INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume3, Issue4)
Available online at www.ijariit.com

Detecting and Overcoming the Black hole in MANET

Irfan Ahmad Wani
CSE PEC Mouli Haryana
irfanwani645@gmail.com

Pooja Garg
CSE PEC Mouli Haryana
pooja.garg990@gmail.com

Abstract: ***The nodes in mobile ad hoc networks are prone to several attacks. This is because these networks are decentralized and any node can join in the network and any node can leave the network. So if any attacker wants to steal some information from the network, the malicious node can be deployed very easily in the network. One of the many possible attacks is the black hole attack. The black hole node shows the source node that it has the shortest route to a destination even if it does not have any. Therefore, the source node forwards the packets to the path, which are dropped and never reaches the destination node. The proposed scheme detects black hole attack based on the maximum sequence number for each path, which should be received. If in any route reply message, the sequence number were greater than this, the source node would reject the reply on the path. The existing and the proposed schemes were implemented in network simulator 2.35. The performance of network was analysed on the basis of the packet delivery ratio, throughput, and remaining energy. These parameters showed improvement over the existing scheme.***

Keywords: ***Black Hole, Base Node, Sequence Number, Packet Delivery ratio, Throughput and Remaining Energy.***

1. INTRODUCTION

In a MANET, nodes inside each other's wireless transmission range can impart straightforwardly; nonetheless, nodes outside each other's range need to depend on some different nodes to transfer messages. Therefore, a multi-hop situation happens, where intermediate hosts transfer the packets sent by the source host to make them achieve the goal node. This announcement can be formalized by characterizing ad hoc network as an independent arrangement of mobile hosts (MHs) associated by wireless connections, the union of which structures a correspondence network demonstrated as a discretionary communication graph. This is as opposed to the outstanding single hop cell network demonstrate that the requirements of wireless correspondence by introducing base stations (BSs) as access points. In these cell networks, correspondences between two mobile nodes totally depend on the wired backbone and the fixed (BSs). In a MANET, no such foundation exists and the network topology may dynamically change in a flighty way since nodes are allowed to move. Concerning the method of operation, ad hoc networks are essentially distributed multi-hop mobile wireless networks where data packets are transmitted in a "store-and-forward" way from a source to an arbitrary goal, through moderate nodes. As the MHs move, the subsequent change in network topology must be made known to alternate nodes so that obsolete topology data can be either refreshed or removed. The dynamic way of MANETs makes network open to attacks. Routing is dependably the most critical part of any networks. Every node ought to work for itself, as well as be agreeable with different nodes. MANETs are defenseless against different security attacks. Henceforth, finding a protected and dependable end-to-end way in MANETs is a challenge. The organization of a MANETs is simple because of the absence of setting up any network for correspondence. For the most part, such sort of networks is required in the military application and emergency saves operations. Nevertheless, gradually MANETs have entered with the regions of gaming, sensing, conferencing, collective and distributive registering. This dynamic network is yet to capture the greater part of the business applications. Research is yet going ahead toward this path so that the MANET can be conveyed in any region where a faster and less expensive network can be setup in a split second for information correspondence.

II. RELATED WORK

Harshil et. al., [2016] [22], This Paper focused on identification of black hole attack in MANET. In mobile network (MANET) security requirement is more as compared to a wired network. In a wireless network, there are many attacks like a black hole; Sybil attack, wormhole attack etc. are possible. So a successful intrusion detection system (IDS) is needed to detect malicious nodes to identify & separate the problem caused by such nodes and notify the information of the malicious node to the other node.

Chinky Jain et. al., [2016] [32], In this paper, Author provide an algorithmic method to concentrate on analyzing and improving the protection of AODV and it is one of the accepted routing protocols for MANET. Main aim of this paper is on ensuring the protection against Black hole attack. The planned resolution is proficient in identifying & removing Black hole node(s) in the MANET in the starting. In addition, the aim of this paper is to give a simulation study, which explains the effects of Black hole attack on network performance. Earlier the works are done on MANETs paying attention mainly to different protection threats and attacks like Impersonation, Wormhole, Jellyfish, and Intrusion detection. Attack of a black hole is essential on routing protocols AODV and OLSR. In addition, ensure which protocol performs improved aligned with black hole attack. There is a requirement to tackle all these types of protocols under the attack, as well as the impacts of the attacks on the MANETs.

