ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 4, April 2016

An Enhance Apporach to Mitigate the Impact of Black Hole and Gray Hole Attacks in AODV Routing Protocol

Amit Nakum, J.H.Joshi
Department of Electronics & Communication, V.V.P Engineering Collage, Rajkot, Gujarat, India.

ABSTRACT: Wireless network has become more and more popular during the past decades. A Mobile AdHoc Network (MANET) is integrating of mobile nodes, in which the packets are forwarded without any centralized network authority. The devices are connected via wireless medium. Due to this characteristic security is high risk because packets are easily trapped in the network. There is no pledge of attack free communication due to heterogeneity in the network. AdHoc on Demand Vector (AODV) is a reactive routing protocol in MANET. This is a typical MANET protocol so in this protocol malicious node tries to attack on this protocol. The operation of AODV is loop-free, and by avoiding the "counting to infinity" difficulty offers quick junction when the ad hoc network topology changes.
In this paper, propose a friend-ship value based detection algorithm which aims to detect malicious nodes. We have proposed a approach for securing AODV against black hole attack as well as gray whole attack. This approach also prevents and detects black hole/gray hole node or malicious node in the network. The propose algorithm identifies malicious node as well as improve the performance parameter using NS-2.35 simulator.

KEYWORDS: Black hole attack, Gray hole attack, AODV protocol, friend-ship value.

I. INTRODUCTION

MANET (Mobile AdHoc Network) is a collection of mobile nodes. Evolved from Packet Radio Network (PRNET) and Survivable Adaptive Radio Network (SURAN).This type network supports mobility to the users because the main objective of MANET is to make available access anywhere and anytime without any predefined infrastcture. The transmission of packets is multi-hop fashion. The topology of this type network is not fixed i.e. dynamic in nature. Due to this future this type network have several applications like Military Applications, Disaster Management, Wireless Sensor Networks, Vehicular Ad hoc Networks, Personal Area Network (PAN) etc.
In the earlier all the researchers‟ focus on throughput of MANET networks. They refuse that there is no any malicious node existing in the network and all the nodes are trustworthy But in present scenario this network is more vulnerable to the internal as well as external attacks. This attack emerges to security threat which disturbing the routing.
Ad hoc On-demand Distance Vector is a reactive protocol which creates routes when demanded by the source host and the routes are maintained and used when needed. AODV allows mobile nodes to obtain routes quickly for new destinations, and does not require nodes to maintain routes to destinations that are not in active communication [8]. It consume less energy because it is on demand, it does not protect the route from source to destination whenever it is necessary at that time discover the route.
As in AODV protocol, in black hole attack node advertise fake routing information and claims that it has the shortest routing path to the destination. Due to this false routing information source node sends data packets to this path, so all the data packets will drop out by this malicious node. Gary hole attack is the variation of black hole attack, in this attack some data packets will drop out. Because gray hole affected malicious node sometimes behaves like malicious node as well as trusted node in routing.
The attacker or malicious node mainly targets RREP packets also route discovery of network. If the communication is not working on regarding the nodes then route is damaged so RREP is hot target for attacker or malicious node
The goal of the proposed approach is the avoidance of malicious node which is present in the network and attack free communication between sources to the destination using friendship value based approach. In this approach friendship Value is checked with every RREP and RREQ with threshold friendship. Friendship value of any node is defined by as follows:

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 4, April 2016

$$\textbf{Friend Ship value} = \frac{E*Fr}{H*Dsn}$$

Where E; Energy, Fr; frame rate
H; hop count Dsn; Dest. Seq. no. (1)

Section II shows background about this attack. In section III shows related work, in section IV shows propose algorithm and section V we conclude the paper with future work.

