Research Journal of Computer and Information Technology Sciences _____________________E-ISSN 2320 – 6527
Vol. **4(8),** 4-7, August **(2016)** *Res. J. Computer and IT Sci.*

Review Paper

Sinkhole Attacks in Wireless Sensor Network Routing: A Survey

Kavita Tandon
Department of Computer Science and Engineering, Bhilai Institute of Technology, Durg, Chhattisgarh, India
tinkytandon@gmail.com

Available online at: www.isca.in, www.isca.me
Received 24th Feburary 2016, revised 1st August 2016, accepted 14th August 2016

Abstract

The capacity of Wireless Sensor Network (WSN) is often limited by many factors like communication range, memory, battery but security is the measure concern as wireless networks are most vulnerable to the attacks. Because of inherent resource and computing constraints in unattended environments, the risk of secure transmission over the network has increased. There are many attacks possible on WSN like selective forwarding, denial of service attack, Sybil attack, jamming, black hole attack, sinkhole, wormhole and hello flood attacks. One of the most notably routing attacks is Sinkhole attack in which attacker lure the network by advertising the high quality routes to the base station. It is very likely that these nodes prevent the arrival of information to the base station. When these achieve their objective, the attack will be launched along with the invitation to the dangerous threats like black hole or gray hole. In this paper, we have described various strategies for detecting sinkhole attacks and methods to neutralize them.

Keywords: Sinkhole, Attacks, Wireless, Sensor, Network, Routing.

Introduction

Wireless Sensor Network (WSN) consists of autonomous nodes which are used to collect physical or environmental information from a supervised specially an isolated area and delivers it to centralized base station. Smart sensor nodes are low power devices equipped with one or more sensors, a processor, memory, a power supply, and a radio. Generally, the nodes monitor temperature, sound, pressure etc and cooperatively pass these data to the center. A variety of mechanical, thermal, biological, chemical, optical, and magnetic sensors may be attached to the sensor node to measure these properties. The basic applications include monitoring of Habitat, Ecosystem, Health, Seismic, Groundwater contamination, Rapid emergency, Industrial process, automated building climate control etc[1]. But sensor devices often lack in energy, computation, and communication capabilities in order to make the network cost-wise feasible. To overcome this we can make use of secondary power supplies like solar energy, wind energy etc but again it will solely depend upon the location and nature of the sensor device deployed.

Data transmission to the base station is also difficult because of the remote locality. For this, a radio can be installed to transfer the data to a base station[2]. Also, these are often deployed in accessible areas which posses the risk of physical attack on the nodes. The unattended operation of sensors along with limited number of computational and communicational resources makes this network susceptible to several attacks. In this paper, we will discuss different Sinkhole attacks among them and try to propose their remedies.

In the sinkhole attack, attacker tries to lure the other nodes in network through a compromised node to launch an attack by showing the attractive routing metrics. Because of the rigorous verification of the routing information sent by nodes in network, it is equally difficult to counter this attack. Once Sinkhole attacks enter into a network, they lead to further attacks like Selective Forwarding attack, Black hole attack, Wormhole attack, Flooding attack etc. If casted with sinkhole attack, it can also result in more severe form of selective forwarding[3]. Many existent sinkhole attack detection technique is based on hop-count based routing. Hence, Sinkhole can be stopped by improving the routing protocol but routing also faces various issues in wireless sensor network.

Routing and Security Challenges

Despite of numerous applications of sensor network, these have several limitations such as limited power or bandwidth. Here, the nodes are stationary and have constraints on energy, storage and processing capacity. IP based protocols cannot be applied because there is no global ID addressing. Even, the data sent by nodes are very redundant in nature. These constrains must be addressed before the start of communication. Routing protocol should also include the goal of prolonging the network life. Data aggregation and Quality of services are the additional services to improve efficiency of the network.

Routing in WSN is indeed unique and distinguished from other wireless network because here the flow of almost all the applications is towards single base station. A simple change in node status (in case of failure or any other emergency) leads to the unpredictable change in topology. The probability of redundancy in data is also very high because most of the data are generally collected from similar nodes working for common phenomena. Moreover, if the node is mobile (e.g., a tracking application), routing becomes more challenging.

Thus, the routing in WSN is characterized by three network structures: i. Flat Based, ii. Hierarchical Based, iii. Location Based.

