Proc. of Int. Conf. on Emerging Trends in Engineering & Technology, IETET

A Study on Various Blackhole Attacks Measures and Methods

Jyoti Chauhan[1] and Sahil Gupta[2]
[1]M.Tech Student, ECE Department, G.I.M.T (Kanipla),India
jichauhan21@gmail.com
[2]Assistant Professor, ECE Department, G.I.M.T (Kanipla), India
sahil.btech.ece@gmail.com

***Abstract*—Security is always the critical challenge for mobile network and it suffers from various internal and external attacks. These attacks use the dynamic and cooperative communication features of the network and disrupt the communication. In this paper, a study on various network attacks and their impact is defined. The paper also explored the blackhole attack in larger extent. The work procedure of these attacks, features and characterization of blackhole attack are defined. The paper also discussed some of the major methods defined to detect and prevent the black hole attack**.

***Index Terms*— Blackhole, Preventive, Security, Mobile Network.**

I. INTRODUCTION

A mobile network is the public area network which provides the wireless communication in critical real time network without specification of any infrastructure. The dynamic nature of mobile environment in terms of topology, new node participation and the cooperative node based communication also increases the criticality of this network form. The absence of any centralized control required to observe the neighbor nodes instantly without any prior knowledge. Because of these all restrictions and challenges, the network always suffers from various internal and external attacks. These attacks are either node based or communication based to reveal the information or to destroy the communicating contents. The cooperative nature and functioning of nodes is defined to convey the data and share the responsibilities to manage the network. To provide the communication relative to this conveying communication method is controlled by various routing protocols. These protocols are able to identify the feasible neighbor node based on which the most eligible next node can be identified for communication. But, if this intermediate neighbor is having the fake identity or intentionally want to disturb the communication, some attack can be applied by the node. Some of the common network attacks applied by internal and external nodes are listed here under

A. Wormhole Attack

It is tunnel based attack, in which two nodes form a cyclic tunnel and send and receive data to each other normally. But as some other communicating node uses any of these nodes as intermediate node, it rotates the communication within tunnel and not pass it to the destination node. This tunnel in the network is considered as wormhole attack. The tunnel is considered as the dedicated link between the attackers. The tunnel can be single or multi hop based on the attack criticality and involvement in the network. Generally, an intermediate node pair forms this tunnel by including some internal or external nodes.

Grenze ID: 02.IETET.2016.5.23

B. Flooding Attack

This attack form actually increases the network traffic abnormally and acquires the maximum bandwidth and the network resources including the battery power. The objective of this attack is to slow down the network communication that can also result as the network failure. This attack form degrades the network performance and cause the information loss at during communication. This attack is generally performed by some internal authenticating node by spreading the large number of RREQ packets for a short period.

C. Black hole Attack

In this attack form, the routing protocol is used by the attacker to advertise itself to intercept the communicating packets and acquires the communication. The attacker applied the communication flooding of its own RREQ for all neighbors at various levels. As the attacker node processed the distributed broadcast request, the reply to the route is generated by the attacker node as reply. This reply is submitted back to the initial source node so that the fake route is generated. The attacker captures all the communicating packets of other nodes and blocks the communication to the destination end. This packet drop or non-forwarding increases the communication and the routing criticalities. This attack form is also known as man-in-the-middle attack.

D. Sinkhole Attack

This particular attack form captures all the communication control of a network region and creates a fake sinkhole so that that all the communication is diverted to that new node. It works as a compromised node with quality routing feature so that the communication is shifted over that node. These kinds of diverted sharing not allow passing the data packets to actual destination. It becomes difficult to select the other neighbor so that overall communication affected and large data loss occurs.

E. Node Replication Attack

In this attack form, the attacker generates and adversary on the network nodes to set the same ID on other network nodes. This form of generating the duplicate identity of attacker implied by attacked is called replica attack. As the communication is performed to the attacker and because of multiple copies of attacker node, multiple communications are performed over the network. This attack is launch itself several inside attacks so that the complete network severe the destruction. Because of the mobility, the replica attack also increases the collision and increase the network traffic abnormally.

