Impact Factor (SJIF): 3.632

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

(Special Issue for ITECE 2016)

Improved Technique for Detection and prevention of Blackhole Attack in Wireless Sensor Network

Kashyap Dave[1], Prof. Vaseem Ghada[2]

[1] *Dept. of Computer Engineering, B.H.Gardi college of Engineering and Technology, Rajkot*
[2] *Dept. of Computer Engineering, B.H.Gardi college of Engineering and Technology, Rajkot*

Abstract — Wireless Sensor Networks (WSN) is a growing innovation in today's world and has an widespread variety of usages for example forest fire detection, traffic surveillance, flood detection, battlefield surveillance etc. However WSN can be pretentious by various attacks which obstructs ordinary operation of the system. Security and reliability of sensor network is in a smaller amount because of random architecture of sensor nodes in uncluttered environment, power limitations, memory limitations and unattended nature. In general, two types of Attacks are in WSN- active attacks and the passive attacks. Black-hole attack is harmful active attacks. We have reviewed many technique regarding Blackhole Detection and Removal. And proposed a mechanism for discovery and removal of Blackhole attack from network.

Keywords-WSN; OLSR; Blackhole; Detection mechanism; networks

I. INTRODUCTION

A WSN contains numbers of sensor nodes that are distributed in environment. This allows arbitrary distribution of nodes in unreachable terrains, calamity relief actions and some other applications. Other applications of Wireless Sensor Network are environmental control such as fire-fighting or installing sensors on buildings or bridges to understand earthquake vibration patterns also aquatic ground floor erosion, surveillance tasks etc. Due to no infrastructure environment and wireless environment of WSN, they are more pretentious by many types of security attacks.

1.1. OLSR overview

This protocol is Proactive routing protocol that is known as table driven protocol. It has three types of control messages which are below.

- **Hello:** Hello control messages are transmitted for sensing the neighbor and for Multi Point Relays (MPR) calculation.
- **Topology Control:** These are link state signaling that is performed by OLSR. Multi Point Relays(MPRs) are used to adjust these messaging.
- **Multiple Interface Declaration (MID) :** MID messages holds the list of all IP addresses used by all node in the network. All the nodes running OLSR transmit these messages on more than one interface.

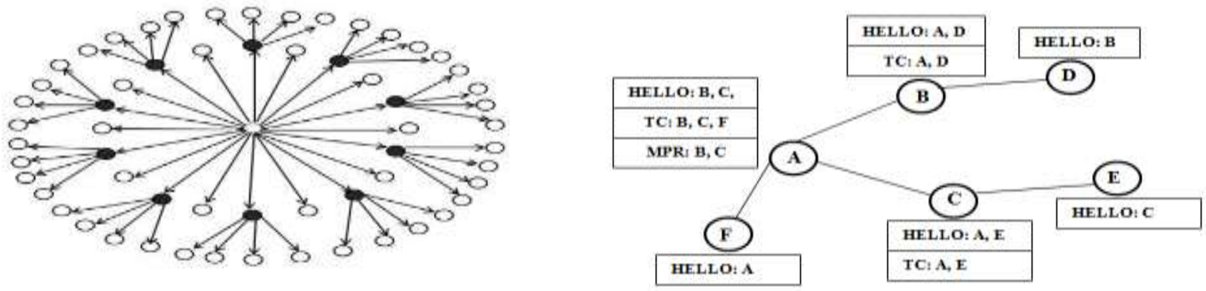

Figure. 1. OLSR protocol [12]

Above figure describes how OLSR actually works. All node selects own MSR from their neighbor nodes. In figure node A is selecting his MPR so, its neighbors sends their 1 hop and 2 hop neighbors to node A. After gating replies from all neighbor nodes, Node A will select its MPR which has maximum neighbor links. Neighbor request will be send by Hello messages and replies will be send by TC messages [9].

II. BLACKHOLE ATTACK

Blackhole attacks happen when trespasser captures and reprograms a set of nodes in the network to block the packets they receive as an alternative of passing them towards the base station. As a result any information that enters in the black hole region is caught. Blackhole attacks are easy to found and they are capable of undermining network effectiveness by separating the network, such that main event information do not reach the base stations [8]. The network performance parameters, as example throughput and end- to- end delay are affected in the attendance of black hole nodes; throughput becomes very less and end- to- end delay increases.