II. BACKGROUND

A MANET is an infrastructure-less type network, which consists of number of mobile nodes with wireless network interfaces. [1, 2]
In order to make communication among nodes, the nodes dynamically create paths between one another. The nature and structure of such networks makes it attractive to various types of attackers. This type of the network is defenseless to various types of attacks not only from outside but also from inside the network. These types‟ attacks can be generally classified as:

1) Passive Attack and
2) Active Attack

A passive attack won't interrupt the common process of MANET; while data have been exchanged from the network. The nature of passive attack is to isolate the data exchanged in the network. The attacker eavesdroppers the data exchanged in the network without altering it. One of the solutions to the problem is to use powerful encryption mechanism is used. [10]
An Active attack always tries to modify normal operation of MANET, which means the disturbance has been made in the network. Active attacks can be internal or external. Some of the active attacks that are Gray hole attack, Black hole attack, Worm Hole attack, and Routing attacks. These attacks can be occurred at any point of time in the network. [10]
In AdHoc networks routing mechanism has three layers namely Network, Physical and MAC layers play a dynamic role. [10] AODV is sensitive to various types of attack because it is a one of the best routing protocol of ad hoc network. As we mentioned above MANETs are more vulnerable to various attacks, all these three layers suffer from different attacks and it because routing disorders. The different kind of attacks in the network layer varied such as selective forwarding attack and modifying some parameters of routing messages.

The Network layer attacks classified as:
1) Black Hole attack
2) Gray Hole attack

As a node which receives the RREQ packet, it will send a false RREP packet instantly with a renewed high sequence number. So source node will rumored that there is a new route is available towards the destination. The source node ignores the RREP packet from the other nodes containing the correct nodes and automatically it will start sending the packets towards these malicious nodes. The malicious nodes will drop all the data packets. This is called black hole attack.
A malicious node which sometimes acts as reliable as well as malicious which drop all as well as some packets respectively in route discovery, this type attack is known as gray hole attack. The route discovery is same as mentioned above. This type attack is big challenge to detect compare to black hole attack.

III. RELATED WORK

Dhaka, A. Nandal et al. in [1] proposed a solution that in the existing AODV Routing protocol have been introducing two packets which are Response sequence (R_{seq}) packet and Code Sequence packet (C_{seq}). These packets are transmitted when a node wants to access the channel. Each intermediate node sends the Cseq to all its neighbors then

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 4, April 2016

neighbors intern send their Rseq to the intermediate node. If the C_{seq} and R_{seq} matches from the neighbor then the intermediate node allow the link to the network layer, Otherwise, it discard the node and send the information to all other nodes that particular node as malicious one. Due to this propose algorithm the malicious nodes are identified at the initial stage itself and immediately removed.

A.Gupta et al in [2] introduced the proposed scheme through which malicious node can be find out in real time monitoring. Moreover promiscuous mode is used to find the malicious node. Two counters fvalue and rvalue are used to check whther the node is malicious node or not. When malicioius id is detected intruder notification (INTNOT) is generate and this broadcasts this malicious id to every node, so malicious id has been removed from the network.

Sridevi, K. et al. [3] in this method every node in a network listens to it neighboring nodes promiscuously. In promiscuous mode, every node observers the packet being forwarded by its neighbors in order to spot the behavior of neighbor regarding packet operation. Every node matches the neighbor information with the information it stores in its knowledge table. The knowledge table contains the information which have been recently transmitted. Every node in promiscuous mode maintains a table containing two fields „fm" and „rm". If both are same the node assumes that the packet is forwarded further, otherwise node waits for particular amount of time and checks the reasons for packet dropping.

Kanthe, et al. [4] in this paper attempted to mitigate the gray hole attack and proposes a credit based approach based on Ad-hoc On Demand Distance Vector (AODV) routing protocol. In this approach, initially each and every node assigns a fixed value for its every neighbor node as the neighbor credit value. This credit value is incremented by when it receives a route request packet (RREQ) and decrement when it receives the route reply (RREP) packet. When a node finds credit for one of its neighbors as a negative value, then it identifies the gray hole node. Also it removes all existing paths from its routing table going through that node.To evaluate the performance consider the impact of the nodes, mobility and pause time vs. throughput, end to end delay and normalized routing load.