Mohammed et. al., [2016] [30], Statistics demonstrates that remote innovation Is picking up popularity day by day. Today, individuals sitting at either end of the nation can speak with each other with the assistance of wireless technology. Mobile Ad hoc Networks are also known as Mesh Networks, which are self-configuring, networks of mobile devices connected by wireless links. This paper proposes an enhancement in an AODV protocol, which is an upgrade in the current AODV protocol. The protocol calculation, which is received by Energy Efficient Ad Hoc Distance Vector convention (EE-AODV), has upgraded the RREQ and RREP taking care of procedure to spare the vitality in cell phones. In this paper AODV, the protocol is implemented by using 30 nodes. The objective of this paper is to measure the efficiency of protocol at 30 nodes. The execution measurements utilized for assessment are a delivery ratio, throughput, system lifetime and normal energy consumed. The simulation will be done using NS2.

W.K.Kuo et. al., [2016] [**31],** In this paper, they explore EE optimization as measured in bits per Joule for MANETs based on the cross-layer design paradigm. They model this problem as a non-convex mixed integer nonlinear programming (MINLP) formulation by jointly considering routing, traffic scheduling, and power control. Because the non-convex MINLP problem is NP-hard in general, it is exceedingly difficult to globally optimize this problem. We, therefore, devise a customized branch and bound (BB) algorithm to efficiently solve this globally optimal problem. The novelties of our proposed BB algorithm include upper and lower bounding schemes and branching rule that are designed using the characteristics of the nonconvex MINLP problem. We demonstrate the efficiency of our proposed BB algorithm by offering numerical comparisons with a reference algorithm that uses the relaxation manners proposed in some papers. Numerical results show that our proposed BB algorithm scheme, respectively, decreases the optimality gap 81.98% and increases the best feasible solution 32.79% compared with the reference algorithm. Furthermore, our results not only provide insights into the design of EE maximization algorithms for MANETs by employing cooperation between different layers but also serve as performance benchmarks for distributed protocols developed for real-world applications.

Vanitha et al. [2015] [**23],** Proposed a probabilistic trouble making detection plan is exceptionally desirable to guarantee the protected DTN routing and the foundation of the trust, among DTN nodes. A zone (routing zone) of a node is utilized to gather the node information inside the range. In this protocol, it cannot accomplish the packet delivery ratio, execution and information loss rate. This paper is giving the explanation alongside black hole attack, which is based on the fuzzy rule. Fuzzy control is utilized to determine the tainted node and additionally convey the solution to lessen information misfortune over the network. Fuzzy rule ranges between the incentive as {0, 1}. Geographic routing is one of the most reasonable routing systems in wireless mobile Ad hoc network predominantly because of its adaptability. Multi Input Multi Output strategy used to send information much of the time in routing protocol. Examination and simulation come about demonstrate the adequacy and productivity of the drop node investigation, high packet delivery ratio, throughput, and delay.

Kaur et al. [2014] [**24],** Proposed a technique to outline a system of black hole detection based on artificial neural networks (ANNs). Utilizing a simulated MANET environment, ANNs demonstrating for recognizing the black hole attack is examined and it is demonstrated that model can recognize nodes under black hole attack adequately.

Singh et. al., [2014], proposed a strategy in which broadcast synchronization (BS) and relative separation (RD) strategy for clock synchronization are utilized to keep the black hole nodes. In this inner and outer clock node contrast and the limit clock if both the clock time is more noteworthy than the limit then it is found that the node is malicious. This technique can easily distinguish and keep the black hole node X.