These protocols define the architecture of the network and the heterogeneity among the nodes. Some WSNs consist of homogenous nodes, whereas some consist of heterogeneous nodes. This classifies whether the nodes are operating on a flat topology or on a hierarchical topology. In Flat-based routing, each node is treated equally as these have same functionalities whereas in Hierarchical- based which comprises of more than one layer. Higher energy nodes are used for transmission and lower energy nodes are used for sensing. This discrimination also increases lifetime of the nodes. Last category is the Location based technique in which nodes are addressed based on their location. The locations are acquired by GPS or via coordination among nodes. This routing can be made more efficient by incorporating local state information e.g. residual energy, link quality and distance etc[1]. Robust routing is also a desired condition of these networks which means robust delivery of information is must even when the links are wireless, unreliable and time varying.

The protocol operation also classifies WSN in different categories like Query based routing, QoS based routing, Aggregation routing, multi-path routing etc. A distributed routing may be used to evade any central path computation that could be very expensive in large networks.

Initially, WSN was evolved basically for military application which was a very challenging job. Even today, when civilian applications have been recognized, it is the major source of information for military in remote areas. Because of the unique requirements of the routing, WSNs need specific routing algorithm. And naturally, there is always a demand of routing algorithms which are energy efficient, optimized, data centric and secure. These routing algorithms must be able to achieve following security contributes: i. Confidentiality: Data must not be disclosed to unauthorized person. ii. Integrity: Data must not be altered before reaching to the destination. iii. Authentication: Only authenticated must be able to access the network and its data. iv. Availability: Data must be available when needed. v. Data Freshness: Latest Data should be updated as soon as possible. vi. Non-repudiation: Sender cannot deny from the fact that he has sent data. vii. Authorization: The authorized person must be able to access the data.

The Routing protocol should be able to select the optimum route that can be characterized by several elements such as hop-count, bandwidth, link quality and its delay[4]. In the procedure to find out the optimum route to the destination, it can be deceived by an attacker node which has feigned itself to be on the shortest path and the sinkhole attack can be easily instigated. Even if there is only one such hole in the network, the impact can be hazardous.

Due to the wireless and distributed nature of WSNs, these are less protective, and hence more prone to security attacks. These attacks can be broadly classified into two categories; Active attacks and Passive attacks. Passive attacker just monitors and listen the communication channel but active attacks can also modify the data stream. Former includes Eavesdropping, Traffic analysis whereas later concludes all other attacks which are discussed earlier. Since many nodes send data to a single base station because of the many to one communication pattern and the nature of the network is ad hoc, WSNs are particularly vulnerable to sinkhole attacks.

Sinkhole Attack

Sinkholes do not target all the nodes in the network (actually these do not need because of the communication flow) but only those nodes whose are close to the base station[5]. The intruder nodes (nodes which are compromised by the attacker) can have same or more power than other nodes in network and claim to have the shortest path to the base station. If the intruder node has greater computational and communicational power, it manages to create a high quality single hop connection with the base station. Then it advertises these luring features to the other nodes and as the consequences, others will send their traffic to the intruder only. Likewise the intruder nodes call for the attack. Sinkhole attacks can also track the nodes using a tunnel or wormhole. These form the base for other attacks which includes Denial of Service, Sybil, Wormhole, Blackhole etc[6].

In most of the literature, basically two types of Sinkhole attacks are discussed. First one is Sinkhole attacks using a highly qualified node and second one is using a wormhole[2]. As shown in Figure-1, the attacker node announces itself as the shortest route to the destination. This compromised node is generally equipped with high computational and communicational power which routes itself at one hop count from the base station. The route is advertised as the high quality route, which spoofs the surrounding nodes creating a sinkhole.

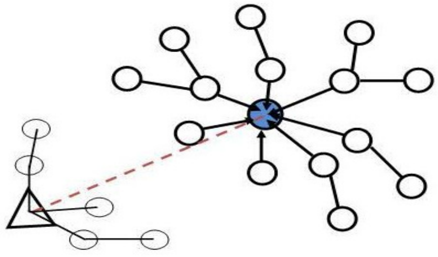

Figure-1
Sinkhole using a qualified node[7]

The Figure-2, illustrates the second technique in which the sinkhole is created using the intruder/malicious nodes. This malicious node attracts all the information from its neighbors and tunnels the collected data to another malicious node routing towards the base station.

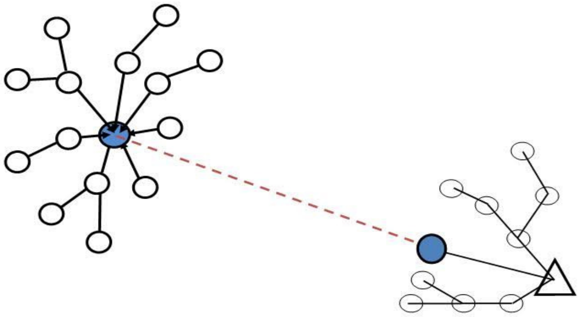

Figure-2
Sinkhole using a Wormhole[7]

Various Security Approaches against Sinkholes

Different researchers have given a number of solutions for sinkhole attacks in WSN which can be broadly classified in to two steps: i. Sinkhole Detection, ii. Sinkhole Prevention.