In this paper, a study on various security issues and challenges for mobile network is provided. The paper has explored the black hole attack with associated measures and preventive methods. In this section, the mobile network challenges are discussed. In this section, different attacks forms applied on internal and external nodes is defined. In section II, the work defined by earlier researchers for different network attacks is provided. In section III, the work exploration on black hole attack is presented along with various measures and methods. In section IV, the conclusion of work is presented.

II. RESEARCH BACKGROUND

Mobile network is open area network in which private information of users in different forms is communicated publically. The absence of the centralized controller or infrastructure also increases the communication challenges and issues. Because of this the network suffers from various kinds of internal and external attacks. There is the requirement of different preventive, authentication based and detection based approaches to provide secure communication against these attacks. Some of the work defined by earlier researchers to explore these attacks, security features and various methods for secure communication are described in this section. A study on different network attacks was provided by Noureldien et. al.[7]. Author described different attacks, their structure and the associated characterization. The communication and resource driven observations are defined to set the detection criteria. Various variant and behavior of attacks are also defined by the author. Some of the generalized attack independent and attack dependent techniques were discussed by Rajakumar et. al.[18]. Author explored the fundamental features, resource specification, architectural observations and the physical service and confidence exploration to define some defensive measures to provide safe network communication. Attack behavior and relative solutions were discussed by the author. A study work Rushing and flooding attack using AOMDV protocol is provided by Sukiswo et. al.[3]. Author applied the simulation scenario with different data collection methods to provide the safe and

reliable communication in the network. A normal condition specific communication statistics was observed by the attack to identify the critical communication under attack type. Another study on different routing attacks and their impact on network performance were identified by Desai et. al.[9] for OLSR protocol. Author observed the impact of link spoofing attack and routing table overflow attack under various performance measures to identify the degradation in network communication. An investigational study on various security features and attack preventive methods and measures was provided by Soni et. al.[17]. Author identifies the attack impact on routing protocol and suggested the relatively effective communication to provide safe transmission.

Most of the researchers have provided the attack detection algorithm specific to the attack type. These methods are based on the parametric observation along with statistical and behavioral estimation. Abiranmi et. al.[2] has defined a work specific to the replica attack based on the confidence value analysis. The interactive time and global information are collected to identify the communication overhead in the network. The communication is observed under geographical range to provide accurate parameter specific communication. Another novel approach against the chunk dropping attack using cluster based method was provided by Katal et. al.[4]. Author communicated the different forms of datagram to identify the communication drop over the main stream. The method was applied on transport layer and set a cluster head to observe the communication for group communication analysis. This cluster and chunk specific observation applied collectively to generate the optimum communication route. A rank [5] based scheme was proposed to provide preventive solution against packet drop attack. The featured observations were applied to identify the trusted and disjoint loops in the network to generate reliable communication routes in the network. A criteria specific analysis based on hop count, sequence number, timer and ranking measure was defined to recognize the malicious behavior. After identifying the attacked node, the safe communicating node was identified and applied communication over it. Node Reputation[8] analysis is another technique to provide the safe communication against flooding and DDOS attack. The periodic behavior of nodes is observed with structural information to identify the abnormal communication pattern. The investigation was applied on neighbor knodes to classify the normal and the malicious nodes based reputation constraint identification. Khatkar et. al.[10] has provided a location aided preventive routing method to provide safe communication against Replay attack. Author applied the time chock based communication analysis to achieve synchronized communication in mobile network. The preventive node isolation mechanism was applied for node election in disturbed network. Another work using DRI table and cross checking method was proposed by Madhurikkha et. al.[12] against packet dropping attack. This adaptive method stored the route discovery in table and applied the cross checking by using bit verification method. The statistical observations on various communication measures were applied to verify the neighbor and based on the selective route updation. Shashi et. al.[13] has generated an alternate routing path by isolating the sinkhole attack. A phase driven analysis on sequence number and hop count was applied to observe the malicious behavior of node and generate the effective network route. A preventive solution against Flooding attack was provided by Laeeq et. al.[16]. The attack behavior analysis under different schemes was obtained to provide the effective route discovery with reasonable punishment. The time out and the flooding imprisonment were considered the featured vector for route selection.