In below figure , in network nodes A,B,C,D,E and Fare there. Node C is Blackhole. All node will pass the data to their next node but, node C will not pass any data to other nodes. It will dropp all the data

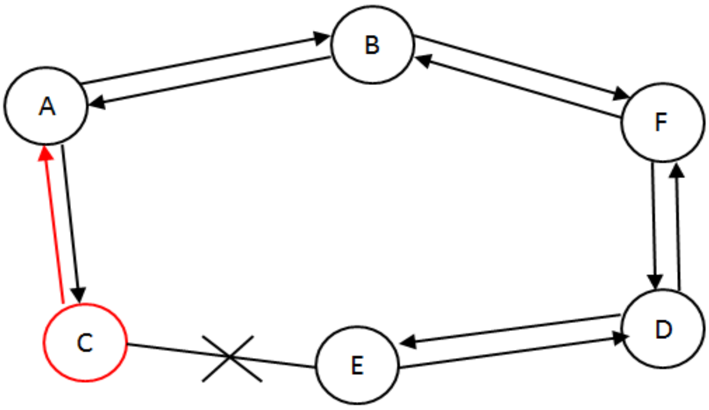

Figure 2. Blackhole attack [11]

2.1. Related work

We have studied many techniques regarding detection and prevention of Blackhole attack. That techniques are described in bellow literature survey table.

Sr. No.	Technique	Routing protocol	Tool of simulation	year	Parameters	conclusion
1	Fictitious Node [1]	OLSR	NS2	2015	Throughput , PDR	Packet loss decreases
2	ACK based SCHEME [2]	OLSR	OPNET	-	Packet delivery ratio, throughput	Increase Detection Rate
3	MOLSR [3]	OLSR	NS2	2014	Data Packet Lost, Detection Rate , PDR	Packet Delivery Ratio
4	DFOLSR [4]	OLSR	-	2014	Throughput	Increase Throughput
5	Trust based [5]	OLSR	-	2009	Detection Rate	Increase Detection Rate
6	Authenticated end-to-end ACK based approach [6]	AODV , OLSR	OPNET modeller	2014	network load , End to end delay	Decrease end to end delay, increase network load
7	Injection and Evaluation of Attacks on Ad hoc Proactive Routing Algorithms [7]	OLSR	NS2	2012	PDR, End-to-End Delay , Throughput	Increased packet delivery ratio

Table 1. Literature Survey

III. PROPOSED WORK

In order to run a Blackhole attack in OLSR, it is functional to fake HELLO and/or TC messages, because they are used to provide the basic connectivity in the network. The first option is faking only TC messages. This is not reasonable because it is probable to detect a fake TC message by means of local probability checks . The second probability is to fake HELLO and TC messages. This method is not chosen in this work, as a single node getting a TC message includes its address while not seeing the originator, a neighbor will be able to discover the attack. We will implement a third method. A node executing as black hole sends fake HELLO messages. In these messages an violent node claims to have links to more neighbors than it actually it has. Thus, there is a high possibility that this node is chosen as an MPR by its neighbor.

In this proposed solution uses trust analysis to verify whether corresponding node is malicious or not. Trust based analysis is useful for detect attacking node. My method will uses HOP_INFORMATION table, 2-hop request and 2-hop reply i.e. hello message. Generally, OLSR nodes trust all information that received from its 1-hop neighbors. Here we analyze the pattern of HELLO message of the node that advertise all 2-hop neighbors as its 1-hop neighbors and verify whether that node is malicious or not. In OLSR, TC and HELLO message are used to select MPR and route calculation. Each node must broadcast periodically HELLO message to indicate its existence. In this mechanism, each node maintains HOP_INFORMATION table which consist of HELLO message sender and its 2-hop neighbor. Each node maintain 2 hop away node list which getting from hello message from mpr. Attacking nodes send fake hello which contain fake information of 2 hop away node so using comparison of node id in HOP_INFORMATION table we will detect attacker. After that by watch dog mechanism all mpr will be analyze because external attacker will be caught by fake hello but if internal node is malicious node so it will be in all nodes HOP_INFORMATION table. If by watch dog any mpr is kept to loosing data so through hello we inform to other node about ATTACKING nodes.

