International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

An Opportunistic Routing to Secure Data Transmission against Black Hole Attack in MANETs

[1]Mohan Babu G, [2]S Balaji

[1]Department of Computer Science and Engineering,
Jain Global Campus, Jain University, Jakkasandra Post, Kanakapura Taluk, Ramanagara District, India

[2]Center for Emerging Technologies,
Jain Global Campus, Jain University, Jakkasandra Post, Kanakapura Taluk, Ramanagara District, India

Abstract: ***A Mobile Ad hoc Network (MANET) is a set of mobile nodes in which every node in the network communicate with each other without any predefined infrastructure and due to mobility the nodes are free to move. Providing security to the moving nodes is a challenge and hence the MANETs are vulnerable to many attacks. One such attack is a black hole attack which blocks the successful delivery of the data to the destination. In this paper, a new routing approach is designed to detect the black hole attack and to achieve secure data transmission by splitting the data into shares. Next propagating the shares in multiple paths, in which the shortest path is selected to reach the destination based on the hop count.***

Keywords: MANETs, Black Hole Attack, Routing, Security, Data Splitting

1. Introduction

Mobile Ad hoc Networks (MANETs) are infrastructure less, nodes communicate with each other and are free to move in the network [1]. All the nodes in the network act as a routers in sending and receiving the. Because of mobility, network topology changes frequently and maintaining the connectivity in network for routing is very important [2]. Because of changing topology, security is a major challenge. MANETs suffer from various kinds of security attacks because of the features like continuously changing topology, open medium, lack of central management [1][3]. Consequently, the mobile ad hoc networks are vulnerable to many attacks.

There are four types of broadcasting approaches in MANET's [5]: (i) Unicasting – one to one communication between two nodes, (ii) Multicasting - sending the data from one source to a selected number of destination nodes in the network, (iii) Broadcasting - sending data from source to all other nodes in a network and (iv) Geocasting- sending data from source to all the nodes inside the specific geographical region. There are several types of attacks in MANETs like passive attacks, active attacks, network layer attacks, resource consumption attacks, routing attacks, transport layer attacks, application layer attacks and multilayer attacks [4]. There are various sub-attacks in all the above mentioned attacks. This paper is dealt with black hole attack that occurs in the network layer.

Because the network is vulnerable to various kinds of attacks, providing end-to-end security to the data is a challenging issue [12]. Various types of security mechanisms have been proposed 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 number of shares in which only M out of N shares (M < N) are needed to obtain the original data. In this way even if some shares are lost during transmission, (if the destination receives minimal shares) original data can be obtained.

In black hole attack nodes utilizes the routing protocol to claim itself of being the shortest path to the destination node but these nodes will drop the routing packets and does not forward packets to their neighbours [5][8]. For sending data to the destination, source node sends a Route Request (RREQ) to all the other nodes by creating paths based on the Route Response (RREP). Figure 1 shows the black hole attack in the mobile ad hoc networks where, node S represents the source node and node D represents the destination node. Node A is a misbehaviour node which replies the RREQ packet sent from source node (black hole attack); node A advertises itself as having shortest path to reach the destination. Therefore, node S judges the path along the node A as the shortest and starts sending data to node A. Then, the node A possibly drops the packets received from source S. As a result, node A is able to misroute the packets easily and the network operation suffers from this problem.

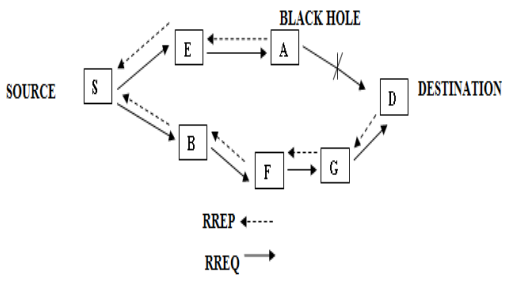

Figure 1: Black Hole Attack on AODV

There are two types routing protocols [6][7], used to overcome various attacks in MANETs. They are:

1.1. Reactive Protocols - These protocols are consistent, maintain up-to-date information about each node in the network and share the correct information with other nodes in the network. These protocols require each node to maintain one or more routing tables to store the routing information and they update the changes if there is a change in the topology. Some of the protocols are Destination-Sequenced Distance-Vector (DSDV), Optimized Link State Routing (OLSR) Protocol, Wireless Routing Protocol (WRP), etc [6].

