An Opportunistic Routing to Encounter Black Hole Attack in Mobile Ad Hoc Network

Mohan Babu G
Department of Computer Science and Engineering,
Jain Global Campus, Jain University, Jakkasandra Post,
Kanakapura Taluk, Ramanagara District, India
mbabu270@gmail.com

S. Balaji
Center for Emerging Technologies,
Jain Global Campus, Jain University, Jakkasandra Post,
Kanakapura Taluk, Ramanagara District, India
drsbalaji@gmail.com

***Abstract*—A Mobile Ad hoc Network (MANET) is a spontaneous network that can be established with no fixed infrastructure, where nodes behave as routers and take part in its discovery and maintenance of routes to other nodes in the network. The network topology changes dynamically due to the addition and exit of nodes frequently in the network at any time. From security perspective, MANETs are vulnerable to various types of malicious attacks. Black hole attack is one type of malicious attack that can be easily employed against data routing. Therefore, providing the secure transmission over the mobile network is a challenging issue. In the proposed approach, packets are routed based on purely random propagation algorithm, simple path diversity algorithm and multicasting technique. For the security issues data is divided into shares.**

Keywords*—MANET, Black Hole Attack, Ad Hoc on Demand Distance Vector, Data Splitting, Propogation Of Shares.

1. INTRODUCTION

A mobile ad-hoc network consists of a collection of mobile nodes in which nodes are communicating with each other without help from a fixed infrastructure [2]. These networks are self-configuring network of mobile devices connected by wireless links. Mobile hosts are used to form mobile ad hoc network [1].

Routing protocols in ad hoc wireless networks can be classified into three broad categories. They are proactive (or table-driven) protocols, reactive (or on-demand) protocols, and hybrid routing protocols [3]. There are various routing attacks in ad hoc wireless networks like Attacks using Impersonation, Modification, Fabrication, Replay, and Denial of Service. Three main routing protocols are proposed for MANETs [4]: Ad hoc On Demand Distance Vector (AODV) routing, Dynamic Source Routing (DSR), and Destination Sequence Distance Vector (DSDV) routing protocols. AODV and DSR belong to on-demand routing protocols and DSDV is a table-driven routing protocol [9]. These protocols are vulnerable to different security attacks. AODV is one of such reactive routing protocols with weaker design, which is prone to numerous security threats including Denial-of-Service attacks such as Black hole and Gray hole attacks [7].

As the network is vulnerable to various kinds of attacks, providing end-to-end security to the data is a major challenge. There are various types of security mechanisms for secure transmission of data over the network. One such mechanism is splitting of data into shares. The data is split in to a total of N shares in a way that only M of the N shares (M < N) is needed to form the original data. This way even if some shares are lost during transmission, (if the base station receives minimal shares) it can form the original data [12].

A black hole attack is a type of attack in which node utilizes the routing protocol to claim itself of being the shortest path to the destination node, but drops the routing packets and does not forward packets to its neighbors [11]. Figure 1 is an example of black hole attack in the mobile ad hoc networks.

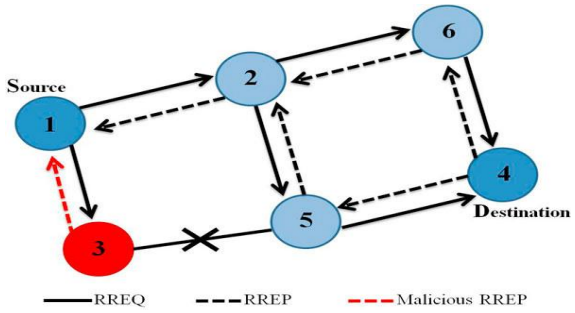

Figure 1: Black Hole Attack

Here the node 1 stands for the source node and node 4 represents the destination node. Node 3 is a misbehavior node who replies the RREQ packet sent from source node, this node advertises itself as having shortest path to reach the destination. Therefore, node 1 erroneously judges the route

discovery process with completion, and starts to send data to node 3. Then the node 3 probably drops or consumes the packets. This suspicious node can be regarded as a black hole problem in MANETs. As a result, node 3 is able to misroute the packets easily, and the network operation suffers from this problem.

Multicast is the communication paradigm of one-to-many or many-to-one, based on defined groups and constituted by members, whose interest is to receive/share the same information for a specific application. A multicast group can also have one or more senders. All the management tasks are performed at the routing level, hence to route the packets from the source to each multicast group member it is necessary to implement specific multicast routing protocols [10].

This paper proposes a routing mechanism that is designed to prevent a black hole attack on Ad-hoc On-demand Distance Vector-based Mobile Ad-hoc Networks. The proposed approach will provide security to the data that is sent from source to destination using multiple paths and it will protect the data from the Black Hole Attack.