Some of the researchers also applied the optimization methods and classifiers to detect the attacks more effectively. Patel et. al.[1] has defined a novel method using SVM (Support Vector Machine) to detect the malicious attack. This machine learning algorithm has process the salient features under context change and applied the learning algorithm to categorize the attacked and normal nodes. The analysis was applied on communication patterns to separate the misbehaving communication patterns more accurately. The metric specific simulation signifies that the method improved the communication rate and modification rate effectively. An ACO based defensive method was applied by Kumari et. al.[11] to improve network performance against selective forwarding attack. Author used the ant agents to generate the pheromone path between source and destination and applied an updated backward path generation method for safe route formation. Indirani et. al.[20] suggested a swarm based method to locate the packet replication attack and generated a disjoint path for effective route formation. A tree id based communication solution was provided to distinguish the attack node so that the safe route will be formed for reliable packet delivery.

One of the well-known and critical attacks in mobile network is black hole attack in which a node generates the fake reply and avoided to work as intermediate node. The node captures the information and does not forward to other nodes. Different forms of black hole attacks are identified by different researchers and relatively provided different solutions. A study on black hole behavior and various methodologies on attack

detection and prevention were studied by Sarma et. al.[14]. The performance impact of black hole attack was analyzed by Bala et. al.[15] under fundamental characterization including dynamic topology, open medium and constraint capability analysis. A sequence number analysis based black hole detection method was suggested by Zhang et. al.[19]. Author observed the attack form and provided the relative communication support to provide safe communication in attacked network. Cooperative black hole is the another form of black hole in which black hole nodes acts in a group. An agent based security solution for cooperative black hole detection was provided by Gaikwad et. al.[6]. This new technique used the Table driven mapping to track the communication of each node and a method for attack detection and route discovery. This history driven attack has identified the attacker accurately and effectively.

III. BLACKHOLE ATTACK: MEASURES AND METHODS

In this attack form, the attacker node distributed its fake information to the neighbour nodes and tries to captu re the RREQ packet from any communication request in the network. Once it receives the request, it sends th e reply as the effective neighbour because of which the node is selected as the next effective cooperative nod e. This behaviour of node uses it as the intermediate node, but as it receives the packet, it does not forward it and considered itself as the receiver node. The type of black hole nodes is listed here under

A. Single Black hole Attack

Black hole attacker is the anonymous network node that presents it is identified as the effective neighbour and captures the communication. It considered itself as the destination node and does not forward the packets to next cooperative node. The single black hole attack is shown here in figure 1.

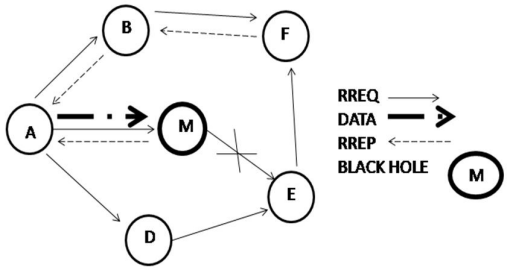

Figure 1 Single Black whole Attack

Here figure shows, as the communication between node A and E is established, a broadcast is set up through the request message to its neighbour nodes. The attacker node M also receives this RREQ packet and replies i t in effective time. It ensures that node M will be selected as the next effective neighbour. Based on the fake i nformation, as the node is selected as effective neighbour, the node captures the communication and not deliv er it node E.

B. Cooperative Black hole Attack

Here cooperative black hole attack is the attack applied on node pair or pairs with cooperative communication analysis. The attackers here behave as the normal communicating node but each of the attackers accepts the packets and not forward to any other network node. The cooperative black hole attack is shown here in figure 2.