1.2. On Demand-Driven Reactive Protocols - These protocols are on demand and create routes only when a node requires a route to the destination. Once the route is discovered, it is maintained by route maintenance procedure until the destination becomes inaccessible from every path. The table driven protocols are Ad hoc On-Demand Distance Vector (AODV), Dynamic Source Routing (DSR), Temporary-Ordered Routing Algorithm (TORA), etc.

In this paper, we use the dynamic source routing protocol [10]. This protocol will continuously update the node IDs in the routing table which is essential to control the node repetition during the data transmission.

2. Related Work

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 networks; the DOA and AODV routing protocols. Black hole attacks were injected and evaluated 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.

Jyoti Rani and Naresh Kumar [9] propose an approach to mitigate the black hole attack using AOMDV routing protocol. Improvements have been made in AOMDV protocol that makes 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. Isaac Woungang, Sanjay Kumar Dhurandher et.al [10], proposes a novel scheme for detecting black hole attack using dynamic source routing protocol. The potential black hole attack is detected and avoided before the routing mechanism by sending fake route requests. The main advantage is high performance and high packet delivery ratio.

P. Karthik Kannan and K. P. Lavanya Priya [11] 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 Unobservable Secure On-demand Routing (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.

Hizbullah Khattak, Nizamuddin [12] propose a hybrid approach for preventing black/gray hole attacks by selecting second shortest route for secure routes election and hash function and timestamp base solution for consistent data transmission. The main disadvantage is that the throughput delay is high.

3. Proposed Approach

A routing approach is proposed to detect black hole attack in mobile ad hoc networks. There are several solutions proposed by various authors to deal with black hole attacks in MANETs that are based on the AODV protocol; they also introduced time stamp and hash function methods [12].

Security is a major issue in MANETs. The proposed approach provides high performance which detects black hole and successfully delivers the data from source to destination. It includes two main modules:

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

3.1. Splitting of Data into Shares

The proposed approach will be able to detect black hole attack and also provides secure transmission of data. Here, the original data at source node is divided into a number of packets called shares. Each share has certain amount of information. The original information is 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 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 received 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 Shares

Once the splitting of data into shares is done, the shares are propagated from source to destination. Each node has a unique ID based on which propagation of shares takes place. The challenge here lies in the random and distributed nature of the propagation; a share may be sent one-hop farther from its source in a given step, but may be sent back closer to the source in the next step and wasting both steps from the security point of view. Some control needs to be imposed on the random propagation process to ensure that in each step the share is more likely to be forwarded outwards from the source to overcome the above challenge.

4. Algorithms Used

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 to 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.

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 = 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 neighbourhood information. A mobile node maintains a neighbour list, which contains the IDs of all the nodes. The main challenge of PRP is that its propagation efficiency can be low, because a share may be propagated back and forth multiple times between neighbouring hops. One of the solutions is to increase the value of Time-To-Leave (TTL).

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 that is, each time the data moves from one node to another node the id of the node will be stored in the routing table.
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)

This algorithm incorporates source routing, finds an alternate path from source to destination and distributes the traffic over the best alternate path.

Step 1: The BGP (a routing protocol that keeps the updated network information needed to receive and transmit the traffic correctly) protocol is extended by saving the multiple path information in the routing table to any Destination.
Step 2: The source node will detect the point of congestion in the path.
Step 3: If congestion, the source will select an alternate path
Step 4: Directs the traffic over the best alternate path.

Algorithm 5: Direct Random Propagation (DRP)

Direct random propagation improves the propagation efficiency by using two-hop neighbourhood information. The main advantage of the DRP algorithm is that it reduces the chance of propagating a share back and forth by eliminating this type of propagation within any two immediate consecutive steps. Compared with PRP, DRP attempts to push a share outward away from the source, and thus, leads to better propagation efficiency for a given TTL value.

Step 1: START
Step 2: Identify the number of nodes (50), shares (5), 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 5 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: Fetch the data from routing table and send share5 to some neighbor within distance. Then, call DRP for share 5
Step 11: STOP

5. Analysis

As the MANETs are resource constrained and infrastructure less, the nodes are free to move in the network. Because of mobility security is a major issue. Achieving efficient and secure transmission over the network is essential. In this project, data is divided into shares and propagated in randomly selected paths, if there is an attack in the path; the source will choose alternate paths out of which the source will select the shortest path to reach the destination. Entire data can be obtained if minimal shares are arrived at the destination.

In order to provide secure transmission, data is split into shares before transmitting from source to destination. If any loss in the shares during transmission, original data can be

retrieved using minimum number of shares received at the destination. In case of traffic or congestion in the existing path, the source node will select an alternate path for data transmission by evenly distributing the data over the network and utilizes the resources efficiently.

