IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 4, Issue3, June - July, 2016
ISSN: 2320 – 8791 (Impact Factor: 2.317)
www.ijreat.org

Location Hiding To Mitigate The Sinkhole Attacks In WSN

Roopa S.N[1], Chinnaswamy C.N[2], Dr.T.H.Sreenivas[3]

[1]PG student, Department of IS&E, The National Institute of Engineering, Mysore, India..
[2]Associate Professor, Department of IS&E, The National Institute of Engineering, Mysore, India.
[3] Professor, Department of IS&E, The National Institute of Engineering, Mysore, India.

Abstract
With the advances in innovation, there has been an increasing interest in the use of Wireless Sensor Networks (WSNs).WSN is a collection of numerous sensor nodes which are capable to sense, collect and disseminate information for multiple applications. WSNs are susceptible to many attacks such as Jamming, Sybil, Wormhole and Sinkhole. Among which sinkhole attack is most destructive where the colluded node pretends to have a shortest routing path to base station by which it entices the traffic of its nearby nodes to perform malicious operation. The idea is to detect the sinkhole attack by monitoring hop count and to mitigate it through the reconfiguration. This report describes the way to detect and mitigate the attack.

Keywords: *Sinkhole, Hop count monitoring, RESIST-0 Reconfiguration protocol, RESIST-1*

1. Introduction

WSN consist of large number of autonomous sensors that monitors environmental and physical conditions later forwards the data sensed to the BS for maintaining the network [1]. Gathering information and monitoring is the important objective of these kinds of networks. These networks are capable of self organizing and healing. Wireless sensor network has a major difference with the traditional wireless network in which the sensors are sensitive to consumption of energy. The performance of the applications of wireless sensor network is highly dependent on the network lifetime. A sensor network comprises of numerous detection stations called sensors, each of which is small, lightweight and portable. The sensors are inexpensive, small in size, and are deployed in unreachable locations. They have limited power source, processing capabilities and energy, and restricted memory. The above constraints challenge the task of security. For the purpose of transmission radio communications are used as media in these kinds of networks which are liable to numerous security attacks.

2. Types Of Attacks

Security [2] in WSN is an important aspect that has to be considered as they are vulnerable to a numerous collection security attacks. Nowadays designing a good security mechanism with respect to numerously increasing applications which include military, medical, environmental etc is necessary. The Routing threats are as follows:

2.1 Wormhole Attack: In this attack, whole packet or message is copied by an attacker, tunneling them to another network from the originator. Latter the copied message is forwarded to the destination node.

2.2 Selective forwarding: In Selective forwarding attack, a node selectively discards the packets by dropping which are coming into that network from an individual node or a group of individual nodes.

2.3 Sybil attack: A Sybil attack is an advanced version of an impersonate attack in which a malicious user may steal many identities. In technical terms, a malicious node

represents itself to the other nodes by obtaining multiple identities within it.

2.4 Sinkhole attack: Sinkhole attack is most destructive where the colluded node pretends to have a shortest routing path to BS by which it entices the traffic of its nearby nodes to perform malicious operation

2.5 Altered, Spoofed/ Replayed Routing Information: This is the most direct attack. By altering, spoofing, or replaying routing data the attacker is successful to complicate the network and create routing loops, attracting or repelling traffic, generating faulty error messages, extending source routes or partitioning the network.

2.6 Hello Flood Attack: In multiple routing protocols, nodes broadcast hello messages to announce their presence to their neighbours. A node receiving such a hello message can assume that the node that sent the message is within its range. Each attacker with a excessively powered antenna can persuade every node in the network that it is their neighbor.

Among these attacks Sinkhole attack is the most devastating routing attack for these networks. It causes a serious threat to sensor networks, which in turn increases overhead of network, decreases network lifetime by boosting energy consumption and finally destroy the network. Solution to security can be classified as prevention based- where encryption and authorization are used but results in high computation, detection based- uses system's behavior to discover attacks.

3. Sinkhole Attack:

Sinkhole attack is most destructive where the colluded node pretends to have a shortest routing path to BS by which it entices the traffic of its nearby nodes to perform malicious operation and hence causes serious threat to WSN. Sinkhole attack works with reference to routing algorithm by making a colluded node alluring to neighboring nodes. Verification of the routing information provided by a node is difficult hence detection of the sinkhole attack is arduous. Fig1.1 shows the sinkhole attack architecture.

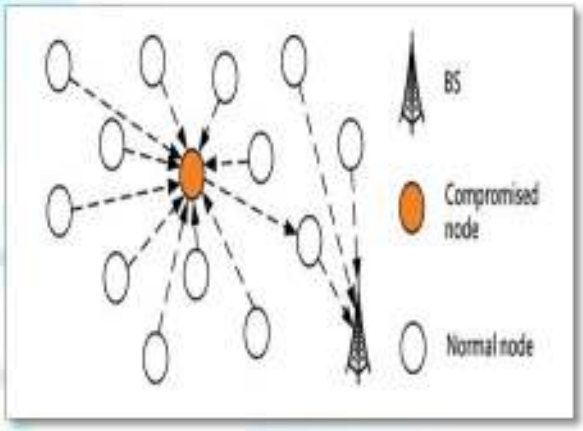

Fig1: Scenario of Sinkhole Attack.

