ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 13, March 2016

AUTHENTICATED ANONYMOUS SECURE AND FASTEST ROUTING FOR MANET

A.Chitrajeyavathy[1], K.Vijayananth[2]
PG Student[1], Assistant Professor[2]
Department of Electronics and Communication Engineering.
VV College of Engineering.

Abstract- ***Anonymous communications are important for many applications of the mobile ad hoc networks (MANETs) deployed in adversary environments. The existing system uses the topology based anonymous on demand secure routing protocol. However, these are vulnerable to the attacks of fake routing packets or denial-of-service (DoS) broad-casting even the node identities are protected by pseudonyms. In this work, an authenticated anonymous secure routing protocol is proposed which provides security against vulnerable attacks. By using this protocol the data is authenticated by a group signature to defend the potential active attacks without unveiling the node identities. This group signature scheme is designed to prevent intermediate nodes from inferring a real destination. The key encrypted onion routing scheme protects the data being modified by the malicious node. So we can safeguard the information's of one client from the other.***

Keywords:MANET, Secure, Communication, intermediate.

I.INTRODUCTION

A mobile Adhoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires. Ad hoc is Latin and means "for this purpose". Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. They may contain one or multiple and different transceivers between nodes. This results in a highly dynamic, autonomous topology.

MANETs are a kind of Wireless ad hoc network that usually has a routable networking environment on top of a Link Layer ad hoc network. MANETs consist of a peer-to-peer, self-forming, self-healing network in contrast to a mesh network has a central controller (to determine, optimize, and distribute the routing table). MANETs circa 2000-2015 typically communicate at radio frequencies (30 MHz - 5 GHz).

II.PROPOSED METHOD

In this, propose an authenticated anonymous secure routing (AASR) to overcome the pre-mentioned problems. adopt a key-encrypted scheme to record a discovered route and design an encrypted secret message to verify the RREQ-RREP linkage. Group signature is used to authenticate the RREQ packet per hop, to prevent intermediate nodes from modifying the routing packet.The performance of AASR to that of ANODR, a representative on-demand anonymous routing protocol. The results show that, it provides more throughput than ANODR under the packet-dropping attacks, although AASR experiences more cryptographic operation delay.Once a path is identified by the returning searchcontrol packets, this entire path is embedded in each datapacket to that destination. Thus, intermediate nodes do noteven need a forwarding table to transfer these packets. Because of its reactive nature, it is more appropriate for occasional or lightweight data transportation in MANETs. AODV, DSDV, and other DV-based routing algorithms were not designed for source routing; hence, they are not suitable for opportunistic data forwarding. The reason is that every node in these protocols only knows the next hop to reach a given destination node but not the

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 13, March 2016

complete path. In this, introduce the basic concepts in anonymous routing, and provide a short survey on the existing routing protocols.

III. OPERATION

a. Time is divided into equal slots of duration T. Atthe beginning of each slot, each node s generatesa temporary public-private key-pair: PK-TMPsand SK-TMPs, respectively. PK-TMPs is subsequentlyused by other nodes to encrypt sessionkeys to establish secure channels with s. Notethat these keys can be generated offline.

b. Each node broadcasts a Location AnnouncementMessage (LAM), containing its location (GPScoordinates), time-stamp, temporary public key(PK-TMPs), and a group signature computedover these fields. Each LAM is flooded throughoutthe MANET[3].

c. Upon receipt of a new LAM, a node first checks that it has not received the same LAM before, itthenverifies the time-stamp and group signature.
If both are valid, the node rebroadcasts the LAMto its neighbors. Having collected all currentLAMs, each node constructs a geographical mapof the MANET[2] and a corresponding nodeconnectivity graph. Between successive LAMs, a node can be reached (addressed) using a temporary pseudonym formed as current location concatenatedwith the group signature in the last LAM(TmpID=fLocationkGSigg). Note that thepseudonym represents a valid address even if the actual node moves in the interim. Thelocation is included in the pseudonym in order to minimize required state and assist in theforwarding process. If the location is not part of the pseudonym, a node forwarding a message toa pseudonym would have to look up the associated location and decide how to forwardto that location. Including location in the pseudonym speeds up the forwarding process and requires fewer look-ups.

