ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 3, Issue 3 , March 2016

An improved Trusted Authority Routing protocol in Mobile Ad hoc Network

K.Papithasri, M.Thangamani

PG Scholar, Department Of Computer Science and Engineering,Knowledge Institute of Technology, Salem, India

PG Scholar, Department Of Computer Science and Engineering, RVS Technical Campus, Coimbatore, India

ABSTRACT: Many applications in Mobile ad hoc network (MANET) security are an important for adversary locations. To achieve security, it is important to be capable to authenticate messages between sensor nodes. While a number of anonymous secure routing protocols have been proposed, but the requirement is not fully satisfied. Existing protocol satisfies the requisite and protects the attacks. In this proposed system an Efficient Security for Trusted Authority Routing Protocol (ESTAR) in MANET which provides a framework to study the securitykey pre-distribution schemes. In this, a new key pre-distribution scheme is used which significantly increases the resilience of the network compared to previous approaches, and provided an in-depth study of the scheme in terms of network resilience and accompanying overhead. This proposed protocol shows a fine threshold property. To achieve security service, this paper consumes much less energy, however achieves higher security than existing works.

KEYWORDS: Security of Routing Protocols, Anonymous Routing, Authenticated Routing, Efficient Security for Trusted Authority Routing Protocol.

I. INTRODUCTION

Mobile Ad-hoc Networks (MANETs) are vulnerable to security threats due to the essential characteristics of networks, such as the dynamic topology and open wireless medium. It is hard to provide secure and trusted communications in adversarial surroundings such as battlefields. Ad-hoc network is used to prolonging the battery lifetime, minimize the energy efficiency, scalability and inherent. The adversaries outside a network may gather the information about the traffic flows by passive traffic observation or communicating nodes, even if the communications are encrypted. Hence, the nodes inside the network cannot be always reliable; meanwhile a valid node may be captured by enemies and then it becomes malicious. It results the anonymous communications are important for ad-hoc network in adversarial surroundings, in which the nodes credentials and routes are replaced by random numbers or aliases for security purpose.

MANETs are more vulnerable to both active and passive attacks by comparing it with wired networks. Numerous researchers have involved in designing protocols for various security related task such as authentication, confidentiality, key management, etc. A mobile ad-hoc network is a self-sufficient collection of mobile users that communicate over relatively bandwidth constrained wireless communications. Network scenarios that include establishing survivable, dynamic communication for emergency/rescue operations, efficient, military networks, and disaster relief efforts cannot depend on organized and centralized connectivity and may be considered as applications of Mobile Ad Hoc Networks. Due to the mobility of the nodes, network topology changes unpredictably and rapidly over time. These ascend the need of combining the routing functionality into nodes. Many security protocol suites have been designed and organized to protect wireless communication. Nevertheless, they do not give significance to anonymity protection and then it leaves mobile node to be traceable by wireless traffic analysts.

II. RELATED WORK

D. Kelly, R. Raines, R. Baldwin, B. Mullins, and M. Grimaila [1] presented about anonymity which is defined as the state of being unidentifiable within a set of subjects both in wired and wireless networks. The necessities of anonymous communications can be defined as a combination of unlinkability and unindentifiability. The main aim of

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 3, Issue 3 , March 2016

this is to improve suitable anonymous secure routing protocols. The authors of C. Perkins, E. Belding-Royer, S. Das [2] and D. Johnson, Y. Hu, and D. Maltz [3] proposed a different but related means of anonymizing mobile ad hoc on demand routing protocols such as AODV [2] and DSR [3].The anonymous security associations have to be established among every intermediate node along a route, the source and the destination.

