International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 6 318 - 320

A Survey on Anonymous On-Demand Routing Protocols for MANETs

Sunetra P. Salunkhe[#1]
Master Student, Computer Engineering,
SSVPS's B.S.Deore College of Engineering,
Dhule, India
salunkhesunetra.p@gmail.com

Dr. Hitendra D. Patil[#2]
Professor and Head, Computer Engineering,
SSVPS's B.S.Deore College of Engineering,
Dhule, India
hitendradpatil@gmail.com

Abstract **-** At present Mobile ad hoc networks (MANET) is used in many real time applications and hence such networks are vulnerable to different kinds of security threats. MANET networks suffered more from security attacks due to use of free wireless communication frequency spectrum and dynamic topology. Therefore it becomes very tough to provide security to MANET under different adversarial environments like battlefields. For MANET, anonymous communications are vital under the adversarial environments, in which the identification of nodes as well as routes is replaced by pseudonyms or random numbers for the purpose of protection. There are many protocols presented for anonymous communication security for MANET, which hide node identities and routes from exterior observers in order to provide anonymity protection. This paper presents review of various anonymous on demand routing protocols.

Keywords **-** *MANET, Anonymous Routing, On-Demand Routing.*

*****

I. INTRODUCTION

Mobile Ad-hoc Network (MANET) is a wireless and dynamic topology network medium which suffers from many open security issues. The major issue is to send information in secure manner from source to destination node in rival environment (node traffic, node attack, data accessing of intermediate nodes). MANET routing protocols basically divided into two categories namely, topology based and position based. Node identity centric protocols classified into reactive (on demand) and proactive (table driven) protocols. For this purpose, the anonymous security associations must be set up among the source, destination, and each intermediate node along a route. There are many routing protocols proposed in last decade. These protocols are vulnerable to security threats.

In MANET it is difficult to provide trusted and secure communications in adversarial situations, such as battlefields. On one hand, the adversaries case a network may reason the information about the conveying nodes or traffic streams by passive traffic observation, even if the communications are encrypted. Then again the nodes interior the network can't be perpetually trusted, subsequent to a valid node might be caught by adversaries and becomes malicious [3]. Node identifications and routes are replaced by random numbers or aliases for protection purposes in adversarial environments of MANETs.

II. LITERATURE SURVEY

Many anonymous on-demand routing protocols have been proposed which uses different approaches for anonymous routing.

- ***Cryptography and Network Security using trapdoors***

Trapdoor is a typical system in cryptographic functions that is generally utilized as a part of anonymous secure routing. Trapdoor defines a one-way function between two sets. A global trapdoor is a data gathering mechanism in which moderate nodes may include information elements. Only source and destination nodes can open and recover the elements using pre-established secret keys. The utilization of trapdoor requires an anonymous end-to-end key understanding between the source and destination [1].

- ***Anonymous Connections and Onion Routing***

This mechanism is utilized to give private interchanges over an open system. The source node sets up the center of an onion with a specific route message. Each sending node attaches an encrypted layer to the route request message during a route request phase. The source and destination nodes do not essentially know the ID of a sending node. The destination node accepts the onion and conveys it along the route back to the source. The intermediate node can confirm its part by decrypting and deleting the external layer of the onion. Eventually an anonymous route can be set up [2].

- ***Short Group Signatures***

Group signature scheme [3] can give validations without upsetting the anonymity. Each member in a group may have a couple of group public and private keys issued by the group trust power. The member can create its own signature by its own private key, and such signature can be confirmed by different individuals in the group without uncovering the signer's identity. Only the group trust authority can follow the signer's identity and revoke the group keys.

There are number of anonymous routing protocols associated with the on demand routing.

- ***Ad hoc On-Demand Distance Vector Routing Protocol (AODV)***

C. Perkins, E. Belding-Royer, S. Das (2003), proposed the Ad hoc On-Demand Distance Vector (AODV) routing protocol, which is expected for use by mobile nodes in an ad hoc network. It offers quick adjustment to element association conditions, low processing and memory overhead, low network utilization, and decides unicast routes to destinations within the ad hoc network. It utilizes destination sequence numbers to guarantee loop freedom at all times, avoiding problems like "counting to infinity", associated with traditional distance vector protocols [4].

