,NIE college,Mysuru,Karnataka,India
[2]Associate Professor, Department of ISE,NIE college,Mysuru,Karnataka,India

ABSTRACT

Wireless Sensor Networks are mainly made up of small nodes with sensing, computation and wireless communication capabilities. These are widely used in areas such as ecological, military and health-subjected fields. There applications also includes monitoring of few sensitive information's therefore security is the most important subject in WSNs. Routing attacks have devastating effect on WSNs and gives a very major challenged situation when designing security mechanisms. There are different types of attacks on sensor network such as jamming, sinkhole, selective forwarding, wormhole, sybil and hello flood attacks. Sinkhole attack is the most destructive attack for sensor networks, it also enable many other attack .During this attack sinkhole node tries to attract data through broadcasting fake routing information to it by convincing neighbors. This paper has a detailed picture of different sinkhole detection algorithm.

Keywords: *Wireless sensor network, Sinkhole Attack, Mobile agent.*

1. INTRODUCTION

WSNs are made up of multifunction and sensor nodes which are spatially distributed these are small in size and can communicate wirelessly also over short distances. Wireless Sensor Networks are self-healing, self-organizing networks. A few years ago, WSNs were used only for military. Now, many organizations use WSNs for their purposes such as pollution ,traffic control, weather, and healthcare agriculture monitoring, forest fire monitoring etc. These applications have several different levels such as monitoring ,tracking ,and controlling. For example, we can use WSNs to build intelligent center, to collect machine information for real-time control at companies ,and to have a track over the enemy movements in battle field areas. In medical applications, these sensors can be very helpful in patient diagnosis and health monitoring. Hence, security is an important issue for these networks. In WSN, Message is transferred from the source to destination. There is no security for data such as confidentiality, integrity, availability as the communication medium is wireless.

The main drawbacks of the WSNs is their characteristics which include low memory, low computation power ,they are remained in hostile region and left unattended, small range of communication capability and low energy capabilities. Based on the above characteristics makes this network to face several attacks, such as sinkhole, selective forwarding, wormhole or Sybil attacks.

In Sinkhole attack the compromised node tries to attract network traffic by advertise its fake routing update. Further compromised node may alter the message and can deliver it to the destination. At the same time few packets are dropped by the compromised node. This paper is mainly focused on analyzing the currently available solutions which can be used to detect sinkhole attack in WSNs.

2. SECURITY IN WSNs

Security is the important aspects of any system. According to security requirements attacks can be classified as:

- **Attacks on secrecy and authentication**

  Cryptographic techniques are used to protect communication channels authenticity and secrecy from packet replay attacks, eavesdropping and spoofing of packets.

- **Silent attacks on service integrity**

  In this attack, the attacker tries to compromise node and add false data value.

- **Attacks on network availability**

  Network availability attacks is also known as Denial of Service attacks. This attack targets any layer of network.

3. SECURITY CONCERN IN WSNs

- **Data Confidentiality**
  Data confidentiality refers to keep the data secret between sender and receiver. Encryption is used for secure communication.
- **Data Integrity**
  In data integrity, received data should not change by any adversary.
- **Data Authentication**
  Assuring the identities of communicating nodes referred as authentication.
- **Self-Organization**
  Sensor nodes are enough to be self-organizing and independent to all situations.
- **Secure Localization**
  It is an important feature and should be satisfied with the implementation of protocol.
- **Availability**
  Service is available all the time.
- **Data Freshness**
  Data freshness suggests the communicated data is recent and ensures that no previous message have been replayed.
- **Robustness and Survivability**
  Network should be robust across different attacks.
- **Flexibility**
  Sensor networks are used in areas where environmental circumstances are changes frequently.
- **Time Synchronization**
  Most of the sensor network applications depends on time synchronization.

4. TYPES OF ATTACKS

Security is the most important subject in WSNs. Routing attacks have devastating effect on WSNs and gives a very major challenged situation when designing security mechanisms. Different types of attacks on sensor network are as follows,

- Selective forwarding
- Jamming
- Wormhole
- Sybil attack
- Sinkhole attack
- Hello flood
- Traffic Analysis

4.1 Selective forwarding

In the selective forwarding attacks[8], malicious nodes acts just like normal nodes and then selectively drop the packets. The selection of dropping nodes are random. Identifying these attacks is highly difficult and in some cases it’s impossible.

4.2 Jamming

Jamming attacks are those which interfere along with transmission and reception of wireless signals by producing RF signals. There are various types of jammers that try to intentionally add false data during communication between two different nodes which mainly affects the data transmission and also which reduces the performance of WSN as it leads to overutilization of few resources like memory ,battery power etc.

