IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 3, Ver. IV (May-Jun. 2014), PP 109-113
www.iosrjournals.org

Resource Aware Node Authentication Framework for Secure MANET

[1]Komal Naik (Joshi), [2]Arati Dixit
[1,2](Computer Department, P.V.P.I.T. College, University of Pune , Maharashtra, India)

Abstract: *MANET comprises mobile nodes, which are links to each other by wireless connections without any base infrastructure. MANETs are vulnerable to security attack due to their features such as autonomous nature, infrastructure-less network and multi-hop communication. Therefore every node in MANET must be secure; node security can be provided by using node authentication techniques. Every node in MANET consists of resources such as battery power, bandwidth, and a memory to keep routing information. These resources provided by the MANET node are limited resources. A MANET faces various security attacks; one of them is flooding attack whose aim is to drain off limited resources of MANET node by continuously sending Route Request control Packet, false route information or fake data packets. The main goal of our approach is to provide resource aware node authentication framework to prevent flooding attack in MANET.*

Keywords: *AODV, Flooding Attack, MANET, Node authentication.*

I. Introduction

MANET comprises mobile nodes, which links to each other by wireless connections without any base infrastructure. MANET is an ad hoc network; therefore a node in MANET can join or leave the network at any time. In a MANET, every node has to co-operate with each other to forward packets hop-by-hop (see Fig 1). Therefore, every node acts as host as well as router. MANETs are highly vulnerable to security attacks because of their features such as autonomous nature, infrastructure-less network, multi-hop communication. Since all nodes in MANET receive data transmitted by a node, a malicious node could easily obtain the data being transmitted in the network. Furthermore, because of multi-hop communication MANET faces security problems during route discovery and packet forwarding such as flooding attack, black-hole attack, gray-hole attack, etc. There is no pre-existing network for central control of the network operations, so the control of the network is spread among the nodes in the network. Therefore, every node in MANET must be secure. To provide node security, authentication must be performed for every node in the network.

Node authentication can be performed by using the cryptography – based authentication [1] or the offline trust relationship based authentication [2]. The cryptography based authentication uses public/private key pair and a certificate for the public key of each node. As MANET does not have pre-existing infrastructure, no central authority can provide certificate for each node. Consequently, every node has to keep a credential repository for storing certificates of other nodes. Also, whenever request arises, every node has to exchange certificates to the certificate requester node. In offline trust relationship based authentication, trust relationships are generating from general social relationships. The initialization process depends on the formation of a network of trust relationship between them.

An Ad-hoc On-demand Distance Vector (AODV) [3] is a reactive routing protocol, in which routing table of every node is refreshed whenever any node enters in MANET or leave the MANET. The AODV routing protocol uses RREQ, RRES, and RERR control packets. RREQ is route request control packet send by node to find a route for packet forwarding, RRES is route response packet send against RREQ, and RERR is route error packet broadcast when node leaves the network.

Whenever a new node enters in a MANET, it sends RREQ control packet to its one or more neighboring node to establish a fresh route in a MANET for packet delivery. The newly entered node can be a malicious node whose aim is to drain off limited resources of a MANET node such as battery power, bandwidth or memory required to store routing table information by repeatedly sending RREQ control packets or false routing information to its neighboring nodes. This type of attack is called as control packet flooding attack in a MANET (see Fig. 1). Another type of flooding attack is data packet flooding attack. To launch the data flooding, first malicious node built a path to all the nodes then sends the large amount of bogus data packets. These useless data packets exhaust the network resources and hence legitimated user can not able to use the resources for valid communication.

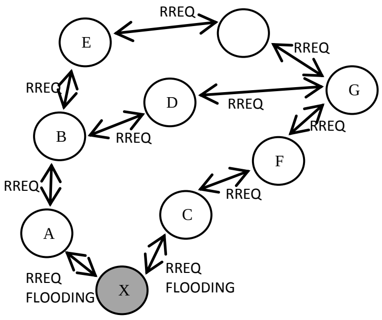

Fig. 1 communication between nodes in MANET with flooding attack

To prevent MANET from flooding attack by detecting malicious node, we are using the node authentication framework. This framework is based on a challenge – response protocol and a hash function. In this framework, a node gets authenticated by its legitimate neighbor node present in the network. If the malicious node is detected during the authentication, its information will be broadcasted by legitimate neighbor nodes. Other legitimate nodes keep this information in their Malicious_Node_Table (MNT). Then other legitimate nodes will discard all incoming packets from malicious node by checking its entry in MNT. In this way legitimate nodes will get prevention from flooding attack by the malicious node. For data packet delivery from source node to a destination node, AODV routing protocol will be used [3].

