Volume 8, No. 4, May 2017 (Special Issue)
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

A Node Authentication Mechanism for Securing MANETs

Raman Preet,
Research Scholar, I.K. Gujral Punjab Technical University, Kapurthala, Punjab, INDIA
Email: kohliramanpreet@yahoo.com

Dr. Paramjeet Singh,
Professor, Gaini Zail Singh Campus College of Engineering & Technology, Bathinda, Punjab, INDIA
Email: param2009@yahoo.com

Dr. Shaveta Rani,
Professor, Gaini Zail Singh Campus College of Engineering & Technology, Bathinda, Punjab, INDIA
Email: garg_shavy@yahoo.com

***Abstract*— In Mobile Ad-hoc Networks (MANETs) the wireless nodes move frequently around the space and mutually cooperate with each other to perform routing and forwarding data. MANETs are infrastructure-less networks without any kind of central administration for the management of network. Due to this reason MANETs are comparatively more vulnerable to security threats than conventional wired or wireless networks. The network nodes in MANETs are susceptible a number of attacks due to the inherent nature and depicted properties of MANETs. Thus to prevent attacks it becomes very much mandatory to identify and authenticate each and every node during route discovery phase so that data can be communicated safely later on. In this paper we introduce an authentication mechanism that will enhance the security of standard AODV protocol. The protocol deploys unique prime factorization principle to achieve node authentication with minimal overhead. It detects and isolates unauthorized nodes from the network so as to avoid any kind of attacks from them.**

***Keywords*— *MANET, Authentication, Routing, mobile nodes*.**

I. INTRODUCTION

A MANET (Mobile ad-hoc Network) is a wireless network that comprises of a number of mobile nodes which have the flexibility of entering and exiting the network freely any time. Nodes that participate in the network formation are connected to each other by wireless links [1]. MANETs are mainly deployed in situations where either the infrastructure has been destroyed due to any reason or is not feasible to have a fixed infrastructure for the network management. Such networks are usually deployed in military battle scenarios, disaster recovery sites etc. [1][2][3][4][5].

In MANET, nodes act as router as well as hosts. Nodes forward data to others in the network assuming them to be trustworthy. This property of MANETs make them vulnerable to many attacks such as Denial of Service (DoS), grey hole attack, black hole attack, Sybil attack etc. These attacks lead to degradation in the network performance to great extent. Like conventional wired networks routing is one of the main prime area that is required to be handled efficiently for the successful deployment of network. Routing selects best path for the data transmission. Due to the dynamic nature of MANETs dynamic routing protocols are needed for them.

Dynamic routing protocols fall under two categories namely proactive and reactive protocols. The proactive routing protocols are table-driven routing protocols that maintain routing information to every node in the network before it is needed. Protocols like DSDV fall under this category. Reactive protocols on the other hand are the ones that do not maintain the routing information to the network nodes unless and until it is actually required. In simple terms routes are created on-demand whenever a source node needs to send some data to a destination node. One of the most widely used routing protocol in this category is Ad-hoc On Demanding Distance Vector (AODV) [6].

AODV is a reactive routing protocol. It establishes routes only on demand when user wants to send the some data. AOV is most efficient routing protocol for MANET. It has two phases of working (1) Route Establishment and (2) Route Maintenance.

In this paper we propose a protocol that is a modified version standard AODV protocol which authenticates each node before establishing routes to destination node. This paper is organized as follows: Section II presents an overview of the standard AODV, section III discusses the literature survey in this direction. Section IV elaborates on the proposed mechanism for node authentication.

II. WORKING OF AODV PROTOCOL

The AODV is a simple and efficient reactive routing protocol that is based on distance vector approach [6]. It is composed of two phases namely: (1) Route Establishment and (2) Route Maintenance. Each node has its own sequence number that increases automatically with the change in topology. AODV includes three control packets, RREQ (route request), RREP (route reply) and RERR (route error). During route establishment, the source node broadcasts a RREQ packet to intermediate nodes, and these intermediate nodes will send RREQ to other nodes. The process continues until the RREQ reaches the destination node. After receiving RREQ from intermediate nodes, nodes which have fresh route to the destination will send RREP packet to source. Destination sequence number of nodes which are having route to destination will be greater than the destination sequence number of source. RREP with greatest destination sequence number nodes are selected. RERR packets are sent to source node when there is no path between the specified source and destination node.

