ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

Clustered Organization for Manets with an Approach to Prevent Black Hole Attack

Shilpa Gopinath[1], Arun KumarG[2]

M.Tech final year, Electronics and Communication Engineering, STJIT, Ranebennur, India [1]

M.Tech, (PhD), Electronics and Communication Engineering, STJIT, Ranebennur, India [2]

Abstract: Mobile Ad-hoc Networks are cooperative networks that don't have a centrally managed fixed infrastructure. As the mobile nodes in these networks have sufficient freedom to move in and out of the network at any time randomly, securitizing of the routing appears to be a challenging task, thereby leaving MANETs open to serious attacks and this raises questions on reliability of these networks. All these characteristics and challenges of MANETs grab the attention of many researchers and engineers. This paper sheds some light on a cluster oriented concept to enhance efficiency of the network and an approach for Black Hole attack detection and prevention.

Keywords: MANETs, Black Hole, routing security, simulation, performance analysis

I. INTRODUCTION

Mobile ad hoc network is a collection of mobile nodes which are equipped with both receiver and transmitter that helps them to communicate in a shared wireless medium in the absence of a definite infrastructure and central authority. The nodes can enter or leave the network at any time randomly thus have a dynamic approach of network topology and each of the node will carry the responsibility of router and host [3]. This contemporary brand of self-organizing network allows to a quicker deployment of a very wide field of communication. This network which is a blend of wireless communication and high degree mobile nodes, edges to a topology of the network that keeps on changing rapidly over time which is frivolous. This litheness in these networks makes them attractive for many applications like military operations and disaster recovery operations where, it gives surpassing coverage, high throughput with very low operating cost [2].

MANETs are one of the heading and briskly growing areas in research fields and hence are an attractive technology for various applications because of the flexibility that is provided by the dynamic infrastructure in MANETs [1]. MANET also has amenabilities as, Lack of central system of management, resource availability, cooperativeness, scalability, dynamic topology, bandwidth constraint and limited power supply [5]. Routing protocols in MANET are pigeonholed into, Proactive, Reactive and the tertiary type is Hybrid routing protocols depending on how the routing information will be acquired and maintained by mobile nodes. [7]. Proactive protocols use a proactive routing method. Here every network node cultivates and retains the rational updates of routing information from and to all the nodes in the network. These routing protocols have a really low route acquisition delay as each node always will be having a fresh route to all the other nodes in the network and the memory, the bandwidth, and the demand for the power are high as each of the nodes in the network must maintain its routing table updates in order to exchange messages between the nodes. Typical table driven protocols are Destination-Sequenced Distance Vector Routing (DSDV) and Optimized Link State Routing (OLSR). [8][7]

Reactive protocols use a reactive routing method; where in at least one single route is established when needed. On-demand protocols are likely to place a lesser load on the network when compared to proactive protocols, as each node need not invariably maintain their table updates. But the routing appeals for routes and acknowledgement messages must be exchanged no matter when the communication is to be made over a newly born route. Most beetling MANET reactive routing approaches may be named as, Ad hoc On-demand Distance Vector (AODV) and Dynamic Source Routing (DSR). [7][8] A hybrid routing protocol is a combination of proactive and reactive protocol methods with the aim of complimenting both types of protocols in which proactive schemes are being used in order to find the routes to nearer nodes and reactive schemes will be used to discover nodes that are at longer distances. One of the archetypes of this stripe of protocol is Zone Routing Protocol (ZRP). [7][8]

Security of network that is being used in military needs, rescue operations, short-lived conferences, is now a dominant affair. MANETs that use a wireless medium has their traffic open to outsiders. Hence, there will always be a greater chance for malicious attackers to interrupt the traffic between the nodes in a network and destroy communication. There are two main types of possible attacks; they are Passive attacks and Active attacks. [9]
In Passive attacks, the attacker just wants to silently listen to the communication channel without modifying the information packets and without destroying the connection in the midst of the nodes. In Active attacks, hijacker will not just listen to communication between the mobile nodes but also modify and destroy the original data packets. These two vital attacks are again sub assorted into external attacks and internal attacks. [3] One of type of active attacks is a Black hole attack; which is a special type of

