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. 2, Issue 3, March 2015

Authenticated Anonymous Routing Using Cryptography for MANETs

Mr. E. Sivanantham[1] G. Kamini[2]
[1]Associate Professor [2]PG Student
[2]Department of Electronics Communication Engineering
[1,2]Dhanalakshmi Srinivasan College of Engineering and Technology, Mamallapuram, India

Abstract— Mobile-ad hoc Networks are networks in which nodes are mobile and link connectivity might change all the time. Anonymous communications are important for many applications of the mobile ad hoc networks (MANETs) deployed in adversary environments.The requirement of the network is to provide unidentifiability and unlinkability for mobile nodes and their traffics. The routing protocol is authenticated anonymous secure routing (AASR), is to combine using advanced encryption standard(AES) and trust based routing is proposed to offer complete unlinkability and content of network unobservability. The effectiveness of AASR have implemented the security technique so that we can prevent the data loss at the time of transmission and also achieves strong protection.

Key words: MANETs, Advanced Encryption Standard , Authenticated Anonymous Secure Routing

I. INTRODUCTION

A mobile ad hoc network (MANET) is a collection of nodes that are connected through a wireless medium. It is lack of any kinds of fixed infrastructure that provide network management operations like the traditional fixed network. In this network each node both acts as a router and a host at the **same** time. In addition, every node moves irregularly and network topology changes frequently. Mobile ad hoc networks (MANETs) are vulnerable to security threats due to the inherent characteristics of such networks, such as the wireless medium and frequent dynamic network topology. It is difficult to provide secure communications in adversarial environments, such as battlefields. On one hand, the adversaries outside a network may infer the information about the communicating nodes. On the other hand, the nodes inside the network cannot be always trusted, since a trust node may be captured by enemies and becomes malicious. As a result, anonymous communications are important for MANETs in adversarial environments, in which deployment of nodes identifications and routes are replaced by random numbers for protection purpose.

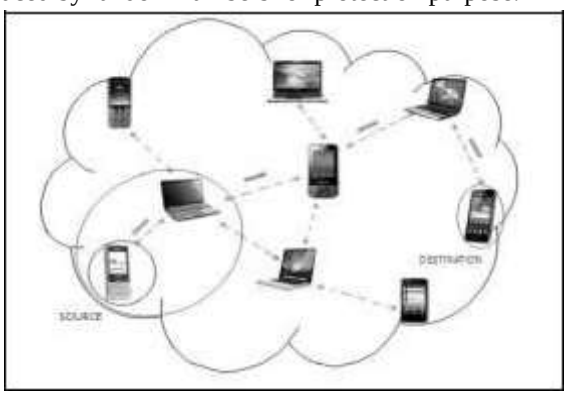

Fig. 1: Mobile Ad-Hoc Network

A. Anonymous Communication:

Anonymity is defined as the state of being unidentifiable within a set of subjects. In MANETs, the requirements of anonymous communications can be described as a combination of unindentifiability and route unlinkability. The reruirement of unindentifiability means that the identities of the source and destination nodes cannot be revealed to other nodes. Unlinkability means that the route and traffic flows between the source and destination nodes cannot be recognized or the two nodes cannot be linked. There are many anonymous routing protocols proposed in the past decade of adversial environment. The focus of protocol is the type of topology-based on-demand anonymous routing protocols, which are general for MANETs. To develop the anonymous protocols, a method is to anonymize the commonly used on-demand ad hoc routing protocols such as AODV and DSR. For this purpose, the anonymous security associations have to be established among source, destination and every intermediate node along a route.

Fig. 2: Anonymous Communication

II. RELATED WORK

A. Anonymous Routing Protocol for Mobile Ad Hoc Networks:

S. Seys and B. Preneel proposed the source and destination share a secret key and a secret pseudonym.

Anonymity is a very important part of the overall solution for identities of the source and destination nodes are anonymous to other nodes. The source will include this pseudonym in the route request message. The destination will have a number of pseudonym used by different sources its memory and it verifies whether the message is targeted at it or not. This pseudonym can be used only once. On the receipt of the reply message source starts to send the data along with the onetime identifier attached with them.

