ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

EAASR to Provide Anonymity Protection in Manet

V. Nandhini[1], A.Vijay [2]

III M.E., Dept of CSE, Karpagam University, Coimbatore, India[1]

Assistant Professor, Dept of CSE, Karpagam University, Coimbatore, India[2]

ABSTRACT*:* Anonymous communications are important for many applications of the mobile ad hoc networks (MANETs) deployed in adversary environments. An existing scheme is Anonymous Secure Routing (AASR), to satisfy the requirement and defend the attacks. More specifically, the route request packets are authenticated by a group signature, to defend the potential active attacks without unveiling the node identities. The key-encrypted onion routing with a route secret verification message, is designed to prevent intermediate nodes from inferring a real destination. But there is a chance for Timing and counter section attacks and lack of anonymity protection.

EAASR proposed to solve the existing problem. In this, 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/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.

KEYWORDS: AASR , protocol, EAASR

I. INTRODUCTION

MANETS rely on wireless transmission, a secured way of message transmission is important to protect the privacy of the data. An insecure ad-hoc network at the edge of communication infrastructure may potentially cause the entire network to become vulnerable to security breaches. There is no central administration to take care of detection and prevention of anomalies in Mobile ad hoc networks. Mobile devices identities or their intentions cannot be predetermined or verified. Therefore nodes have to cooperate for the integrity of the operation of the network. However, nodes may refuse to cooperate by not forwarding packets for others for selfish reasons and not want to exhaust their resources. Various other factors make the task of secure communication in ad hoc wireless networks difficult include the mobility of the nodes, a promiscuous mode of operation, limited processing power, and limited availability of resources such as battery power, bandwidth and memory. Therefore nodes have to cooperate for the integrity of the operation of the network. Nodes may refuse to cooperate by not forwarding packets for others for selfish reasons and not want to exhaust their resources

A community of ad-hoc network researchers has proposed, implemented, and measured a variety of routing algorithms for such mobile, wireless networks. While these ad-hoc routing algorithms are designed to generate less routing protocol traffic than the above-mentioned shortest-path routing protocols in the face of a changing topology, they nevertheless compute shortest-path routes using either topological information concerning the entire network, or topological information concerning the entire set of currently used paths between sources and destinations. Thus, their ability to find routes depends similarly on describing the current wide-area topology of the network to routers.

II. RELATED WORK

In [1] author presented ANODR, an anonymous on-demand routing protocol for mobile ad hoc networks deployed in hostile environments. We have addressed two close-related unlinkability problems, namely route anonymity and location privacy. Based on a route pseudonymity approach, ANODR prevents strong ad- versaries, such as node

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

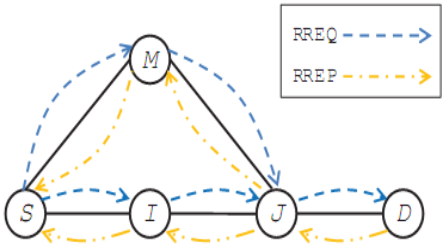
intruders and omnipresent eavesdroppers, from exposing local wireless transmitters' identities and tracing ad hoc network packet flows. Moreover, ANODR also demonstrates that untraceable data forwarding without encrypted routing header can be efficiently realized. [2] Geographical secure path routing, a privacy preserving ad-hoc routing protocol, which geographically routes messages through anonymous nodes to destination locations. The secure routing protocol also authenticates the public key and the geographic location of destination nodes. Geographical secure path routing protocol requires associative cryptographic one-way hash functions for security. These hash functions are derived from the discrete logarithm problem which uses expensive modular arithmetic. Superior resource provisioning of vehicular networks makes our solution suitable for securing location aware services on VANET. Geographical secure path routing protocol was evaluated with the NS2 network simulator for various values of node density, node mobility, and the proportion of malicious nodes. Evaluation results show that the protocol tolerates malicious nodes with an increased routing path length. The geographical secure path routing protocol is also able to maintain a low loss rate even when the majority of nodes are malicious. [3] The ALARM frame-work which supports anonymous location-based routing in certain types of suspicious MANETS. ALARM relies on group signatures to construct one-time pseudonyms used to identify nodes at certain locations. The frame-work works with any group signature scheme and any location-based forwarding protocol can be used to route data between nodes. Authors have shown through simulation that node privacy under this framework is preserved even if a portion of the nodes are stationary, or if the speed of movement is not very high. In [5] authors presented the design and evaluation of Ariadne, a new secure ad hoc network routing protocol. Ariadne provides security against one compromised node and arbitrary active attackers, and relies only on efficient symmetric cryptographic operations. Ariadne operates on-demand, dynamically discovering routes between nodes only as needed;the design is based on the basic operation of the DSR protocol. Rather than generously applying cryptography to an existing protocol to achieve security, however, we carefully re-designed each protocol message and its processing. The security mechanisms we designed are highly efficient and general, so that they should be applicable to securing a wide variety of routing protocols. Because we did not secure the optimizations of DSR in Ariadne, the resulting protocol is less efficient than the highly optimized version of DSR that runs in a trusted environment. In [8] authors presented a novel secure distributed anonymous routing protocol for MANET, which was referred as SDAR. authors have discussed the protocol and highlighted its main features, which include (i) Non-source-based routing (ii) Flexible and reliable route selection, and (iii) Resilience against path hijacking.