- ***Anonymous on Demand Routing with Untraceable Routes for Mobile Ad hoc Networks (ANODR)***

J. Kong et.al (2003) proposed a methodology which comprises of three stages. Anonymous route discovery, Anonymous route preservation and Anonymous route forwarding. Route discovery phase contains route request and route reply message. It implements 1) symmetric key harmony between two back to back RREP forwarders and 2) implements destination-started RREP strategy. The worldwide trapdoor holds mystery data for the planned destination and an open duty for the same destination. RREP receipt from the destination is obtained to avoid an adversarial network node to send back fake RREPs to disturb ANODR. Routing table entries are recycled for the maintenance of the anonymous route. As the movement of the nodes increases, performance of ANODR decreases. Trapdoor data is utilized as a part of this yet it is not reasonable since the destination node does not know which shared session key ought to be utilized for the trapdoor if the destination node has numerous mutual session keys so the route can be recognized by an unveiled trapdoor message, which might be discharged to the middle of the road nodes in reverse RREP sending [5], [6].

- ***A Secure Distributed Anonymous Routing Protocol for Mobile and Wireless Ad Hoc Networks (SDAR)***

Boukerche et.al (2004) proposed a protocol which permits only the reliable nodes to participate in transmission. The source node does not require gathering information about the topology of the network; it broadcasts the path disclosure message with some trust prerequisite, the intermediate nodes fulfilling the trust, embeds its ID and session key and encrypts the message. This message achieves the destination and the it gets decrypted in each intermediate node and achieves the source. Source node obtains complete information about the intermediate nodes. Neighborhood nodes IDs are potentially uncovered. This protocol uses multicast mechanism and layered encryption. SDAR is not secured against Denial of Service attack. Messages are vast and rely on the quantity of bounces. This protocol restrains the efficiency [7].

- ***Anonymous Dynamic Source Routing For Mobile Ad-Hoc Networks (AnonDSR)***

R. Song et.al (2005) provides three levels of security assurance. This routing comprises of three protocols. The first protocol is utilized to make shared key and a nonce between the source and the destination for the safe correspondence. The second protocol utilizes the mutual key and the nonce to make a trapdoor and utilize anonymous onion routing between the source and the destination. In the last protocol the source and the destination utilizes their session key imparted to the intermediate nodes to encrypt all interchanges with the cryptographic onion technique. The anonymous route establishment relies upon the quantity of jumps between the source and the destination; time will be increased as number of hops increases. The halfway hubs on the way might be uncovered to the destination hub [8].

ANODR, SDAR, and AnonDSR utilize a cryptographic onion structure to develop the routing message. Each transitional node and destination node needs to perform asymmetric encryption/decryption and signature operations, which have high computational intricacy and use significant CPU time. So they have adaptability issues for huge scale systems.

- ***MASK (A novel anonymous on demand routing protocol to achieve anonymous MAC-layer and network layer communication)***

Y. Zhang et.al (2005) says that anonymous verification with low cryptographic overhead and high routing efficiency can be acquired by using proactive neighbor identification. MASK depends on a unique sort of open key cryptosystem, the pairing-based cryptosystem, to accomplish unknown correspondence in MANET. MASK requires a trusted authority to produce adequate sets of secret points and corresponding pseudonyms as well as cryptographic parameters. Henceforth the setup of MASK is very costly and might be helpless against key pair depletion attacks. The RREQ flag is not protected and this empowers a latent enemy to find the source node. In route request packets destination node's identity is clear. Though this would not reveal the identity of destination node, an adversary can easily recuperate linkability between various RREQ packets with the same target, which actually violates receiver anonymity. A clear node ID is used in the route discovery [9], [10].

- ***Discount Anonymous On Demand Routing For Mobile Ad Hoc Networks (Discount-ANODR)***

Liu Yang et.al (2006) provides the same system of ANODR at a lower cost. It utilizes the same techniques utilized as a part of ANODR. It has the advantage of accomplishing considerably lower computation and correspondence complexities at the cost of expense of a slight lessening of security insurances. Route requests in Discount-ANODR and in ANODR are parallel but the limitation is that intermediate nodes only know the destination of the request and the identity of the previous intermediate node but not the source node [11].

