SAJET

South Asian Journal of Engineering and Technology Vol.2, No.15 (2016) 151–160

ISSN No: 2454-9614

An Analysis and Prevention of Black Hole Attack by Sequence Number based Intrusion Prevention Reactive Routing Algorithm in MANET

G. Gunalakshmi[a], M. Subha[a*]

[a)] *Department Of Computer Science and Engineering, Theivanai Ammal College for Women (Autonomous), Villupuram-605 401, Tamilnadu, India.*
[b)] *Department Of Computer Science and Engineering, Theivanai Ammal College for Women (Autonomous), Villupuram-605 401, Tamilnadu, India.*

*Corresponding Author: G. Gunalakshmi
E-mail: guna.kalpana12@gmail.com,

Received: 22/11/2015, Revised: 21/12/2015 and Accepted: 2/03/2016

Abstract

In mobile Ad-hoc networks (MANETs), nodes are worked together and forward each other's packets in order to enable out-of- range communication. Routing protocols are exposed to a variety of security attacks. Black hole attack is one such type of an active attack. During the route detection process, the source node sends route detection packets to the intermediate nodes to find a fresh path to the intended destination. A malicious node responds immediately to the source node as an intermediate node which does not refer the routing table. Source node assumes that the route discovery process was completed and selects the path through the malicious node to route the data packets. Black hole attack made the packet dropping and unable to send the packets to the destination. The scope of the proposed SNBIP (Sequence Number based Intrusion Prevention) algorithm is to analyze and prevent black hole attack in MANET, during routing process. Proactive routing table is created using AODV. Then the new route is established using the proposed reactive routing algorithm SNBIP. To find the malicious node the proposed technique use sequence number in the RREQ and RREP during route discovery. Destination node sends RREP packet, after increasing the sequence number of the source node by random percentage. Depends on the starting number of the sequence number increment of the percentage differs. Variation of the random percentage increment in the RREP introduces the malicious node. Proposed solution provides better performance in terms of packet dropping, throughput, data rate and end-to-end delay.

Keywords: SNBIP, AODV, Sequence number, Black Hole Attack, Routing, MANET.
Reviewed by* **ICETSET'16 *organizing committee*

1. Introduction

Mobile Ad-Hoc Network (MANET) is a self-designing base less system of cell phones associated by remote connections. It is an accumulation of specialized gadgets or nodes that wish to convey with no settled framework and pre-decided association of accessible connections.

The essential test in building a MANET is preparing every gadget to consistently keep up the data required to appropriately course activity. The primary test is his helplessness to security attacks.

The Packet Dropping in MANET can be arranged into a few classes as far as the procedure embraced by the malevolent node to dispatch the attack. Specifically the noxious node can purposefully drop all the sent bundles experiencing it (black hole), or it can specifically drop the packets started from or bound to specific nodes that it disdains. Moreover, an exceptional instance of black hole attack named dim-hole attack.

Keeping in mind the end goal to dispatch a black hole attack, the initial step for a pernicious node is to discover a way that permits it to get included in the steering/sending way of information/control packets. To do as such, it abuses the vulnerabilities of the hidden steering conventions which are for the most part composed with solid suspicion of reliability of the considerable number of nodes taking part in the system. Accordingly, any node can without much of a stretch act playfully and incites a serious damage to the system by focusing on both information and control bundles.

2. Literature review

Mobile Ad-Hoc Network (MANET) is a self-designing base less system of cell phones associated by remote connections. It is an accumulation of specialized gadgets or nodes that wish to convey with no settled framework and pre-decided association of accessible connections. The essential test in building a MANET is preparing every gadget to consistently keep up the data required to appropriately course activity. The primary test is the helplessness to security attacks.

The Packet Dropping in MANET can be arranged into a few classes as far as the procedure embraced by the malevolent node to dispatch the attack. Specifically the noxious node can purposefully drop all the sent bundles experiencing it (black hole), or it can specifically drop the packets started from or bound to specific nodes that it disdains. Moreover, an exceptional instance of black hole attack named dim-hole attack.

Keeping in mind the end goal to dispatch a black hole attack, the initial step for a pernicious node is to discover a way that permits it to get included in the steering/sending way of information/control packets. To do as such, it abuses the vulnerabilities of the hidden steering conventions which are for the most part composed with solid suspicion of reliability of the considerable number of nodes taking part in the system. Accordingly, any node can without much of a stretch act playfully and incites a serious damage to the system by focusing on both information and control bundles.