The One time identifier protects the data from the attacker. It is secure against both nodes actively participate in the network and a passive global adversary who monitors all network traffic.

B. MASK: Anonymous On- Demand Routing in Mobile Ad hoc Networks:

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. 2, Issue 3, March 2015

Y. Zhang, W. Liu, W. Lou, and Y. G. Fang proposed anonymous authentication with low cryptographic overhead

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. 2, Issue 3, March 2015

and high routing efficiency can be obtained by using proactive neighbor detection.

Mobile adhoc networks (MANETs) are finding ever increasing applications in both military and civilian operations. The shared wireless medium of mobile ad hoc networks provide passive, adversarial eavesdropping on data communications whereby adversaries can launch various attacks on the target network. The novel anonymous on-demand routing protocol named as MASK, which can accomplish both MAC-layer and network-layer communications. It offers the anonymity of senders, receivers, and sender-receiver relationships.

It uses a three-stage handshake for key exchanges among a node and its new neighboring nodes. After the method of handshake, each pair of nodes shares a chain of secret key and locally unique LinkID pair which corresponds to the pseudonyms used during handshake

C. USOR: An Unobservable Secure On- Demand Routing Protocol for Mobile Ad Hoc Networks:

Z. Wan, K. Ren proposed to protect privacy preserving routing is crucial for some ad-hoc networks that require stronger privacy protection.

The sensitive information such as mobility behaviour should be kept private from adversaries in wireless environments. However, none of these schemes offer complete unlinkability or unobservability property since data packets and control packets are still linkable. It uses a novel combination of group signature and ID based encryption for route discovery. The security analysis of routing not only provide strong privacy protection, also resistant against attacks.

III. PROPOSED STRATEGY

A mobile ad hoc network is a temporary infrastructure less network, formed by set of wireless mobile hosts that dynamically establish their own network without relying on any central administration. The authenticated anonymous secure routing (AASR), to satisfy the requirement and defend the attacks. Hence well known cryptographic algorithm such as AES Algorithm is used for providing a secure routing between mobile nodes even in presence of malicious nodes.

A. AASR Protocol:

Considering the nodal mobility of nodes, on-demand ad hoc routing as the base of protocol, including the phases of route discovery, data transmission and route maintenance. Assume that there is no online security or localization service available when the network is deployed. A possible method is to combine it with a trust based routing. In this approach, every group have trust node and this node must all information about destination. In the route discovery phase, the source node broadcasts Route Request packet to every trust node in the network. If the trust node receives the Route Request to itself, it will reply Route Reply packet back along the incoming path of the Route Request and forward to destination node. In order to protect the anonymity when exchanging the route information, we redesign the packet formats of the Route request and Route reply and modify the related processes.

B. Advanced Encryption Standard:

Cryptography is the study of mathematical techniques concerned with protecting information or data from adversaries. It provides security of information such as Availability, Authenticity, data confidentiality, Data integration and Non repudiation. Also it provides secure routing in MANETs.

The Advanced Encryption Standard algorthim is a Federal Information Processing Standards (FIPS) that can be used to encrypt and decrypt electronic data. AES is a symmetric block cipher to protect classified information and encrypt sensitive data. It is currently used to encrypt government classified information up to the top Secret level.

The Advanced Encryption Standard (AES) selected by Rijndael procedure to encrypt data and is useful to changed data for some communication . As encrypted, the data is unable to read if a key is not used to decrypt the message. AES is an iterated block cipher with a fixed block size of 128 and variable key length. It has fast speed and very low resources consumption. This algorithm is best and strongest cryptology algorithm because of security, cost and implementation.

The basic idea is used Advanced Encryption Standard (AES) algorithms to secure the data and maintained privacy between the sender and receiver which will improve the services provided by the MANET.