4. Literature Survey

In [3], the main goal of this protocol is to discover the sink hole utilizing the one-way hash chains. In this method destination/sink identifies the attack solely when the digest obtained from the trustable forward path and the digest acquired through the trustable node to the sink are different. It also ensures the data integrity of the messages transferred using the trustable path, low computation overhead but increases time and power requisite to forward the message in different paths which result in high communication overhead. This algorithm is also robust to deal with cooperative malicious nodes that make an effort to hide the real intruder. The functionality of this algorithm is tested in MAT lab. The performance of this algorithm is appraised through simulations, and that confirmed the accuracy of the algorithm in terms of

Success rate, false positive and negative rate. Thus the digest method of detection meets the security goals such as data integrity, data authenticity and availability, confidentiality, data authenticity and time synchronization

In [4] sometimes the adversary node receives all data by advertising itself as a fake BS in the network. It intercepts data from reaching the BS, or else changes the data received and then transmits them to the main BS. . In the proposed approach, when a node desires to transmit data to the BS, it firstly sends a control packet directly to the main sink. Later it begins to transfer data packets to the BS in the form of hop by hop routing. When the data packet arrives at the sink, the control fields are compared with the similar ones of the real control packet. If any changes are made to these control fields in the data packet, it shows that there is a malicious node; the BS detects it using the proposed strategy. This approach provides efficiency in terms of energy consumption. It increases the communication overhead as the control packet is sent again before data transfer. The performance of the proposed method has assessed, compared with the algorithm proposed by Ngai's. The results of simulation state that the proposed algorithm is more efficient than it.

In [5] two approaches are used to detect the sinkholes in the networks. The rationale behind this method is that the node located around the sinkhole depletes their energy higher than other nodes because the route to the BS through sinkhole node is more attractive so are used regularly. Hence, energy holes are formed around each sinkhole. In the first approach the BS utilizes a geostatistical method to compute the residual energy of every sensing area and estimates the possibility of the presence of the sinkhole in individual area by an statistical estimat○r. Based on this value, the BS instructs all of the nodes to avoid the suspicious region in their routing. Distributed monitoring approach to detect areas with lower residual energy level is the second approach.

The purpose of this detection scheme is to discover sinkhole attacks using Mintroute based WSNs. In Mintroute protocol [6], the LQI value is utilized to discover the next hop to the sink. This value is compared by the packet loss rate. Hence the network adopts the routing tree structure; each node examines the violation of the rules on each parent-child pair throughout the tree. There are two regulations that are used to identify the sinkhole attack. The proposed detection architecture has two modules. The first module is the local sinkhole detection module which is implemented in each sensor node; whereas the second module is the decision module implemented in the sink.

5. Existing System

WSN are already been used in many applications such as ecological, military and areas related health. These applications often include the observation of sensitive information in this manner security is important in WSN's. Routing attacks have devastating effect towards WSN and presents a major difficulty when designing the mechanism of security. Sinkhole attack is the most dangerous routing attack for WSN's, it enable numerous other attacks. AODV based secure routing algorithm based on mobile agent method [7] is used for detecting the malicious node in sinkhole attack. The algorithm discovers sinkhole node by discovering the difference between the sequence numbers assigned to the nodes using threshold value. It shows performance assessment of AODV with the enhanced secure algorithm and existing secure algorithm through simulations, which confirms the algorithm accuracy and effectiveness which takes into account the performance metrics as Throughput, PDR and Packet loss.

This approach is well used not only for avoiding sinkhole attack but also used to detect the sinkhole node in the network precisely. This algorithm provides low communication overhead, but the usage of mobile agent leads to new computing paradigm, which is contrast to traditional client/server-based computing.

6. Proposed System

In this paper, we have presented a scheme based on hop count monitoring for detecting sinkhole attacks in wireless sensor networks. Since the hop-count feature is effortlessly obtained from routing tables, the Anomaly Detection System is simple to implement with a small footprint. Anomaly Detection System (ADS) which analyzes the magnitude of hop-counts stored in a node's routing table. Moreover, the proposed ADS are applicable to any routing protocol that dynamically maintains a hop-count parameter is a measure of distance between the source and the sink.

Our main idea is to construction of tree using reconfiguration protocol [8] and then to route the packet from the source to BS. During the process of routing the data packet the sinkhole node is detected by comparing the hop count of each node in the route towards the base station. There are multiple scenarios that can be considered when the route is being identified a) the packet can dropped due to link failure or it may intentionally drop because of the existence of sinkhole node and latter may not reach the BS, b) when the sinkhole node is detected, the reconfiguration protocol is called to get rid of sinkhole node during the discovery of new path. Our simulation of the sinkhole attack showed that, in an unprotected routing protocol, the attacker was able to successfully capture almost the entire network by broadcasting a single routing message.

