ANALYSIS THE MITIGATION OF BLACK HOLE NODE FOR RAPID ENERGY DISSIPATION IN WSN: A REVIEW

Kundan Pandit[1], Prof. Anas Iqbal[2]
[1]M.Tech. (Digital Communication), [2]Dapartment Of Electronics And Communication Engineering,
All Saints' College Of Technology, Bhopal (M.P)

ABSTRACT: A Black Hole attack is a kind of denial of service attack where a malicious node advertise itself having the shortest path to the destination it wants to intercept.This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it. In protocol based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from actual node therefore a malicious and forged route is created. When this route is establish source node forward data packet through this route.Mobile ad hoc network faces various security challenges due to its nature. Hence, more packet delivery ratio is achieved. This approach identifies and avoids black hole node in the path discovery phase and hence path chosen by the source node will be secured for data transmission. This approach also has a high point that it does not depend upon the relationship between the nodes. The simulation is carried out in MATLAB. Thus, we evaluated that our algorithm shows better routing performance than an existing approach in terms of end to end delay. Security in MANET is a very vast area of research; we have just touched the surface of this field. In our algorithm, we have managed to mitigate only packet dropping attack. This algorithm can be further expanded to mitigate more other attacks.

Key Word: Black Hole, MANET, WSN, AODV, MATLAB

I. INTRODUCTION

1.1 Black hole Attack

In this attack, a malicious node acts as a black hole to attract all the traffic in the sensor network. Especially in a flooding based protocol, the attacker listens to requests for routes then replies to the target nodes that it contains the high quality or shortest path to the base station. Once the malicious device has been able to insert itself between the communicating nodes (for example, sink and sensor node), it is able to do anything with the packets passing between them. In fact, this attack can affect even the nodes those are considerably far from the base stations. The black hole attack is one of the simplest routing attacks in WSNs. In a black hole attack, the attacker swallows (i.e. receives but does not forward) all the messages he receives, just as a black hole absorbing everything passing by refusing to forward any message he receives, the attacker will affect all the traffic flowing through it. Hence, the throughput of a subset of nodes, especially the neighboring nodes around the attacker and with traffic through it, is dramatically decreased.

II. LITERATURE SURVEY

Researchers have proposed number of solutions to identify and eliminate a single black hole node. But they have many drawbacks. And few solutions are proposed to solve Collaborative Black hole Attack but still these solutions are not very effective, efficient and need improvement. So black hole problem in MANET is still an active research area.P.Goyal, V.Parmar and R. Rishi proposed Time-based Threshold Detection Scheme to detect single black hole attack based on secure AODV. End-to-end delay increased when malicious node away from the source node.P.N.Raj and P.B.Swadas proposed Detection, Prevention and Reactive AODV Scheme (DPRAODV). Algorithm improves the packet delivery ratio but it generateshigher routing overhead and end-to-end delay.Mistry N, Jinwala DC, IAENG, Zaveri M Improved AODV protocol by adding new table and a new timer. Proposed method can achieve high packet delivery ratio but end-to-end delay is high.Yu CW, Wu T-K, Cheng RH and Chang SC used Distributed Cooperative Mechanism (DCM) to detect collaborative black hole attack. Proposed mechanism improved the packet delivery and can achieve higher detection rate. And also it improves the control overhead.Min Z and Jiliu Z proposed MAC and Hash based PRF Scheme using AODV protocol. Mechanism can achieve higher packet delivery ratio and can detect co-operative black hole nodes. The drawback of the mechanism is the malicious node is able to forge a fake reply to dodge the detection scheme.

Tsou P.C., Chang J.M., Lin Y.H., Chao H.C. and Chen J.L. proposed Bait DSR (BDSR) based on Hybrid Routing Scheme to detect collaborative black hole attack. Proposed protocol always can achieve higher packet delivery ratio. The overhead is slightly higher than the original DSR routing protocol.Black Hole attack is studied under the AODV routing protocol and its effects are elaborated by stating how this attack disrupt the performance of MANET. Very little attention has been given to the fact to study the impact of Black Hole attack in MANET using both Reactive and Proactive protocols and to compare the vulnerability of both these protocols against the attack. There is a need to address both these types of protocols as to analyze black hole attack effect on MANET.