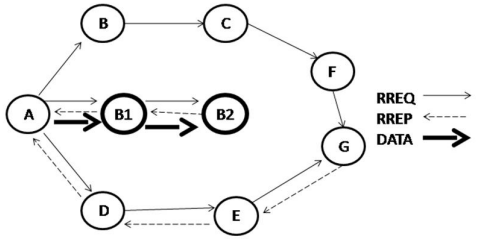

Figure 2 Cooperative Black hole Attack

Here figure is showing node B1 and B2 are the cooperative attacker nodes. Both nodes publish the fake information to capture the communication. Once the communication is captured, they can transfer data to one other but will not forward to any other network node.

C. Detection Method

The basic idea of this attack detection method is to provide the correct destination information to the source node so that the black hole will be identified in the network. The source node compares the information of attacker and the destination node to identify the effective destination. The detailed process of attack detection is shown here in figure 3.

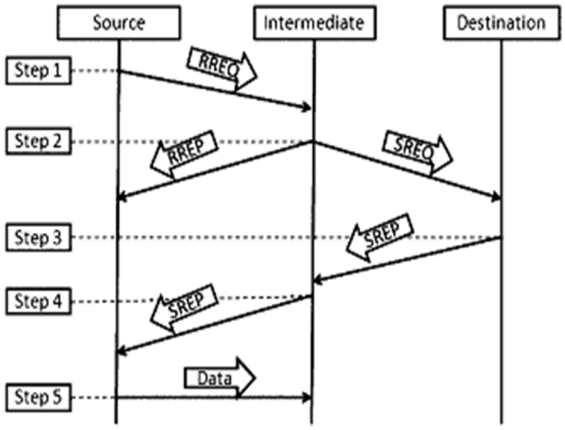

Figure 3 Single Black hole Detection Process [19]

The figure is showing the procedural behavior of attack detection. The figure shows that the RREQ is the me ssage broadcast to all the neighbor nodes. The intermediate node is processed under the route formation and t he RREQ message is sent by the source node and the intermediate node based communication is applied. The RREP is the message defined to provide the source specific request generation. The destination route is here generated based on the request messages. The table specific featured analysis is applied on the REQ message s. The reply is provided by the destination node via the intermediate nodes. These intermediate nodes can be processed under source specification under various measures for attack detection. The reply message of the in termediate nodes can be captured to identify the most effective designation and neighbor node. The performa nce of these nodes can be observed to identify the effective neighbor node and the malicious node.

III. Conclusion

In this paper, a study on different network attack is provided for mobile network. The paper has discussed different attack forms, their actions and the preventive process methods. The main stress of work is given on black hole attack. The paper identified the type of attacks, work behavior and defined the method for attack detection in global environment.

References

[1] M. Patel and S. Sharma, "Detection of malicious attack in MANET a behavioral approach," *Advance Computing Co nference (IACC), IEEE 3rd International, Ghaziabad,* , pp. 388-393, 2013.

[2] K. R. Abirami, M. G. Sumithra and J. Rajasekaran, "An enhanced intrusion detection system for routing attacks in MANET," *Advanced Computing and Communication Systems (ICACCS), 2013 International Conference on, Coimb atore,* , pp. 1-6, 2013

[3] Sukiswo and M. R. Rifquddin, "Performance of AOMDV routing protocol under rushing and flooding attacks in M ANET," *2nd International Conference on Information Technology, Computer, and Electrical Engineering (ICITAC EE), Semarang,* pp. 386-390, 2015.

[4] A. Katal, M. Wazid, R. H. Goudar and D. P. Singh, "A cluster based detection and prevention mechanism against no vel datagram chunk dropping attack in MANET multimedia transmission," *Information & Communication Technolo gies (ICT), IEEE Conference on, JeJu Island,* , pp. 479-484, 2013.