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

attack that most probably occurs in the Reactive protocols. A black-hole node is a malicious node that shows itself and claims that it has the shortest and fresh route to the destination, while it heckles the communication, it starts oozing out the packets it receives from its neighbouring nodes and blocks the communication between the source and destination. This attacker shows harmful behaviour such as; firstly, it may operate like a source by making bogus Route Request packet. Secondly, it may start performing like a destination node by making deceitful Route Reply packet or it may start depressing the hop count numbers while forwarding Route Request packet. This causes the packets communicated to be consumed or finally lost. [8][9]

II. LITERATURE REVIEW

This portion vitally describes the backgrounds that are acting as a backbone to our proposed work.

In this direction, this paper is likely to provide a comprehensive survey of attacks against a specific type of routing protocols used by MANETs [1]. Firstly, there is a presentation of vulnerabilities of MANETs and also a discussion on AODV protocol. Then there is survey on types of routing protocols with proactive and reactive types placed as top classified. Because of insecurity seen in these protocols a spot light is being focused on active attacks classification and attacker types. Furthermore, there is a discussion on difficulty of key management on this environment. Finally, there is a summarization of all these with survey on intrusion detection systems with many kinds of detection techniques.

Another major contribution is given in [2], where it talks about the advantages of Ad Hoc Network in spite of these advantages, MANETs become amenable to many active and passive security attacks that usually affects the, integrity, confidentiality and availability of data that is being transmitted. Black Hole Attack comes under one of these attacks. The Black hole can either cause a total failure of network by dropping all the traffic especially when the nodes are not in any movement. In case of some protocols where we usually use cluster heads, a traducer could be placed in between two clusters which may then cause isolation. This study presents a new protocol that acts like AODV and it is being seen in some study cases where this new protocol is being used this to see how the packets losses go on increasing during Black hole attack and a comparison is being made between protocol with nodes when in mobility and when they non-mobile. This paper also sheds some light on security issues in both MANETs and AODV protocol.

In the same way the analysis of the behaviour and challenges of security threats in mobile ad hoc networks with solution finding technique is being developed [4]. The Proposed method is being used to find the secured routes and then prevent the black hole nodes in the MANET by checking if by any chance there is large difference between the sequence number of source node or intermediate node who has sent back RREP or not. Generally, the initial route reply will be from the malicious or corrupt node with very high destination sequence number, which will be now stored as the first entry in the Route Request Table (RRT). Then later by comparing the first sequence number of the destination with the source node sequence number, if there exists really a lot of differences between them, then surely that node will be a malicious node. After that the corrupt node is detected, that node needs to be eliminated from the RRT entry immediately. This paper shows simulation results of providing fast message verification, identification of black hole, discovering the safe routing and avoiding the black hole attack.

An IDS model has been developed [5] based on some assumptions like, all the nodes in the network are identical in their physical characteristics; Suppose if one node is in the range of communication of another node, then the other node is also within the range of communication of the previous node, all the mobile devices are authenticated and are able to participate in communication. By default, source, destination and IDS nodes are considered as trusted nodes. Each IDS node will be set to promiscuous mode whenever needed only. Each IDS node is always a neighbour of any other IDS node. Because of multiple routes from source to destination, in order to mitigate the overhead incurred at the time of discovery of new route process, the source must cache the other routes. This proposed protocol describes that, whenever a node wants to transmit traffic to a host to which it has no route, it will generate a RREQ message that is flooded in a limited way to other nodes. This causes dynamic control traffic overhead and it results in an initial delay when initiating communication. A route is considered to be found when this RREQ message reaches either the destination or an intermediate node with a route entry for the destination that is valid. As long as a route exists in between two endpoints, AODV is going to remain passive. Whenever this route becomes invalid or lost, AODV once again will issue a request. A RREP message is unicasted back to the generator of a RREQ if the receiver will be either the node that is using the requested address, or it is having a route that is valid to the requested address. Nodes will be monitoring the status of links of next hops in active routes. Whenever a breakage in an active route link is detected, a RERR message is used to notify to other nodes regarding the loss of link. Each node keeps a “precursor list” to enable this mechanism of reporting to other nodes. This paper talks of selective black hole problem and performance analysis.