CONFERENCE PAPERS
National Conference on Emerging Trends on Engineering & Technology (ETET-2017)
On 21st April 2017
University Inst. of Engg. & Tech. & University Inst. of Computer, SBBS University, Punjab (India)

III. LITERATURE SURVEY

The problem pertaining to security and cooperation enforcement through node authentication mechanism has received considerable attention by researchers in the ad hoc network community. In this section, some of these contributions are discussed.

Sapna et al [7] have proposed a PPN (Prime Product Number) scheme for detecting and removal of malicious nodes. This technique assigns a specific prime number to each node to uniquely identify it within the network. The entire network is organized into a number of clusters such that every node is a member of at least one cluster. Cluster management is performed by a cluster head (CH). There will be a single cluster head per cluster. Every cluster head maintains a separate table called Neighbor Table for storing information regarding every node in the network. The PPN scheme is embedded in the standard AODV protocol. The scheme relies on reliable trustworthy nodes and broadcasts RREQ for discovering route to its desired destination node. An intermediate node generates its RREP to provide data regarding its CH and product of all prime numbers from destination node to source node. The source node checks for the divisibility of the product by its node id. For this it searches its Neighbor Table. If it finds that the product is completely divisible, it accepts the RREP otherwise discards marking it as a malicious node. There after it invokes its malicious node removal process. The scheme involves deputation of additional cluster heads. The node ids are not encrypted or hashed due to which , this information could be spoofed and misused.

Arvind et al [8] modified the standard AODV protocol by adding with two more additional packets namely- Response sequence packet (Rseq) and Code sequence packet Cseq). Here the Route discovery process takes place in AODV MAC layer. Control packets are broadcasted during the route discovery process. Each node sends its Cseq packets to its intermediate nodes to send their Rseq. If Cseq and Rseq packets of intermediate node match then intermediate node allows connection to network layer. If match does not happen it discards the node from network and broadcasts information to other nodes so that they delete the malicious node from their respective tables. It checks the sequence packet with Cseq packet which is stored in table. If Cseq packet and sequence packet match then node is accepted otherwise discarded. This protocol introduces additional packets and exchanges the control packets in MAC layer.

A technique is proposed in [9] that utilizes digital signature for authentication. In this technique initially route is established using RREQ control message and the receiver replies back with the hash value of its IP address. The receiver's IP address value is compared with sender's IP address. If both the IP addresses match, then receiver is trusted. Digital signature with MD5 and RSA is issued by the trusted node. Data is encrypted using Symmetric key algorithm AES and sends it to the receiver with digital signature. Intermediate nodes check the validity of digital signature. If digital signature is found valid, data is forwarded otherwise the node is declared a malicious one. The receiver decrypts the data using AES. This technique involves heavy computational load due to the usage digital signatures.

Mingyu et al [10] also proposed a technique for authentication of nodes by altering the standard AODV protocol. In this technique initially a node gets a secret key. By using one way hash function on time stamp, key and message MAC are generated. Symmetric cryptography is applied to encrypt the packet before injecting it into the network. Each intermediate node forwards the packet to its next node. At any node if the computed hash value of destination node matches with stored value, it is considered a valid node otherwise that node is discarded node from the network. Another route discovery process takes place. This technique deals with end-to-end secrecy during route discovery process.

Anuj et al [11] proposed a protocol namely -Enhanced Modified AODV (EMAODV). Researchers here have enhanced AODV by using two control packets namely - Secure Reliable Route Discovery Request (SRRD_REQ) and Secure Reliable Route Discovery Reply (SRRD_REP). SRRD_REQ packets are the route request packets with SRRD_ID as destination sequence. SRRD_REP is response packet to SRRD_REQ by destination to the source after matching SRRD_ID. The Routing table contains additional fields namely- reliable list (RL) and Threshold value (TV). As per the proposed technique the source node sends SRRD_REQ packet to other nodes. Nodes which already have route to destination will send SRRD_REP to source after checking route entry in routing table. After getting reply from destination node, source will send SRRD packet as acknowledgement to nodes from which it received SRRD_REP. Once SRRD packet is received from source, destination will again send SRRD_REP packet to source node to establish route. Since EMAODV takes two cycles to establish a secure route to the destination, it consumes more time.

IV. MECHANISM TO PERFORM NODE AUTHENTICATION

Following assumptions are made for achieving node authentication:

- It is assumed that a network key is distributed to all the nodes before the deployment of the network and remains unchanged.
- A unique ID is provided to each and every node in the network. For this a unique prime number is assigned to every node which will basically serve for individual node's identification in the network, once it is deployed. Every node decrypts this ID with the network key before forwarding it to other nodes through its RREP packet.