The remainder of this paper is organised as follows: section II presents ongoing related research in security in MANET, in section III we have described Implementation of our work including architecture and algorithm, section IV represents analysis and results of our work, in section V we conclude our system.

II. Related Work

To secure MANET from various attacks significant research is going on. Some researches proposed the techniques for secure routing but secure routing also cannot handle the flooding attack.

C. Perkins et al. [3] presents concept of AODV routing protocol. The AODV routing protocol uses RREQ, RRES, and RERR control packets. RREQ is route request control packet send by node to find a route for packet forwarding; RRES is route response packet send against RREQ and RERR is route error packet broadcast when node leaves the network. In this paper authors explained working of AODV routing protocol [3]. Djamal DJENOURI et al. have presented different security requirements in MANET, MANET features and their impact on security in MANET. Also different routing attack and their impact in network is discussed. Furthermore different existing solutions to different attacks have been discussed [4]. Nikos Komninos et al. used the challenge response protocol and the zero knowledge protocol for the node’s validity in the network [5]. In this work, a non-interactive zero knowledge protocol used to determine the true identity of the communicating nodes and a challenge-response protocol used to perform node authentication of communicating nodes. The main problem with this method is control overhead increases due to multiple packets used for the node authentication [5]. Yiu-Chun hu et al. have presented rushing attack defence mechanism using Secure neighbour detection, Secure route delegation, and Randomize route request forwarding [6]. Problem with this mechanism is node overhead increases if multiple nodes send route requests at same time or with very little time span [6]. Madhavi et al. have proposed a methodology to detect and prevent the flooding attack using signal strength and client puzzle method [7]. To implement this, authors uses concept of Hello message with two variables Allowed_Hello_Loss and Hello_Interval. This approach decreases the control overhead by 2%. The result obtained in this work is preventing only one kind attack that is flooding attack. Presence of more than one kind of attacker may affect the performance of the network [7]. Ping Yi et al. have proposed the distributive approach to prevent the flooding attack, in which three threshold values are used; Rate_Limit, Blacklist_Limit and Blacklist_Timeout [8]. This approach analyses RREQ count of each node with Rate_Limit threshold value and Blacklist_Limit threshold value. This method can handle the network with high mobility [8]. Jian-Hua Song et al. have analyzed the flooding attack in anonymous communication [9]. In this approach, the threshold tuple is used which consist of three components: Transmission_Threshold, Blacklist_Threshold and Whitelisting_Threshold. Problem with this approach is node overhead increases as every time node has to check status of other nodes [9]. Venkat Balakrishnan et al. used the extended DSR protocol based on the trust function to mitigate the effects of flooding attack [10]. In this technique, authors have categorized the nodes based on the trust value: Friends, Acquaintance and Stranger. Friends are trusted nodes, Stranger are non trusted nodes, and Acquaintance has the trust values more than stranger and less than friends. Based on relationship they defined the three threshold value. The main problem with this method was it does not work properly with higher node mobility [10]. H Deng et al. have used concept of Identity-based cryptography and threshold secret sharing for distributed key management and authentication [11]. Authors have used a self-organizing way to provide a key generation and a key management service instead of using traditional pre-fixed trust relationship between nodes. In this scheme authors avoid centralized certificate authority to distribute public keys and certificates which saves network bandwidth and reduces network overhead [11].

In our work, we are providing the node authentication framework using a challenge response protocol (CRP) and a hash key which will exchange fewer messages to authenticate a node which in turn reduces the control overhead and battery consumption. This framework will prevent flooding of memory provided by the legitimate node from the malicious node by identifying a malicious node and discarding all incoming packets from a malicious node. In the AODV routing protocol, a node uses RREQ and RRES control packets to establish route for packet forwarding. Our Node authentication framework is based on RREQ control packets generated by the AODV routing protocol and a secret questions and answers generated by CRP. Also we are using MNT for keeping information about the malicious node detected by CRP. For routing and packet forwarding, we are using AODV routing protocol, security will be maintain by MNT.

III. Implementation Details

The main goal of our approach is to provide resource aware node authentication framework to prevent flooding attack in MANET, i.e which consumes less resources to perform node authentication and flooding attack prevention.

- Node authentication using CRP

  Our Node authentication framework is based on RREQ control packet generated by the AODV routing protocol and secret questions and answers generated by CRP.

