ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 2, Issue 2, pp: (40-43), Month: October 2015 – March 2016, Available at: www.paperpublications.org

EAASR: Enhanced AASR Protocol to Reduce Traffic and Eliminate the Malicious Node in the Adversary Environment

Aida Andrews

M.G University, Kottayam, Kerala, India

Abstract: **Mobile ad hoc networks (MANETs) are self-organizing the mobile nodes. It placed in adversary environments and it is vulnerable to security threats due to the characteristics of such networks. The main requirement on the networks is to provide unidentifiability and unlinkability for mobile networks. The existing protocols are not fully satisfied in this requirements. In this paper propose a new routing protocol that is enhanced authenticated anonymous secure routing (EAASR), to satisfy the unidentifiability and unlinkability. The new protocol provides less delay as compared with other protocol.**

Keywords: **Anonymous routing, group elliptical signature, mobile ad hoc networks (MANETs).**

I. INTRODUCTION

Mobile ad-hoc networks (MANETs) are self-configuring, infrastructural less networks, it deployed in adversary environments. Ad hoc wireless network is a temporary and dynamic environment where a group of mobile nodes with radio frequency transceivers communicate with each other without the intervention of any centralized administration or established infrastructure. Due to the limited transmission range of each mobile node, communication sessions between two nodes are usually established through a number of intermediate nodes, which are supposed to be willing to cooperate while forwarding the messages they receive to their destination. Unfortunately, some of these intermediate nodes might not be trustworthy and might be malicious, thereby forming a threat to the security and confidentiality of the exchanged data between the mobile nodes. While data encryption can protect the content exchanged between nodes, analysis of communication patterns may reveal valuable information about end users and their relationships. Using anonymous paths for communication provides security and privacy against traffic analysis. To establish these anonymous paths, in a traditional wired network, nodes build a global view of the network by exchanging routing information, whereas in an ad hoc wireless network, building this global view is not an option.

MANETs are vulnerable to security threats due to the basic characteristics of mobile nodes. A major requirement of this network is to provide unlinkability and unidentifiability for mobile nodes and their networks. Many of the anonymous secure routing protocols have been proposed, but the requirement of these protocols is not completely satisfied. Generally MANETs in adversarial environments focused in on-demand anonymous routing protocols. The commonly used on-demand routing protocols are ad-hoc on-demand distance vector (AODV) and dynamic source routing protocol (DSR). The anonymous security functions are established in source, destination and intermediate nodes in the routing path. The another on-demand routing protocol is anonymous on-demand routing in mobile ad hoc network (ANODR). ANODR provides route anonymity and location privacy. These routing protocols are not completely satisfied in many applications. So the enhanced authenticated anonymous secure routing protocol is to reduce traffic and eliminate the malicious nodes in the adversary environment. EAASR is to satisfy the requirement and defend against the attacks. The route request packets are authenticated by a group elliptical curve to defend against attacks without unveiling the node identity. EAASR

ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 2, Issue 2, pp: (40-43), Month: October 2015 – March 2016, Available at: www.paperpublications.org

provide better security mechanisms as compared with authenticated anonymous secure routing for MANETs. Enhanced authenticated anonymous secure routing protocol which guarantees security, its reduced end-to-end delay and high reliability of the established route in adversarial environment, such as ad hoc wireless network, by encrypting routing packet abstaining from using unreliable intermediate node. The key encrypted onion routing is also used with a route secret verification message is designed to prevent intermediate nodes from inferring a real destination. Simulation results have demonstrated the effectiveness of the proposed EAASR protocol with improved performance as compared with the existing protocols. In enhanced authenticated anonymous secure routing (EAASR) is misinterpreting the attackers to attacks the nodes. The EAASR networks nodes communicate with each other nodes using dummy nodes. It dummy node use small energy as compared with AASR. The malicious node misunderstood the real communicating path between source and destination, because of the neighbourhood communication of dummy nodes. It provides efficient transmission and improves the reliability of the networks. But the real communication was already established in between the source and destination trough the reliable path using secured intermediate node. This path does not identifying the attackers due to anonymity protocols.

II. BACKGROUND AND RELATED WORK

Here introduce some basic concepts in anonymous routing protocols that are trapdoor, onion routing and group elliptical curve signature.

1) Trapdoor: Trapdoor is a one way function between the two neighboring nodes. It is one of the information collection mechanisms. The information's are node identity, destination identity and intermediate identities in to the trapdoor. The intermediate nodes may add information's into the trapdoor; the particular source or destination nodes retrieve the information's. Its provide end-to-end security mechanisms.

2) Onion Routing: Its onion routing provides private communication s over public networks. The source node transmitting the information's to destination through the intermediate nodes. Then each node decrypting to identifying the destination, but each node add the encrypted layer to this packets and transmitting another nodes. Then the destination node retrieve the information's and send its backs to source node.

