International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-4, November 2019

Two-Step Verification Technique for Isolation of Black hole Attack in MANETs

A Sai Venkateshwar Rao Siddhartha Chauhan

Abstract: ***A network in which the nodes can configure themselves and change their locations is known as mobile ad hoc network. For connecting to other networks, MANETs use wireless connections since they are mobile. Signal protection and reliability of mobile nodes are the major challenges faced by the applications which use MANETs. An active intrusion attack that is initiated by a malicious node to degrade the network's performance is known as black hole attack. A new approach is proposed in this research that uses the blacklist and clustering approaches to remove this attack from networks. NS2 simulation is used to conduct simulation experiments for evaluating the performance of proposed method. The outcomes show that the performance of proposed method is better in terms of different performance parameters as compared to the traditional approaches.***

Keywords: Blackhole, MANET, Clustering

I. INTRODUCTION

MANET is a self configuring network. In this network, mobile routers or nodes are connected to each other through wireless links without any access point. All mobile device or nodes deployed within the network are independent in nature. The mobile devices can move randomly. These nodes arrange themselves in random order. Within MANET, the mobile nodes share the wireless channel [1]. A random and dynamic change is noticed in the topology of these networks. Link breakdown within MANET is a very common thing. This happens due to the free movement of the nodes. The applications using MANET decide the density and the amount of nodes. Several applications such as tactical networks, wireless sensor network, data networks, device networks, etc are made possible due to MANET. Various mobile wireless nodes are deployed within a "Mobile Ad-hoc Network". These networks do not require any centralized control to establish communication between these mobile nodes.The conventional routing protocols are not sufficient for real time communications. Security is one of the major concerns of MANET. It is a complex task to provide security to MANET. A better solution for security attack can be provided by identifying and understanding the attack.

Manuscript published on November 30, 2019.
* Correspondence Author
A Sai Venkateshwar Rao*,Computer Science and Engineering, National Institute Of Technology,Hamirpur,INDIA. Email:saibittu.rao@gmail.com
Dr Siddhartha Chauhan,,Computer Science and Engineering,National Institute Of Technology,Hamirpur,INDIA.Email: sid@nith.ac.in

Security is a difficult task in wireless communication due to the non-existence of any centralized control. The intruder does not distort the shared information in passive kind of attack. The attacker or intruder only listens to this information [2]. The attacker tries to get the access of secret information. The attacker also analyzes the transferred traffic patterns. It is not easy to detect these types of attacks as these attacks do not disrupt or change the information being forwarded or received. The intruder dynamically takes part in the network activities in active attack. The attacker tries to transform the messages being transferred [3]. The attacker can disturb the overall functioning of the network by modifying, injecting, forging, fabricating or dropping data packets. These attacks are highly vulnerable as they can damage the whole performance of the network. As these attacks degrade the network's performance in a significant manner, therefore, these attacks can be detected easily. Grayhole attack is somewhat similar to Blackhole attack. There is just a minor difference between both of these attacks. Like Blackhole attack, fake RREP message is sent by the malicious to the source or victim node in this attack. However, the grey hole attack does not drop all data packets like Blackhole attack. In this attack, just few selective packets are dropped while the remaining packets are forwarded to the source [4]. Wormhole Attack is one of the severe and well planned attacks. Therefore, it is a challenging task to protect network against this attack. Two or more than two compromised nodes collaborate together to trigger this intrusion. A compromised node gives signal to a fake set of neighbors or promotes bogus links with distant nodes in link spoofing attack. This phenomenon disrupts the regular routing procedure. Sometimes, these nodes also utilize the identity of an authorized node for generating a fake identity of that node. The attack launched by Sybil nodes is termed as Sybil attack. In this attack, various data packets are to be routed towards the nodes having false identity. Jellyfish Attack is a selective type of black hole intrusion. In this attack, the attacker node disturbs the normal functioning of the network [5]. The attacker node changes packets' order drops selective packets or increases jitter of the packets that go through it, to create disruption within the network. Therefore, this attack cannot be detected easily. An effort to make a machine or network resource inaccessible to its anticipated customers is called denial-of-service attack. This attack momentarily or for an indefinite period suspends services of a host linked to the Internet. At different network layers, this attack can be triggered. The usual communication is disturbed by launching signal jamming attack at the physical layer.

