Key Encrypted Onion Routing with Route Verification for MANETs

[1]Shweta K.Y, [2] Mrs. Mary Vidya John
[1]PG Scholar, [2] Assistant Professor
Department of Computer Science and Engineering
Vemana IT, Visvesvaraya Technological University, Belgaum, Karnataka, India.

***Abstract* - A mobile ad hoc network (MANET) is a continuous infrastructureless, selfconfigured network of mobile devices connected without wires. Particular devices in MANET is free to move independently in all directions, and therefore change its links frequently to other devices. The proposed system introduces a new routing protocol, which is used to authenticate anonymous secure routing protocol as Authenticated Anonymous Secure Routing(AASR), to satisfy the requirement andto defend the attacks like DoS. It chooses a high efficient energy shortest path to transfer the packets. The key encrypted onion routing with a route secret verification message is designed to prevent intermediate nodes from understanding a real destination. More specifically, the route request for the packets to be authenticated via a group signature, to defend the potential active attacks without introducing the node identities. By providing 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.**

1. INTRODUCTION

MANET's are vulnerable to security threats due to their inherent characteristics of network,such as the dynamic topology and open wireless medium. Itis difficult to provide secure and trusted communications inadversarial environments[5], such as battle fields. On one hand,the adversaries outside a network may try to infer the informationabout the communicating nodes or in traffic flow observation, even if the communications nodes are encrypted.On the other hand, the nodes inside the network cannotbe trusted always, since a valid node may be captured byuntrusted node and makes it malicious. As a result, in adversarial environment anonymouscommunications are important for MANETs, in which the identification of nodes and routesare replaced by random pseudonyms or numbers for protectionpurpose.

The anonymity[4] is defined as state of being unidentifiablewithin a set of subjects. In MANETs, anonymous communications is required to describe the combination of unindentifiability and unlinkability. Here unindentifiability means that the identities of the source and destination nodes cannot be revealed to the other nodes which are present in the network and unlinkability means thatthe route and traffic which flows between the source and destinationnodes cannot be recognized or the two nodes cannot be linked.The key for implementing the anonymous communications isto develop an appropriate anonymous secure routing protocols.

There are many anonymous routing protocols proposed inthe earlier authors, but the main focus is the type of topology basedon demand anonymous routing protocols with high efficient energy to choose the shortest path, by choosing the shortest path for multiple times the nodes energy get low. So, it's better to choose an alternative shortest path when other path node energy goes low. To develop theanonymous protocols, a direct common method is used to anonymize on demand ad hoc routing protocols, suchas Ad Hoc on Demand Routing Vector (AODV) and Dynamic Source Routing (DSR). For this purpose, the anonymous security associations has to be established among thesource, destination, and each intermediate node along the route. In this the resulting protocols include ANODR[3], SDAR,AnonDSR, MASK, and Discount ANODR.After examining these each protocols, it that the objectivesof unindentifiability and unlinkability are not satisfied fully.

By considering an example, Anonymous on Demand Routing (ANODR) which just focuses on protecting the node orroute identities during a route discovery process,speciallyon the routing packets, e.g., Route REQuest (RREQ)andRoute REPly (RREP). ANODR accepts a global trapdoormessage for RREQ, instead using the ID of the destinationnode. However, the route can find by using a disclosedtrapdoor message, which may be released to any of the intermediatenodes in backward RREP forwarding. The other protocols dependson the neighbourhood for detection and authentication purpose, but it maypartially violate the anonymity requirements for performanceconsiderations.

The protocols which are considered above also vulnerable to the Denial of Service(DoS) attacks, such as RREQ. Due to less number of packet authentication. So, it is difficult for the protocolsto check whether a packet has been modified by a maliciousnode or not. Most recently, group signature is introduced for the anonymousrouting.

The focus of MANETs in the adversarialenvironment, where the public and group key can be deployed initially in the mobile nodes. By assuming that there is no on line security or service available when the networkis deployed. This paper proposes an Authenticated Anonymous SecureRouting (AASR) to overcome above mentioned problems. Key encryption onion[10] is adopted to record a discovered route anddesign an encrypted secret message to verify the RREQ-RREPlinkage. The group signature is used to authenticate the RREQ packet per hop, so as to prevent intermediate nodes from getting modified bythe routing packet. For this extensive simulations are used to comparethe performance of the AASR to that of ANODR. The result showsthat, it provides higher throughput than the ANODR under thepacket dropping attacks, although AASR experiences more cryptographic operation delays.