3) Group Elliptical Curve: The elliptic curve is used to solve to two cryptographic problems, factoring integers and constructing public-key cryptosystems. Elliptic curves are believed to provide good security with smaller key sizes, something that is very useful in many applications.

III. PROTOCOL DESIGN

Here, present the design of the EAASR on-demand ad hoc routing protocols. It's completely depends on on-demand protocols because this new method is does not depending on tables. Its avoid the tables such as destination table, neighbourhood tables, routing tables and forwarding tables. The source node broadcast the route request (RREQ) in the networks and the destination nodes receives the RREQ and send its route reply as RREP. To protecting the security or anonymity when exchange the path of continuously. The three phases of communications are route discovery, data transmission, and route maintenance. For example, use a five node network [1] shown in figure 1(as refer in the previous paper), the source node S and its destination node D.

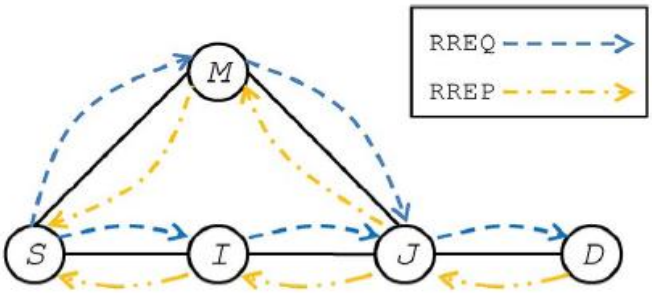


Fig.1. Network topology

ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 2, Issue 2, pp: (40-43), Month: October 2015 – March 2016, Available at: www.paperpublications.org

A. Anonymous Route Request:

1. Source Node: The source node broadcast the RREQ packets through the dummy node to all other nodes. The corrects messages is only decrypting the destination node D. S broadcast the information packets in the format is

$$S \rightarrow *: [RREQ, N_{SQ}, V_D, V_{SD}, Onion(S)]\ G_{ES}- \quad (1)$$

Where the RREQ is the packet-type identifier, N_{sq} is a sequence number, V_D is an encrypted message at the destination node, V_{SD} is an encrypted message at the intermediate node, and onion(S) is a key-encrypted onion created by S. This RREQ packets is signed by S with its group elliptical private key G_{ES}-

2. Intermediate Node: The RREQ packet receives the intermediate node I from source node S. The node I decrypt the packet, and its understood that I is not the destination of this packet. Then again it retransmitting the packet to other node of this format is

$$I \rightarrow * : [RREQ, Nsq, V_D, V_{SD}, Onion(I)]\ G_{EI}- \quad (2)$$

3. Destination Node*:* The RREQ packet reaches the destination D, D validates its intermediate node I or J. The destination node can decrypt the packets and its identifying that this node is the destination of this packets.

B. Anonymous Route Reply:

1) Destination Node: The node D receives the RREQ from its neighbor node J, the RREP packet and send it back to J. The route reply format [1] is

$$D \rightarrow * : (\ RREQ, N_{rt}, <K_V, Onion(J)> K_{JD}) \quad (3)$$

Where RREP is the packet-type identifier, N_{rt} is the route pseudonym generated by D, and K_v and Onion(J) are obtained from the original RREQ and encrypted by the shared key K_{JD}.

2) Intermediate Node : The intermediate node J has already communicate with other nodes I ,D and M. J ,s RREP reply towards the previous hop I in the format is

$$J \rightarrow * : (RREQ, N_{rt}, < K_V, Onion(I)> K_{I\,J}) \quad (4)$$

C. Data Transmission:

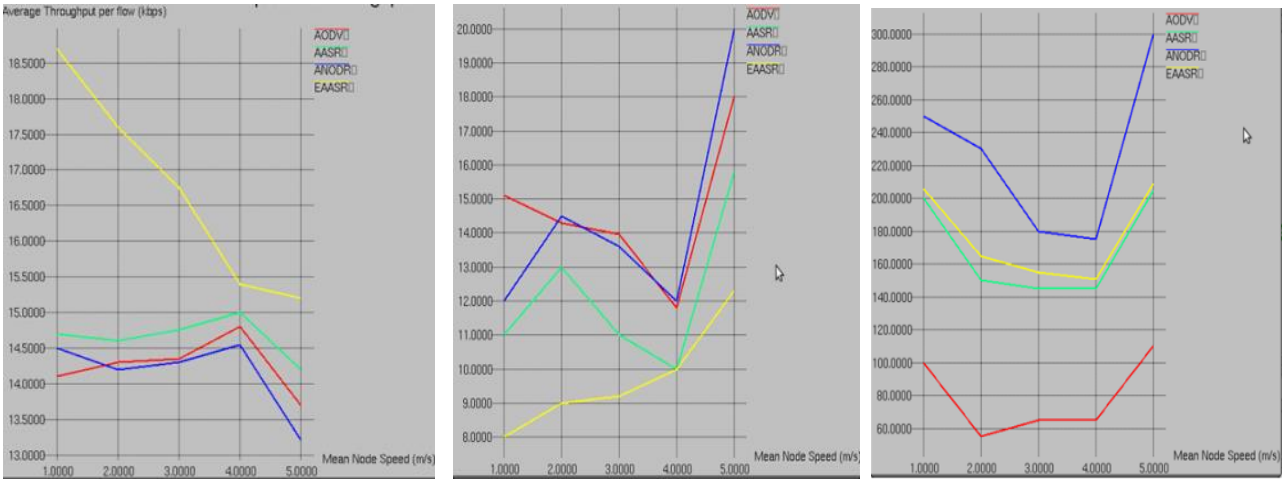
The source node can transmit the data to the destination node D. The format of the data packet is given below

