International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463
Vol. 3 Issue 6, June-2014, pp: (377-380), Impact Factor: 1.252, Available online at: www.erpublications.com

A Survey of Sinkhole-Based Attack and Detection Techniques in WSN

Khushboo Tunwal[1], Rakhi Khandelwal[2], Divya Acharya[3], Priyanka Singh Dabi[4]
[1234]M.Tech in Computer Science, GWECA, Ajmer , RTU, Kota, Rajasthan

Abstract: Wireless Sensor network made by the small independent sensor nodes having low power low cost. The environment of WSN makes them very attractive to attackers. Security is therefore essential in WSNs. WSNs have limited energy resources, including low computation capability, many constraints, memory and small vulnerability to physical capture. These constraints are challenge for WSNs. There are many feasible attacks on wireless sensor network such as sinkhole, wormhole, sybil, jamming, and hello flood attacks. In this paper we are focusing on the routing attack identified as sinkhole attack as the biggest threat in wireless sensor network which is measured that spoils the overall communication and a data failure between a pair of nodes. Finally this attack attempts to disrupt the sensor networks completely. In this paper we have presented some detection techniques against the sinkhole attack.

Keywords: Adversary Node, Security Attack, Sinkhole Attack, WSN.

Introduction

Wireless sensor network is in order to use several applications, and resources are accessed remotely so every security evaluate regarding confidentiality, accessibility, verification, authorization, integrity etc. should be considered. Wireless sensor networks are vulnerable to various attacks. WSN must be protected from attackers who may devise different types of security attacks to create the system unstable [1].

Network made by the small independent sensor nodes that deploy over a geographical area for a wireless Sensor monitoring physical facts like humidity, events vibrations, temperature and so on. Small sensor nodes are the key component for data transmission in communication in wireless network [2]. The motivation of development of wireless sensor network is use in military applications like medical care, battlefield surveillance, and forest monitoring. This paper mainly includes classification of detection of sinkhole attacks using different matrix with different techniques. Section 2 focuses on the some different kinds of attack on wireless sensor network. Focuses on the sinkhole attack on wireless sensor network with using some routing protocol discussed in section 3. Section 4 discusses about the different techniques to detect sinkhole attack in wireless sensor network .The end section we show the conclusion.

Attacks on Wireless Sensor Network

The wireless sensor networks are self-configured and self-organizing networks which once organize are run autonomously [4]. These following are the major attack in wireless sensor network:

A. Jamming

Jamming in the sensor nodes comes with the (RF) radio frequencies. Some jamming nodes put a very large amount of the sensor nodes out of order. This is a DOS type of attack on the wireless network that cconstitutes complete DoS when adversary can block the entire network then. It requires a lot of capable hardware, as it is not a very common attack.

B. Tampering

A tampering attacker may break a sensor node, replace the part of its hardware or entire node or to get access to sensitive information that attacker entire node, for example access higher communication layers and shared cryptographic keys.

C. Altered or replayed, spoofed routing information

This is common attack. By altering or replaying, spoofing routing information the intruder can make difficult the network and create loops, attract or repel traffic, generate error messages, extend routes or partition the network. In this process, data is repeated maliciously in sensor network.

D. Selective forwarding

In such tupe of attack the intruder itself include in a data flow path. Then the attacker does not forward certain packets and drops some packets. It may also called gray hole attack.

E. The Sybil Attack

A attacker or malicious node make multiple identities of same sensor node in the network is a Sybil attack. So this attack is confusing because the adversary appears in a multiple location and that difficult to identify the node.

F. Wormholes

In wormhole attack the adversaries communicate via tunnels and data send or received form one network to another network. Routing can be disrupt when transmission of messages are tunnelled. So in this when two attackers creating a tunnel between them is referred as a wormhole.

G. Hello flood attacks

In this attack the nodes broadcast hello messages to all other nodes to show their presence in the network. After that whose node that receives such message can suppose that such node that sent message is in into the network range.

Sinkhole Attack

The sinkhole attack, the attacker node try is to attract all network traffic towards us through a compromised node. Using routing algorithm sinkhole attacks creates compromised node which attract all surrounding nodes.The node exploit the routing protocol, such as AODV and DSR, and the node to advertise itself as have a valid route to reach to the base station, with the purpose of intercept packets. [5].