2.1 Attacks in MANET

The attack surface of the software environment is in different points where an unauthorized user can try to enter data to or extract data from an environment **[12].**

A. Passive Attack

A passive attack screens decoded activity and searches for clear-message passwords and sensitive data that can be utilized as a part of different of attacks.

B. Dynamic Attack

In a dynamic attack, the aggressor tries to sidestep or break into secured frameworks. This should be possible through stealth, infections, worms, or Trojan steeds.

C. Circulated Attack

A circulated attack requires that the attackers present code.

D. Insider Attack

An insider attack includes somebody from within, for example, a disappointed representative, attacking the system Insider attacks can be malignant or no noxious.

E. Close-in Attack

Close physical vicinity is accomplished through surreptitious passage into the system, open access, or both.

2.2 Routing

Routing algorithm is classified into 2 types they are **[12].**

Proactive routing

All the nodes present in network shares the routing information with each other periodically, because of its consistent and accurate information is always updated.

Reactive routing

In reactive routing source node does not know the path between source and destination only at that time rout discovery mechanism is initiated

2.3 Black Hole Attack in AODV

In order to find another way towards a faraway destination, the source node telecasts a RREQ (Route Request) message with one of a kind identifier to every one of its neighbours. Every recipient rebroadcasts this RREQ to every one of its neighbours until coming to the proposed destination. On accepting the RREQ message, the destination node overhauls the succession number of the source node and sends a RREP (Route Reply) packet to its neighbour which has transferred the RREQ. Be that as it may, the aggressor node sends fake RREP to source node by setting most noteworthy arrangement number. In this way, the source node starts another course revelation to supplant the fizzled way. **[6]**

The Black hole attack is distinguished in way steering process itself. The fake RREP parcel is recognized by irregular number. Arbitrary number is same for all RREQ packets that are gotten from same source node. The irregular number is appended in each RREP bundle by destination node. At the point when fake RREP is gotten from a way, this way again checked to recognize which is attacker. Information gathering table likewise used to affirm whether suspicious node is attacker or not.

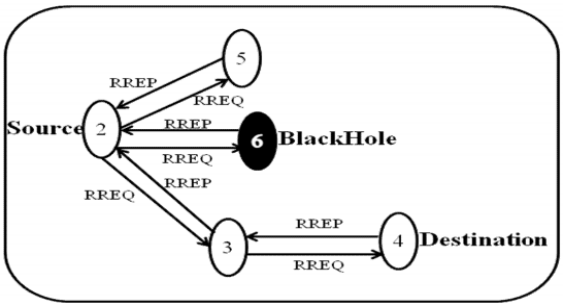

Figure 1 Black Hole Attack in AODV

3. Proactive Routing Table using AODV

Ad-hoc on-demand distance vector algorithm is a pure on-demand route achievement system nodes that do not lie on active paths neither maintain any routing information nor participate in any periodic routing table exchanges Further a node does not have to discover and maintain a route to another node until the two need to communicate unless the former node is offering its services as an intermediate forwarding station to maintain connectivity between two other nodes.

The local connectivity of the mobile node is of interest each mobile node can become aware of the other nodes in its neighborhood by the use of several techniques including local not system wide broad casts known as hello messages The routing tables of the nodes within the neighborhood are organized to optimize response time to local movements and provide quick response time for requests for establishment of new routes The primary objectives of algorithm are

1. To broadcast discovery packets only when necessary
2. To distinguish between local connectivity management neighborhood detection and general topology maintenance
3. To disseminate information about changes in local connectivity to those neighboring mobile nodes that are likely to need the information

AODV uses a broadcast route discovery mechanism as is also used with modification in the Dynamic Source Routing DSR algorithm. The different pays off in networks with many nodes where a larger overhead is incurred by carrying source routes in each data packet. To maintain the most recent routing information between nodes we borrow the concept of destination sequence numbers from DSDV. Unlike in DSDV however each Ad-hoc node maintains a monotonically increasing sequence number counter which is used to supersede stale cached routes The combination of these techniques yields an algorithm that uses bandwidth efficiently by minimizing the network load for control and data traffic is responsive to changes in topology and ensures loop free routing[12]

3.1 Reactive Routing SNBIP Algorithm

```
1 SN Broadcasts RREQ
2 SN Receives RREP
3 SN Stores DSN and NID in RT
4 Retrieve First entry from RT
5 IF (DSN>>>=SSN)
6 {
7 MN-ID=NID
8 Black Hole Node
9 }
10 ELSE
11 {
12 Normal Node
13 }
SN-Source Node
DSN-Destination Sequence Number
SSN-Source Sequence Number
NID-Node ID
MN-ID-Malicious Node ID
RT-Routing Table
```

3.1.1 Architecture diagram for SNBIP

At the point when the Node with highest Sequence number is gotten by the source it is considered as a dark opening and that course toward that dark gap is disposed of and the directing table is flushed or upgraded what's more, sorted by destination grouping number.