The paper is organized as in section 2 deals with the related work and section 3 deals with protocol design.

2. BACKGROUND AND RELATED WORK

Anonymity and Security Primitives-Some common mechanisms have been introduced for widely used anonymous secure routing.

Trapdoor: A trapdoor is a common concept in cryptographic functions that defines a one way function between multiple sets. A global trapdoor is an information collection mechanism in which intermediate nodes may add information, such as node ID’s. Only for certain nodes, such as the source and destination nodes can unlock and retrieve the elements using pre mentioned secret keys. The usage of trapdoor requires an anonymous end to end key agreement between the source and destination.

Onion Routing: It is a mechanism to provide secure communications over the public network. Here the source node set up an onion core with a specific route message. While a route request phase, each forwarding node adds an encrypted layer to the route request message. Source and destination nodes do not know the ID of a forwarding node. When the destination node receives the onion, it delivers it back along the route to source. As the intermediate node verifies its role by decrypting the outer layer of the onion. Simultaneously, an anonymous route can be established.

Group Signature: Group signature[8] mechanism provides an authentications without disturbing the anonymity. In a group every member may has a pair of group public and private keys provided by the group trust authority. The member of a group signature can generate its own sign by its own private key, and such signature can be checked by other members in the group without revealing the signer’s group identity. But only the group authority trust can trace the signer’s identity and get back the group keys.

A. Short Group Signatures

To construct a short group signature scheme, signatures should be approximately the size of a standard RSA signature with the same security. The security of our group signature is based on strong Diffie Hellman assumption and the new assumption in a bilinear groups called Decision Linear assumption.

Group signatures, has been introduced by Chaum and Van Heyst, by providing anonymity for signers. Any member of a group can sign number of messages, but the resulting signature keeps the identity secret. In some systems there is a chance of third party presence that can trace the signature, or undo its anonymity using a special trapdoor messages. And some systems support revocation of messages where group membership can be selectively disabled without affecting the signing ability of the unrevoked members.

B. ARM: Anonymous Routing Protocol for Mobile Ad Hoc Networks

This paper describe a novel anonymous on demand routing protocol for MANETs, that is secure against both the nodes which actively participate in the network and in a passive global adversary who monitors all the traffic in network. Finally, it provides a detailed analysis of the privacy ordered by hiding the routes in limited broadcast groups, and for padding messages.

Whereas the wireless links that are used to connect nodes in a MANET are vulnerable to both active and passive attacks. Wireless transmissions are inherently easy to capture remotely and undetected in network, while the lack of central network management makes ad hoc networks susceptible for active attacks. Therefore, by providing security solutions for ad hoc networks is the primary importance for future large scale deployment got MANET’s.

C. ALARM: Anonymous Location-Aided Routing in Suspicious MANETs

In the most common MANET scenarios, nodes establishes the communication based on long lasting public identities. However, in some hostile and suspicious settings, node identities must not be exposed and node movements should not be traced. Instead, nodes need to communicate on the basis of their current locations. While such MANET settings are not common, they do occur in military and battle field domains and require high security and privacy.

In this paper, it address a number of issues arising in suspicious location based MANET settings by designing and analysing a privacy preserving and secure link state based routing protocol (ALARM). ALARM uses nodes current locations to securely disseminate and construct the topology snapshots and forward data. With use of advanced cryptographic techniques such as group signatures, ALARM provides security and privacy features including data integrity, anonymity, untraceability and node authentication. It also protect against passive and active attacks. To the best of the knowledge, its work represents the initial comprehensive study of security, privacy and performance trade off in the context of link state of MANET routing.

D. Privacy-Preserving Location-Based On -Demand Routing in MANETs

MANET’s are particularly useful and well suited for critical scenarios, including law enforcement and military, as well as in emergency rescue and disaster recovery.

While operating in hostile or in suspicious settings, MANETs require communication with security and privacy. Specially, in underlying routing protocols. Unlike in the most networks, where the communication is based on long term identities (i.e addresses), by arguing the location centric communication paradigm is better suited for privacy in suspicious MANET's. To this end, constructing an on demand location based anonymous MANET routing protocol (PRISM) that backup the privacy and security against both outsider and insider adversaries. By analysing the security, privacy and performance of PRISM and compare to its alternative techniques. Results show that PRISM is highly efficient and offers better privacy than prior work.