2. RELATED WORK

Ketan S. Chavda, Ashish V.Nimavat [1], propose a novel approach that makes a modification in the existing AODV routing protocol. This approach finds the safe route between sending and receiving nodes. The main advantages are more efficient, highest packet delivery ratio, and the throughput. Drawback is that there is no security for the data because the main focus is to find the path from source to the destination for the successful delivery of data from source to destination using destination sequence number.

Seryvuth Tan and Keecheon Kim [2] propose a mechanism that provides Secure Route Discovery for the AODV protocol (SRD-AODV) to prevent black hole attacks. This mechanism requires the source node and the destination node to verify the sequence numbers in the Route Request (RREQ) and Route Reply (RREP) messages, respectively, based on the defined thresholds before establishing a connection with a destination node for sending the data. The major disadvantage is that it mainly concentrates on discovering secure route but there is no strong attempt to detect the attack and to secure the data.

Jyoti Rani and Naresh Kumar [3] propose an approach to mitigate the black hole attack using AOMDV routing protocol. Some improvements have been made in AOMDV protocol. These improvements make the protocol robust against black hole attack along multipath route discovery process. The major disadvantage is that it is time consuming and degrades the performance.

P.R. Jasmine Jeni et. al. [4] explores a secure transfer of information via large scale wireless network and the challenges involved. This work analyzes two routing protocols used in large scale network; the DOA and AODV routing protocols and injected them using black hole attack and evaluated its quality parameters like packet delivery ratio and average end to end delay. The problem with this approach is in finding the paths to send information through intermediate nodes is difficult.

P.Karthik Kannan and K.P.Lavanya Priya [5] propose a scheme to avoid the black hole attacks using sequence number identification method to reduce the data transfer delays. Also, they evaluate the performance by comparing with USOR protocol to achieve the high level privacy protection in MANETs. The disadvantage of this approach is the repetition of node sequence number that is affected by the attack and there may be a chance of low performance.

3. PROPOSED APPROACH

A routing approach is proposed to prevent black hole attack in mobile ad hoc networks. There are many solutions proposed by various authors to deal with black hole attacks in MANETs that are based on the AODV protocol and other protocols. However, the proposed approach provides high performance, detects black hole and successfully delivers the data from source to destination. The proposed approach includes two main modules that is

1. Splitting of Data into Shares
2. Random Propagation of Information Shares

The modules are described below:

3.1 Splitting of Data into Shares

The proposed approach will be able to detect black hole attack and prevent the data loss from an attack. Here, the original data is at source node which is divided into a number of packets called shares. Each share has certain amount of information. The original information divided into shares are called as secret shares because the data are encrypted using an encryption algorithm. Each share is so highly protected that it is very difficult to decode the data using one single share. In order to obtain a complete data there should be a minimum amount of shares that needs to be at the destination to obtain the original information. They should be deciphered in such a way that the information is not lost during any period of the data transfer.

3.2 Random Propagation of Information Shares

Once the splitting of data into shares is done, the shares are propagated from source to destination. However, it is highly desirable to have energy

efficient propagation which actually calls for limiting the number of randomly propagated hops.

4. ALGORITHMS USED

The algorithms used are as follows:

Algorithm 1: Shamir's Secret Sharing

The data to be sent from the source node is split into shares according to Shamir's algorithm. The data is split in N total shares such that only M of the N shares (M < N) is needed to form the original data. This way even if some shares are lost while transmission, if the base station receives minimal number of shares it can form the original data.

The algorithm is as shown:

Step 1: start
Step 2: Let total data payload be 'T'
Step 3: Let number of shares be 'M'
Step 4: for each share 'I' in 'T'
Step 5**:** If I<=M calculates packet size
Else
Go to step 9
End if
Step 6: Packet size = $\frac{\text{Data payload}}{M}$
Step 7: If start size = end size
Step 8: I = I+1
End if
Step 9: Divide the data payload based on size calculated.
Step 10: All the packets formed
Step 11: STOP

Algorithm 2: Purely Random Propagation (PRP)

In PRP, the shares are propagated using one hop neighborhood information. A mobile node maintains a neighbor list, which contains the IDs of all the nodes [12].

The algorithm is as shown below:

Step 1: Start
Step 2: Let 'S' be the source node
Step 3: Fetch the information from routing tables
Step 4: For each node 'I' in 'N'
Step 5: If I=contain destination
End if
Step 6: pick 'I' randomly
Step 7: TTL = TTL-1
Step 8: If TTL! =0 go to source node
Step 9: Else if go to alternate path from source to destination
End if
Step 10: Stop

Algorithm 3: Non Repetitive Random Propagation (NRRP)

This algorithm is used to control the repetition of nodes while choosing alternate path.

The algorithm is as shown below:

Step 1: Start
Step 2: For each node I, in routing table R
Step 3: Extract the NIR field from the packet
Step 4: Compare NIR field list with neighbor list obtained from R
Step 5: Randomly pick neighbor from compared list
Step 6: TTL =TTL-1
Step 7: Send data to neighbor then neighbor=source
Step 8: If TTL =0 do,
Apply minimum hop routing then
Node in destination
End if
Step 9: If TTL! =0
Step 10: Node is not in destination
Step 11: Stop

Algorithm 4: Simple Path Diversity (SPD)

The SPDA uses source routing to find an alternate path from a source to a destination, and allows flexible division of traffic over the best and alternate path [14].