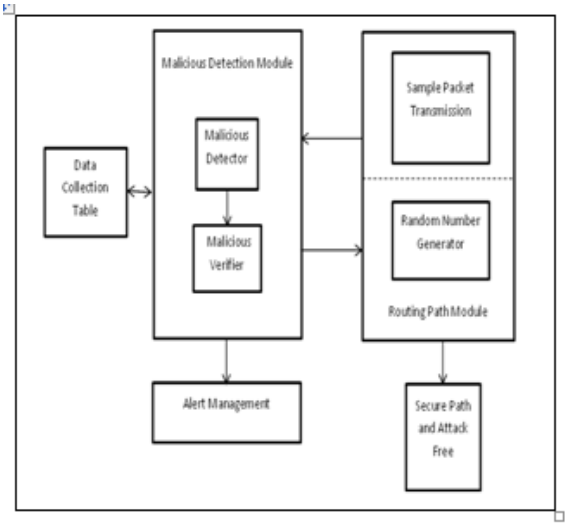

Figure 2 SNBIP Architectural Diagram

The figure1.2 represents that the data is sending securely from source to destination without dropping data.

The architecture diagram works based on the following

1. Data Collection Table
2. Malicious Detection Module
3. Routing path module
4. Alert Management

3.2 Data Collection Table

Data Collection Table contains number of data packets sent and received from/to neighbor nodes. Data Collection Table contains four fields. Each field having specific information about a particular node. This table has four fields named as IP_ADD, SENT, RECEIVED, TIME BIT. IP_ADD field store IP address of a node. Base on this IP address sent and received packets to be calculated. Second field SENT contains number of packets sent to this node (i.e., IP address). Third field contains number of packets received from a node. Last field TIME_BIT used to check whether stored data (i.e., send and received packets) fields are fresher or not. TIME_BIT field provides record freshness. This TIME_BIT have two possible values are 0 and 1. Value 1 indicates the specific node's Data collection table is created freshly. Value 0 indicates that specific node is out of range to current network or link failure.

3.3 Malicious Detection Module

Malicious node Detection Module has two main process called malicious detection and malicious confirmation. Malicious detection process is acknowledgment based detection process that detect suspicious node. The term suspicious node is like, fail to participate or poor participation in data transmission in most of time. Malicious verifier process is work based on data collected form DCT(Data Collection Table). It finalizes whether suspected node is malicious or not.

3.4 Routing path module

Routing path module is used to find a valid route between source and destination for data transmission. For routing path discovering, AODV-Ad-hoc On Demand Vector protocol is used. In this project during path routing, sequence number is increased by some percentage and attached with every RREP packets to determine all RREP packets are generated by destination node.

3.5 Alert management

Alert management broadcast alert messages to all nodes present in network. The alert message is about a one or more attacked nodes and these nodes should not be used in data transmission in future. Meanwhile these attacked nodes details to be removed from routing table in every node

At the point when a source node needs to correspond with destination node, it first checks for a rout to the destination in the steering table. Source node propagate RREQ packet to its neighbor in order to find a rout to destination. At that point the source node waits for RREPs (Route Reply) to be gotten from the destination node. Source node chooses the RREP which has high destination sequence number. Then Source node drops other

incoming RREP packets. In-order to prevent malicious node to participate in data transmission, destination node follows a novel solution. Destination node increments source node's sequence number in certain number of times. So source node's sequence number will be changed in RREP. The new sequence number is used for differentiating legitimate RREPs and malicious RREPs. Increasing of sequence number is based on source node's sequence number appended in RREQ packet. So every RREP has source's sequence number and certain percentage of increased number. It differentiates legitimate node's RREP packet and malicious node's RREP packet.

Source node knows that number of sequence number increased by destination number. So it can easily identify sequence number sent by legitimate node and malicious node. Then source selects route with free of attacks by drops malicious node's RREP.