Howarthet et. al., [2013] [28], Proposed a study of MANET intrusion detection and prevention approaches for network layer attacks. This empowers a protection system to gain from experience and utilize the current learning of attacks to infer and identify new nosy exercises. Protection component needed to sufficiently vigorous to protect from new vulnerabilities into the system.

Jaspal and Daya [2013] [3], Proposed the impacts of Black hole attack on mobile ad hoc routing protocols Because of the huge existing vulnerabilities in mobile ad-hoc networks, they might be uncertain against attacks by the malicious nodes. For the most part, two protocols AODV and Improved AODV have been considered. Simulation has been performed on the premise of execution parameters and impact has been investigated in the wake of adding Black-hole nodes in the network. Finally, the outcomes have been figured and contrasted; unearth which protocol is minimum influenced by these attacks.

III. METHODOLOGY

The source node broadcasts route request messages in the network to find a route to original destination node but not fake destination route request. If any node has a route to the destination, it replies to the source node else it forwards the route request to its neighbors. When the route request reaches the destination node, it replies to the source node via the paths from which the

route request was received.

Now, if in any path malicious node had existed, it would have driven the sequence number to very high value. The source node compares all the sequence numbers generated at the destination node for all the route replies, with a maximum sequence number for each path. If in any route reply message, the sequence number were greater than this, the source node would reject the reply on the path.

To check which node has replied back with the high sequence number the source node would send test packets over the path. If any node were found to forward very less number of packets, then the destination node would mark the node as malicious and inform the source node about the same.

The source node would inform other nodes not to communicate with the detected node in the network and resume data communication over the path not having the malicious nodes.

IV. RESULTS

This graph showed in figure 1 shows the amount of energy remaining in the network. Initially, the nodes were given an average of 50 Joules of energy. At the end of the simulation time, the average energy remaining in the network was 33 Joules for the proposed scheme and 31 Joules for the existing scheme. This shows proposed scheme consumes lesser amount of energy.

This graph shown in figure 2 shows the packet delivery ratio is defined as the ratio of a number of packets received to the number of packets sent in the network. The graph of packet delivery ratio shows a big slide downwards for the proposed scheme, it is because the source node is required to send test packets to the suspected nodes. The suspected nodes drop those packets; therefore, the value of the packet delivery ratio goes down.

This graph shown in figure 3 shows the amount of data received at the destination node per unit of time. Since the detection of the malicious nodes happens earlier in the proposed scheme, the source node could forward more data to the destination node. Thus, the throughput goes high. The throughput is 500 Kbps for the proposed scheme and 300 Kbps for the existing scheme

