Sinkhole Attack Detection In Hierarchical Sensor Networks

Radhikabaskar, Dr.P.C.Kishore Raja, Suhasini Komara, Varsha Paul

Abstract:- Wireless sensor networks are used in many applications including military environments, environmental monitoring, health related applications, tracking applications. Security issues are very important as the wireless sensor networks are applicable to harsh and unattended environments. Multiple sensors send sensed data to the base station for further processing. Considering the deployment, computation and battery power, sinkhole attack is one of the severe network layer attack in sensor networks where an intruder attracts surrounding nodes with unfaithful routing information, and then performs selective forwarding. In this paper we propose a method to detect the sinkhole attack in hierarchical sensor networks based on energy level. Performance evaluation is analysed based on packet loss, packet delivery, delay and network throughput

Index Terms: - wireless sensor networks(wsn), sinkhole attack,ns2,cluster head.

1 INTRODUCTION

Wireless sensor networks rely of many to-one communication approaches for data gathering.This approach is extremely susceptible to sinkhole attack, where an intruder attracts surrounding nodes with unfaithful routing information which causes an important threat to sensor networks. Wireless sensor networks (WSNs) have been used as a low cost solution for data measurement and collection[1] WSN's monitor critical infrastructure such as water distribution such that the integrity of the WSN is protected against malicious attacks. The connectivity in the network can be disrupted by the routing protocols used in WSNs which are potentially vulnerable to routing attacks. The wired networks are protected by traditional cryptographic defenses. The limited communication and Central processing unit resources in low-cost wireless sensor nodes makes resource intensive cryptography impractical so the second line of defense – intrusion detection system detects the various attacks. In general, routing attacks are classified as active and passive attacks. In an active attack, the adversary monitors, listens and modify the data stream in the communication channel.

In passive attacks, the adversary monitors listens to the communication channel. Sniffer, eavesdropping are passive attack. The active attacks alter, spoof, replay routing information and they are selective forwarding, sinkhole attack; sybil attack, wormhole attack, and hello flood attack. The detection rules and countermeasure techniques is presented in [4,12].

2 SINKHOLE ATTACK

A sinkhole attack in wireless sensor networks can cause serious problem in the operations and services of the networks. It may lead to the problem of system failure in terms of network availability and it makes the sensor node unable to transmit and receive information. It is a kind of denial of service attack where a malicious node can attract all packets by falsely claiming a fresh route to the destination and without forwarding them to the destination as shown in Fig.1

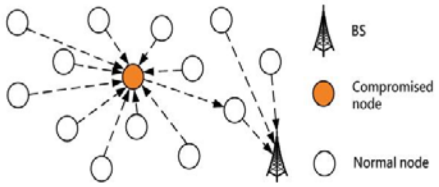


Fig.1 Sinkhole attack

The work of a sinkhole attack is to make a compromised node look attractive to surrounding nodes with respect to the routing algorithm. Protocols may try to verify the quality of route with end-to-end acknowledgements containing reliability or latency information. The sinkhole attack will forward packets destined for a BS through the adversary and also propagate the attractiveness of the route to its neighbour.

2.1 Sinkhole attacks in wireless sensor networks

The basic idea of the sinkhole attack is to change the routing information and attract the traffic in the network. In [1,2,3] a low overhead algorithm for base station which collects the network flow information from the attacked area and an efficient identification algorithm to analyze

- *RadhikaBaskar is currently pursuing Ph.D degree program in Electriconis and Communication Engineering, Saveetha University. E-mail: radhikabaskr@gmail.com*
- *Dr.P.C.Kishore Raja, Professor and Head , Department of Electriconis and Communication Engineering, Saveetha University. E-mail: pckishoreraja@gmail.com*
- Suhashini Komara,Varsha Paul , student, Saveetha School of Engineering, suhasini.komara@gmail.com varshapaul@gmail.com

the routing pattern and identify the intruder is presented for detecting the sink hole attack. Accuracy of the algorithm is analysed by success rate, false positive rate and false negative rate. Sinkhole attack is detected in [5] by a beacon message which checks the whether the sender field is the node ID of one of its neighbour and the past cost difference between the parent and child should not exceed. This method is aiming at whether a node is sending a fake LQI.[14] uses LQI as the metric to detect attack.