Hiremani, V. et al. [5] in proposed work, it is intended to detect and eliminate co-operative black hole and gray hole attacks by maintaining MEDRI (Modified Extended Data Routing Information) Table at each node. The fields of this table are used to detect a malicious node as well as maintain a history of its previous malicious instances to accommodate the gray hole behavior. So in this propose scheme introduce three new columns which are 'Packet size at source', 'Packet size at destination' and 'Result' which checks the complete data transmission from source to the destination. Due to this approach we can find secure path from source to the destination. This technique keeps the records and maintains the history of every malicious node.

Ahmed, M. et al. [6] in this paper, a novel Intrusion Detection System (IDS) introducing to identify malicious nodes. The ultimate aim of these schemes is to provide the necessary security cover to the network by adding encryption to maintain privacy and reliability. The AODV protocol in Ns simulator is modified (black holeaodv and grayholeaodv protocol) to simulate both the attacks. Similarly, the AODV protocol is modified (idsaodv protocol) to implement the IDS (Intrusion Detection System) for the attacks. While carrying out the simulation two parameters which are, Data Transmission Quality (DTQ) and Stability of model Behavior (STB) is calculated. Once the malicious node is identified, it is isolated from the system or is ignored for future communication, in the network.

Khattak, H. et. al. [7] in this paper present a hybrid approach for preventing black/gray hole attacks by choosing second shortest route selection and hash function and timestamp base solution for consisting data transmission. When the receiver sends the RREP message after receiving the second RREQ then source node will have to send the data packets on the second shortest path. In this way, this solution makes it difficult for the malicious node to place itself in the second shortest path between source and destination. The probability of the presence of malicious node in the second shortest path decreases and the second shortest route for data packets transmission can provide a safer route in MANET using AODV. This also makes AODV safer and secure which can ensure the security of all data packets.

S. Ramaswamy et. al. [8] in this paper presents a technique to identify many black holes cooperating with each other and a solution to discover a safe route evading this cooperative black hole attack. It starts a route discovery process by broadcasting the Route Request (RREQ) message to its neighbors, which is further propagated until it reaches an intermediate node with a fresh enough route to the destination node specified in the RREQ, The technique works with slightly modified AODV protocol and makes use of the Data Routing Information (DRI) table in addition to the cached and current routing tables.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 4, April 2016

IV. PROPOSED METHOD

Node should have more residual battery energy (RBE) A propose method, designed for identifying and removing black hole attack and gray hole attack under AODV protocol. The algorithm used to detect malicious node. We have proposed an approach for securing AODV against DoS attacks. This approach also prevents and detects malicious node in the network, for this consider following network as shown below:

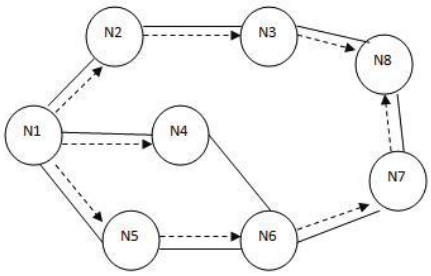

Figure 1: Propagation of RREQ.

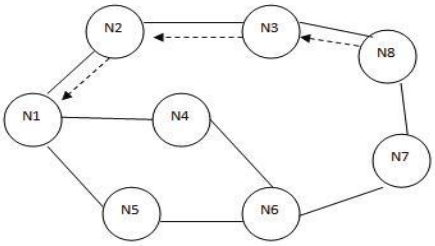

Figure 2: Propagation of RREP.

In this proposed procedure an intermediate node receiving anomalous routing statistics from its neighbour node. This algorithm identifies the malicious nodes through friendship value. This value is calculated over RREQ and RREP. Main parameter for finding friendship value is Energy, Data frame rate, HOP count and Destination seq. Number.
The algorithm starts from source node, as shown in above figure 1. Source node N1 starts route discovery process with all intermediate neighbouring nodes. RREQ messages is broadcast to all intermediate nodes. Now this intermediate node checks whether this id is for destination or not. If it contains destination id then it unicast RREP to the source node, otherwise it stores this value and calculates the friend-ship value of this node from equation (1) and stores this value in its routing table to check whether the node is trusted node or malicious node.