C. Protocol Evaluation:

Assume that all the nodes including on the discovered route are potential adversaries and privacy information about the two communication parties that discover the route.

1) Identity Anonymity: All the nodes generate random nonce to indicate themselves. Consequently, the intermediate nodes cannot acquire the identities of source and destination nodes.
2) Route Anonymity: During the route discovery, the source, intermediate and destination nodes only have information about the nodes pseudonyms of the previous and next hop of network.
3) Location Anonymity: It does not include any information related to the network topology and number of participating nodes. Thus the inside malicious node cannot infer the network topology.

D. Security Analysis:

Mobile Ad hoc networks are vulnerable to various attacks not only from outside but also from within the network itself. During deployment of nodes, security emerges as a central requirement due to many attacks that affects the performance of the ad hoc networks.

The basic idea behind is to use advanced Encryption Standard (AES) algorithms to secure the data and maintain privacy between the sender and receiver which will improve the services provided by the MANET.

1) DoS Attacks: It aims to deplete the nodes resources among the network topology. If the attacks are launched by the inside adversaries, more damage will be caused. However, once an inside adversary

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. 2, Issue 3, March 2015

Passive Attacks: It is a global eavesdropper and impossible for an eavesdropper to obtain the identity information about the source or destination node.

2) Authentication: This service verifies a user's identity and assures the recipient that the message is from the source that it claims to be from.

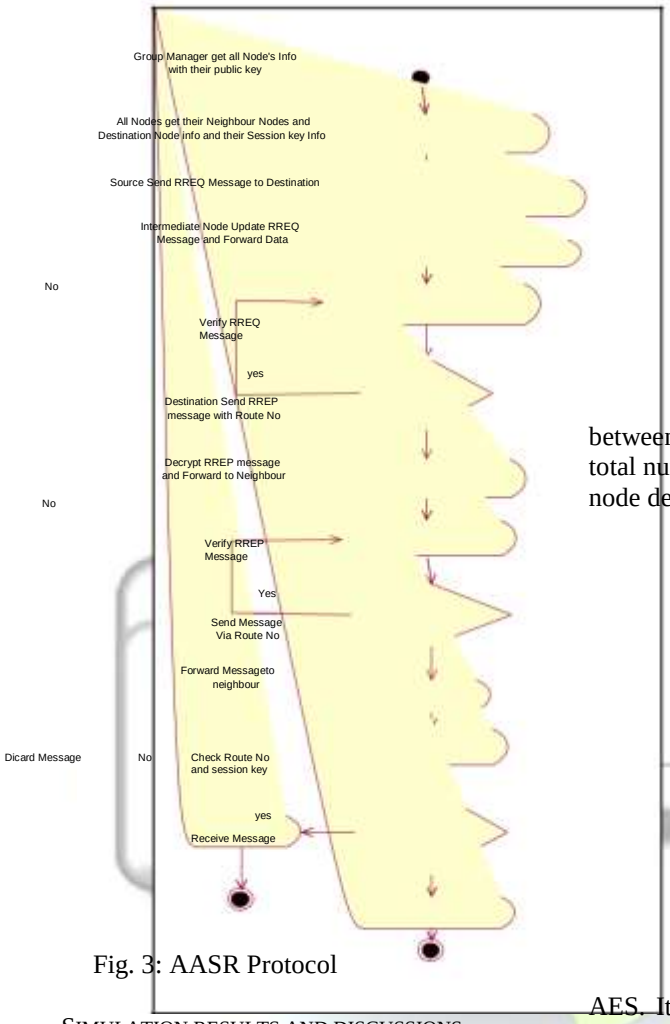

Fig. 3: AASR Protocol

IV. SIMULATION RESULTS AND DISCUSSIONS

The performance can be evaluated using algorithms and is simulated using NS-2 simulator. In the simulations, the network consisting of random numbers of nodes are generated. Thus, the algorithm results in achieving the routing from source to destination. Fig 4.1 represents data packet ratio versus time. In AASR protocol packet ratio is low compared to AODV.In existing protocols there is fake routing packets through denial of service attacks.But AASR provides higher data delivered.