4.3 Wormhole

Wormhole nodes fakes a route that is shorter than the actual original one in the network, this attack confuses the routing mechanisms which mainly depends on knowledge about distance between two nodes. It has one or more malicious nodes and a tunnel between them. The attacking node collects the packets from one location and transmits the same to other distant located node which then distributes them locally.

4.4 Sybil attack

In this attack, the WSN is subverted by a special malicious node which produces number of fake identities mainly to disrupt the networks protocols. This attack mainly confuses the geographic routing protocols as the adversary appears to be in multiple locations at one time

4.5 Sinkhole attack

Sinkhole attack is the most destructive attack for sensor networks, it also enable many other attack. During this attack sinkhole node tries to attract data through broadcasting fake routing information to it by convincing neighbors.

4.6 Hello flood

In WSN some routing protocols requires nodes to spread their hello messages to announce themselves among their neighbors. A node which receives this kind of message may assume that this is within a radio range of the sender. However in some cases this kind of assumption may turn false. In this attack, attacker broadcast hello packets to networks to add themselves as the neighbor to the other nodes. An attacker which have high powered antenna can convince every node in network that it is present in their neighbor.

4.7 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.

Among these attacks sinkhole attack is the most destructive attack. It cause the adversary to draw most of the data at the base station.

5. SINKHOLE ATTACK

This type of attack in WSNs can cause major problem in operations and services of the networks. Sinkhole attack is the most complex attack. Sinkhole attack is a very dangerous attack that leads the base station to have entire and accurate sensing data, In this attack sinkhole node attracts data towards itself by convincing the other neighbors through broadcasting fake information. It is a kind of denial of service where a malicious node will attract all packets by falsely showing fresh route to the destination and without forwarding them to destination. The aim of denial of service attacks is to disrupt the routing and prevent data generated from the source nodes to reach the sink or destination nodes. The attacker announces the false optimal path by showing the bandwidth, attractive power or high quality routes to particular region. Other nodes will further consider the path through this attacker node better than which currently used one, and move the traffic onto it. It may lead to problem of system failure in terms of the network availability. And this makes sensor node unable to transmit or receive information. It also enable many other attack.
A sinkhole attack can be launched by,

- a laptop with high range that can provide less hop paths to other nodes
- a spoofed/fake message indicating a node is closer to base station (BS) or a BS
- a wormhole (hidden tunnel) providing low latency and less hop distance links or
- a hello flood attack providing unidirectional links to unreachable nodes

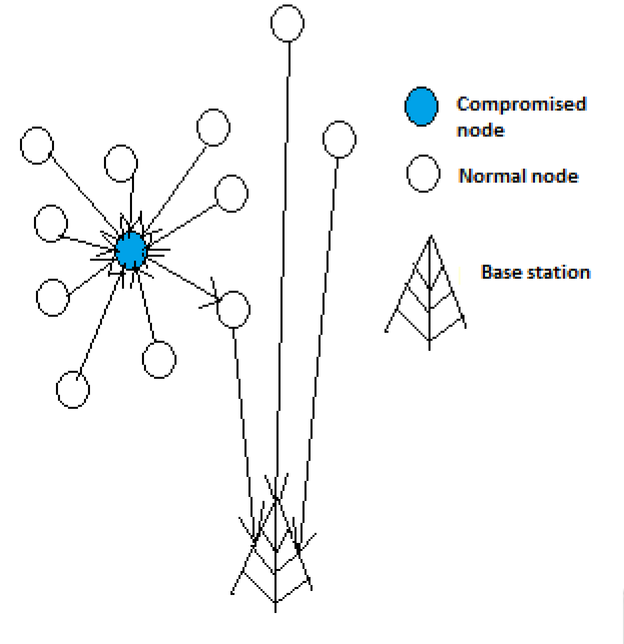

Figure 5.1: Sinkhole attack scenario

Sinkhole attack scenario in wireless sensor network is as shown in the figure 5.1. It consists of compromised node, normal node and base station. As shown in the above figure sinkhole attack is launched by compromising the node. A compromised node will attract all packets by falsely showing fresh route to the destination and without forwarding them to destination. Further compromised node may alter the message and can deliver it to the destination. At the same time few packets are dropped by the compromised node.

6. TECHNIQUES TO DETECT SINKHOLE ATTACK

6.1 Hop Count Monitoring Scheme

The subject presented in [1] includes Anamoly Detection System (ADS) scheme based mainly on hop count monitoring to detect the sinkhole attacks in WSNs. Since hop-count feature can be easily obtained from the routing tables, the ADS system is very simple to implement with small footprint. This scheme analyzes the magnitude of hop-counts which is stored in node's routing table. Moreover, this ADS can be easily applicable to all routing protocol that maintains hop-count parameter as a measure of distance between the source and destination nodes. When base station initialize the network this scheme collects the training data as a source of hopcount measurements. By using this training data can construct as expected hopcount and compare this with threshold limits to differentiate normal updates and attack updates network failure updates. By using single ADS, we are able to obtain a detection rate of 96% with zero false alarms for attacks in the simulated network. In addition, we were able to achieve a 100% detection rate by using small number of ADSs at strategic locations in the network.