2.1 Literature Reviews

[1] S. Taruna1, Rekha Kumawat2, G.N.Purohit3 proposed a multi-hop cluster based routing protocol which is more energy efficient than single hop protocol. Simulation results show that the protocol offers a better performance than single-hop clustering routing protocols in terms of network

lifetime and energy consumption by improving FND. These sensor nodes can sense, measure, and gather information from the environment and, based on some local decision process, they can transmit the sensed data and send it to source to destination. A WSN typically has little or no infrastructure. It consists of a number of sensor nodes it may be ten or thousands that working together to monitor a region to obtain data about the environment. These sensors have the ability to communicate either among each other or directly to an external base-station (BS). A greater number of sensors allows for sensing over larger geographical regions with greater accuracy. The sensor sends such collected data, usually via radio transmitter, to a command center (sink) either directly or through a data concentration center (a gateway).In the wireless network there is no. node by which we can communicate .the number of node make a cluster and within the cluster all nodes make cluster head. The cluster head communicate with base station through another cluster head. Those whose distance is less to the base station they can communicate direct to the base station of cluster which contain no. of nodes and these nodes make cluster head with in cluster. These cluster head communicate with the base station.

[2] Taruna, 2Sheena Kohli 3G.N.Purohit Computer Science Department, Banasthali University, Rajasthan proposed a routing algorithm is related with energy and distance factors of each nodes. This scheme is then compared with the traditional LEACH protocol which involves selecting the cluster head which is nearest to the particular node. We conclude that the proposed protocol effectively extends the network lifetime with less consumption of energy in the network.

[3]Avani Patel1, Chandresh R. Parekh proposed an only deals with cluster based hierarchical protocol TEEN (Threshold Sensitive Energy Efficient Sensor Network Protocol). The sensor network architecture in TEEN is based on a hierarchical clustering. TEEN is data-centric, reactive, event-driven protocol which is best suited for time critical application. It transmits data based on hard threshold and soft threshold values. If the thresholds are not reached, then nodes will never communicate.

[4] Md. Zair Hussain1, M. P. Singh2 and R. K. Singh3 1Maulana Azad College of Engg. & Tech., Patna, India proposed the routing protocols differ on the basis of application and network architecture. With awareness is a compulsory design criterion, many new protocols have been specifically designed for routing, power management and data dissemination. Efficient routing in a sensor network requires that routing protocol must minimize network energy dissipation and maximize network lifetime.

[5] Aswini Kavarthapu Department of Computer Science and Engineering, QIS College of Engineering and Technology, Ongole, Andhra Pradesh, India. Narasimha Rao Sirivella proposed a method faulty sensor node is detected by discrete path selection technique by compare the actual RTT with present RTT. This method is simulated in NS2 on WSNs with eight sensor nodes designed using circular topology.

[6] Abderrahmane Baadache et. al. have suggested an approach that uses acknowledgments to authenticate and to correctly forward packets on the path. In this method, each packet receiving node sends a reply to the sender node to mark the successful reception of the message. The communication is authenticated using hash values. This approach is very computation intensive. Each node on the path has to recomputed the hash value and check. Also, there is communication overhead due to lack being sent by each node on the route.

2.2 Induction of problem

After performing analysis to identify which routing protocol is more vulnerable to Black hole attack, it is identified that performance of AODV is more affected than OLSR. Therefore OLSR can perform under black hole attack without much interruption. But AODV cannot perform well under the attack. Therefore a security solution for AODV routing protocol must be implemented to mitigate black hole attack. At the current stage of the research, implementing security solution for AODV routing protocol is in progress.

III. PROPOSED ROUTING PROTOCOL

3.1 Assumptions & Network Model

The network consists of devices, which are of similar type and can communicate over a wireless medium. We term each device as a network node. All the nodes will be identified using a unique ID. Each node in the network is free to leave the network at any time also; new nodes can join the network. Any node can malfunction at any point of time. Each node can be mobile at any time. The node can decide to move or halt at any location freely. There is no time constraint on the timing of movement or being stationary. Nodes communicate peer-to-peer over the wireless medium. The communication channel is multi-hop, error-prone and shared. In our network model server, node will be the receiver and the client node will send the data to the server node.

IV. PROPOSED WORK

This thesis investigates the whole scenario from MATLAB and rapid degradation of energy level. For this research it needs to implement 50 nodes in the area of MANET/WSN. This thesis has been focused on Adhoc network so it will work for both WSN and MANET. Simulation provides the two buttons first consist of simply the sinario of WSN/MANET containing the black hole node. It has not a clear that how much black hole node is being converted from the ordinary node. It is totally dependent on the automatization of proposed work that how much number of black hole nodes formed during or before the simulation formed. It is just for attending the actual scenario so that in real situation can be bitterly analyzed. Here this technique is the enhancement of AODV. So this named as EODV (Energy on demand Vector).