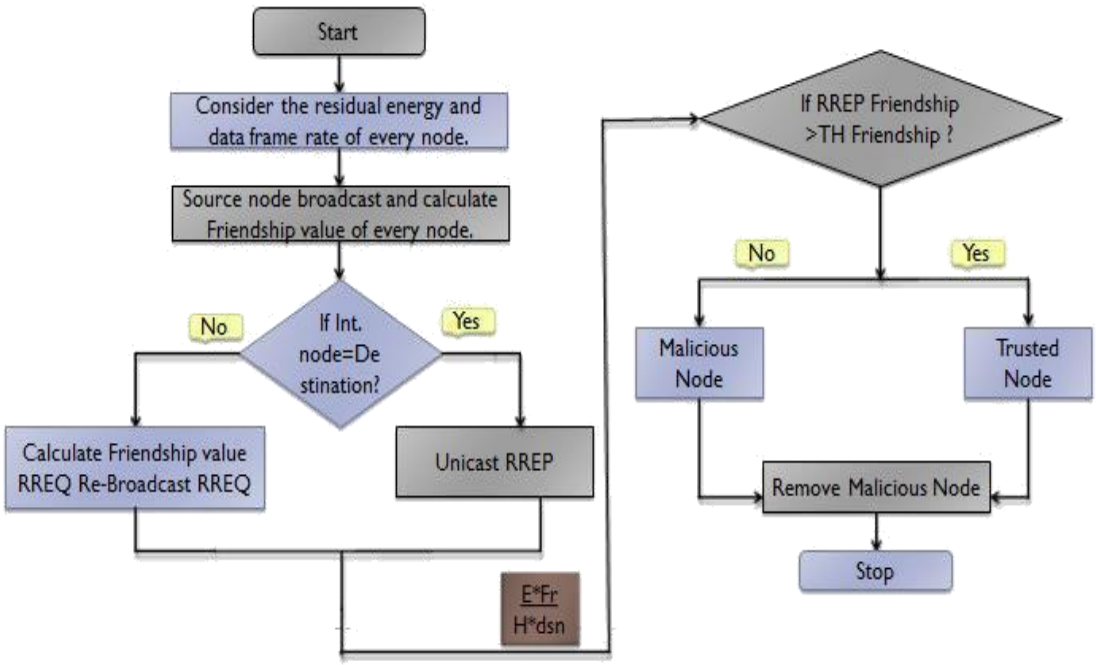

Figure 3: Propose Algorithm.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 4, April 2016

After storing this id, RREQ broadcast to other intermiddiate node,to check path between source to destination with min. hop count and max. Destination seq. No. The node which contains destination id will now matches with source id to establish the path between sources to destination.

The node which accepts this RREP which also checks Friendship value from equation (1) and stores this value in its routing table to check whether the node is trusted node or malicious node. This calculated friend-ship value of RREQ and RREP is compares with Threshold friend-ship value (TF). TF value can be chosen according to the network scenairo.

This calculation checks whether it is grater or less than from calculated friend-ship value. If it is less than it is malicious node and if it is greater than then it is trusted node. More friendship value of node is shows more trusted node. When it values becomes less than desired threshold then it identifies as malicious node. As the denominator is high friend ship value will less and as the denominator is low friend ship value is more. This shows malicious node or it is a trusted node. This establishes the path between source to destination with Min. hop count and Max. Seq. number.

If the node is trusted node then it sends unicast RREP to the source node and if this is malicious node then it purposefully reduces hop count and increase destination sequence no. to allow shortest path from source to the destination. If this node is malicious node then it drops out data packets.

If the malicious node is black-hole attack then it drop out all the data packets and the malicious node is gray hole attack then drop some data packets. Because during route discovery the node acts as a honest node. As a result all communication coming from this node will be blocked, and the communication coming from or going through this node will be blocked.

On the identification of malicious node, Neighbor node takes an initiative to notify all nodes by broadcasting this malicious id is present in the network. This malicious id will remove from the network. The energy here is included to find best routing path.