This algorithm works in three steps as shown below

Step 1: The BGP (a routing protocol used to keep the systems up-to date with the information needed to receive and transmit the traffic correctly[13]) protocol is extended to allow the BGP routing table to save the multiple paths for any Destination.
Step 2: Here a given source node is able to detect whether the point of congestion along the best path occurs or not.
Step 3: If congestion occurs, the source will specify an alternate path and direct traffic over the best and alternate path.

Algorithm 5: Direct Random Propagation (DRP)

Direct random propagation improves the propagation efficiency by using two-hop neighborhood information [14].

The algorithm is as shown below:

Step 1: Start
Step 2: Identify the number of nodes (50), shares (4), source node, TTL, destination node
Step 3: based on the above information it will create routing tables.
Step 4: Feed the information of the neighbors then identify the neighbor node and measure the distance from source.

Step 5: Divide the data into 4 equal shares.
Step 6: Fetch the data from routing table and send share1 to some neighbor within distance then, call DRP for share 1
Step 7: Fetch the data from routing table and send share2 to some neighbor within distance then, call DRP for share 2
Step 8: Fetch the data from routing table and send share3 to some neighbor within distance then, call DRP for share 3
Step 9: Fetch the data from routing table and send share4 to some neighbor within distance then, call DRP for share 4
Step 10: Stop

5. SIMULATION AND EVALUATION

In this project, we plan to simulate by developing a Java application and demonstrate the random propagation of shares using graphs and also we plan to evaluate the performance based on packet delivery ratio, throughput, and network load.

6. CONCLUSION

The nodes in Mobile Ad hoc networks are free to move due to mobility and they are vulnerable to many attacks. Therefore, providing security is a major challenge in MANETs. The proposed approach will be able to detect the black hole attack which is one of the major attacks that consumes the data or block the data to the other nodes. Thus, the proposed approach will provide the security to the data that is sent from source to destination with good performance. High packet delivery ratio can be achieved.

REFERENCES

[1] Ketan S. Chavda, Ashish V.Nimavat, in IEEE "Removal of Black Hole Attack in Aodv Routing Protocol of MANET" 4th ICCCNT – 2013 July 4 -6, 2013, Tiruchengode, India
[2] Seryvuth Tan Keecheon Kim "Secure Route Discovery for Preventing Black Hole Attacks on AODV-based MANETs" 2013 IEEE, ICTC 2013
[3] Jyoti Rani1, Naresh Kumar "Improving AOMDV Protocol for Black Hole Detection in Mobile Ad hoc Network " 2013 IEEE
[4] P.R. Jasmine Jeni, A. Vimala Juliet, R.Parthasarath/ A.Messiah Bose . In "Performance Analysis of DOA and AODV Routing Protocols with Black Hole Attack in MANET" 2013 International Conference on mart Structures & Systems (JCSSS-20 13), March 28 - 29, 2013, Chennai, India
[5] P.Karthikkannan, K. P. Lavanya Priya, "Reduction of Delays in Reactive Routing Protocol for Unobservable Mobile Ad-Hoc Networks"
[6] Hizbullah Khattak, Nizamuddin, Fahad Khurshid and Noorul Amin " Preventing Black and Gray Hole Attacks in AODV using Optimal Path Routing and Hash " IEEE 2013
[7] Rutvij H. Jhaveri " MR-AODV: A Solution to Mitigate Black hole and Gray hole Attacks in AODV Based MANETs "Second International Conference on Advanced Computing & Communication Technologies published by CPS. © 2012 IEEE
[8] Hizbullah dKhattak, Nizamuddin" A Hybrid Approach for Preventing Black and Gray Hole Attacks in MANET" © IEEE 2013
[9] Dr.S.Dhenakaran, A.Parvathavarthi "An Overview of Routing Protocols in Mobile Ad-Hoc Network" International Journal of Advanced Research in Computer Science and Software Engineering, February – 2013
[10] Simek, M. Boavida, F. "Why Should multicast be used in WSNs" IEEE 2008
[11] Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao" A survey of black Hole attacks in mobile ad hoc networks" human centric computing and information science 2011
[12] P.B. Manoj, Sai Sandeep Baba, Random Routing Algorithms for Wireless Sensor and Networks", International Journal of Advanced Research in Computer communication Engineering
[13] Rick Kuhn, Kotikalapudi Sriram, Doug Montgomery "Border Gateway Protocol security National institute of standard and technology, special publication, 2007
[14] Yuh-Pyng Shieh,Sheng-Cheng Yeh, Pei-Siou Hung," A Simple Path Diversity algorithm for inter domain Routing", Dept. of CSE, ming chuan university Taoyuan, taiwan, IEEE 2011