The control of the channel goes to the attacker node in this attack at the link layer. In computer networks, security in MANET is the major focus of research for different researchers [6]. Black Hole attack is one of the most popular attacks launched by intruders. The attacker node powerfully gets the route having highest sequence number and least hop count in black hole attack. All data packets are subsequently overheard or dropped by the attacker node [7]. Security is a fundamental requisite in these networks due to their extensive utilization in hazardous environment. It is possible for nodes to destroy the network as they contribute in the routing procedure. Trust among nodes is the main principal of routing. Hence, attackers can degrade the network performance by disordering routing procedure.

II. LITERATURE REVIEW

Avni Tripathi, et.al (2016) proposed a novel confirmation packet based approach in this work. The main aim of this approach was to identify and blacklist black hole nodes from communication. The source node transmitted a black packet in this approach if the confirmation packet did not reach earlier than threshold time. This black packet blacklisted the blackhole node. The value of Threshold time was based on the hop count value in RREP packet [8]. The tested results demonstrated that the average packet delivery ratio (PDR) of 31.08% was obtained for AODV during black hole attack. The implementation of packet based approach improved the ratio up to 60.85%. This research field provided massive opportunity to researchers for developing new solutions by considering the security needs, concerns and enhancement scope of MANET.

Vaishali Gaikwad Mohite, et.al (2015) proposed a novel approach for the detection and prevention of cooperative black hole attack. The proposed approach used Cooperative Cluster Agents for this purpose [9]. DRI and SRT-RRT table were applied as input to Cooperative Security Agents in the proposed technique. In order to detect cooperative blackhole attack, Cooperative Cluster Agents utilized cross checking and detection flow schemes on the basis of these inputs. Alert message was transmitted within MANET after detecting attack to prevent this attack. A network simulator called NS-2.35 was utilized in this work to implement proposed approach. The proposed approach was compared with regular AODV protocol in terms of different performance parameters. These parameters included network throughput, packet delivery ratio and end-to-end delay.

Nikhil G. Wakode, et.al (2017) presented a discussion to secure network against blackhole attack [10]. In this work, Ad hoc demand distance vector (AODV) routing by cooperative bait detection approach (CBDA) along with Malicious node detection algorithm was used to provide solution of malicious node issue. Reactive and proactive routing schemes were used by cooperative bait detection approach. In order to identify malevolent node within the network, malicious node detection algorithm was used. Reverse tracing technique was implemented by this algorithm for achieving the required aim. The simulations results demonstrated the occurrence of malevolent nodes in AODV. The CBDA approach along with malicious node detection algorithm protected AODV by malicious nodes. The performance of proposed approach was measured in terms of packet delivery ratio, end-to-end delay, standardized routing overhead and packet drop ratio.

Pradeep R. Dumne, et.al (2016) stated that ensuring security within MANET was a big challenge. A lot of researches were carried out to detect malicious nodes within the network. Within MANET, routing protocols were prone to the collaborative blackhole or grayhole intrusions [11]. CBDS (cooperative bait detection system) approach was utilized in this work. In this work, an improved CBDS technique was presented. The proposed approach utilized AODV protocol for reducing routing overhead. The proposed approach was called CBDS using AODV. The obtained simulation outcomes depicted that a better performance was given by CBDS using DSR as compared to DSR protocol. In contrast to CBDS using DSR approach, CBDS using AODV approach gave better performance in terms of network throughput and packet delivery ratio.

Amar Taggu, et.al (2018) proposed an uncomplicated and effectual application layer based attack detection algorithm. The main aim of proposed approach was to identify blackholes within MANET [12]. In order to find out black holes in DSR protocol, the proposed approach used mobile agents (MA) and an improved adaptation of Traceroute called wtracert within Mobile Ad-Hoc Network. The mobile agents were used to ensure that there was no need to implement any amendments in the basic routing algorithms or other lower layers. The Simulation outcomes depicted that the proposed detection algorithm efficiently detected single and numerous blackhole nodes athwart changeable mobility rate of the sensor nodes.

Mohamed A. Abdelshafy, et.al (2016) introduced a novel approach called Self-Protocol Trustiness (SPT). In the proposed approach, the normal behavior of protocol was implemented to detect a malevolent attacker. The malevolent node was fascinated to confer an inherent confirmation of its malevolent activities [13]. In order to counter intrusions, a Blackhole Resisting Mechanism (BRM) was proposed in this work. It was not required to modify the formats of packet. Thus, the overhead was less number of computations at nodes. The proposed approach had no further communication expense. The performance of networks employing AODV was compared in blackhole attacks with and without using SAODV with the help of NS2 simulation. The simulation results showed that the proposed approach efficiently reduced the influence of blackhole intrusion.