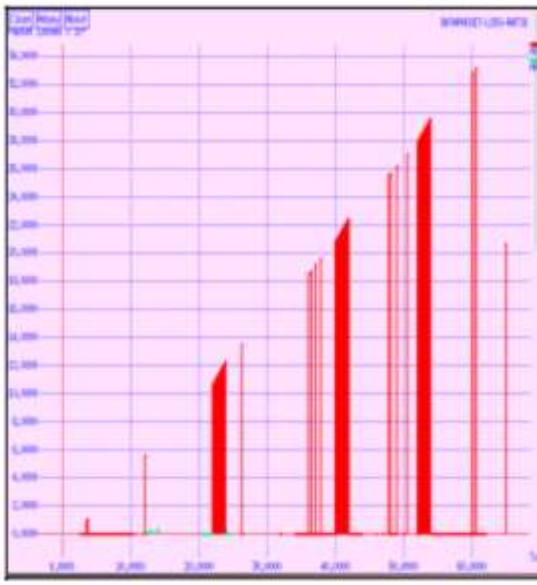

Fig. 4: Packet Loss Ratio

Fig 4.2 shows Node Delivery Ratio. It is the ratio between the number of packets delivered successfully to the total number of nodes to be delivered. This graph shows that node delivery is high for AASR compared to AODV.

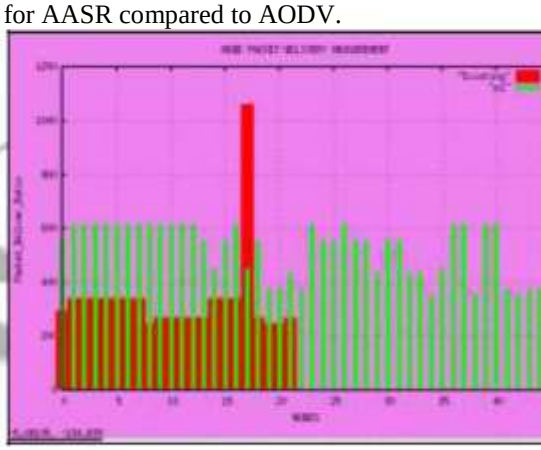

Fig. 5: Node Delivery Ratio

Fig 4.3 represents performance of protocol with AES. It is the packet reaches the destination by collecting the packets using trust based routing. Thus the AASR protocol used for encryption standard provides higher security in anonymous communication.

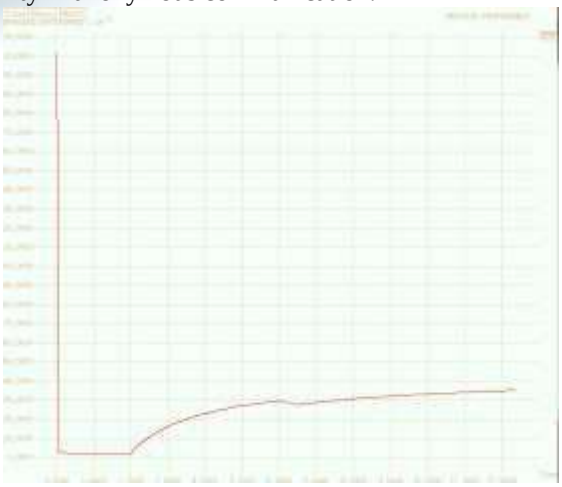

Fig. 6: Protocol Performance

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. 2, Issue 3, March 2015

Fig 4.4 represents throughput workload of protocol using AES encryption standard. The ratio of data delivered to the destination to the data sent out by the source.