In [6] a light weight detection scheme is proposed for detecting the sinkhole attack in wireless sensor network. The new message digests algorithm with high complexity and less collision resistant is proposed in order to identify the sinkhole attacks. The scheme detects the sinkhole, when the digest transmitted in the trustable route and new route are different. The functionality of the detection scheme is tested and the performance is analyzed in terms of detection accuracy. Another notable intrusion detection system (IDS) for detecting sinkhole attack is presented in [7]. This system assumes a routing layer that is based on link quality metrics to form a routing tree towards the base station. Every node acts as a watchdog for its immediate neighbouring nodes. In each node, there is an IDS client which contains a key component, a cooperative detection engine, that stores and applies all the rules and monitors data to determine whether there are rule violations. If one node observes a rule violation, its local detection engine knows that one of its neighbouring nodes is the attacker and it broadcasts an alert to all its neighbouring nodes. On receiving such an alert, the watchdog calculates the inter section between its own neighbour list and the node list found in the alert. The nodes in the intersection are stored in a table and used for computing the intersection with the next alert. The attacker is identified and isolated.

In [8] a statistical GRSh-based algorithm for detecting malicious nodes is presented. By monitoring the CPU usage of each node in fixed time interval, the base station calculates the difference of CPU usage of each node. After comparing the difference with a threshold, the base station identifies whether a node is malicious or not. Detection time, false positive rate, and effectiveness are three metrics in designing the algorithm. A secure routing algorithm against sinkhole attacks for mobile wireless sensor networks based on mobile agents is proposed [9]. Firstly, A few mobile agents communicate with each node to collect the network connection information to build the global information matrix of nodes by which data packets are routed and transferred. Then, through the routing algorithm for data packets the sinkhole node is effectively avoided.

A new approach of robust and lightweight solution for detecting the Sinkhole attack based on Received Signal Strength Indicator (RSSI) readings of messages[10]. The proposed solution needs collaboration of Extra Monitor (EM) nodes apart from the ordinary nodes. RSSI values are used from four EM nodes to determine the position of all sensor nodes where the Base Station (BS) is located at origin position. This information is used as weight from the BS in order to detect Sinkhole attack. The simulation results show that the proposed mechanism is lightweight due to the monitor nodes were not loaded with any ordinary nodes or BS. Moreover, the proposed mechanism does not cause the communication overhead. Hop count monitoring scheme for detecting sinkhole attacks in wireless sensor networks is presented in [11] and a non cryptographic method of detecting sinkhole attack is presented in [13]

2.2 Malicious node detection

WSNs typically consist of small and inexpensive devices deployed in open, unprotected, and unattended environments for long term operations to monitor and collect data. This data is subsequently reported back and base station checks its node id and energy level. If the energy level is less than the required level, it easily identifies and removes the attacker. The current routing protocols in sensor networks show usually vulnerability to the sinkhole attack. In this paper we present a algorithm in order to detect the sinkhole attack and to recognize the engaged intruder. It is a lightweight algorithm as hierarchical sensor network is analysed.

In this section we learn to find a sinkhole attack in hierarchical wireless sensor network and how to identify the intruder in the area. The sinkhole attack tempts almost all the traffic from a special network by way of a compromised node making a metaphorical sinkhole with the adversary at the base station. Sinkhole attack acts by making a compromised node which appears to be interesting to encircling nodes concerning the routing algorithm. Sinkhole attacks are difficult to counter because of the difficulty to confirm routing information provided by the node.