After examining these protocols, we find that the objectives of unindentifiability and unlinkability are not fully satisfied. So that J. Kong, X. Hong, and M. Gerla [4] and J. Kong, X. Hong, and M. Gerla [5] proposed An identity-free and on demand routing(ANODR).It mainly focuses on protecting the route or node identities during a route discovery process, particularly on the routing packets. For example RREQ i.e. Route REQuest and RREP i.e. Route REPly. This proposed scheme adopts a global trapdoor message in RREQ, as a replacement for using the ID of the destination node. Though, the route can be identified by a disclosed trapdoor message that may be released to the intermediate nodes in backward RREP forwarding. A. Boukerche, K. El-Khatib, L. Xu, and L. Korba [6] presented the rely on the neighborhood detection and authentication. A Secure Distributed Anonymous Routing Protocol is proposed for its onehopneighbors are made to identify each other's ID during the routing procedures. Anonymous routing is becoming applicable in the present scenario of networks as there is an improved use of wireless networks. Wei Liu and Ming Yu [7] designed an authenticated and anonymous routing protocol named AASR for MANETs . In this paper, the route request packets are authenticated by group signatures. It can protect the possible active anonymous attacks without unveiling the node characteristics. From the above observations, it is difficult for the protocol to modify routing packet. This design results heavy packet loss.

III. PROPOSED SCHEME

In proposed protocol, a new routing protocol called an Efficient Security for Trusted Authority Routing Protocol (ESTAR) in MANET. This framework provides to study the securitykey pre-distribution schemes. In this, a new key pre-distribution scheme is used which significantly increases the resilience of the network compared to previous approaches, and provided an in-depth study of the scheme in terms of network resilience and accompanying overhead. This proposed protocol shows a fine threshold property. In this ESTAR, source nodes forward information to their respective trusted authority.

The information is collected and forward to destination by the trusted authority. The destination and trusted authority are usually form a single hop or multi-hop network. These are energy-efficient on demand routing protocols essential to be functional. The nodes are spited according to the radio range and then form a group of trusted supporters; each trusted group specifies a network thus form heterogeneous networks. The random pair-wise key scheme assigns a common key for trusted authorities. This proposed protocol reducing the delay, network overhead and also energy expenditure related with the secure data retrieval process.

A. Generating Digital Signatures

Consider two inputs for encryption.

1. Key
2. Data

Data is used for the write functions to generate some key values that will use as digital signatures.
It has been done by Trusted Authority node for neighborTrusted Authority nodes and its member's communications.

B. Key Distribution among Trusted Authority Node and its Members

Write a separate function for encode and decode which will encrypt the data and give one digital group signature is attached with request packet and as decode get an encrypted data as input then decrypt it. The encode function need two parameters which as data and the key in our project we used the node position as key. For decryption the key or digital group signature will be matched with the node id as well as its position if matched the node is in routing process else attacker.

Trusted Authority node and Trusted Authority node – Common keys Distribution

Members and Trusted Authority node – Pair wise keys Distribution

These functions should be embedded in routing protocol thus completion of proposed routing protocol.

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 3, Issue 3 , March 2016

IV. PERFORMANCE ANALYSIS

First, the necessary input parameters are needed to stipulate the Config.in file as said above. For simulation process, certain parameters are specified as mentioned below to enable hassle free simulation.

Terrain range – (500,500)

Number of nodes – 30

Number of nodes is a scalable simulator. Henceforth, they can be increased at will.

i) **Throughput**- Throughput, which is defined as the average number of messages that can be successfully decoded in each sensing period.

ii) **Average end-to-end delay**- The average time passed for delivering a data packet within a successful transmission.

iii) **Communication overhead**- The average number of transmitted control bytes per second with both the control packets and the data packet header.

iv) **Energy consumption**- The energy consumption for the entire network with transmission energy consumption for both the control and data packets.

Fig 4.1 and Fig 4.2 explains the performance level of the proposed protocol.