III. PROPOSED SYSTEM

A. *Description of the Proposed system:*

PATH DISCOVERY

- EAASR provides route anonymity, identity, and location anonymity of source and destination.
- Rather than relying on hop-by-hop encryption and redundant traffic, EAASR mainly uses randomized routing of one message copy to provide anonymity protection
- The source node broadcasts an RREQ packet to every node in the network.
- If the destination node receives the RREQ to itself, it will reply an RREP packet back along the incoming path of the RREQ.
- In order to protect the anonymity when exchanging the route information, the packet formats are to be redesigned, and modify the related processes.
- Source Node: We assume that S initially knows the information about D, including its pseudonym, public key, and destination string.
- The destination string dest is a binary string and can be recognized by D (as shown in Figure 1).
- If there is no session key, S will generate a new session key KSD for the association between S and D.



ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

Figure 1 : Path Discovery

ANONYMITY ANALYSIS

- Identity anonymity - EAASR adopt an encrypted secret VSD as the verification message in the RREP phase.
- Nv and Kv will be known by the intermediate nodes in route discovery, they are not related to the destination's identity. AASR provides better unidentifiability and unlinkability.
- Route anonymity - The source, intermediate, and destination nodes only have information about the nodes' pseudonyms of the previous and next hop.
- Even if a node participates in route discovery, it has no idea about the entire route, neither an exterior adversary.
- Location anonymity - The packet format of EAASR does not include any information related to the network topology and the number of participating nodes (such as TTL and sequence).
- Thus the inside malicious node cannot infer the network topology.

ATTACKER PREVENTION

- EAASR has a strategy to effectively counter intersection attacks, which have proved to be a tough open issue. EAASR can also avoid timing attacks because of its non fixed routing paths for a source-destination pair.
- Using "Malicious node detection" scheme to prevent the network from Active attackers.

IV. SIMULATION RESULTS

The simulation analysis for EAASR is implemented using Network Simulator NS2
The simulation is done for packet delivery ratio and delay whose results are shown in Figure 2 & 3 respectively.

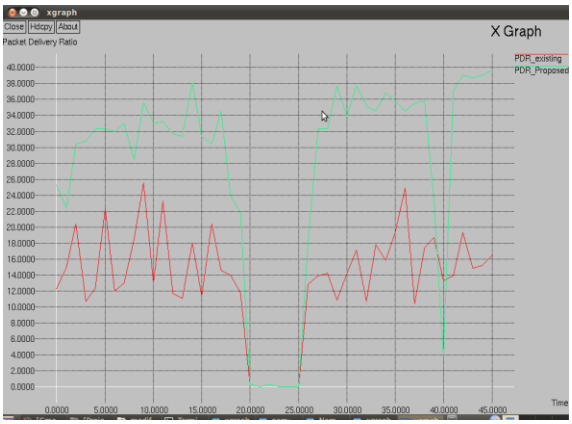


Figure 2 : Packet Delivery Ratio

The above figure shows that the Packet delivery ratio of the proposed system is better than the existing system.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