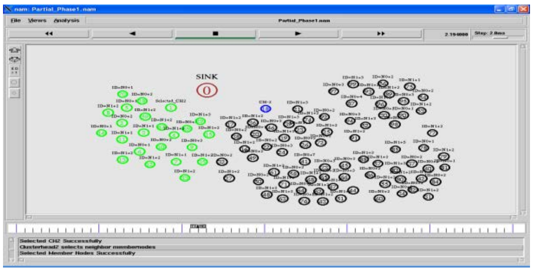
A broad area of the network can be obtained by permitting laptop-class adversary to supply a high quality route by transmitting with adequate power. We focus on single malicious node and then work can be enhanced to find multiple malicious nodes. The list of suspected nodes are found by the algorithm by checking the data consistency and then effectively it identifies the intruder in the list through analyzing the network flow information.

3 PROPOSED SINKHOLE ATTACK DETECTION METHOD

The mechanism of Detection of sinkhole attack on the context of AODV protocol is implemented by considering the working of AODV & behaviour of sinkhole attack which is mainly done by the packet forwarding algorithm. In the proposed system the base station selects the cluster head initially and also assigns the node id for the cluster head and the base station monitors only the selected cluster head.

Then the cluster head forms its sub nodes based on coverage area. as shown in the Fig.2. Then the formed cluster head selects the other cluster head and selects the surrounding node depending upon the coverage area. Depending upon the nodes that are created the number of clusters can be formed as shown in the Fig.3. All the nodes are given an amount of 100joules of energy and all the nodes are specified with an different node id. The transmission of the data from the source node to the destination node is designed by the algorithm called as the packet forwarding algorithm. This algorithm will be placed at intermediate nodes in the network. When transmitting the data packets, request will be distinguished between routing which refers to choosing the path for a packet and packet forwarding, which is the actual delivery of the packet. Routing can either happen automatically using an algorithm or manually by the Network administrator. If the destination node of packet is the interfaces then it is delivered to the information response using packet forwarding algorithm. When the data is transferred from one node to the other node some amount of energy of the node gets reduced. The node which losses highest amount of energy and blocks the transferred information is detected as the sinkhole attack.

The analysis of the energy is displayed and the node with lowest energy is detected and the node is blocked for the further transmission of the packet. A command called class.cache is programmed to automatically increase the energy level of the all the cluster heads since all the data from the node is transferred to the cluster heads.



Selected CH2 Successfully
Clusterhead2 selects neighbor membernodes
Selected Member Nodes Successfully

Fig.2: cluster head selection

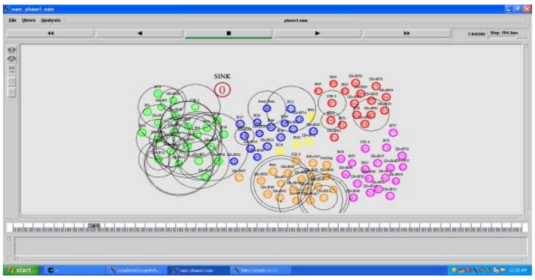


Fig.3:- cluster heads formation

3.1 Simulation

In this section the simulations were designed on the NS-2 network simulator. The simulation configuration is shown in detail in Table1. A wireless sensor network with a 150 meter by 150 meter field in which 100 nodes are placed with uniform random distribution. The sensors adopt IEEE 802.11 MAC protocol. In order to collect data from the sensors a base station is placed at the centre of the network. Furthermore, a sinkhole attack is added to the network at x-and y- coordinates(50,50)in order to emulate. It is important to evaluate the accuracy on intruder identification. The packet size is given as 1000.the traffic type is the CBR(constant bit rate).the simulation time is given to 200 seconds. The parameters analysed are energy level, cluster formation, packet loss, delay, packet delivery, throughput for the layered sensor network(--) and the proposed hierarchical network(--). It is seen that there is an effective reduction in packet loss, packet delivery rate and delay and there is an effective increase in throughput.