d. Whenever a node desires to communicate with acertain location, it checks to see if any nodecurrently exists at (or near) that location. If so, itsends a message to the destination's currentpseudonym (TmpID). This message is encryptedwith a session key using a symmetric cipher. The session key is, in turn, encrypted under thecurrent public key (PK-TMP) included in thedestination's latest LAM. When the destinationreceives the message, it first recovers the sessionkey and uses it to decrypt the rest. ALARM is notrestricted to any specific public key technique. One obvious choice is Diffie-Hellman (DH), whereby each LAM includes an ephemeral (period-specific) DH half-key. The sender thensimply generates its own DH half-key, computesa shared key and encrypts the session key with it. Clearly, the sender's half-key must be includedin the clear-text part of the message. Other keyagreement schemes can also be used.

e. Forwarding: As described above, nodes disseminatecurrent topology by periodically floodingLAMs. Once each node has the entire topologyview, it decides whether to communicate with a certain location (node). Message forwarding isindependent of topology dissemination. Oneoption is for a node to create a source route, explicitly encoding locations of nodes on thepath to the destination. The actual path can becomputed using the shortest path algorithm orany other location-aided routing algorithm. Assume that the nodeat location1 (TmpID1 = fLocation1kGSig1g) requiressending a message to another node atlocation4 (TmpID4 = fLocation4kGSig4g). Thesender calculates the route to location4 anddetermines that it has to pass through location2and location3. It then generates a session key(Ks) and encrypts data with that key using asymmetric cipher (e.g., AES). It then uses thepublic key in the last LAM of location4 toencrypt Ks and assembles a data message withthe destination set to (TmpID4) and source—to(TmpID1). It finally composes a source route:< TMPID2; TMPID3 >.
Despite the amount of effort in routing in ad hoc networks, data forwarding, in contrast, follows the same paradigm as in Internet Protocol (IP) forwarding in the Internet. IP forwarding was originally designed for multihop wired networks, where one packet transmission can be only received by nodes attached to the same cable. However, in wireless networks, when a packet is transmitted over a physical channel, it can be that channel. Traditionally, overhearing apacket not intended for the receiving node had been consideredcompletely negative, i.e., interference. Thus, in a sense, the goalof the research in wireless networking was to make wirelesslinks as good as wired links.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 13, March 2016

IV.RESULT AND DISCUSSION

A. Network Model

In this module, first forming the network and send hello packets to the particular node networks. Forming a group. Grouping means number of nodes.

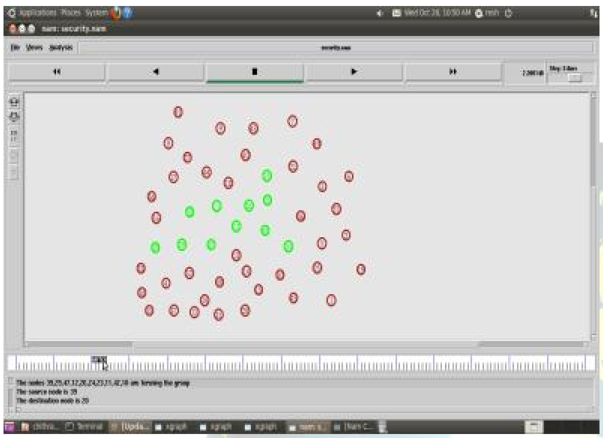

Figure 4.1 Group Formation

B. Path selection

In this module, the node decrypting the location and it is not a destination so encrypt the text and send to another node. There is a packet loss in source side.

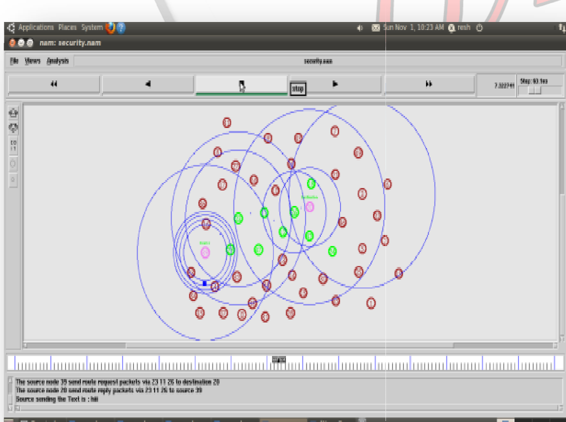

Figure 4.2 Path Selection

C. Data Transmission

In this module ,data transmitted from source to destination and the lossless path is selected.