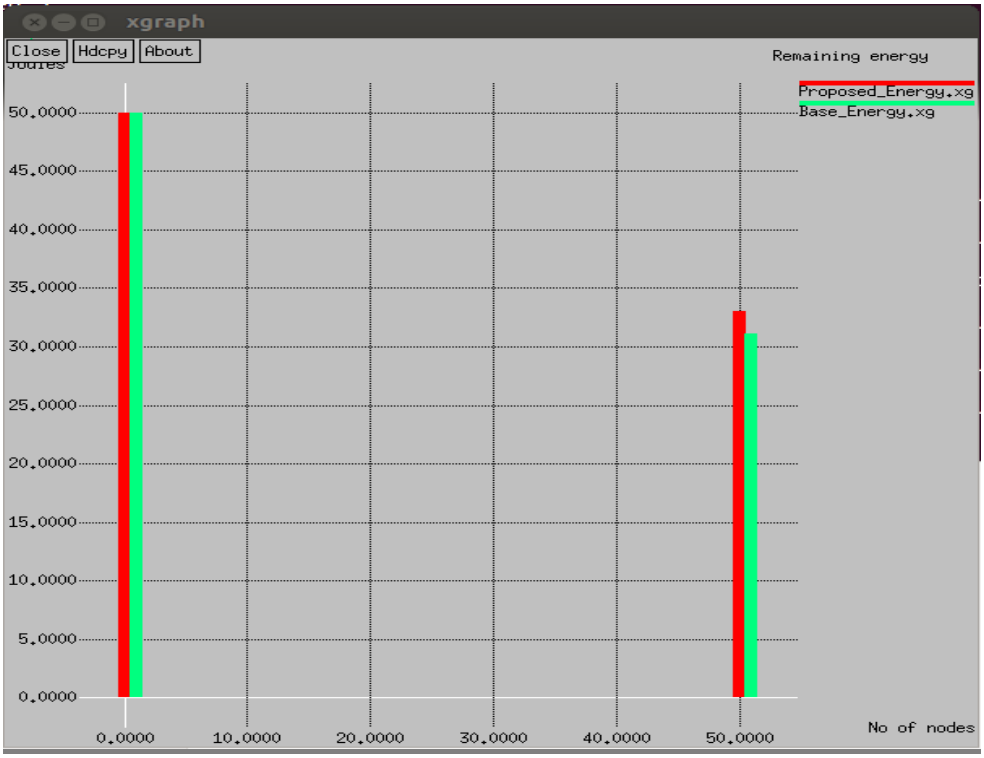

Figure1: Remaining energy Comparison

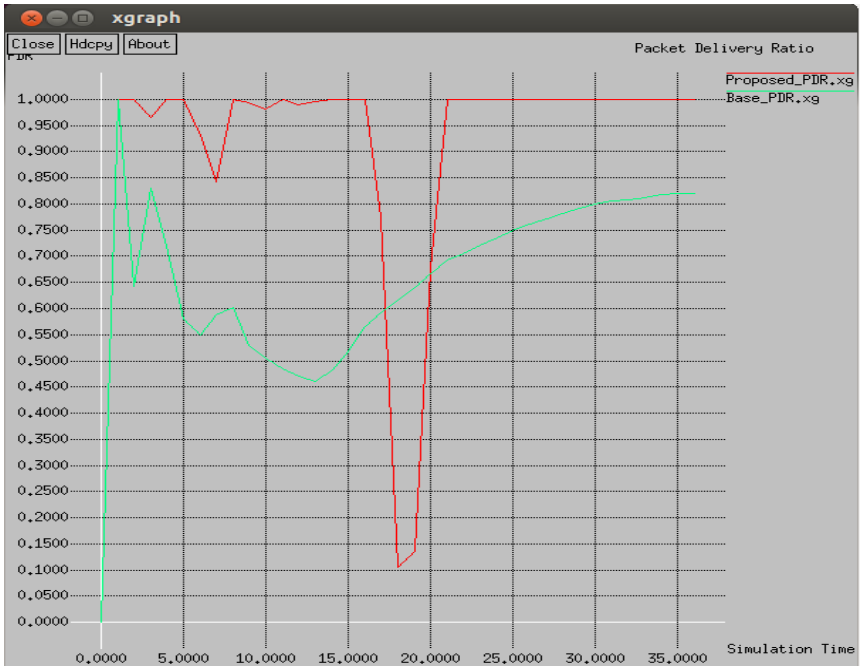

Figure2: PDR Comparison

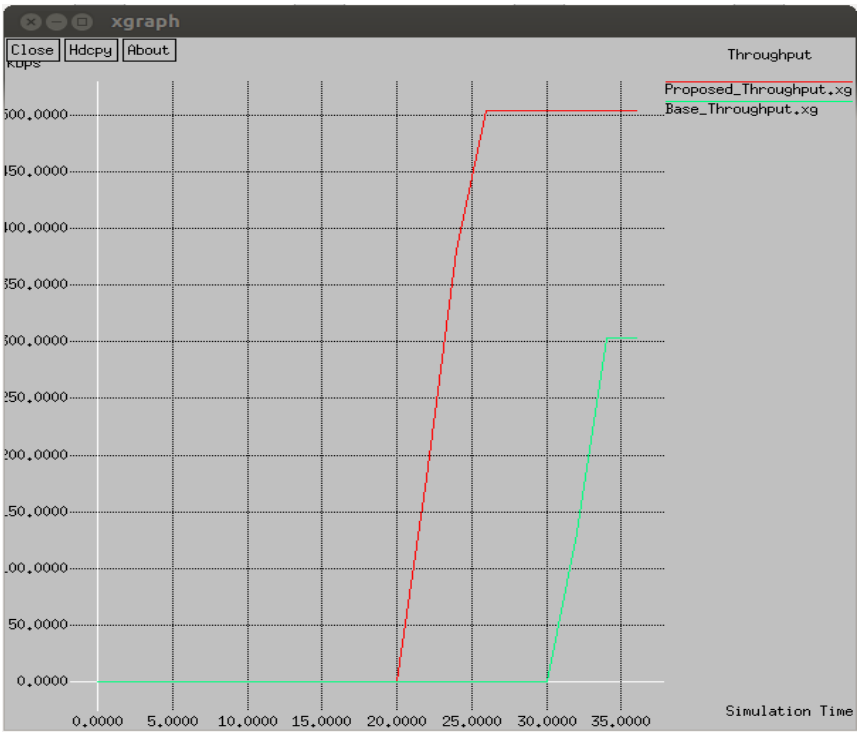

Figure3: Throughput Comparison

CONCLUSIONS

The proposed scheme aimed at the detection of the malicious black hole nodes in the network and conserve energy at the same time. The existing and the proposed schemes were implemented in network simulator 2.35. The performance of network was analysed on the basis of the packet delivery ratio, throughput, and remaining energy. The existing scheme requires the three times broadcasting of the message by the nodes. Now, such a huge amount of broadcasting consumers up the energy of the nodes. The proposed scheme, on the other hand, requires one time broadcasting only. However, after the successful detection of the malicious nodes, the value again reaches the higher levels. Similarly, the throughput also shows higher values. Since the detection of the malicious nodes happens earlier in the proposed scheme, the source node could forward more data to the destination node. Thus, the throughput goes high. All the three parameters have shown improvement, therefore it can be concluded that the proposed scheme has outperformed the existing scheme.

REFERENCES

[1] **Jaspal Kumar, M. Kulkarni, Daya Gupta**, "Effect of Black Hole Attack on MANET Routing Protocols" in International Journal of Computer Network and Information Security (IJCNIS) Volume 5, Issue 5, April 2013.