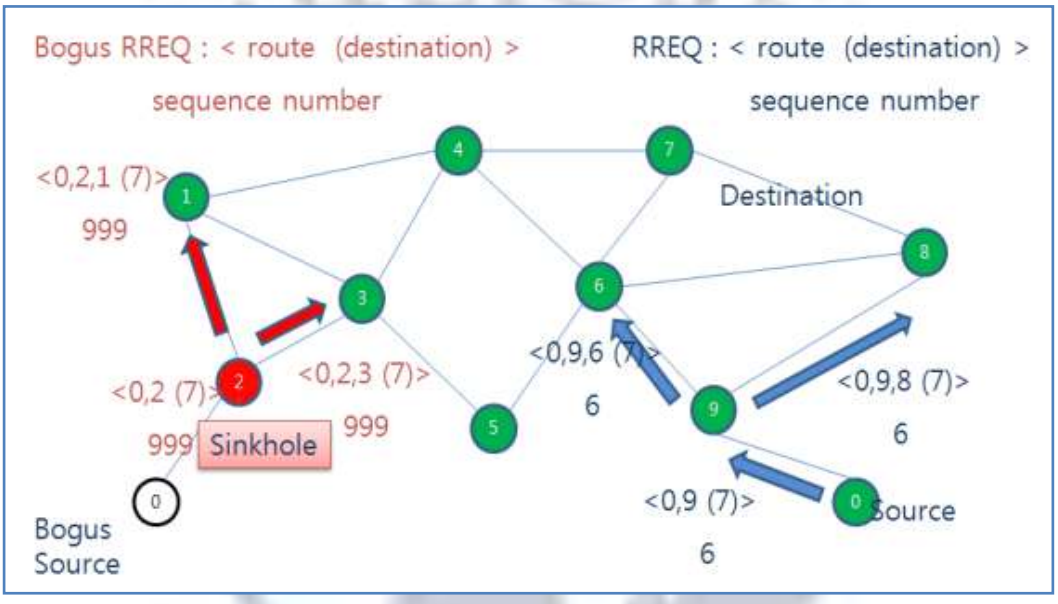

Figure 1: Generation of False RREQ by Sink-Hole Attacker.

We take a look of wireless sensor network that collection of distributed independent sensor nodes and base station, each have unique identifier. The sensor nodes continuously receive and send the message to the base station by hop by hop forward packets.

A sinkhole attack involves at least one attack node that falsely advertises itself as having an extremely efficient route to an important destination node, such as a base station functioning as a collection point in a sensor network. This can mislead the dynamic routing protocol in use, which then updates tables on sensor nodes so that all traffic on route to the base station (collection point) will be misdirected toward the sinkhole, which is believed to be in proximity with the base station [5][7].

Detection Techniques of Sinkhole Attack

This section discusses about the various countermeasures of sinkhole attack.

A. Network Flow Information & Multiple Malicious Approach

The network flow information and multiple malicious approach presented in [6] includes the base station in the detection process, for the protocol results are high communication cost. Request date containing the identity of the affected nodes and base station floods the network. The affected nodes reply a message containing their IDs to the base station, and ID of the next hop and the related cost. For identifying the sinkhole the received information is used from the base station to create a flow graph of sensor network. This proposed work is also strong that attempt to hide the real intruder and to deal with cooperative malicious nodes.

The countermeasure of algorithm has been tested through both numerical analysis and simulations. Now the results show effectiveness and accuracy of the approach. In this algorithm also suggest that its computation overheads are practically less for WSNs.

B. Hop Count Monitoring Approach

A hop count monitoring scheme is based on novel intrusion detection system that detects the occurrence of a sinkhole is viewed in [7]. The hop-count value is easily obtained from data routing tables, the Anomaly Detection System (ADS) is simple to implement with a small footstep. Also, it is valid to any routing protocol that measure distance between source and destination nodes for a hop-count parameter that dynamically maintains. The hop count monitoring scheme can sense attacks with 96% correct and in a simulated network no error false using a single detection system.

C. Received Signal Strength Indicator Based Scheme

A new approach Received Signal Strength Indicator (RSSI) is robust and right solution for detecting the sinkhole attack is proposed in [8]. The proposed solution correlates some Extra Monitor (EM) nodes separately from the ordinary nodes. At origin position (0, 0) Base Station (BS) is located at there and values of RSSI get from position of all sensor nodes that determine four EM nodes. In order to sense Sinkhole attack this information is used for the BS. The simulations results of proposed mechanism are lightweight due to the EM nodes were not associate with any ordinary nodes or BS. There is no communication overhead.