In order to analyse the attacks in MANETs and the security protocols for them a survey related to it is found in [7]. According to this author, in a MANET there is absence of routers that are dedicated and all nodes in the network must and should contribute in routing process. An overview on active attacks based on modification attacks, impersonation/spoofing attacks, fabrication attacks, wormhole attack and selfish behaviour is presented. One of the main contributions of this paper is the categorization of routing protocols in MANETs and providing extensions

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

to them. This paper also throws some light on the issue of importance of cryptography and trust in securing MANET routing. Another main contribution of this author work is the comparison of secure routing protocols that exist also while some future research challenges in securing the MANET routing are being discussed.

III. PROPOSED METHOD

This section likely provides some of the major and vital contributions and surveys on routing protocols, attacks in MANETs and securing of this environment. Next section is a framework of description on proposed method and some details on how this method can be utilized to detect and prevent the black hole attack.

The proposed method gives an advantage of clustered architectural organization over random architecture of mobile nodes in MANETs.

In a random organization, specific number of nodes is first deployed where all the mobile nodes are considered to belong to a single large cluster without specifically allotting a boundary for this structure. Therefore, every node in the network can communicate with every other node as there is no specific central authority to control communication in this network. In this organization, the mobile devices are mobile nodes where they will be chosen as source or destination considering the wishes of the nodes to transmit and to receive as shown in figure 1.

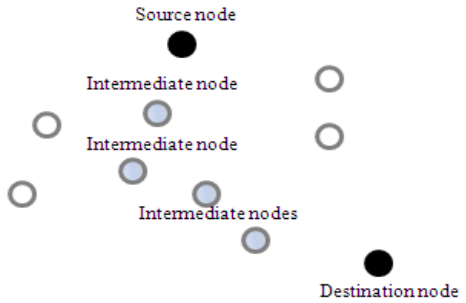

Fig 1: Random organization of mobile nodes

Source and Destination nodes: Whenever a mobile node wants to transmit data packets, that node will be chosen as a source node and the node to which it needs the transmitted data to reach will be chosen as the destination node.

Intermediate nodes: Depending on the next nearest mobile node that is available to route the packets is chosen as the first intermediate router. Similarly, a series of intermediate mobile nodes are chosen in order to route the packets to destination mobile node.

An attacker if it enters as an external attacker in between source and destination posing to be having a shortest path entering this random organization based on boundary conditions as in this structure no specific boundaries are provided and there are no central management points allotted to stop them from entering this organization. This malicious node or a Black Hole behaving to have the shortest path may consume all the packets or ooze out all the packets to completely breakdown the communication. In order to overcome this disadvantage in a random organization, the mobile nodes are arranged into clustered organization, where mobile devices are sorted as shown in figure 2.

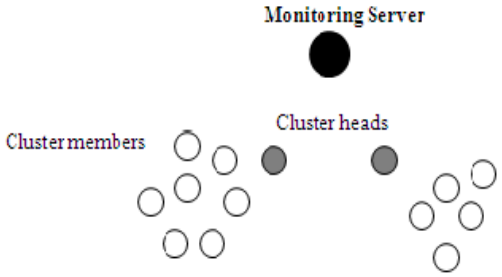

Fig 2: Proposed network organization

Cluster members or Mobile nodes: These nodes are a congregation of several mobile devices that likely follow independent mobility law. They frequently take part in communication and are able to transmit, receive and route data during the course of communication.

Cluster heads: These nodes are recognized to be static access points that will be installed independently. These become the main participants in intra-cluster communications. The superior priority and responsibility of these nodes is to handle the data packets transmission and reception between trusted nodes or between new mobile nodes trying to communicate with the trusted nodes in the internal cluster.

Monitoring server: This node is allotted based on its residual energy being highest of all other nodes and then making it responsible of controlling the group of clusters and communication among them as a whole. It is likely to be used as a medium to secure the network from attacks by using the attacker characteristics.