A number of modifications as well as few additions are made in the functionality of standard AODV protocol to perform the required node authentication mechanism.

A new field is inserted in RREP Packet. This field is termed as IDENTITY_CHECKSUM and it carries the encrypted ID of nodes.

CONFERENCE PAPERS
National Conference on Emerging Trends on Engineering & Technology (ETET-2017)
On 21st April 2017
University Inst. of Engg. & Tech. & University Inst. of Computer, SBBS University, Punjab (India)

Every node maintains one additional table namely MALICIOUS_LIST along with standard routing table. Provision for MALICIOUS_LIST is kept for logging information about malicious or unauthorized nodes detected after the deployment of the network.

When a source node S wants to communicate with any destination node say D, it initiates the regular route discovery process by broadcasting its RREQ packet to discover a secure route to the destination node D. In the course of time when any intermediate node finds a fresh route to the desired destination D, its sends the route information along with encrypted product of all IDs of nodes from the destination node to source node via IDENTITY_CHECKSUM field in RREP packet.

When RREP packet is received by the source node S, it decrypts the IDENTITY_CHECKSUM field by the network key and divides it with its own ID. If the IDENTITY_CHECKSUM value is completely divisible by its ID then it concludes that RREP has come from an authorized node otherwise it is considered unauthorized/malicious and discarded. Node IDs of such unauthorized nodes are inserted into MALICIOUS_LIST. This MALICIOUS_LIST is further broadcast to all network nodes which then check their respective routing tables and delete all routing entries with the ID of unauthorized nodes. To secure further network communication every recipient node adds an entry of the malicious node in their respective MALICIOUS_LIST.

V. CONCLUSION

In this paper we have proposed a protocol which is an improvement in the standard AODV protocol. The proposed protocol performs node authentication in a simplified and efficient manner without involving heavy computational overhead. In this context we have also reviewed some of the schemes proposed by researchers for authenticating nodes in MANETs. The proposed protocol achieves authentication of nodes during route establishment phase with minimal computation overhead. As our future work we will be simulating this protocol using NS2 and compare its performance with standard AODV and with some of the existing protocols in this direction. We also intend increase the functionality of this protocol for detecting and preventing RREQ flooding in the network.

REFERENCES

[1] Jun-Zhoa Sun, "Mobile Ad Hoc Networking: An Essential Technology for Pervasive Computing", IEEE Info-tech and Info-net, proceedings, 2001, pp.316-321.

[2] C. Siva Ram Murthy, B.S. Manoj,"Ad Hoc Wireless Networks:Architecture and Protocols",Prentice Hall PTR, May 2004, New Jersey.

[3] M. Frodigh, P. Johansson, and P. Larsson,"Wireless Ad Hoc Networking: The Art of Networking without a Network", Ericsson Review 2000,pp. 248-263.

[4] IETF Working Group: Mobile Adhoc Networks (manet), http://www.ieft.org/html.charters/manet-charter.html.

[5] C. Perkins, E. Beldin-Royer and S. Das, Ad hoc on-demand distance vector (AODV) routing, IETF RFC 3561, July 2003.

[6] X.Cheng, X. Huang, D.Du, "Ad Hoc Wireless Networking",Springer 2004 Edition.

[7] S.Gambir, S.Sharma,"PPN:Prime Product Number based Malicious Node Detection Scheme for MANETs", IEEE 2012, pp.335-340

[8] A. Dhakaa, A. Nandaib, R. S. Dhakac, " Gray and Black hole attack Identification using Control Packets in MANETs",11th International Multi-Conference on Information Processing-2015.

[9] A.Bhosle, Y. Pandey, " Review of authentication and digital signature methods in Mobile Ad hoc netorks",International Journal of Advanced Research in Computer Engineering & Technoloy (IJARCET), Volume 2, Issue 3, March 2013.

[10] J. Luo, M.Fan,, Danxia, "Black hole prevention based on authentication mechanism", School of Computer Science & Engineering, University of Electronics Science and Tehnology of China, Chengdu, China, 610054.

[11] A. Ranaa, V. Ranab, S. Gupta, "Emaodv:Technique to prevent collaborative attacks in Manets", 4th International conference on Eco-friendly computing and Communication systems 2015, Sonipat, Haryana-131023, India.

CONFERENCE PAPERS
National Conference on Emerging Trends on Engineering & Technology (ETET-2017)
On 21st April 2017
University Inst. of Engg. & Tech. & University Inst. of Computer, SBBS University, Punjab (India)