Table 4.1: Important Proposed parameter

Parameter	Value
Area	100*100
Number of Nodes	50
Initial Network Energy	100

Simulation Round	2000

Transmission Rate	Efs=10*10^(-12);
	Emp=0.0013*10^(-12)

Data Aggregation Energy	EDA=5*10^(-9)
Mobility Model	Random Way-point
Probability of converting Black hole node	Automatic

The propose algorithm detects and eliminates both Blackhole attack in the network. In our algorithm, we consider 3-4 Nodes out of which the node having the highest residual energy is considered as the Backbone Node (BBN). The other nodes are in passive form and BBN work is performed by one active node. If at any point the energy of the active node decreases then it transfers control to the next candidate node having the max energy and all other nodes become passive. The proposed parameters and insertion of black hole used for detection are shared among all the candidate nodes and only the active node acting as the BBN node has to find out.

V. CONCLUSION AND FUTURE SCOPE

Packet dropping attack reduces the network performance. Our secured EODV protocol is capable of mitigating the packet dropping attack in MANET. Our approach doesn't need any extra massive computational support to withstand this attack. Hence, more packet delivery ratio is achieved. This approach identifies and avoids black hole node in the path discovery phase and hence path chosen by the source node will be secured for data transmission. This approach also has a high point that it does not depend upon the relationship between the nodes. Thus, even if a trusted node turn into a malicious node then also our approach can stop the attack from happening.

REFERENCES

[1] S. Taruna1, Rekha Kumawat2, G.N.Purohit3 1Banasthali University, Jaipur, Rajasthan "Multi-Hop Clustering Protocol using Gateway Nodes in Wireless Sensor Network" International Journal of Wireless & Mobile Networks (IJWMN) Vol. 4, No. 4, August 2012.

[2] Taruna, 2Sheena Kohli 3G.N.Purohit Computer Science Department, Banasthali University, Rajasthan "Distance Based Energy Efficient Selection Of Nodes To Cluster Head In Homogeneous Wireless Sensor Networks" International Journal of Wireless & Mobile Networks (IJWMN) Vol. 4, No. 4, August 2012.

[3] Avani Patel1, Chandresh R. Parekh2 1Department of Wireless and Mobile Computing, GTU PG-School, BISAG, Gandhinagar, "DEAD NODE DETECTION IN TEEN PROTOCOL: SURVEY" IJRET: International Journal of Research in Engineering and Technology eISSN: 2319-1163 | pISSN: 2321-7308.

[4] Md. Zair Hussain1, M. P. Singh2 and R. K. Singh3 1Maulana Azad College of Engg. & Tech., Patna, India 2National Institute of Technology Patna, India 3Muzaffarpur Institute of Technology, Muzaffarpur, India "Analysis of Lifetime of Wireless Sensor Network" International Journal of Advanced Science and Technology Vol. 53, April, 2013.

[5] Aswini Kavarthapu Department of Computer Science and Engineering, QIS College of Engineering and Technology, Ongole, Andhra Pradesh, India. Narasimha Rao Sirivella "A Failure Node Detection based on Discrete Selection in WSNs": International Journal of Computer Applications (0975 – 8887) Volume 106 – No. 15, November 2014.

[6] Abderrahmane Baadache and Ali Belmehdi. Struggling against simple and cooperative black

[7] Anuj Rai, Rajeev Patel, RK Kapoor, and DS Karaulia. Enhancement in security of aodv protocol against black-hole attack in manet. In Proceedings of the 2014 International Conference on Information and Communication Technology for Competitive Strategies, page 91. ACM, 2014.

[8] Nabarun Chatterjee and Jyotsna Kumar Mandal. Detection of blackhole behaviour using triangular encryption in ns2. Procedia Technology, 10:524–529, 2013.

[9] S Sankara Narayanan and S Radhakrishnan. Secure aodv to combat black hole attack in manet. In Recent Trends in Information Technology (ICRTIT), 2013 International Conference on, pages 447–452. IEEE, 2013.

[10] Anand A Aware and Kiran Bhandari. Prevention of black hole attack on aodv in manet using hash function. In Reliability, Infocom Technologies and Optimization (ICRITO)(Trends and Future Directions), 2014 3rd International Conference on, pages 1–6. IEEE, 2014.

[11] Debarati Roy Choudhury, Leena Ragha, and Nilesh Marathe. Implementing and improving the performance of aodv by receive reply method and securing it from black hole attack. Procedia Computer Science, 45:564–570, 2015.

[12] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto. Detecting blackhole attack on aodv-based mobile ad hoc networks by dynamic learning method. IJ Network Security, 5(3):338–346, 2007.