V. CONCLUSION & FUTURE WORK

Security is one of the essential aspects of routing protocol because it is very easy to disruption the security of the routing protocol of the mobile ad hoc network. In a previous work the attacker is decide based on trust value, comparison of hop count etc. methods. So using this method overhead will be increases. This overhead will be increases due to extra control packets, and also cost function is also increases. Because cost function is basically hop count.

From this propose work we can isolate the malicious node which reduces the heterogeneity of the network and also reduces cost function as well as overhead of the network.

In future this proposes work will be implemented which isolates the malicious nodes and also improves the performance parameter like throughput, good put pdr and nrl in AODV protocol. The performance parameter which improooved is compared with other reactive routing protocol using NS- 2.35.

REFERENCES

1. Dhaka, A Nandal, et al. Gray and Black Hole Attack Identification Using Control Packets in MANETs. Procedia Computer Science, 2015; 54: 83-91.
2. Gupta, A Mitigation Algorithm against Black Hole Attack Using Real Time Monitoring for AODV Routing Protocol in MANET.
3. Siddiqua, A Sridevi, et al. preventing black hole attacks in MANETs using secure knowledge algorithm. In Signal Processing And Communication Engineering Systems (SPACES), 2015 International Conference on IEEE. 20154; 421-425.
4. Lokare, D Kanthe, (2014). Cooperative Gray Hole Attack Discovery and Elimination using Credit based Technique in MANET.International Journal of Computer Applications, 2014; 88.
5. Hiremani, Jadhao, et al. (2013, December). Eliminating co-operative blackhole and grayhole attacks using modified EDRI table in MANET. In Green Computing, Communication and Conservation of Energy (ICGCE), 2013 International Conference on IEEE. 2013; 944-948.
6. Ahmed, Hussain, et al. (2014, January). Performance of IDS in an Adhoc Network under Black Hole and Gray Hole attacks. In Electronics, Communication and Instrumentation (ICECI), 2014 International Conference on IEEE. 2014; 1-4.
7. Khattak, H. (2013, September). A hybrid approach for preventing Black and Gray whole attacks in MANET. In Digital Information Management (ICDIM), 2013 Eighth International Conference on IEEE. 2013; 55-57
8. S Ramaswamy, H Fu, et al. Prevention of cooperative black hole attack in wireless ad hoc networks. In Proceedings of 2003 International Conference on Wireless Networks (ICWN″03), Las Vegas, Nevada, USA, 2003; 570–575.
9. Perkins, C Belding-Royer, et al. (2003). Ad hoc on-demand distance vector (AODV) routing (No. RFC 3561).
10. Gagandeep, Kumar P, Analysis of different security attacks in MANETs on protocol stack a-review. International Journal of Engineering and Advanced Technology (IJEAT), 2012; 1: 2249.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 4, April 2016

11. Suresh, HN Vara prasad, et al. (2014). Designing Energy Routing Protocol with Power Consumption Optimization in MANET. Emerging Topics in Computing, IEEE Transactions on, 2014; 2: 192-197.
12. Aarti, DS (2013). Tyagi, Study Of Manet: Characteristics, Challenges, Application And Security Attacks, International Journal of Advanced Research in Computer Science and Software Engineering, 2013; 3: 252-257.
13. Rafsanjani, MK Anvari, et al. (2011). Methods of Preventing and Detecting Black/Gray Hole Attacks on AODV-based MANET. IJCA Special Issue on Network Security and Cryptography, NSC.
14. Singh, HP Singh, et al. Cooperative Blackhole/Grayhole Attack Detection and Prevention in Mobile Ad hoc Network: A Review. IJCA, ISSN, 2013; 0975-8887.
15. Suresh, HN Varaprasad, et al. Designing Energy Routing Protocol with Power Consumption Optimization in MANET. Emerging Topics in Computing, IEEE Transactions on, 2014; 2:192-197.
16. Eissa, T Razak, et al. (2013). Trust-based routing mechanism in MANET: design and implementation. Mobile Networks and Applications, 2013; 18: 666-677.