III. RESEARCH METHODOLOGY

The main motive behind this research work is to detect and remove black hole intrusion from the network. A malevolent node is forced to establish a path from source node across it after its entry within the network. This causes a black hole intrusion. During attack, the source node floods route request packets within the network. The nodes having route to the destination send Route reply packets. However, the malevolent node pretends to have a path to the destination even in absence of path.

This node also pretends to have highest sequence number. Following are the steps that are applied to discover the malevolent nodes within the network.

1. In the first step, the deployment of mobile nodes is performed within the network.
2. The source nodes and destination nodes are defined to establish communication within the network
3. Source node floods fake route request packets within the network.
4. The node responding to the fake route request packets will be detected as malevolent node.
5. Otherwise, the source node will trace the time at which route reply packets are received.
6. The node responding back with minimum sequence number in the least possible time will be marked as least trusted node.
7. The least trusted node will be affirmed as malicious node.
8. Clustering algorithm is implemented for the isolation of malevolent nodes from the network.
9. The entire network is partitioned into clusters on the basis of location based clustering.
10. The node having maximal trust will be selected as cluster head from every cluster.
11. The data is routed to the destination by that cluster head which isolates the malevolent node from the network.

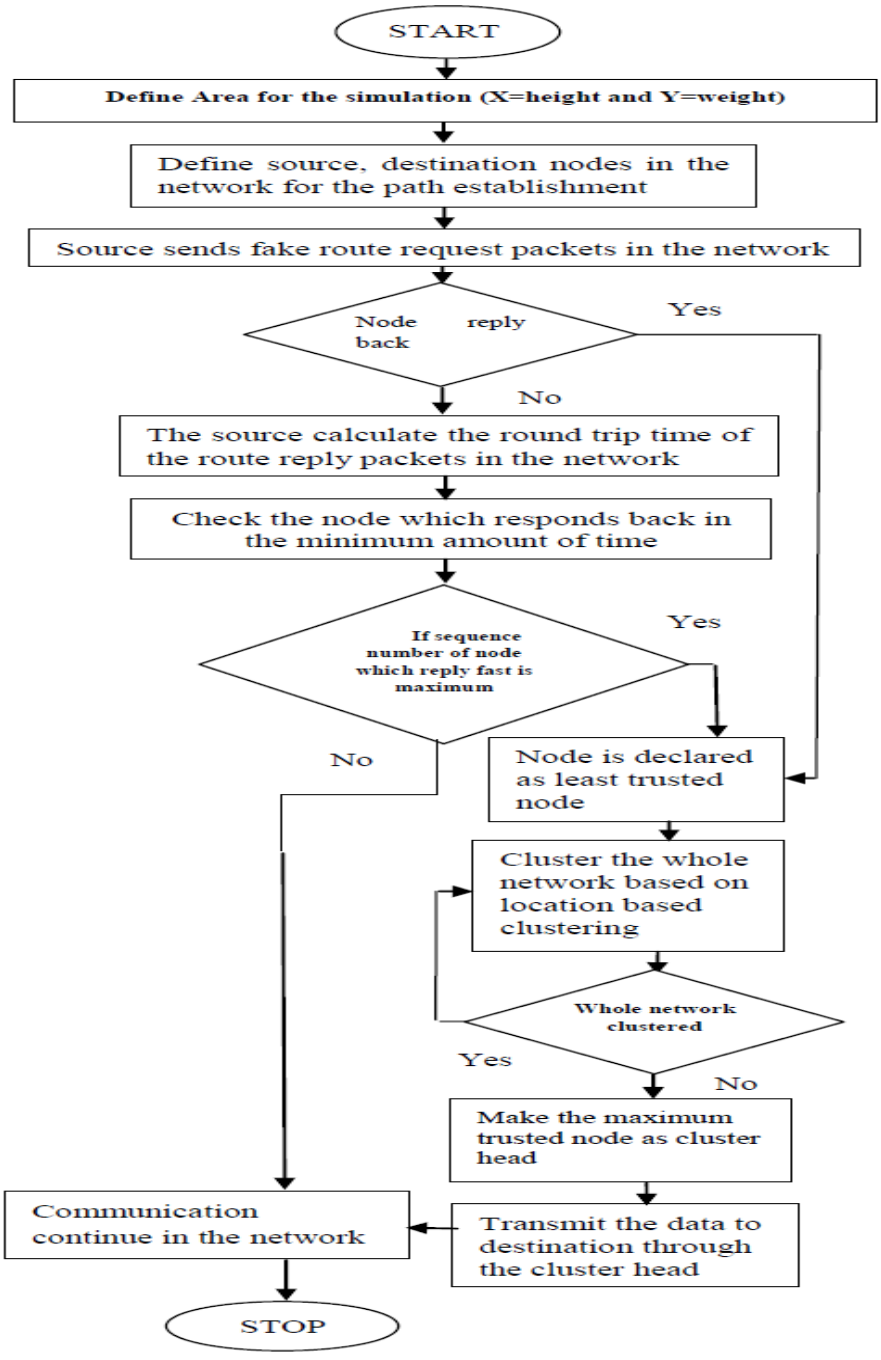

Figure 1:Proposed algorithm

IV. EXPERIMENTAL RESULTS

The proposed research is implemented in NS2 and the results are evaluated by comparing proposed and existing techniques in terms of different performance parameters.

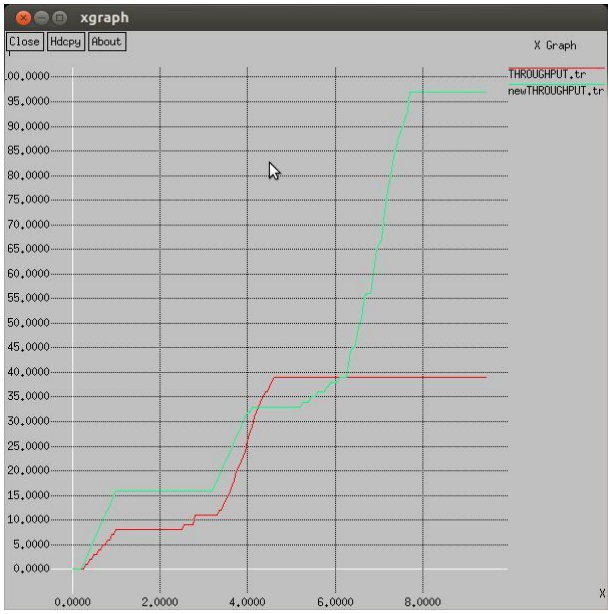

Figure 2: Throughput graph

The projected approach and existing attack scenario are compared in terms of throughput as demonstrated by the figure 2. The network throughput is increased after detecting and isolating attack from the network.

Figure 3: Delay Graph

The proposed and existing intrusion is compared in terms of delay to analyze the performance of network as shown by the graph 3. The malevolent nodes are eliminated from the network to reduce the delay within the network.

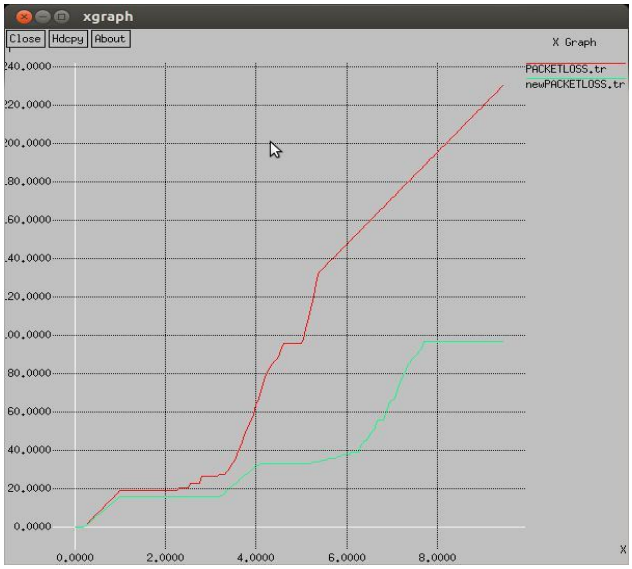

Figure 4: Packet loss Graph

The proposed and existing intrusion is compared in terms of packet loss to analyze the performance of network as shown by the graph 4. The malevolent nodes are eliminated from the network to reduce the packet loss within the network.