In order to simulate the complete communication, detection and elimination process of malicious node, we put forth three step scenarios:

1. **Internal cluster communication:** This scenario facilitates mobile nodes to communicate with each other within their respective clusters.
2. **External cluster communication:** During this scenario all the originated traffic will go from one cluster to another through the cluster heads and server node.
3. **Communication between stranger nodes:** During this process the second scenario is being carried out with traffic and data monitored. If this stranger node acts as a sink to the packets and never forwards the packets to its neighbor nodes then, this node is to be eliminated from the network and then marked as malicious node.

This portion of the paper presents the clustered organization that is secured and the following portion of the paper gives a clear picture of implementation of the proposed method and its simulation results.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

IV. SIMULATIONS AND RESULTS

This section of the paper provides clear description on environment of simulation and presents clarified simulation results that are being simulated in NS2 simulator. The simulation parameters utilized are summarized in the Table 1 shown below.

Table 1: Simulation parameters

Parameters	Values
Simulation area	1000*1000
Channel	Wireless
MAC layer	802.11
Link layer	LL
Number of nodes	43
Node type	Wi-Fi
Mobility	Random2way
Traffic type	CBR
Simulation time	1200s

Utilizing these simulation parameters the proposed method is designed and then put to simulation.

To show the attack of black hole and its effect, a traditional MANET is considered with its nodes communicating using a simple AODV routing protocol. This simulation describes the way the communication is being initiated between source and destination nodes and the way in which a malicious node tries to cut down connection between them either by consuming all the packets or by dropping out all the packets. These simulation results can be seen in fig3 shown below.

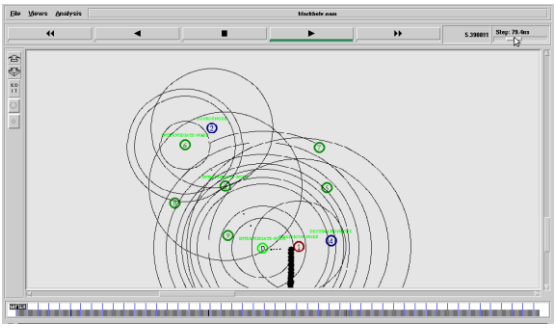

Fig 3: The Black Hole attack

Now in order to detect and prevent the Black Hole attack a method is been proposed where nodes are organized into a clustered structure. As it is presented in fig 4, there are four clusters having their respective cluster heads in place and a monitoring server to monitor their communication.

In additional to these, there is a green node that is of an unknown identity without any trust value. All other remaining nodes are assumed to be trusted nodes that are allowed to communicate comfortably. Right after implementing its simulation in NS2 simulator the performance of this network organization is evaluated and compared with performance of the network during the course of black hole attack.

Fig 4: The proposed method

During attack the attacker blocks all the data packets that are being sent between sender and receiver, this makes the throughput to fall to zero. The below given results show the comparison of performance between a traditional and clustered organization during black hole attack and after elimination of attacker respectively.

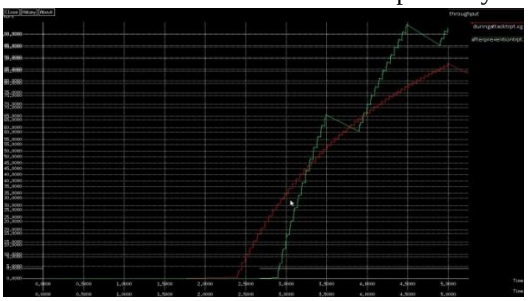

Fig 5: Comparison of throughput during attack and after elimination of attack

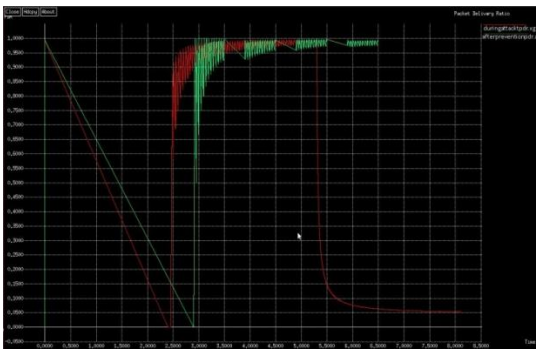

Fig 6: Comparison of Packet delivery ratios

This portion puts a spotlight on the simulation and results; next section of the paper concludes this paper and predicts some the future extension of this work.