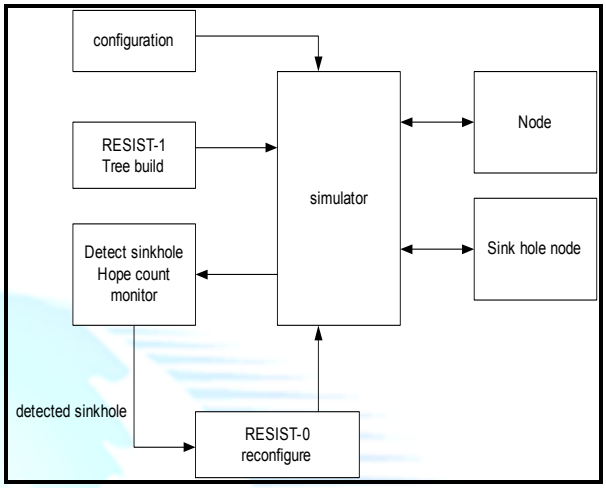

Fig 2: Architecture of the proposed system

7. Result

The proposed solution is implemented in NS2 .the number of sent and deliver packets with and without the existence of sinkhole node was observed. Our simulation results have been compared with AODV routing method and performs better than this.

Performance analysis based on delay and delivery ratio is shown in the above graph. When compared to AODV the proposed approach offers lower delay and higher delivery ration.

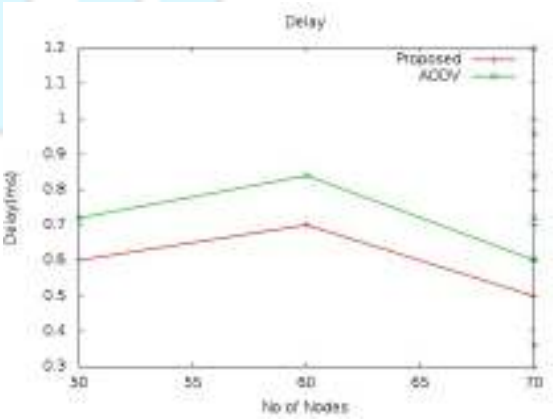

Chart 1-Delay graph for AODV and hop count monitoring

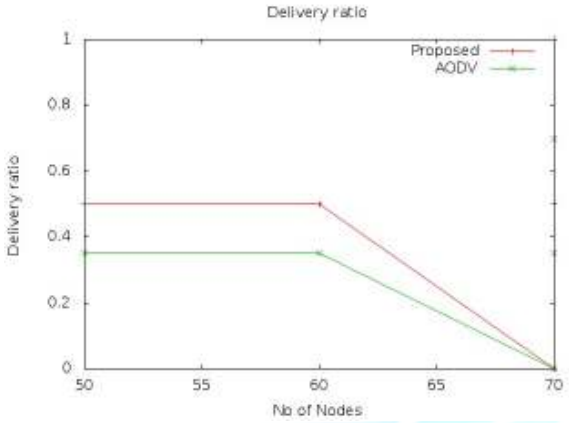

Chart 2-Delivery ration graph for AODV and hop count monitoring

8. Conclusion

We presented a method to detect sinkhole attach with the help of hop count monitoring combined with re-configuration protocol RESIT-0 and RESIST-1.Routing tables are used to obtain the feature of hop-count. . We show that our scheme can detect attacks with 96% accuracy in a simulated network.

References

[1]. Sanjeev Kumar Gupta, Poonam Sinha "Overview of Wireless Sensor Network: A Survey", International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 1, January 2014.

[2].Mr. Manish M Patel, Dr. Akshai Aggarwal," Security Attacks in Wireless Sensor Networks: A Survey" 2013 International Conference on Intelligent Systems and Signal Processing (ISSP).

[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.

[4.] Maliheh Bahekmat, Mohammad Hossein Yaghmaee, Ashraf Sadat Heydari Yazdi, and Sanaz Sadeghi" A Novel Algorithm for Detecting Sinkhole Attacks in WSNs "

[5.] H.Shafieia, A.Khonsaria, H.Derakhshia, P.Mousavia "Detection and mitigation of sinkhole attacks in wireless sensor networks" Journal of Computer and System Sciences 80 (2014) 644–653

[6.] Murad A. Rassam, Anazida Zainal, Mohd. Aizaini Maarof and Mohammed Al-Shabotiz "A Sinkhole Attack Detection Scheme in Mintroute Wireless Sensor Networks "1st IEEE International Symposium on Telecommunication Technologies

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

[8.] Anthonis Papadimitriou, Fabrice Le Fessant, Aline Carnerio Viana and Cigdem Sengul " Cryptographic Protocol to Fight Sinkhole Attacks on Tree-based Routing in Wireless Sensor Networks" 978-1-4244-4865 IEEE