[2] **Supriya Tayal, Vinti Gupta,"** A Survey of Attacks on MANET Routing Protocols," in International Journal of Innovative Research in Science, Engineering and Technology Volume 2, Issue 6, June 2013.

[3] **AA Gurjar, AA Dande,"**Black Hole Attack in MANETS: A Review Study", in International Journal of IT, Engineering and Applied Sciences Research (IJIEASR) Volume 2, Issue 3, March 2013,

[4] **Swati Jain, Naveen Hemrajani,"**Detection and Mitigation Techniques of Black Hole Attack in MANET: An Overview", in International Journal of Science and Research (IJSR) Volume 2, Issue 5, May 2013.

[5] **Ms. Monika Y. Dangore, Mr. Santosh S. Sambare, "** A Survey on Detection of Black hole Attack using AODV Protocol in MANET", in International conference on cloud & ubiquitous computing, IEEE2013.

[6] **Arnab Mitra, Rajib Ghosh, Apurba Chakraborty, Debleena Srivastava, "**An Alternative Approach to Detect Presence of Black Hole Nodes in Mobile Ad-Hoc Network Using Artificial Neural Network", in International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 3, March 2013.

[7] **Puja Vij, V. K. Banga, Tanu Preet Singh, "** Survey on Prevention of Black Hole Nodes in Mobile Ad hoc Networks **",** in International Conference on Trends in Electrical, Electronics, and Power Engineering Volume 12, Issue 5, July 15-16, 2012.

[8] **Sowmya K.S, Rakesh T. and Deepthi P Hudedagaddi, "**Detection and Prevention of Black hole Attack in MANET Using ACO", in IJCSNS International Journal of Computer Science and Network Security Volume 12, Issue 5, May 2012.

.