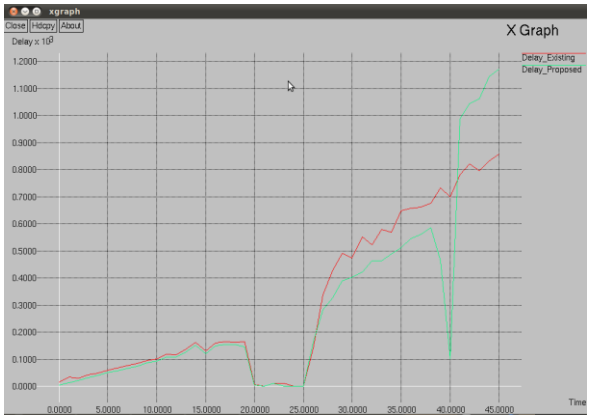


Figure 3 : Delay

The above figure shows that the delay ratio of the proposed system is better than the existing system.

V. CONCLUSION AND FUTURE WORK

An authenticated and anonymous routing protocol has been proposed for MANETs in adversarial environments. 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 designed to not only record the anonymous routes but also prevent the intermediate nodes from inferring the real destination.

Compared to AASR, EAASR provides higher throughput and lower packet loss ratio in different mobile scenarios in the presence of adversary attacks. It also provides better support for the secure communications that are sensitive to packet loss ratio. EAASR proposed to solve the existing's problem. Thus, EAASR offers anonymity protection to sources, destinations, and routes. It also has strategies to effectively counter intersection and timing attacks.

REFERENCES

1. Zhi Zhou and Kin Choong Yow , 'ANORD: Anonymous on demand routing with untraceable routes for mobile ad-hoc networks ', International Journal of Network security, Vol 2, PP 210-218, May 2006
2. Vivek pathak , Danfeng yao , Liviu iftode , 'Securing Location Aware Services Over VANET Using Geographical Secure Path Routing', Proc. ACM Mobile Com, pp. 134-146, 2003.
3. Karim El Defrawy , Gene Tsudik , 'ALARM: Anonymous Location-Aided Routing in Suspicious MANETs , Ad Hoc Networks, vol. 7, no. 5, pp. 918-931, July 2009
4. Karim El Defrawy , Gene Tsudik , PRISM: Privacy-friendly Routing In Suspicious MANETs (and VANETs)', IEEE Comm. Magazine, vol. 39, no. 6, pp. 138-147, June 2001.
5. Yih-Shun Hu & Adrian perrig , David B.Johnson ,'Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks' 2005 Springer science + Business Media Inc, Wireless Networks 11,21-38, 2005
6. Sylvia Ratnasamy, Brad karp, Scott shenker , Deborah Estrin , Ramesh govindan, Li yin and Fang yu , 'Data-Centric Storage in Sensor nets with GHT, A Geographic Hash Table', Mobile Networks and Applications on Wireless sensor networks, Kluwer, mid 2003.
7. Chao-chin chou, David Wei, Jay kuo, 'An Efficient Anonymous Communication Protocol for Peer-to-Peer Applications over Mobile Ad-hoc Networks', IEEE Journal on selected areas in communications , vol 25, no1 , Jan 2007.
8. Azzedine Boukerche, Khalil El-Khatib, Li Xu , Larry Korba, 'SDAR: A Secure Distributed Anonymous Routing Protocol for Wireless and Mobile Ad Hoc Networks', Proceedings of 29th Annual IEEE International Conference on Local Computer Networks 0742-1303/04
9. Bo Zhu, Zhiguo wan, Mohan Kankanhalli, Feng Bao, Robert Deng , 'Anonymous Secure Routing in Mobile Ad-Hoc Networks', Proceedings of 29th Annual IEEE International Conference on Local Computer Networks 0742-1303/04