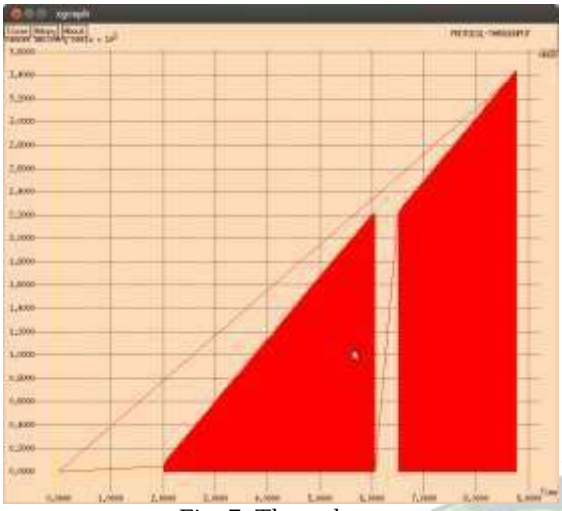

Fig. 7: Throughput

V. Conclusion

To design an authenticated and anonymous routing protocol for MANETs in adversarial environments for anonymous communication. AASR provides higher throughput and lower packets loss ratio in different scenarios in the presence of adversary attacks of network.The cryptographic approach such as Advanced Encryption Standard algorithm is used for secure routing in MANET.Therefore, malicious nodes can be detected since hop count field and sequence numbers are encrypted. Hence Latest sequence number packets are received by destination node and decreasing memory overhead. A possible method is to combine it with a trust based routing , the routing protocols will be more active in detecting link failures caused either by the mobility of nodes. As the security feature is much concentrated, it minimizes some delay and increases throughput. AES has excellent security, low resource consumption, high speed and ability to avoid collision attack of nodes.

In future work ,to improve AASR routing protocol using another standard encryption algorthim and increases security level for anonymous communication in MANET.

References

[1] J. Kong and X. Hong, "ANODR: ANonymous On Demand Routing with Untraceable Routes for Mobile Ad hoc networks," in Proc. ACM MobiHoc'03, Jun. 2003.

[2] Y. Zhang, W. Liu, and W. Lou, "Anonymous communications in mobile ad hoc networks," in Proc. IEEE INFOCOM 2005, vol. 3, Mar. 2005.

[3] Y. Zhang, W. Liu, W. Lou, and Y. G. Fang, "MASK: Anonymous On-Demand Routing in Mobile Ad hoc Networks," IEEE Trans. on WirelessComms.,Sept. 2006.

[4] S. William and W. Stallings, Cryptography and Network Security, 4th Edition. Pearson Education India, 2006.

[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] J. Paik, B. Kim, and D. Lee, "A3RP: Anonymous and Authenticated Ad hoc Routing protocol," in Proc. International Conf. on Information Security and Assurance (ISA'08), Apr. 2008.

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

[8] S. Seys and B. Preneel, "ARM: Anonymous Routing protocol for mobile ad hoc networks," Int. Journal of Wireless and Mobile Computing, vol. 3,no. 3, pp. 145–155, Oct 2009.

[9] K. E. Defrawy and G. Tsudik, "Privacy-Preserving Location-Based On- Demand Routing in MANETs," IEEE Journal on Selected Areas in Communications, vol. 29, no. 10, pp. 1926–1934, Dec. 2011.

[10] Z. Wan, K. Ren, and M. Gu, "USOR: An Unobservable Secure On-Demand Routing Protocol for Mobile Ad Hoc Networks," IEEE Trans. on Wireless Communication, vol. 11, no. 5, pp. 1922–1932, May. 2012.

[11] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in Proc. Int. Cryptology Conf. (CRYPTO'04), Aug. 2004.

[12] R. Song and L. Korba, "A robust anonymous ad hoc on-demand routing,"in Proc. IEEE MILCOM'09, Oct. 2009

[13] X. Hong, J. Kong, Q. Zheng, N. Hu, and P. Bradford, "A Hierarchical Anonymous Routing Scheme for Mobile Ad-Hoc Networks," in Proc. IEEE MILCOM'06, Oct. 2006.

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

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. 2, Issue 3, March 2015