- To prevent flooding attack using MNT information

  We are using the Malicious Node Information Table (MNT) for keeping information about a malicious node detected by CRP. A Flooding attack can be tackle by checking RREQ requester node’s entry in MNT and discarding further incoming packets from requester node, if it is present in MNT.

- Routing using AODV routing protocol

  For t data packet forwarding from originator node to destination node, AODV routing protocol is used.

3.1. System components

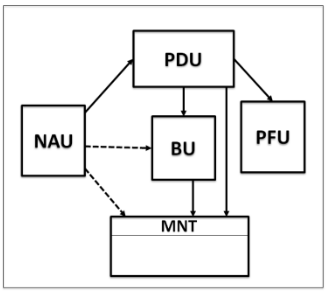

Fig. 2 system components

Fig. 2 shows system components of our system. Our system includes; Node authentication Unit (NAU) to perform new node authentication using CRP; Path Discovery Unit (PDU) to discover secure path for data packet forwarding using AODV routing protocol; Broadcast Unit (BU) to broadcast RREQ control packet generated by PDU also to broadcast data packet containing information about malicious node gathered from NAU; Malicious Node Table (MNT) is used to keep information about malicious node broadcasted by NAU; Packet Forwarding Unit (PFU) to forward data packets from originator node to destination node.

3.2. Proposed system

The proposed system includes two modules viz. Node authentication and Data packet forwarding.

- Input

  RREQ : Route request control packet generated by PDU

- Output

  RRES : Route Response control packet generated by PDU
  MN : Data packet containing information about malicious node generated by NAU

Algorithm for Data Packet Forwarding

1. Consider X is new node and A is legitimate node in MANET.
2. ‘A’ receives RREQ from X
3. i.e A ← RREQ (X)
4. ‘A’ checks its routing table’s status field for X’s validity in network.
5. If (RT_Status (X) in A = = 1) then proceed RREQ for route discovery.
6. Else, check entry of X in MNT
7. If (X present in MNT) then discard all incoming packets from X
8. Else perform Node authentication

Algorithm for Node Authentication

1. ‘A’ generates secret question QA on dynamically generated input and send it to ‘X’
2. Then ‘A’ computes answer for the same question using hash function. ANSA = H(QA)
3. ‘X’ receives input from ‘A’ and computes its answer using Hash function. ANSX = H(QA)
4. ‘A’ receives answer from X
5. If (ANSA = = ANSX) then X is legitimate node
6. Else,
7. ‘A’ declares X as malicious node and broadcast MN to all legitimate nodes in MANET. // MN : data packet containing information about malicious node.
8. All nodes store this information in their MNT
9. set (RT_Status(X) = = 0)

IV. Results

In our approach we are using node’s resource consumption as a result parameters for the node authentication. The node resources includes battery power, memory to store routing information, bandwidth. As shown in table 1, the node resources required to perform the node authentication using the cryptography based technique are high because in this technique every node has to store certificates of other nodes and has to provide other node’s certificate on demand. In the offline trust based technique memory requirement is high to store the trust information about other nodes but bandwidth and battery power requirement is moderate because control packet exchange is less than cryptographic based technique. In our approach, node authentication using CRP, battery power consumption is low because less number of computations have performed, bandwidth requirement is less because minimal control packet exchange and less amount of memory is required to store information about malicious node.

Table 1. Resource consumption in various node authentication techniques

Resources Techniques	Battery power	Memory	Bandwidth
Cryptography based node authentication	High	High	High
Offline trust based node authentication	Moderate	High	Moderate
Node authentication using CRP	Low	Moderate	Low

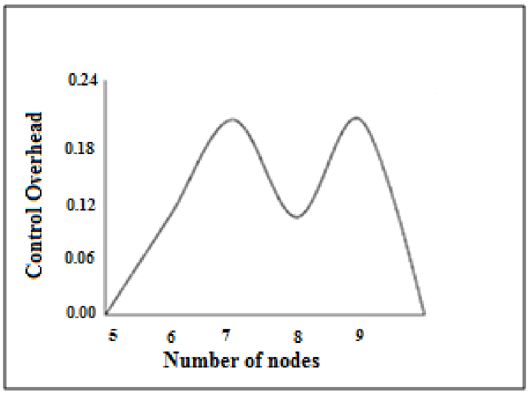

Fig. 3 Control overhead

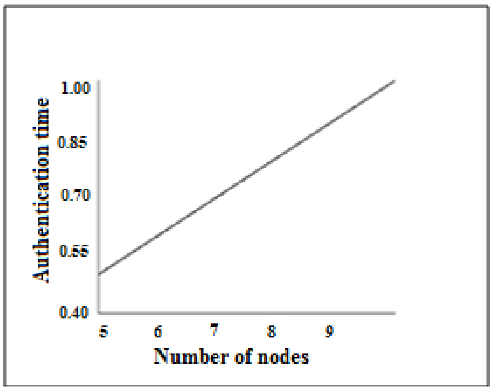

Fig. 4 Authentication time

Fig 3 shows control overhead v/s number of nodes. The term Control Overhead (CO) can be defined as the total number of exchange of control packets from source to destination before transmission of packets divided by total number of packets to be transmitted into the network.