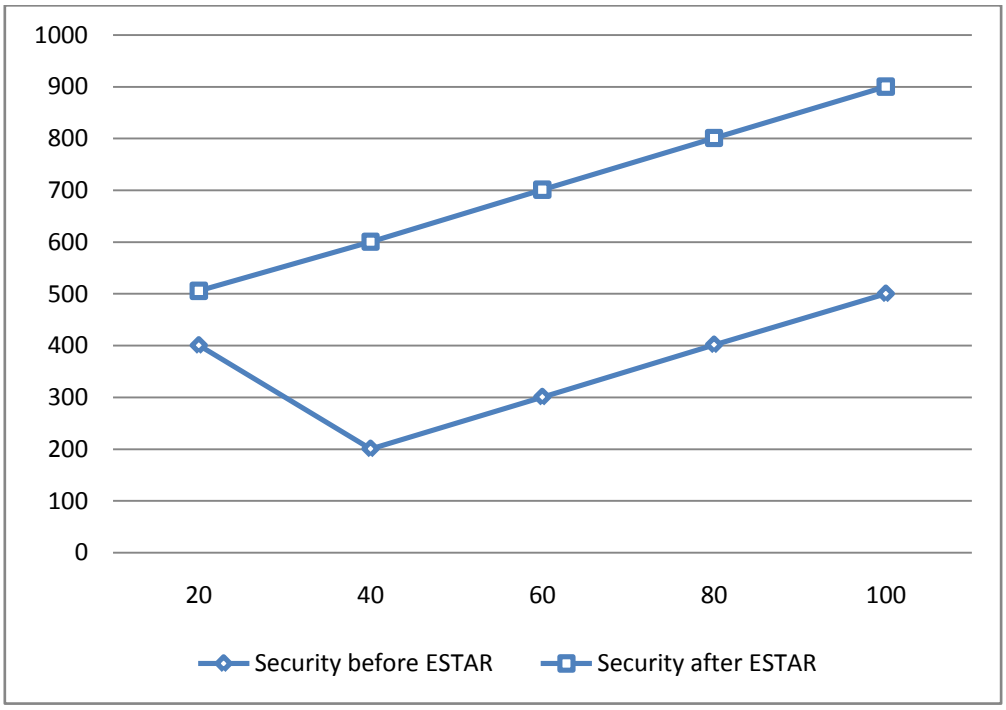

Fig. 4.1 Security Performance

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 3, Issue 3 , March 2016

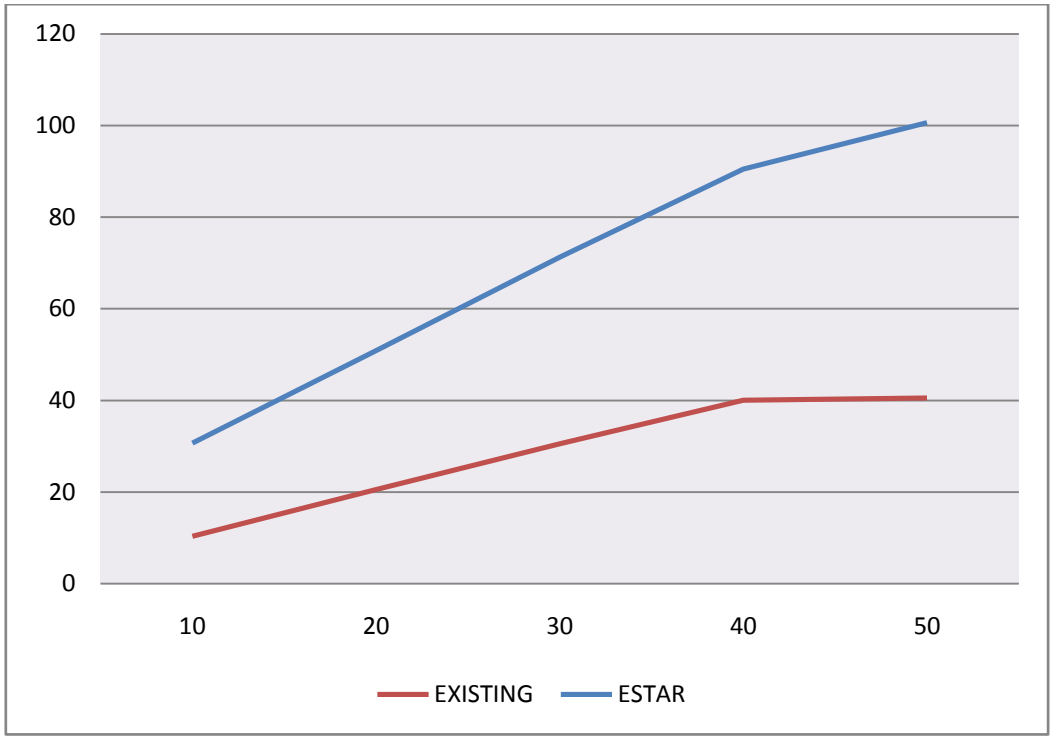

Fig. 4.2Overall Performances

Table 1.1 Comparisons between Existing and Proposed Protocol

Performance Metrics	**ExistingProtocol**	**ProposedProtocol**
Energy Utilization	High	Reduced
Collision Rate	High	Reduced
Throughput	Low	Improved
Security	Weak	Strong