V. CONCLUSION

This research work reaches on the conclusion that MANET is a self configuring wireless network. The mobile sensor nodes are free to join or leave the network whenever they want. Security within MANET is the prime concern. The lapse in security decreases the overall operation of the network. In this work, a new algorithm has been presented to eliminate or detect different types of serious intrusions or malevolent nodes within the network. A trust based technique has been used in this work for the detection and isolation of malevolent nodes. The trust among nodes is computed on the basis of different nodes going to be sent. Malicious nodes were isolated and detected using a novel clustering algorithm. This method is implemented on the network simulator 2. The results are analyzed by considering different performance metrics.

VI. REFERENCES

1. Rashid Hafeez Khokhar, Md Asri Ngadi & Satria Mandala, “A Review of Current Routing Attacks in Mobile Ad Hoc Networks”, International Journal of Computer Science and Security, 2012,volume (2) issue (3)
2. Saritha Reddy Venna , Ramesh Babu Inampudi, “A Survey on Security Attacks in Mobile Ad Hoc Networks”, International Journal of Computer Science and Information Technologies, Vol. 7 (1) , 2016, 135-140
3. Abhay Kumar Rai, Rajiv Ranjan Tewari & Saurabh Kant Upadhyay, “Different Types of Attacks on Integrated MANET-Internet Communication”, 2010, International Journal of Computer Science and Security (IJCSS) Volume (4): Issue (3)
4. Himani Yadav, Rakesh Kumar, “A Review on Black Hole Attack in MANETs”, International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 3, May-Jun 2012, pp.1126-1131
5. Bhoomika Patel, Khushboo Trivedi, “A Review - Prevention and Detection of Black Hole Attack in AODV based on MANET”, International Journal of Computer Science and Information Technologies, Vol. 5 (3), 2014, 2816-2818
6. Aarti Chauhan, Puneet Rani, “A Detail Review of Routing Attacks in Mobile Ad Hoc Networks”, International Journal of Engineering Research and General Science Volume 3, Issue 2, March-April, 2015

7. Dr Sanjeev Yadav, Rachna Jain, Mohd Faisal, "Attacks in MANET", International Journal of Latest Trends in Engineering and Technology (IJLTET), Vol. 1 Issue 3 September 2012
8. Avni Tripathi, Amar Kumar Mohapatra, "Mitigation of Blackhole attack in MANET", 8th International Conference on Computational Intelligence and Communication Networks (CICN), Year: 2016 | Conference Paper | Publisher: IEEE
9. Vaishali Gaikwad Mohite, Lata Ragha, "Security agents for detecting and avoiding cooperative blackhole attacks in MANET", International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), Year: 2015 | Conference Paper | Publisher: IEEE
10. Nikhil G. Wakode, "Defending blackhole attack by using acknowledge based approach in MANETs", International Conference on IoT and Application (ICIOT), Year: 2017 | Conference Paper | Publisher: IEEE
11. Pradeep R. Dumne, Arati Manjaramkar, "Cooperative bait detection scheme to prevent collaborative blackhole or grayhole attacks by malicious nodes in MANETs", 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Year: 2016 | Conference Paper | Publisher: IEEE
12. Amar Taggu, Abhishek Mungoli, Ani Taggu, "ReverseRoute: An Application-Layer Scheme for Detecting Blackholes in MANET Using Mobile Agents", 3rd Technology Innovation Management and Engineering Science International Conference (TIMES-iCON), Year: 2018 | Conference Paper | Publisher: IEEE
13. Mohamed A. Abdelshafy, Peter J. B. King, "Resisting blackhole attacks on MANETs", 13th IEEE Annual Consumer Communications & Networking Conference (CCNC), Year: 2016 | Conference Paper | Publisher: IEEE

AUTHORS FROFILE

A Sai Venkateshwar Rao is a masters student of NIT Hamirpur. He has Completed his bachelors from CSVTU Bhilai. His area of interest is ad hoc networks, wireless sensor networks, MANET and vehicular ad hoc networks.

Dr Siddhartha Chauhan is Associate Professor at NIT Hamirpur. He has a masters degree from IIT Roorkee and a PHD from NIT Hamirpur. His area of intrest is wireless sensor networks ,ad hoc networks MANET. He has 13 journal publications in international journals and 14 conference papers. Many students have successfully completed masters and PHD under his supervision.