$$\mathrm{CO} = \frac{Number\_of\_control\_packets}{Total\_number\_of\_packets(data\_and\_control)}$$

In our approach, we are performing the node authentication for each node only once, therefore control overhead is reduced because minimum control packets are transmitted during the node authentication and a path discovery. As shown in Fig. 3, at number of nodes 7 and 9 control overhead increases as we are performing node authentication for new nodes. Whereas at number of nodes 8 control overhead decreases as at this point RREQs are from the legitimate nodes. Fig 4 shows node authentication time v/s number of nodes. We have calculated time required to perform the node authentication by using system timer. As shown in Fig 4, the authentication time required to authenticate multiple nodes simultaneously is comparatively decreases when the number of nodes increases in the network.

V. Conclusion

Due to existence of large number of MANET applications in society today, the security of MANET plays a significant role. As MANET is intfrastructure-less multi-hop network, every node in MANET is responsible for secure packet delivery. Hence, we have proposed the node authentication framework which prevents MANET from flooding attack in higher mobility. Also this framework reduceses node’s resource consumption. Our node authentication framework required less authentication time to authenticate nodes in MANET than existing system. Also Control overhead is decreases as minimum control packets are transmitted during node authentication and path discovery. We have provided secure data packet delivery by using MNT and AODV. In future we can implement same framework for other routing protocols in MANET.

Reference

[1]. Pushpender Singh and Manik Chandra Pandey, “Evaluation of certificate-based authentication in Mobile Ad-hoc networks”, International Conference on Recent Trends in Engineering and Technology, 2012, 69-74.

[2]. Jaydip Sen, “Robust and Efficient Node Authentication Protocol for Mobile Ad Hoc Networks”, Computational Intelligence, Modelling and Simulation (CIMSiM), 2010 Second International Conference on, 2010, 476-481.

[3]. C. Perkins et al., (2001, 07), “Ad Hoc On-Demand Distance-Vector Routing (AODV)”, IETF draft, 2001.

[4]. Djamal DJENOURI, Nadjib BADACHE, “Survey on security issues in Mobile Ad-hoc Networks ”, IEEE communications surveys, 2005

[5]. Nikos Komninos, Dimitris Vergados, Christos Douligeris, “A Two-Step Authentication Framework in Mobile Ad-Hoc Networks, China Communication Journal, 4(1), 2007, 28-39. Available: openaccess.city.ac.uk/2512/1/TwoStep%20Authentication.pdf

[6]. Yiu-Chun Hu, Adrian Perrig, David B. Johnson, “ Rushing attacks and defense in wireless Ad-hoc network routing protocols”, WiSi ’03 proceedings of 2nd ACM workshop on wireless security [online],2003, 30-40

[7]. Madhavi, S. and K. Duraiswamy, “Flooding Attack Aware Secure AODV”, Journal of Computer Science,,[Online]. 9 (1), 2013, 105-113, Available: http://www.thescipub.com/jcs.toc

[8]. Ping Yi, Zhoulin Dai, Yiping Zhong, Shiyong Zhang, “Resisting Flooding Attacks in Ad Hoc Networks”, Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC’05) IEEE International Journal of Computer Applications, 5(12),2010

[9]. Jian-Hua Song1, 2, Fan Hong1, Yu Zhang1, “Effective Filtering Scheme against RREQ Flooding Attack in Mobile Ad Hoc Networks”, Proceedings of the Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies 2006, 07695-2736-1/06

[10]. Venkat Balakrishnan, Vijay Varadharajan,and Uday Tupakula, ” Mitigating Flooding attacks in Mobile Ad-hoc Networks Supporting Anonymous Communications” The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, 2(7), 2007

[11]. H deng, A. Mukharjee, D. Agrawal, “Threshold and identity-based key management and authentication for wireless network”, Information thechnology: coding and computing,(1), 107-111.