V. CONCLUSION AND FUTURE WORK

The presented paper is an overview on how the organization of the network structure resolves the method of eliminating the attacker. In the direction of extracting an optimum and close to appropriate approach to detect and prevent black hole attack, some of the previous works are being surveyed and additionally the proposed approach for prevention of black hole attack is provided. At last, this proposed solution is being simulated in NS2 simulator and results are evaluated. This method proves to be a

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

performance enhancer as per the comparison of performances during and after prevention of attack. In future this method can be utilized to eliminate attacks other than black hole. This work can further be enhanced towards eliminating the internal black hole attacks too. For this purpose steps are needed to be taken to provide some enhancement to monitoring server node to enhance its rules to for communication in the network. This technique is promising and is capable of implementing itself against various other security problems in MANETs.

ACKNOWLEDGMENT

My deepest gratitude is to my parents and my guide, Mr.Arun Kumar. I feel very much fortunate to have a guide who gave me complete freedom to explore on my own and at the same time guided me to improve my work. I also cherish all those people who have made this work possible.

REFERENCES

[1] Sevil Şen, John A. Clark, Juan E. "Security Threats in Mobile Ad Hoc Networks", *YO10 5DD, UK, 2010*
[2] Fihri Mohammed, Otamani Mohamed, Ezzati Abdellah "The Impact of Black-Hole Attack on AODV Protocol", *LAVETE Laboratory, Morocco, IJACSA, 2014*
[3] Jitendra Sayner, Vinit Gupta, "Clustering of Mobile Ad Hoc Networks: An Approach for Black Hole Prevention", *978-1-4799-2900-9/14/$31.00 ©2014 IEEE.*
[4] Pooja Jaiswal, Dr. Rakesh Kumar, "Prevention of Black Hole Attack in MANET", *IRACST, (IJCNWC), ISSN: 2250-3501,Vol.2, No5, October 2012.*
[5] T.Manikandan, S.Shitharth, C.Senthilkumar, C.Sebastinalbina, N.Kamaraj, "Removal of Selective Black Hole Attack in MANET by AODV Protocol", *IJIRSET, Volume 3, Special Issue 3, March 2014*
[6] Rashmi, Ameeta Seehra, "Detection and Prevention of Black-Hole Attack in MANETS", *(IJCST) – Volume 2 Issue 4, Jul-Aug 2014*
[7] Jonny Karlsson, Laurence S. Dooley, Göran Pulkkis, "Routing Security in Mobile Ad-hoc Networks", *Issues in Informing Science and Information Technology, Volume 9, 2012*
[8] Sudhir Agarwal, Sanjeev Jain, Sanjeev Sharma, "A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks", *ISSN 2151-9617, January 2011*
[9] Sumit Agarwal, Shilpa Jaiswal," Study to Eliminate Threat of Black Hole of Network Worms in MANET", *International Journal of Scientific and Research Publications, vol.2(9), September 2012, ISSN 2250-3153*

BIOGRAPHIES

Shilpa Gopinath has received her B.E. Degree in Electronics and Communication Engineering from UBDTCE, Davangere, Karnataka, India, in 2013 and is presently obtaining M. Tech. degree in Digital Communication and Networking from Visveswaraya Technological University, Karnataka, India. Her fields of interests are networks and its security based issues.

Arun Kumar G has received his B.E Degree in ECE from STJIT, Ranebennur in 2004, M.Tech degree in ECE from UBDTCE, Davangere in 2008 and Pursuing his Ph.D. in ECE from the VTU, Belagavi. He is currently working as Associate Professor in the ECE department of STJIT Ranebennur, Karnataka, India.