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

Privacy preserving routing is crucial for some ad hoc networks which require stronger privacy protection for wireless networks. A number of schemes has been proposed to protect privacy in networks. However, none of these schemes offered to complete the unlinkability or unobservability property since data packets and control packets are still linkable and distinguishable in this schemes. This paper, defines a stronger privacy requirements regarding privacy preserving routing in MANET's. Then by propose an Unobservable Secure Routing Scheme (USOR) to offer complete unlinkability and unobservability for all types of packets. USOR is efficient as it uses a unique combination of group signature and ID based encryption discover the route.

The security analysis demonstrates that USOR can protect well for the users privacy against both inside and outside attackers. USOR implement in Ns2, and evaluate its performance by comparing it with AODV and MASK. The simulation result shows that USORnot only has satisfactory performance compared with the AODV, but also back up the stronger privacy protection than existing schemes like MASK[6].

3. PROTOCOL DESIGN

In this section, it represent the design of onion routing protocol. Considering the mobility, taking an on demand ad hoc routing which is based on the proposed protocol, including the phases of data transmission, route discovery and route maintenance.

In route discovery phase, the source node broadcasts an RREQ packet to each node in the network. If the destination node receives the RREQ to itself, it will reply back an RREP packet back along the incoming path of the RREQ[12]. On other hand, to protect the anonymity while exchanging the route information, redesigning the packet formats of RREQ and RREP, and modify the related process. An example, using five node network to authenticate anonymous routing processes. The network is shown in Fig.1, in which the source node Sdiscovers a route to destination node D.

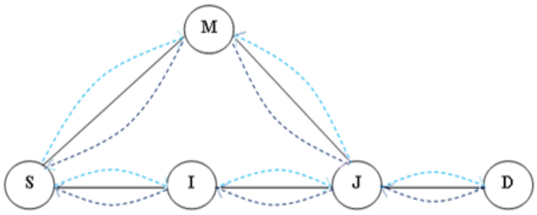

Fig.1: Network topology

Source Node: By assuming that source node S initially knows the information about destination node D, including the pseudonym, public key, and destination string. The destination stringis a binary string, which indicate "You the destination" and can be recognized by the D. If there is no session key provided, S will generate a new session key[14] as KSDfor the association between S and D.

Intermediate Node: We denote MANET by T and make the following assumption. The RREQ packet from source S is flooded in T. Now the focus is on an intermediate node I, which shown in Fig.1. By assuming that I has already generated the neighbour relationship with S and J then I knows where the RREQ packet comes from by decrypting the outer layer which has been encrypted by the source node itself.

Destination node: When the RREQ packet reaches D, Dvalidate it similarly to the intermediate nodes I or J. Since Dcan decrypt the part of the information, and it understand that it is the destination of the RREQ. Dcan obtain the session key KSD[15], and the validation key kv. Then destination D is ready to assemble an RREP packet to reply to source S route request.

Methodologies used

Onion encryption: It is a mechanism to provide secure communications over the public network. Here the source node set up the core of onion with a specific route message. During a route request phase, each and every forwarding node adds an encrypted layer to route request message. As the source and destination nodes do not necessarily know the ID of a forwarding node. When the destination node receives the onion then it delivers it back along the route to the source. Then the intermediate nodes can verify its role by decrypting and deleting the outer layer of the core onion which source has set up. Eventually the anonymous route can be established.

MD-5 algorithm: It is a message digest algorithm used for hashing. This also processes block wise, that is, the data is divided into a fixed length block. It processes variable length data into a fixed length data. The input data is divided into 512 bits of blocks. The padding is done to achieve equal length by padding single bit 1 and then adding as many 0 to attain the fixed length. The algorithm produces 128 bit long fingerprint or 32 words long.

By assuming that the shared key algorithm uses a keyedhashed MAC such as MD5. The following symbols used to denote the time consumed in the security mechanisms:

- Rencrypt: Encryption of Group public key
- Rdecrypt: Decryption of Group public key

- Rsign: Signature of Group private key
- Rverify: Verification of Group private key
- Esymm: Symmetric key of encryption or decryption.
- Onion: One layer onion construction or destruction.