Above we have described our proposed work in flow chart. First step is start. In second step all node will count their neighbor node via HELLO message. That nodes are also contains their reachability of 2-Hop nodes. After that it will check that maximum 2-Hop count member is present in their respective nodes. If that is exist in 2-Hop node table so that node will be select as MPR node, if that node is not exist in 2-Hop table so that node will be detect as BLACKHOLE node. After choosing as MPR node it will be monitor by their neighbor node threw watch Dog Mechanism. If that MPR is losing packets than that will be detect as BLACKHOLE and broadcast as Blackhole attack in HELLO message. If that is no packet loss by MPR so it will be broadcast as MPR node in HELLO message.

IV. SIMULATION

We have implemented Blackholes in NS2 simulator. Implementation details is below,

Simulator	Ns 2.34
Simulation duration	100 second
Simulation area	500 * 500 m
Number of Nodes	10, 20, 30, 40, 50
Packet size	512 bytes
Number of BlackHole	Null,1,2
Number of connection	5, 8, 12, 16, 20

Table 2. Simulation environment

Three metrics are used in the development of Blackhole attack scheme are the Packet Delivery Ratio (PDR), Throughput and End to End Delay. This all metrics are plotted against number of nodes.

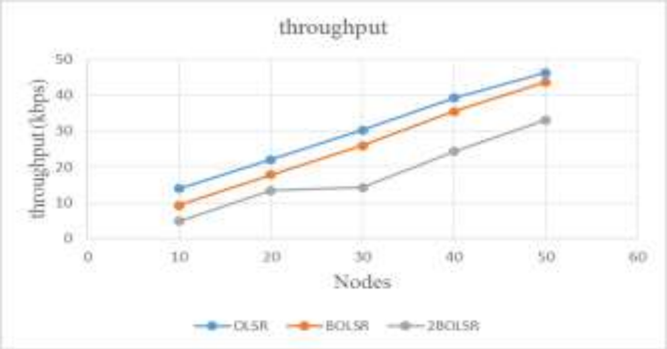

Figure 3. Throughput with Blackholes

Above figure describes graph of throughput with OLSR protocol, BOLSR (OLSR with single Blackhole) and 2BOLSR (OLSR with 2 Blackhole) for 10, 20, 30, 40 and 50 nodes. From graph we can clearly observe that throughput is decreasing with number of Blackhole are increasing in network.

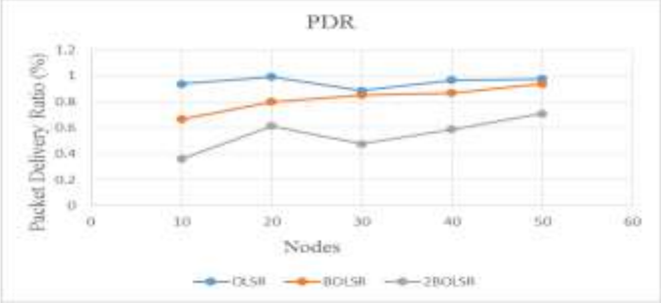

Figure 4. Packet Delivery Ratio with Blackholes

In above figure Packet Delivery Ratio is described for same environment. In that PDR is Decreasing with number of Blackholes are increasing in network.

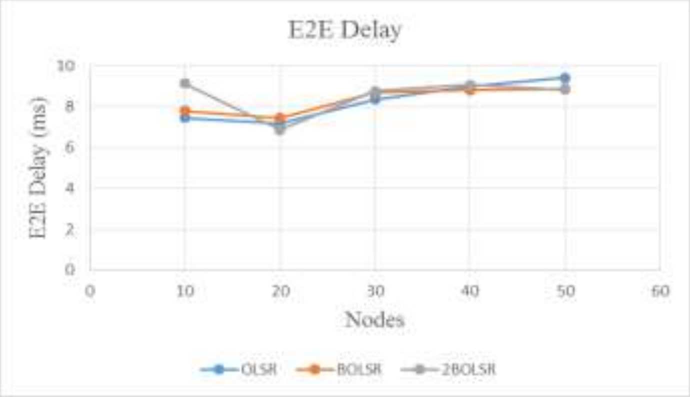

Figure 4. E2E Delay with Blackholes

In above figure E2E Delay is described End to End Delay for same environment. In that E2E Delay is increasing with increasing Blackholes in network.