Sinkhole Detection: As we have already discussed that the detection of Sinkhole attack in a wireless network is difficult to counter. Demonstrating the fact, assume an adversary node having strong power radio transmitter which can transmit enough power to be extended to a wide area network that empowers it to offer a high-quality route[2]. The neighboring node will not understand this and get tricked by these nodes. So, it's very tedious task to detect these sinkholes. However we have various techniques which are already defined in different classifications like anomaly-based, rule-based, statistical methods, cryptographic and hybrid approach.

Anomaly Based defines the legitimate user behavior and anything that appears as anomalous is suspected as intruders. But these can also suspect a legitimate user as defective one generating false alarms. In rule based network, few rules are defined and the node violating the rules are considered as adversary and isolated from network. In statistical one, data associated with certain activities are recorded and a threshold is defined for each one. Any node which advertises more attractive features or exceeds the threshold value, are suspected as compromised node. In this cryptographic approach, encryption technique is used to protect the data and also to detect any modification in the message.

Hybrid approach combines the benefits of the anomaly based detection and cryptographic approach which will reduce the false alarm. It also maintains a blacklist of the suspected nodes and catches the intruders based on their signature if it is not present in detection database.

Sinkhole Prevention: While detecting the sinkholes, several countermeasures are also defined by researchers and authors to take against this attack. Below is the brief of the algorithms described by these authors: In Data Consistency & Network flow approach, base stations are also involved. In this method, a request message is flooded in the network, which contains the IDs of the affected nodes, to get the ID of the next hop and the cost associated with it[7]. Then it constructs a network flow graph using the information collected to identify the sinkhole. Since it involves base station as well, it is comparatively costly but it is very robust even in that case when an insider node tries to hide the intruder.

INTI considers the attacker node can play any role in the network like free node, member node, leader node etc[3]. So, it offers self-organization which coordinates the network configuration, and self-repairs which detects the suspicious nodes along with the cluster re-grouping to maintain network stability. The four modules defined are: i. Configuration of Clusters, ii. Monitoring Routing, iii. Detection of the attacker, iv. Isolation of the attacker.

The configuration of cluster defines the network architecture in which 'initially free nodes' are classified in different clusters of members and leaders. The role can changed based on the network conditions, demands and attacks. After that, a monitoring module is defined to count the number of input and output transmissions. If the number of incoming transmission is equal to outgoing ones, it is not a sinkhole. Otherwise the chances of security leakage are there. The paper gives a brief algorithm to detect the sinkhole which is based on iterations, actions, information exchanges, or the behavior in the transmission of message. After detecting the culpable node, an alarm message is broadcasted in the network to alert the neighboring nodes for the isolation of the culprit. If the sinkhole node is a member or associated node in the cluster, it will be isolated by the leader of the cluster. In case, if the leader is itself the culprit, the members of the group or the associated node will isolate the attacker. If the scenario is mobile, it can detect the sinkholes with 75% accuracy and incase of fixed scenario, the success rate is even 92% with a very low rate of false positives and negatives.

Hop Count Monitoring, which falls under Anomaly Detection scheme described above, has been detailed by Dallas, Leckie, and Ramamohanarao by monitoring the hop count proposed by the nodes[8]. The author has achieved 96% accuracy with no false alarms when they simulated the Hop Count Monitoring on a simple Anomaly Detection System, ADS. Another approach of Hop Count monitoring has been discussed by Choi, Cho, Kim, Hong, and Kim, in which base station monitors the nodes which are not transmitting the data in the predefined duration[4]. The list of such nodes is made by the station and the possibility of selective forwarding is checked. Also, it collects the next hop information from the neighboring node in the savaged area change the entire topology of the network. Certainly, this scheme is only limited for few attacks like Selective forwarding where the attacking node is deliberatively not transmitting message of some selected nodes (Figure-3).

Received Signal Strength Indicator, RSSI, gives a robust and lightweight solution by collaborating come Extra Monitor nodes apart from ordinary nodes[9]. On the other hand, Monitoring CPU usage of the nodes analyzes the consistency of CPU usage by comparing the usage with predefined threshold[10].