[5] S. Vhora, R. Patel and N. Patel, "Rank Base Data Routing (RBDR) scheme using AOMDV: A proposed scheme for

packet drop attack detection and prevention in MANET," *Electrical, Computer and Communication Technologies (I CECCT), IEEE International Conference on, Coimbatore*, , pp. 1-5, 2015.
[6] V. G. Mohite and L. Ragha, "Security agents for detecting and avoiding cooperative blackhole attacks in MANET," *International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), Dava ngere*, pp. 306-311, 2015.
[7] N. A. Noureldien, "A novel taxonomy of MANET attacks," *Electrical and Information Technologies (ICEIT), Intern ational Conference on, Marrakech*, pp. 109-113, 2015.
[8] P. Choudhury, S. Nandi, A. Pal and N. C. Debnath, "Mitigating route request flooding attack in MANET using node reputation," *IEEE 10th International Conference on Industrial Informatics, Beijing*, pp. 1010-1015, 2012.
[9] V. Desai and N. Shekokar, "Performance evaluation of OLSR protocol in MANET under the influence of routing att ack," *Wireless Computing and Networking (GCWCN), 2014 IEEE Global Conference on, Lonavala*, pp. 138-143, 20 14.
[10] M. Khatkar, N. Phogat and B. Kumar, "Reliable data transmission in Anonymous Location Aided Routing in MANE T by preventing replay attack," *Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future D irections), 2014 3rd International Conference on, Noida*, pp. 1-6, 2014.
[11] S. V. Kumari and B. Paramasivan, "Ant based Defense Mechanism for Selective Forwarding Attack in MANET," *D ata Engineering Workshops (ICDEW), 2015 31st IEEE International Conference on, Seoul*, pp. 92-97, 2015.
[12] S. Madhurikkha and R. Sabitha, "Defending against packet dropping attack using DRI & cross checking mechanism in MANET," *Information Communication and Embedded Systems (ICICES), 2013 International Conference on, Che nnai*, pp. 260-264, 2013.
[13] S. P. S. Tomar and B. K. Chaurasia, "Detection and Isolation of Sinkhole Attack from AODV Routing Protocol in M ANET," *Computational Intelligence and Communication Networks (CICN), 2014 International Conference on, Bho pal*, pp. 799-802, 2014.
[14] K. J. Sarma, R. Sharma and R. Das, "A survey of Black hole attack detection in Manet," *Issues and Challenges in In telligent Computing Techniques (ICICT), 2014 International Conference on, Ghaziabad*, pp. 202-205, 2014.
[15] A. Bala, M. Bansal and J. Singh, "Performance Analysis of MANET under Blackhole Attack," *Networks and Comm unications, 2009. NETCOM '09. First International Conference on, Chennai*, pp. 141-145, 2009.
[16] K. Laeeq, "RFAP, a preventive measure against route request Flooding Attack in MANETS," *Multitopic Conference (INMIC), 2012 15th International, Islamabad*, pp. 480-487, 2012.
[17] S. J. Soni and S. D. Nayak, "Enhancing security features & performance of AODV protocol under attack for MANE T," *Intelligent Systems and Signal Processing (ISSP), 2013 International Conference on, Gujarat*, pp. 325-328, 2013 .
[18] P. Rajakumar, V. T. Prasanna and A. Pitchaikkannu, "Security attacks and detection schemes in MANET," *Electroni cs and Communication Systems (ICECS), 2014 International Conference on, Coimbatore*, pp. 1-6, 2014.
[19] X. Zhang, Y. Sekiya and Y. Wakahara, "Proposal of a method to detect black hole attack in MANET," *2009 Internat ional Symposium on Autonomous Decentralized Systems, Athens*, pp. 1-6, 2009.
[20] G. Indirani, K. Selvakumar and V. Sivaaamasundari, "Intrusion detection and defense mechanism for packet replicat ion attack over MANET using swarm intelligence," *Pattern Recognition, Informatics and Mobile Engineering (PRI ME), 2013 International Conference on, Salem*, pp. 152-156, 2013.