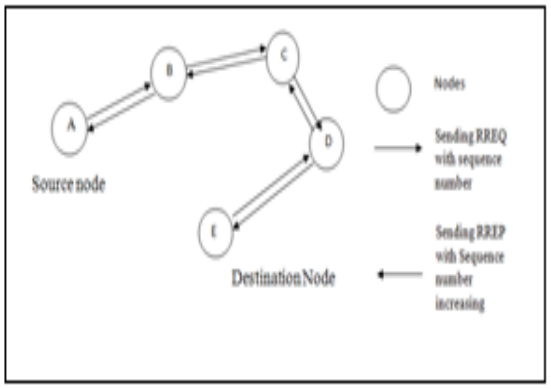

Figure 3 Secure Data Transferring

Figure 1 demonstrates that source node A sending RREQ to destination E with its sequence number. Then the destination E sends RREP with increasing the source sequence number with some percentage. Based on that increased percentage source node can identify the destination node and malicious node.

4. Existing and proposed comparison results

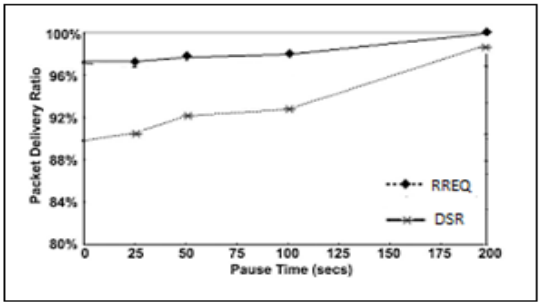

Figure 4 existing and proposed algorithm comparison result

Using AODV algorithm while sending RREQ from source to destination, packet is dropped by malicious node at 90% itself before received by destination node. Using SNBIP Algorithm RREQ is sending securely from source to destination at 100%.

5. Results and Discussion

A system is displayed as set V of nodes that are interconnected by a set E of correspondence connections. V and E change after some time when nodes move. Nodes have the greatest transmission range. Every node is outfitted with an Omni directional receiving wire. Two nodes are quick neighbours and an undirected connection joining them exits on the off chance that they are in the transmission scope of one another. There are a few ways between two nodes. The decision of course could be founded on the accessible data transfer capacity. The reenactments after effects of the proposed technique are investigated.

The re-enactment time is set as 200 secs for 125 nodes with a network size of 1000×1000 m. The qualities decided for CW min and CW max are 31 and 1023 individually. These recreation parameters are set according to IEEE 802.11 standard. Figure 2 demonstrates that the quantity of bundles got at 5 nodes. Packets are steered through these five nodes before attack. Toward the end of 40 secs, 450 bytes are gotten roughly. Figure 3 indicates bundles got under attack. Couple of nodes get packets strangely. Those are distinguished as malevolent nodes. Consequently this way is blocked and interchange way is chosen to transmit the packets

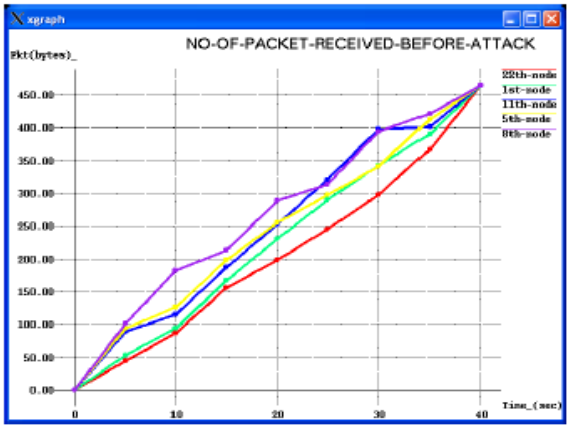

Figure 5 Packets Received Before Attack

With a specific end goal to diminish bundle misfortune and delay, these malignant nodes are recognized by checking the unusual increment in arrangement number of RREP control parcel. Figure 4 demonstrates packets got subsequent to forestalling Black Hole attacks.

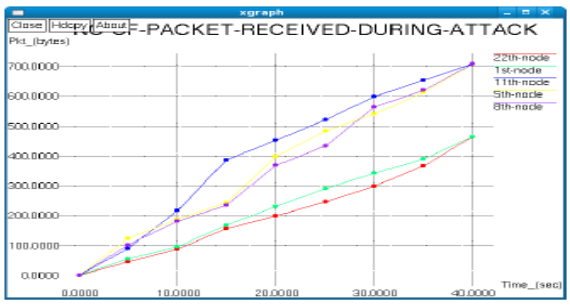

Figure 6 Packets Received During Attack

Distinguishing and controlling pernicious nodes amid course disclosure technique itself lessens bundle misfortune.