No.of nodes	100
No. of sinkhole	1
Packet size	1000
Traffic type	CBR
Sinkhole location	(1119.18,306.673)
Location of BS	(624.774,829.4111)
Transmission range	50m
Protocol	AODV
Grid area	(1900,1100)
Simulation time	200 seconds

Table 1: simulation configuration

3.1.1Packet Loss

It is the measure of number of packets dropped by nodes due to various reasons. The lower value of the packet lost means the better performance of the protocol. Packet lost = No of packet send – No of packet received.

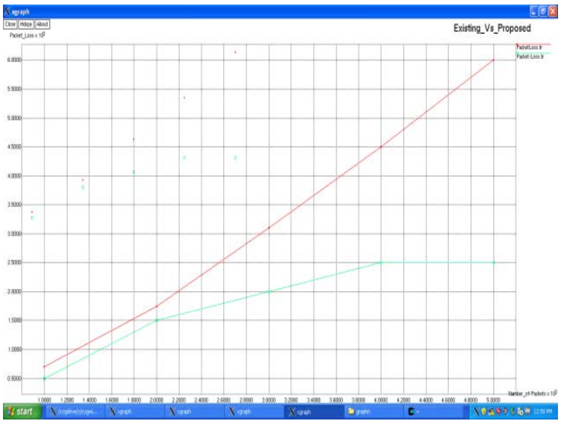


Fig.4 :-packet loss

3.1.2 Network Throughput

Throughput is the number of data packets delivered from source to destination per unit of time. Throughput is calculated as received throughput in bit per second at the traffic destination.

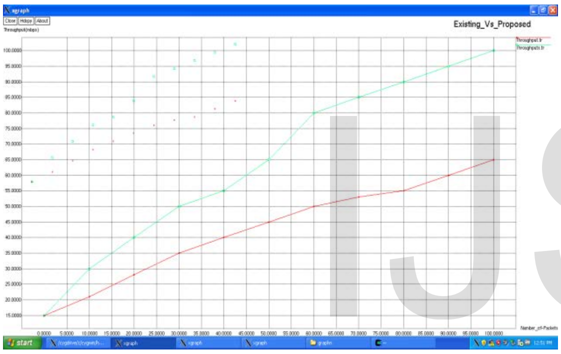


Fig.5:-Network Throughput

3.1.3 Packet delivery rate

It is defined as the packets that are successfully delivered for destination or the received acknowledgement to the number of packets sent by the sender.

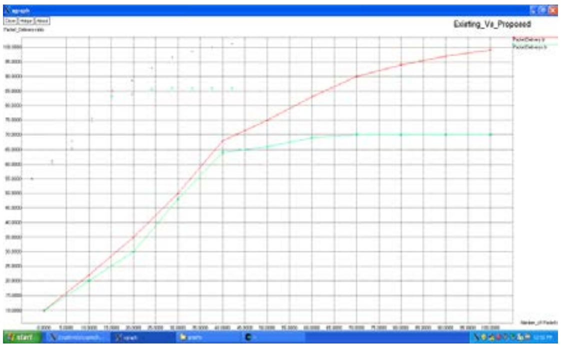


Fig.6:-packect delevery rate

3.1.4 Delay

It is calculated as a difference between the reception time of the first packet and the transimission time of the first packet.

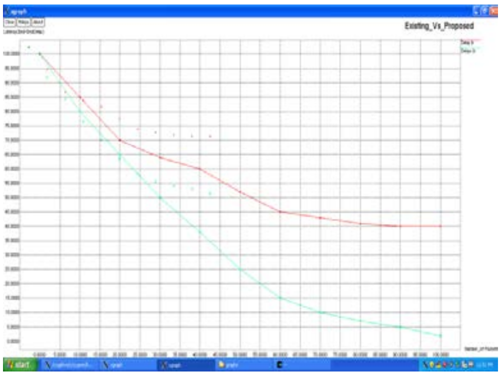


Fig.7:-delay

3.2 Future work

Our future work will mainly focus on to analyze & study sinkhole problem on the context of other routing protocols and to evaluate variation in its performance after applying our detection & prevention mechanism by considering other performance metrics also