CONCLUSION

In this paper, an authenticated and anonymous routing protocol for MANETs in adversarial environment have been designed. Where the route request packets are authenticated by using group signatures, which defend the potential of active anonymous attacks without revealing the node identities. The key encrypted onion routing with a route secret verification message is designed not only to record the anonymous routes but also to prevent the intermediate nodes from getting infer to the real destination. In future work, we will improve the energy efficiency which is been lost while transferring the information, by making use of choosing another shortest path with high efficient energy.

REFERENCES

[1] D. Kelly, R. Raines, R. Baldwin, B. Mullins, and M. Grimaila, “Towards a taxonomy of wired and wireless anonymous Networks,” in Proc. IEEEWCNC’09, Apr. 2009.

[2] J. Kong and X. Hong, “ANODR: ANonymousOn Demand Routing with Untraceable Routes for Mobile Ad hoc networks,” in Proc. ACMMobiHoc’03, Jun. 2003, pp. 291–302.

[3] 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. on Mobile Computing, vol. 6, no. 8, pp. 888–902, Aug. 2007.

[4] 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.

[5] 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.

[6] Y. Zhang, W. Liu, W. Lou, and Y. G. Fang, “MASK: Anonymous On-Demand Routing in Mobile Ad hoc Networks,” IEEE Trans. on WirelessComms., vol. 5, no. 9, pp. 2376–2386, Sept. 2006.

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

[8] D. Boneh, X. Boyen, and H. Shacham, “Short group signatures,” in Proc. Int. Cryptology Conf. (CRYPTO’04), Aug. 2004.

[9] K. E. Defrawy and G. Tsudik, “ALARM: Anonymous Location-Aided Routing in Suspicious MANETs,” IEEE Trans. on Mobile Computing, vol. 10, no. 9, pp. 1345–1358, Sept. 2011.

[10] 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.

[11] R. Song and L. Korba, “A robust anonymous ad hoc on-demand routing,” in Proc. IEEE MILCOM’09, Oct. 2009.

[12] 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.

[13] X. Wu and B. Bhargava, “AO2P: Ad Hoc On-Demand Position-Based Private Routing Protocol,” IEEE Trans. Mobile Computing, vol. 4, no. 4, pp. 335–348, July/Aug. 2005.

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

[15] H. Shen and L. Zhao, “ALERT: An Anonymous Location-based Efficient Routing Protocol in MANETs,” IEEE Trans. on Mobile Computing, vol. 12, no. 6, pp. 1079–1093, 2013.

[16] M. Yu, M. C. Zhou, and W. Su, “A secure routing protocol against Byzantine attacks for MANETs in adversarial environment,” IEEE Trans.on Vehicular Tech., vol. 58, no. 1, pp. 449–460, Jan. 2009.

[17] 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.

[18] C. Perkins, E. Belding-Royer, S. Das, *et al.*, “RFC 3561 - Ad hoc On-Demand Distance Vector (AODV) Routing,” *Internet RFCs*, 2003.

[19] D. Johnson, Y. Hu, and D. Maltz, “RFC 4728 - The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4,” *InternetRFCs*, 2007.

[20] R. Song, L. Korba, and G. Yee, “AnonDSR: efficient anonymous dynamic source routing for mobile ad hoc networks,” in *Proc. ACM WorkshopSecurity of Ad Hoc and Sensor Networks (SASN’05)*, Nov. 2005.

[21] L. Yang, M. Jakobsson, and S. Wetzel, “Discount anonymous on demand routing for mobile ad hoc networks,” in *Proc. Int. Conf. onSECURECOMM’06*, Aug. 2006.

[22] J. Paik, B. Kim, and D. Lee, “A3RP: Anonymous and Authenticated Ad hoc Routing protocol,” in *Proc. International Conf. on InformationSecurity and Assurance (ISA’08)*, Apr. 2008.

[23] M. G. Reed, P. F. Syverson, and D. M. Goldschlag, “Anonymous Connections and Onion Routing,” *IEEE Journal on Selcted Area inComm.*, vol. 16, no. 4, pp. 482–494, May 1998.

[24] 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.

[25] M. Brown, D. Hankerson, J. L´opez, and A. Menezes, *Software implementation of the NIST elliptic curves over prime fields*. Springer, 2001.

[26] M. Scott, “Miracl – multiprecision integer and rational arithmetic c/c++ library,” *Shamus Software Ltd, Dublin, Ireland*, 2003.