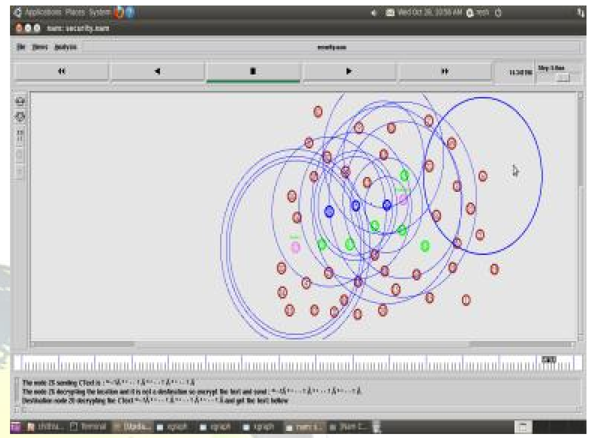

Figure 4.3 Data Transmission

D. Energy Consumption

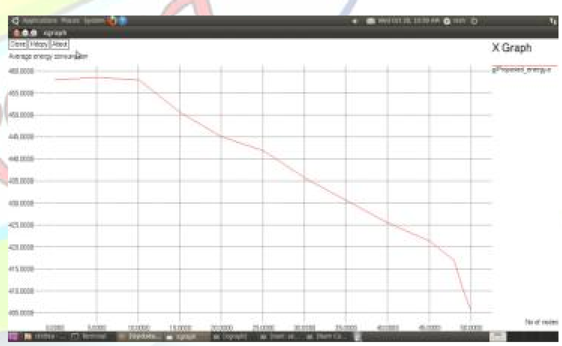

Figure 4.4 Graph of Energy V/S No of Node

E. End to End delay

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 13, March 2016

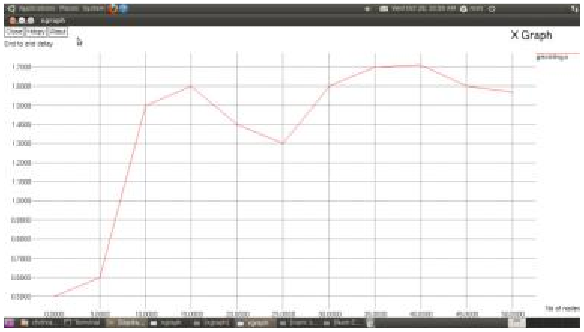

Figure 4.5Graph of Delay V/S No of Nodes

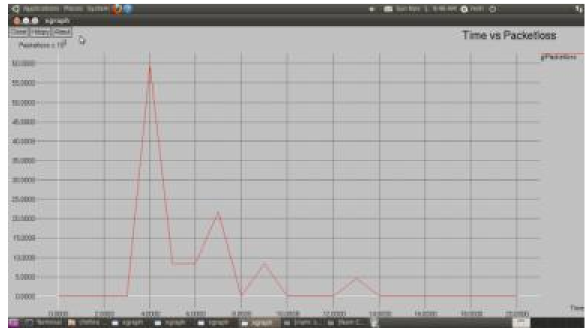

Figure 4.7 Graph of Packet lossV/S Time

F. Throughput

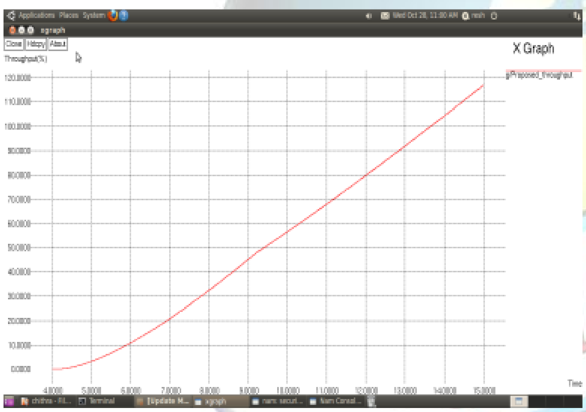

Figure 4.6 Graph of Throughput V/S Time

G. Packet loss

In this graph, packet loss per time time is given.