V. CONCLUSION AND FUTURE WORK

We have analyzed different Blackhole detection techniques. After analyzing them we have described a technique for discovery and prevention of Blackhole attack which contains 2-Hop count and watch dog mechanism. 2-hop count for external node and watch dog mechanism for internal malicious node. Through this proposed technique performance of network will be increase. In implementation phase we have implemented Blackhole attack in OLSR protocol. We have taken result of simple OLSR, single Blackhole in OLSR and 2 Blackhole in OLSR for different number of and also compared them with each other. In our future work we will implement our technique for descovery and prevention of Blackhole Attacks.

VI. REFERENCES

[1] Nadav schweitzer, Ariel Stulman, Asaf Shabtai and Roy David Margalit "Mitigating Denial of Service Attacks in OLSR Protocol Using Fictitious Nodes," IEEE Transaction on Mobile Computing, Vol. 15, Issue 1, pp. 163-172, 2015.

[2] Soufine Djahel, Farid Abdesselam and Ashfaq Khokhar "An Acknowledgment-Based Scheme to Defend Against Cooperative Black Hole Attacks in Optimized Link State Routing Protocol," IEEE international Conference on Communication, pp. 2780-2785, 2008.

[3] Zougagh, Toumanari, Latif, Elmourabit and Noureddine "Modified OLSR Protocol for Detection and Prevention of Packet Dropping Attack," International Journal of Computer Applications, vol. 100, p. 0975 – 8887, 2014.

[4] Devesh Malik, Krishna Mahajan and Rizvi "Security for Node Isolation Attack on OLSR by Modifying MPR Selection Process," IEEE International Conference on Networks and Soft Computing, pp. 102-106, 2014.

[5] Asmaa Adnane, Christophe Bidan and Rafael Timoteo "Trust-based countermeasures for securing OLSR protocol," IEEE International Conference on Computational Science and Engineering, vol. 2, pp. 745-752, 2009.

[6] Abderrahmane Baadache and Belmehdi, "Struggling against simple and cooperative black hole attacks in multi-hop wireless ad hoc networks," Elsevier, vol. 73, pp. 173-184, 2014.

[7] Mahmood Salehi and Hamed Samavati, "Injection and Evaluation of New Attacks on Ad hoc Proactive Routing Algorithms," International Journal for Information Security Research, vol. 2, no. 1/2, 2012.

[8] Gupta "Introduction to Wireless Sensor Network", Science Direct, vol. 56, pp. 156-162, 2008.

[9] Ankita joshi and Lakshmi Priya "Injection and Evaluation of New Attacks on Ad hoc Proactive Routing Algorithms," International Journal for Information Security Research, vol. 2, Issue 1/2, 2012.

[10] Mohammad Wazid and Katal "Detection and Prevention Mechanism for Blackhole Attack in Wireless Sensor Network," IEEE ICCSP, pp. 576-581, 2013.

[11] Junguo Zhang and Zhao "The NS2-Based Simulation and Research on Wireless Sensor Network Route Protocol," IEEE International Conference on Wireless Communication, Networking and Mobile Computing, pp. 1-4, 2009.

[12] Vivek Katiyar, Narottam Chand and Naveen Chauhan "Recent advances and future trends in Wireless Sensor Networks," International Journal of Applied Engineering Research, Vol 3, No 3, 2010.

[13] John Stankovic "Research Challenges for Wireless Sensor Networks", Elsevier, 2012.

[14] Marjan Radi, Behnam Dezfouli, Kamalrulnizam Abu Bakar and Malrey Lee "Multipath Routing in Wireless Sensor Networks: Survey and Research Challenges," Sensors, vol. 12, pp.650-685, 2012.