6. Conclusion and Future Work

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 and protect the data from the black hole attack, which is one of the major attacks that consumes the data or block the data. Thus, high performance, average end-to-end delay and high packet delivery ratio can be achieved. From the security perspective of the MANETs, the existing mechanisms are not enough to ensure security of the data completely. Hence, there is a need to develop a multi-fence security solution that is embedded into possibly every component in the network. The future work is, in Non-Repetitive Random Propagation (NRRP), the propagation of nodes from source to destination increases the Node-In-Route (NIR) field which results in high communication overhead and to overcome this problem, instead of adding NIR field for each share, we plan to develop a new routing protocol that will update the node ID in routing table as soon as the data is traversed. In the proposed work, the power consumption is high due to large number of random path selection. In order to avoid this problem the number of random paths must be minimized based on the number of nodes and the hop count. Development of suitable algorithms to accomplish this is part of our future work.

References

[1] Dr Sanjeev Yadav, Rachna Jain, Mohd Faisal "Attacks in MANET," International Journal of Latest Trends in Engineering and Technology (IJLTET), Vol. 1 Issue 3 September 2012
[2] Ankita Gupta, Sanjay Prakash Ranga "VARIOUS ROUTING ATTACKS IN MOBILE AD-HOC NETWORKS," International Journal of Computing and Corporate Research, VOLUME 2 ISSUE 4 July 2012
[3] Himadri Nath Saha, Debika Bhattacharyya "A REVIEW ON ATTACKS AND SECURE ROUTING PROTOCOLS IN MANET," International Journal of Innovative Research and Review, 2013.
[4] P.R. Jasmine Jeni, A. A.Messiah Bose. In "Performance Analysis of DOA and AODV Routing Protocols with Black Hole Attack in MANET" 2013 International Conference on Smart Structures & Systems (JCSSS-20 13), March 28 - 29, 2013, Chennai, India
[5] Priyanka Goyal, Vinti Parmar, Rahul Rishi, "MANET: Vulnerabilities, Challenges, Attacks, Applications," IJCEM International Journal of Computational Engineering & Management, January 2011.
[6] Rashid Hafeez Khokhar, Md Asri Ngadi, Satria Mandala, "A Review of Current Routing Attacks in Mobile Ad Hoc Networks," International Journal of Computer Science and Security, December-2012.
[7] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, "A Survey on Attacks and Counter measures in Mobile Ad Hoc Networks," WIRELESS/MOBILE NETWORK SECURITY, February-2010.
[8] P. R. Jasmine Jeni, A. Vimala Juliet, R. Parthasarath, "Performance Analysis of DOA and AODV Routing Protocols with Black Hole Attack in MANET," 2013 International Conference on Smart Structures & Systems (JCSSS-20 13), March, 2013.
[9] Jyoti Rani, Naresh Kumar "Improving AOMDV Protocol for Black Hole Detection in Mobile Ad hoc Network," International Conference on Control, Computing, Communication and Materials (ICCCCM), 2013 IEEE.
[10] Isaac Woungang, Sanjay Kumar Dhurandher et.al, "Detecting Black hole Attacks on DSR-based Mobile Ad Hoc Networks," 2012 IEEE.
[11] P.Karthikkannan, K.P.LavanyaPriya "Reduction of Delays in Reactive Routing Protocol for Unobservable Mobile Ad-Hoc Networks," International Journal of Computer and Network security, January 2012.
[12] HizbullahKhattak, Nizamuddin "A Hybrid Approach for Preventing Black and Gray Hole Attacks in MANET," 2013 IEEE.

Author Profile

Mohan Babu G received Bachelor's degree in Information Science and Engineering from Visvesvaraya Technological University. He is currently pursuing MTECH in Computer Science and Engineering in School of Engineering and Technology, Jain Global Campus, Jain University and he is in final semester of his course. His interests lie in the field of mobile computing, mobile ad hoc networks, and wireless sensor networks and continue his research in these areas.

Balaji S. received a Bachelor's degree in Mathematics from Madras University, a Master's degree in Applied Mathematics from Anna University, Chennai and a Ph.D. degree in Computer Science and Engineering from Indian Institute of Science, Bangalore. He has served Indian Space Research Organization for more than two decades before getting into academics. He is currently a Professor at Centre for Emerging Technologies, Jain Global Campus, Jain University. His research interests include fault-tolerant computing, real-time systems, mobile computing, image processing and computer vision, data science and analytics, energy efficient computing, energy scavenging, wireless sensor networks, ground penetrating RADAR applications, biomolecular modelling and simulation, systems biology, and MEMS based systems development for mission and safety critical applications.