D. Monitoring node's and Analysis consistency of CPU usage

A monitoring node's and analysis consistency of CPU usage based on novel algorithm for detecting sinkhole attacks for wide area sensor networks is presented in [9]. A change-point detection problem is formulated that problem. In this scheme consistency of the CPU usage being analyzed and monitor CPU usage of every node. The base station calculates the discrepancy of CPU usage of every node and at the fix time interval that monitoring the CPU usage of each node, than this difference is compared with a threshold, the base station now identify that whether a node is malicious or not. So this proposed algorithm is capable to find difference between the legitimate and the malicious nodes.

E. Mobile Agent Based Scheme

The mobile agent based approach is the scheme to detect sinkhole attacks is proposed in [10]. Mobile agent is a self containing program unit which is self controlling. To transmitting data and doing computation the mobile agent navigate from node to node. A routing algorithm that has multiple constraints is proposed in mobile agents based approach. To create each node aware of the entire sensor network the mobile agents is to gather information of all mobile sensor nodes so that a compromised node which leads to sinkhole attack or right node does not listen in the corrupt information from malicious. This approach does not require extra energy than normal routing protocols.

F. Light weight detection scheme and new Message Digest Algorithm

The light weight detection scheme and new message digest algorithm for detection of sinkhole attack in wireless sensor is proposed in [11]. To detect the exact sink hole we use one-way hash chains in proposed algorithm. That is the main goal of this algorithm. In this method destination or base station detects the attack only when the process obtains difference between trustable node to the destination and the process obtained from the correct path. By using the trustable path it also ensure the data confidentiality and integrity of the data transferred. The algorithm is deal with cooperative malicious nodes that try to hide the real attacker. The functionality is tested in MAT lab.

G. Estimate the attacked area & Identify by intruder

The approach of estimate the attacked area and identify by intruder presented in [12] show how to detect a sinkhole attack in wireless sensor network, and how identify the intruder in area.

This proposed algorithm first focus on single malicious node and then enhances it to find multiple malicious nodes in next section. So, the algorithm first checking the data consistency to finds a record of malicious nodes, then analyzing the network flow information that successfully identifies the intruder in the list. The algorithm is also contract with multiple malicious nodes that together hide the real attacker. The countermeasure of algorithm has been tested both numerical measurement and simulations result. So the results show effectiveness and accuracy of the approach.

Conclusion

In this paper, we summarize the different detection techniques of sinkhole attack in wireless sensor networks and surveyed the some several security attacks related to the security in WSN. Look all strong attacks on wireless sensor networks, sinkhole attack is the vulnerable routing attacks for these networks. We have surveyed various detection techniques for sinkhole attack.

References

[1]. Aashima Singla, Ratika Sachdeva, "Review on Security Issues and Attacks in Wireless Sensor Networks" IJARCS, Volume 3, Issue 4.

[2]. Vinod Kumar Jatav, Meenakshi Tripathi, M S Gaur, Vijay Laxmi, "Wireless Sensor Networks: Attack Models and Detection", 2012 IACSIT Hong Kong Conferences,vol 30.

[3]. T.Kavitha, D.Sridharan, (2010) "Security Vulnerabilities in Wireless Sensor Networks: A Survey" Journal of Information Assurance and Security 5.

[4]. Manju.V.C., "A Survey on Wireless Sensor Network Attacks" (IJEIT) Volume 2, Issue 2 (2012).

[5]. Udaya Suriya Rajkumar, D., Rajamani Vayanaperumal, "A leader based monitoring approach for sinkhole attack in wireless sensor network" Journal of Computer Science 9 (9): 1106-1116, 2013.

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

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

[8]. Ruttikorn Varakulsiripunth, Chanatip Tumrongwittayapak, "Detecting Sinkhole Attacks and selective forwarding attack in Wireless Sensor Networks" International Joint Conference, ICROS-SICE,1966-1971, 2009.

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

[10]. Naveen kumar. C, Dr. G.Mahadevan, D.Sheela, "A Non Cryptographic Method of Sinkhole Attack Detection in Wireless Sensor Networks" ICRTIT, IEEE-International Conference, 527-532, 2011.

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

[12]. Ahmad Salehi S., M.A. Razzaque, Parisa Naraei, Ali Farrokhtala, "Detection of Sinkhole Attack in Wireless Sensor Networks" IEEE International Conference on Space Science and Communication, Melaka, Malaysia, 2013.