4 CONCLUSION

The main goal of sinkhole detection in hierarchical sensor network is to improve the performance based on the parameters compared to layered structure. The detection method locates a list of suspected nodes by testing consistency of data. Then the intruder in the list is recognized by analyzing the network flow information. The performance is investigated by simulations. As a result, the effectiveness and accuracy of the algorithm have been demonstrated at the result in last section. This work can be further improved specifically in greater effective statistical algorithms to recognize inconsistency of data. Therefore they can correctly locate suspected nodes in sinkhole attacks and can identify communication and computation overhead and it also provide a security for data transmission.

REFERENCES:

[1] Ahmad Salehi S., M.A. Razzaque, ParisaNaraei, Ali Farrokhtala 'Detection of Sinkhole Attack inWireless Sensor Networks' Proceeding of the 2013 IEEE International Conference on Space Science and Communication (IconSpace), 1-3 July 2013,pp 361-365

[2] Ngai, E. C. H., Liu, J. and Lyu, M. R. On the intruder detection for sinkhole attack in Wireless Sensor networks. IEEE communication Society matter expert..Published in IEEE 2006. June. Canada. 3383-3389.

[3] Ngai, E. C. H., Liu, J. and Lyu, M. R. An efficient intruder detectionalgorithm against sinkhole attacks in wireless sensor networks.Computer communication. 6 May, 2007. Elsevier locate. 2353-2364

[4] I.Krontiris, ThanassisGiannetsos, TassosDimitriou. "Intrusion detectionof sinkhole att n acks in wireless sensor networks" in Proceedings of the3rd International Workshop on Algorithmic Aspects of Wireless SensorNetworks (AlgoSensors 07), Wroclaw, Poland, July 2007.

[5] Jin Qi, Tang Hong, KuangXiaohui, Liu Qiang'Detection and Defence of Sinkhole Attack in WirelessSensor Network'978-1-4673-2101-3/12/2012 IEEE pp809-813

[6] Sharmila, S. and Umammaheswari, G. Detecting of sinkhole attack inWireless Sensor networks using Message Digest Algorithms.978-1-61284-764-1/11/IEEE pp75-80

[7] I. Krontiris, T. Dimitriou, T.Giannetsos, and M. Mpasoukos, "IntrusionDetection of Sinkhole Attacks in Wireless Sensor Networks," AlgorithmicAspects of Wireless Sensor Networks, Lecture Notes in ComputerScience, Springer, Vol. 4837, pp. 150-161, Article number 12, February2008.

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

[9] LipingTeng, Yongping ZhangSeRA: A Secure Routing Algorithm against Sinkhole Attacks for Mobile WirelessSensor Networks , 2010 Second International Conference on Computer Modeling and SimulationDOI 10.1109/ICCMS.2010.95

[10] Chanatip Tumrongwittayapak and Ruttikorn Varakulsiripunth,'Detecting Sinkhole Attacks In Wireless Sensor Networks',ICROS-SICE International Joint Conference 2009

[11] Daniel Dallas, Christopher Leckie, Kotagiri Ramamohanarao; "Hop-Count Monitoring: Detecting SinkholeAttacks in Wireless Sensor Networks" 15th IEEE International Conference on Networks, 2007, ICON 2007, pp.176-181.

[12] Karlof, C. and Wagner, D. Secure Routing In Wireless Sensor Networks :Attack and Countermeasures. International confrance in Canada. (2003). 21-24 May Canada

[13] D.Sheela, Naveen kumar. C and Dr. G.Mahadevan; "A Non Cryptographic Method of Sinkhole Attack Detection in Wireless Sensor Networks" IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011, pp. 527-532

[14] Choi, B. G., Cho, H. E., Hong, C. S. and Kim, J. H. A sinkhole Attackdetection Mechanism for LQI based Mesh Routing in Wireless Sensor Networks. International confrance wireless security. 21-24 january (2008). Korea. 65-8