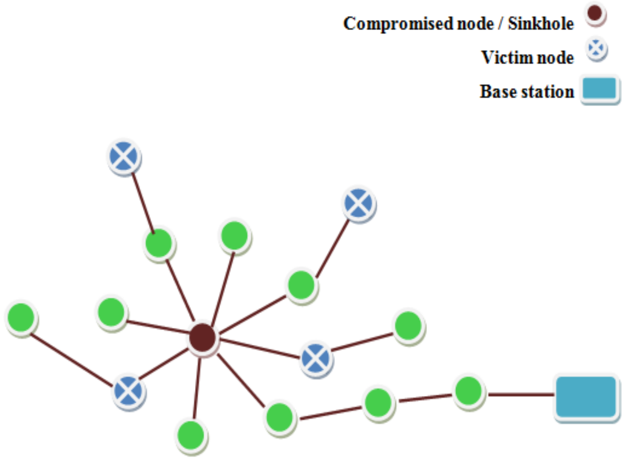

Figure-3
Sinkhole Detection Example

Mobile Agent Based Approach defends against sinkhole using a self controlling program[11]. The agents navigate from node to node not only transmitting data but also doing computation. Their task is to collect information of all mobile sensor nodes to make every node aware of the entire network so that a valid node will not believe the fraud of malicious node. This algorithm is very efficient because it neither needs any encryption or decryption mechanism to detect the sinkholes nor require more energy than other approaches.

Message Digest approach detects the exact sinkhole using the one-way hash chains[12]. If the message digest obtained from the forward path and the digest obtained from the trusted node is different, a possible attack can be detected. This algorithm also ensures the data integrity and is very robust. Integrity of the message is maintained because it is transferred using the trustable path.

Conclusion

This paper presents a review article on several routing and security challenges in WSNs concentrating mainly on Sinkhole attacks. It further gives various approaches to detect and prevent the sinkhole attacks. It finally concludes with the countermeasures used against this attack. According to most of the research paper, anomaly detection can be better solution if implemented with the algorithm which can reduce false alarms.

References

1. Bhaskar Krishnamachari (2005). An Introduction to Wireless Sensor Networks. Second International Conference on Intelligent Sensing and Information Processing (ICISIP), Chennai, India.

2. Soni Vinay, Modi Pratik and Chaudhri Vishvash (2013). Detecting Sinkhole Attack in Wireless Sensor Network. *International Journal of Application or Innovation in Engineering & Management*, 2(2), 29-32

3. Christian Cervantes, Poplade Diego, Nogueira Michele and Santos Aldri (2015). Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for Internet of Things. IM, IFIP/IEEE, 606-611.

4. Choi Byung Goo, Cho Eung Jun, Kim Jin Ho, Hong Choong Seon and Kim Jin Hyoung (2009). A sinkhole attack detection mechanism for LQI based mesh routing in WSN. Information Networking, International Conference, ICOIN, IEEE. 1-5.

5. Chaudhry J.A., Tariq U., Amin M.A. and Rittenhouse R.G. (2013). Dealing with sinkhole attacks in wireless sensor networks. Advanced Science and Technology Letters, 29(2), 7-12.

6. Sharma K. and Ghose M.K. (2010). Wireless sensor networks: An overview on its security threats. *IJCA*, Mobile Ad-hoc Networks, 42-45.

7. Ngai E.C., Liu J. and Lyu M.R. (2006). On the intruder detection for sinkhole attack in wireless sensor networks. In 2006 IEEE International Conference on Communications IEEE. 8, 3383-3389.

8. Dallas D., Leckie C. and Ramamohanarao K. (2007). Hop-count monitoring: Detecting sinkhole attacks in wireless sensor networks. In 2007 15th IEEE International Conference on Networks, 176-181.

9. Tumrongwittayapak C. and Varakulsiripunth R. (2009). Detecting Sinkhole attacks in wireless sensor networks. In ICCAS-SICE, IEEE. 1966-1971.

10. Chen C., Song M. and Hsieh G. (2010). Intrusion detection of sinkhole attacks in large-scale wireless sensor networks. Wireless Communications, Networking and Information Security (WCNIS), 2010. IEEE International Conference on. 711-716.

11. Sheela D., Kumar C.N. and Mahadevan G. (2011). A non cryptographic method of sink hole attack detection in wireless sensor networks. Recent Trends in Information Technology, 2011 International Conference on. 527-532.

12. Sharmila S. and Umamaheswari G. (2011). Detection of sinkhole attack in wireless sensor networks using message digest algorithms. Automation, Control and Computing (PACC), 2011 International Conference, 1-6.