V.CONCLUSION AND FUTURE WORK

In this section, an authenticated and anonymous routing protocol for MANETs in adversarial environments is designed. The route request packets are authenticated by group signatures, which can defend the potential active anonymous attacks without unveiling the node identities. The key-encrypted onion routing with a route secret verification message is designedto not only record the anonymous routes but also prevent the intermediate nodes from inferring the real destination. Compared to ANODR, AASR provides higher throughput andlower packets loss ratio in different mobile scenarios in thepresence of adversary attacks. It also provides better supportfor the secure communications that are sensitive to packet lossratio. In our future work, we will improve AASR to reduce thepacket delay. A possible method is to combine it with a trustbasedrouting. With the help of the trust model, the routing protocols will be more active in detecting link failures, caused either by the mobility or adversary attacks.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 13, March 2016

IV.REFERENCES

1.AzzedineBoukerchea,B, Khalil El-Khatiba, Li Xua and Larry Korbab,(2004)" An efficient secure distributed anonymous routing protocol for mobile and wireless ad hoc networks" IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 9, NO. 12, PP. 1193-1203.

2.HaiyingShen and Lianyu Zhao (2013) "An Anonymous Location-Based Efficient Routing Protocol in MANETs" IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 12, NO. 6, PP.1079-1093.

3.Marvin Mark M and N. Muthukumaran, 'High Throughput in MANET Using relay algorithm and rebroadcast probability', the International Journal of Engineering Research and Applications (IJERA), ISSN: 2248-9622, Vol. 5, pp. 66-71, March 2014.

4.Marvin Mark M and N. Muthukumaran, 'An Advanced Homogeneous Pattern for Mobile Ad Hoc Network', the International Journal of Advanced Research in Computer Science and Management Studies, ISSN(Online): 2321-7782, ISSN(Print): 2347-1778, Vol. 2, Issue 4, pp. 6-8, April 2014.

5.Jun Liu, XiaoyanHong, Jiejun Kong†, QunweiZheng, Ning Hu, Phillip.G and Bradford,(2011) "A Hierarchical Anonymous Routing Scheme for Mobile Ad-Hoc Networks" IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 12, NO. 7,PP.508-528.

6.Jiejun Kong, XiaoyanHong and Mario Gerla, (2007)" An Identity-Free and On Demand Routing Scheme against Anonymity Threats in Mobile Ad Hoc Networks" IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 6, NO. 8,PP.1312-1338.

7.Karim. E Defrawyand Gene Tsudik, (2011)" Privacy-Preserving Location-Based On-Demand Routing in MANETs" IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 29, NO.10, PP.1926-1934.

8.Karim. E, Defrawy and Gene Tsudik, (2011) "Anonymous Location-AidedRouting in Suspicious MANETs" IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 10, NO. 9,PP.1079-1093.

9.Ming Yu, MengchuZhou and Wei Su,(2009) "A Secure Routing Protocol Against Byzantine Attacks for MANETs in Adversarial Environments" IEEETRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 58, NO. 1,PP.449-460.

10.Ming Yu, Kin and Leung. K,(2009), "A Trustworthiness-Based QoS RoutingProtocol for Wireless Ad Hoc Networks" IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 8, NO. 4,PP.1888-1898.

11.Wei Liu and Ming Yu (2014) "Authenticated Anonymous Secure Routingfor MANETs in Adversarial Environments" IEEE TRANSACTIONS ONVEHICULAR TECHNOLOGY, VOL. 7, NO. 4, PP.1-9

12.Xiaoxin Wu and Bharat Bhargava, (2005)" Ad Hoc On-Demand Position-Based Private Routing Protocol" IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 4, NO. 4, PP.335-348.

13.Yanchao Zhang, Wei Liu, Wenjing Lou and Yuguang Fang,(2006)" AnonymousOn-Demand Routing in Mobile Ad Hoc Networks" IEEE TRANSACTIONS ONWIRELESS COMMUNICATIONS, VOL. 5, NO. 9, PP.2376-2385.

14.Zhiguo Wan, KuiRen, and Ming Gu, (2012)" An Unobservable Secure On-Demand Routing Protocol for Mobile Ad Hoc Networks" IEEE TRANSACTIONS ONWIRELESS COMMUNICATIONS, VOL. 11, NO. 5,PP.1922-1932.