V. CONCLUSION

To improve the secure key management, an Efficient Security for Trusted Authority Routing (ESTAR) Protocol is proposed in the networks. In most existing distributed key management schemes common assumptions to all the nodes have the same proficiency. However, existing works have suggested that connectivity and lifetime of a network can be significantly improved if some nodes are given greater transmission and power capability. Hence, how to exploit those features in design of an efficient distributed key management scheme has become an important problem. In proposed system nodes should use keying materials dynamically or to pre-distributed keys directly generate pair wise keys. In such a case, the proposed work is done an efficient way of distributing keys and keying materials to sensor nodes prior to deployment with better QOS. It also scales well to different network sizes and node densities under energy constraints.

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 3, Issue 3 , March 2016

REFERENCES

[1] D. Kelly, R. Raines, R. Baldwin, B. Mullins, and M. Grimaila, "Towards a taxonomy of wired and wireless anonymous Networks," in Proc. IEEE WCNC'09, Apr. 2009.
[2] C. Perkins, E. Belding-Royer, S. Das, *et al.*, "RFC 3561 - Ad hoc On- Demand Distance Vector (AODV) Routing," *Internet RFCs*, 2003.
[3] D. Johnson, Y. Hu, and D. Maltz, "RFC 4728 - The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4," Internet RFCs, 2007.
[4] J. Kong and X. Hong, "ANODR: ANonymousOn Demand Routing with Untraceable Routes for Mobile Ad hoc networks," in Proc. ACM MobiHoc'03, Jun. 2003, pp. 291–302.
[5] J. Kong, X. Hong, and M. Gerla, "ANODR: An identity-free and on demand routing scheme against anonymity threats in mobile ad hoc networks," IEEE Trans. on Mobile Computing, vol. 6, no. 8, pp. 888– 902, Aug. 2007.
[6] A. Boukerche, K. El-Khatib, L. Xu, and L. Korba, "SDAR: a Secure Distributed Anonymous Routing Protocol for Wireless and Mobile Ad hoc Networks," in Proc. IEEE Int'l Conf. Local Computer Networks (LCN'04), Nov. 2004, pp. 618–624.
[7] Wei Liu and Ming Yu, "AASR: Authenticated Anonymous Secure Routing for MANETs in Adversarial Environments", IEEE Transactions on Vehicular Technology, 2014.
[8] Y. Zhang, W. Liu, and W. Lou, "Anonymous communications in mobile ad hoc networks," in Proc. IEEE INFOCOM 2005, vol. 3, Mar. 2005, pp. 1940–1951.
[9] Y. Zhang, W. Liu, W. Lou, and Y. G. Fang, "MASK: Anonymous OnDemand Routing in Mobile Ad hoc Networks," IEEE Trans. on Wireless Comm., vol. 5, no. 9, pp. 2376–2386, Sept. 2006.
[10] L. Yang, M. Jakobsson, and S. Wetzel, "Discount anonymous on demand routing for mobile ad hoc networks," in Proc. Int. Conf. on SecureComm, Aug. 2006.

AUTHOR'S BIOGRAPHY

K.Papithasri is currently pursuing her M.E degree in Computer Science and Engineering from Anna university,Chennai in Knowledge institute of Technology,Salem.She has received her B.Tech degree in Information Technology from Anna University ,Chennai in Indus College of Engineering,Coimbatore.She has presented a paper in 5 International conference.She is a member of (IAENG) International Association for Engineers.

M.Thangamani is currently pursuing her M.E degree in Computer Science and Engineering from Anna university,Chennai in RVS Technical Campus, Coimbatore.She has received her B.E degree in Computer Science and Engineering from Anna University ,Chennai in Indus College of Engineering,Coimbatore. She has presented a paper in 3 International conference. She is a member of (IAENG) International Association for Engineers.