$$S \rightarrow D : (DATA, N_{rt}, <P_{data}> K_{SD}\ ) \quad (5)$$

Where DATA is the packet type, N_{rt} is the route pseudonym, and the data payload is denoted by P_{data}, which is encrypted by the session key K_{SD}.

IV. PROTOCOL EVALUATION

The proposed EAASR protocol in ns-2 by extending the AASR module to support the cryptographic operations. We compare the performances of EAASR to those of AASR, ANODR and AODV in various mobility and adversarial scenarios. Two groups of simulation results are presented here. The first group is to compare the routing performances of AASR AODV, ANODR, and EAASR under different mobility scenarios. The second group is to compare their behaviors under the packet-dropping attacks with different levels. Perform five simulation runs for each configuration and record the per-flow performances, including throughput, packet loss ratio, and end-to-end delay. The effect of malicious attacks EAASR achieves 2% less loss ratio than AASR in average. The average performance of different runs is presented as follows.



(a) **(b)** **(c)**

Fig. 2. Performance comparison under different mobility settings (a) Per-flow throughput(b) Packet loss ratio(c) End-To-End Delay

V. CONCLUSION

In EAASR has improving the efficiency in the terms of route changes. One possible extension is to provide the functionality of repairing broken routes locally without compromising anonymity and security, dynamically partitions the network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a non traceable anonymous route. In addition, it hides the data initiator or receiver among many initiators/receivers to strengthen source and destination anonymity protection. Thus, EAASR offers anonymity protection to sources, destinations, and routes. It also has strategies to effectively counter intersection and timing attacks.

Future work will aims at improving the secured nodes, that means in our enhanced routing protocol such as EAASR only use the secured and shortest path, and avoiding the unwanted nodes in the networks. In improving the anonymity, the avoiding nodes in the networks are rechecking their security and participating the communication networks.

REFERENCES

[1] Wei Liu, and Ming Yu," AASR: Authenticated anonymous secure routing for MANETs in Adversarial environments," in IEEE Trans. vehicular technology, vol.63, no.9, pp.4585-4583, nov.2014

[2] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing," IETF RFC 3561, Jul. 2003. [Online]. Available: www.ietf.org/rfc/rfc3561.txt

[3] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in Proc. CRYPTO, Aug. 2004, pp. 41–55.

[4] D. Johnson, Y. Hu, and D. Maltz, "The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4," IETFRFC4728, Feb. 2007. [Online]. Available: www.ietf.org/rfc/rfc4728.txt

[5] J. Kong and X. Hong, "ANODR: ANonymous on demand routing with untraceable routes for mobile ad hoc networks," in *Proc. ACM MobiHoc*, Jun. 2003, pp. 291–302.

[6] J. Kong, X. Hong, and M. Gerla, "ANODR: An identity-free and ondemand routing scheme against anonymity threats in mobile ad hoc networks," *IEEE Trans. Mobile Comput.*, vol. 6, no. 8, pp. 888–902, Aug. 2007.

[7] Y. Zhang, W. Liu, and W. Lou, "Anonymous communications in mobile ad hoc networks," in *Proc. IEEE INFOCOM*, Mar. 2005, vol. 3, pp. 1940–1951.

[8] K. E. Defrawy and G. Tsudik, "Privacy-preserving location-based on-demand routing in MANETs," IEEE J. Sel. Areas Commun., vol. 29, no. 10, pp. 1926–1934, Dec. 2011.

[9] M. G. Reed, P. F. Syverson, and D. M. Goldschlag, "Anonymous connections and onion routing," IEEE J. Sel. Areas Commun., vol. 16, no. 4, pp. 482–494, May 1998.

[10] M. Yu and K. Leung, "A trustworthiness-based QoS routing protocol for ad hoc networks," IEEE Trans.Wireless Commun., vol. 8, no. 4, pp. 1888– 1898, Apr. 2009.