6.2 Secure Routing Using Mobile WSNs

The secure routing algorithm to detect the sinkhole attacks in mobile WSNs based on mobile agents is discussed in [2]. Since there is no any communication restriction between mobile agents and nodes, mobile agents have enough power to run the algorithm. Firstly, A few mobile agents will communicate with each node to collect network information to set up global information matrixes of the nodes by which data packets are further routed and transferred. Each node knows the entire network since every node has a public cache. The node also erase the outdated information in the cache by using latest information in agent packet. Then, by using these routing algorithms we can easily avoid sinkhole node. In addition, algorithms can achieve more global information by using few agents, so this will mainly reduce the overhead for maintenance of information of the nodes and it will be highly efficient and robust.

6.3 Using Message Digest Algorithm

The new message digests algorithm with high complexity and less collision resistant is proposed [3] in order to detect the sinkhole attacks. The main aim of this protocol is to find out the exact sink hole with the help of one-way hash chains. This scheme can detect the sinkhole only when the digest which is obtained from the trustable forward path and the digest obtained through the trustable node to destination are different from each other. The algorithm is also a bit robust to deal with the cooperative malicious node that tries to hide the real intruder. The working function of this detection scheme is tested and performance is also analyzed in terms of detection accuracy. This algorithm is tested in MAT lab. This digest method detection also meets the security goals such as data availability, data integrity, data authenticity, time synchronization and confidentiality.

6.4 AODV Based Algorithm

AODV based secure routing algorithm are mainly based on mobile agent for detecting the malicious node which are involved in sinkhole attack is proposed in [4]. To send data packets from source to destination it is required to select the correct path. For selection of correct path it is necessary to detect sinkhole node in the network. This algorithm searches the sinkhole node by finding the differences between the nodes sequence numbers using their obtained threshold value. If the difference exceeds the threshold value then it will be considered as sinkhole node. The performance of proposed algorithm will be then examined through simulations which will further confirm the effectiveness and accuracy of the algorithm by taking considerations of few performance metrics as Throughput, PDR and Packet loss. Simulation is then carried out using the simulator NS2.

7. COMPARISON OF SINKHOLE ATTACK DETECTION ALGORITHM

Table 1 shows the comparison of different sinkhole attack detection algorithms by considering the parameters, communication overhead and computation overhead.

Table 1: Sinkhole Attack Detection Algorithms Comparison

Techniques	***Comparison***		
	Parameters	***Communication Overhead***	***Computation Overhead***
Hop-Count Monitoring	Hop-Count,ADS nodes, High broadcast-ID, High sequence number	Low	High
Secure Routing using Mobile WSNs	Mobile agent, Repeated next hop node	High	Low
Using Message Digest Algorithm	One-way hash chains	High	Low
AODV Based Secure Routing Algorithm	Mobile Agent, Threshold Value, Nodes sequence Numbers	Low	Low

8. CONCLUSION

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

9. REFERENCES

[1.] 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.

[2.] Liping Teng, Yongping Zhang, "Sera: A Secure Routing Algorithm Against Sinkhole attacks For Mobile Wireless Sensor Networks", Second International Conference on Computer Modeling and Simulation 2010, PP 79-82.

[3.] 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.

[4.] Vandana B. Salve, Leena Ragha, Nilesh Marathe, "AODV Based Secure Routing Algorithm against Sinkhole Attack in Wirelesses Sensor Networks" IEEE 2015.

[5.] Vinay Soni, Pratik Modi, Vishvash Chaudri: "Detecting Sinkhole Attack in Wireless Sensor Network", International Journal Of Application On Innovation in Engineering and Management 2013,pp. 29-32.

[6.] Kashif Saghar, Mamoona Tariq, David Kendall, Ahmed Bouridane: "RAEED : A Formally Verified Solution to Resolve Sinkhole Attack in Wireless Sensor Network"13th International Bhurban Conference On Applied Science and Technology (IBCAST), 2016,pp.334-345.

[7.] Jio Qi Tang Hong, Kuang Xiaohui, Liu Qiang: "Detection and Defence of Sinkhole Attack in Wireless Sensor Network" IEEE, 2012, pp-809-813.

[8.] Yu, B., Xiao, B .: Detecting selective forwarding attacks in wireless sensor networks. In Proceedings of the 20th International Parallel and Distributed Processing Symposium (SSN2006 workshop), Rhodes, Greece, pp. 1-8 (April 2006).

[9.] Chris Karlof David Wagner, "Secure Routing In Wireless Sensor Networks: Attacks and Countermeasures", 2006, PP 1-20.