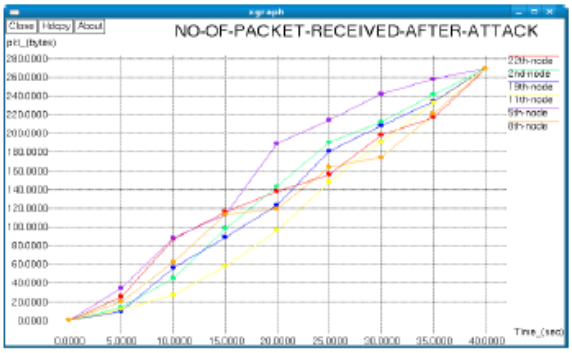

Figure 7 Packets Received After Implementing SNBIP Algorithm

Malevolent aggressors debilitate the system assets, for example, transfer speed and devour the node's assets, for example, computational and battery control and upset the steering operation bringing on extreme debasement in the system execution. These aggressors are distinguished and are blocked.

6. Future Work

Further studies need to be done for a longer time frame. Investigation for the multi-step clustering algorithm. Further work needs to be done to decrease the route discovery time which will affect streaming traffic.

7. Conclusion

The extraordinary qualities of MANETs make steering a testing assignment. Portability of nodes reason continuous course disappointment. As an after effect of these, a viable directing convention needs to adjust to element topology and intended to be transfer speed compelled. Remote channel is transfer speed compelled and shared among numerous systems administration substances. Since MANET has no reasonable line of resistance, it is open to both true blue clients and noxious aggressors. Keeping in mind the end goal to address this issue, different

sorts of attacks are examined. Malignant nodes attack the system which causes parcel misfortune and expend significant measure of data transmission. These sorts of nodes are recognized and obstructed to enhance the accessible data transfer capacity. Nonetheless, Ad-Hoc systems present one of a kind propelled challenges, including the outline of conventions for versatility administration, successful directing, information transport, security, power administration, and QoS provisioning. Once these issues are settled, the pragmatic utilization of MANETs will be feasible.

References

[1] Batra, S., Goyal, P. and Singh, A. A Literature Review of Security Attack in Mobile Ad-hoc Networks, International Journal of Computer Applications, 11-15, 2010.
[2] Chen, Y. and Nasser, N. Enhanced Intrusion Detection System for Discovering Malicious Nodes in Mobile Ad-hoc Networks, IEEE Communications Society subject matter experts for publication in the ICC 2007 proceedings, 2007.
[3] G. S. Mamatha, Dr. S. C. Sharma, "A New Combination Approach To Secure MANETS Against Attacks", In International Journal of Wireless & Mobile Networks (IJWMN), volume 2, page(s):1-10, 2010
[4] J-H. Cho, A. Swami, and I-R. Chen, "A Survey on Trust Management for Mobile Ad-hoc Networks," IEEE Communications Surveys & Tutorials, Vol. 13, No. 4, Fourth Quarter 2011.
[5] Jiao Wen-Cheng, Peng Jing And Zheng Jain-Ling (2010) "Research and Improvement of AODV Protocol in Ad-hoc Network", Wireless Communications Networking and Mobile Computing (WiCOM), 2010 6th International Conference, 1-3
[6] Mistry N, Jinwala DC, IAENG, Zaveri M (2010). Improving AODV Protocol against Black hole Attacks, the International Multi Conf 1-3.
[7] Rutvij H. Jhaveri, Ashish D. Patel, Jatin D. Parmar and Bhavin I. Shah (2010). MANET Routing Protocols and Wormhole Attack against AODV: IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.4, April 2010.
[8] Radhika Saini and Manju Khari (2011).Defining Malicious Behavior of a Node and its Defensive Techniques in Ad-Hoc Networks, Journal of Smart Sensors and Ad-Hoc Networks (IJSSAN) Volume 1, Issue-1 18-21.
[9] S.Kannan, T. Maragatham, s. Karthik, V.P Arunachalam, "A Study of attacks, Attack Detection and Prevention Methods in Proactive and Reactive Routing Protocols", In Medwell journals, volume 5, page No.: 178-183, 2011.
[10] S. Umang, B.V.R. Reddy, M.N. Hoda, "Enhanced intrusion detection system for malicious node detection in Ad-hoc routing protocols using minimal energy consumption", In ITE journals, volume 4, page(s): 2084 - 2094, 2010.
[11] Wang W, Bhargava B, Linderman M (2009) Defending against Collaborative Packet Drop Attacks on MANETs. Paper presented at the 2nd International Workshop on Dependable Network Computing and Mobile Systems (DNCMS 2009) (in Conjunction with IEEE SRDS 2009).
[12] http://www.wikipedia.org.