- ***Anonymous Authentication Protocol in Mobile Ad Hoc Networks (ANAP)***

Tomasz Ciszkowski et.al (2006) presented an Anonymous Authentication protocol which is improved with distributed reputation system. The presumed appropriated framework is fused with trust administration. Reputation depends on the time, own past knowledge, second hand data and it is expressed by level of trust. The end to end unknown confirmation is led in three-stage handshake. The three stages are Anonymous authentication introduction, Anonymous reply, and Anonymous verification. After the effective verification, different unknown information channels are set up. The computational effect on the hubs is high [12].

- ***Anonymous and Authenticated Ad Hoc Routing Protocol (A3RP)***

J. Pail et.al. (2008) proposed Anonymous and Authenticated Ad Hoc Routing Protocol. In A3RP, the routing and information packets are protected by a group signature. It is very important to provide the anonymity to the ad hoc routing protocol so that the protocol preserves the privacy of route information. Lack of authentication, causes basic security issues such like impersonation or the forgery of packet. However, the anonymous route is figured by a secure hash function, which is not as versatile as the encrypted onion mechanism [13].

- ***Anonymous Routing Protocol for Mobile Ad Hoc Networks (ARM)***

Stefaan Seys et.al (2009) presents an anonymous on demand routing design for MANETs. The source and the destination share a secret key and a secret alias. The source will incorporate this alias in the route request message. The destination will have a rundown of alias by various sources in its memory and it checks whether the message is focused at it or not. This pseudonym can be utilized once. The destination sends the reply with the same pseudonym. On the receipt of the reply message source begins to send the data next to the onetime nonce connected with them. One time identifier shields the information from the aggressor. Delay increases when the network size is extensive. ARM assumes that the source and destination nodes share a durable session key in advance, which is not handy for genuine MANETs [14].

- ***Robust Anonymous Ad-hoc On Demand Routing (RAODR)***

R. Song et.al (2009) proposed RAODR which is based on an anonymous neighborhood trust model utilizing an expert key and pseudonym certificates to provide a powerful, secure, anonymous, and versatile routing protocol for mobile ad hoc networks. It cannot give the anonymity, traceability, and enforceability that are supported by a group signature [15].

- ***Unobservable routing protocol (USOR)***

Z. Wan et.al. (2012) proposed an Unobservable routing protocol (USOR) taking into account group signature, secure hash functions and ID-based cryptosystem for ad hoc networks. The configuration of USOR offers strong privacy insurance, complete unlinkability and content unobservability for ad hoc networks. USOR scheme not safe against wormhole and DoS attacks [16].

III.CONCLUSION

In this paper, all the anonymous on demand routing protocols discussed in the literature survey focuses on providing anonymous protection to the data sources, destination, and routes. They have their own advantages and disadvantages. Most of the anonymous routing protocols provide anonymous protection with increase in delay.

REFERENCES

[1] S. William and W. Stallings, *Cryptography and Network Security*, 4th ed. Delhi, India: Pearson Education India, 2006.
[2] 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.
[3] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures", in *Proc. CRYPTO*, pp. 41–55, Aug. 2004.
[4] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing," IETF RFC 3561, Jul. 2003.
[5] J. Kong and X. Hong, "ANODR: ANonymous on demand routing with untraceable routes for mobile ad hoc networks", in *Proc. ACM MobiHoc*, pp. 291–302, Jun. 2003
[6] 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. Mobile Comput.*, vol. 6, no. 8, pp. 888–902, Aug. 2007.
[7] 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. Conf. LCN*, pp. 618–624, Nov. 2004.
[8] R. Song, L. Korba, and G. Yee, "AnonDSR: Efficient anonymous dynamic source routing for mobile ad hoc networks", in *Proc. ACM Workshop SASN*, pp. 33–42, Nov. 2005.
[9] Y. Zhang, W. Liu, and W. Lou, "Anonymous communications in mobile ad hoc networks", in *Proc. IEEE INFOCOM*, , vol. 3, pp. 1940–1951, Mar. 2005.
[10] Y. Zhang, W. Liu, W. Lou, and Y. G. Fang, "MASK: Anonymous on-demand routing in mobile ad hoc networks", *IEEE Trans. Wireless Commun.*, vol. 5, no. 9, pp. 2376–2386, Sep. 2006.
[11] L. Yang, M. Jakobsson, and S. Wetzel, "Discount anonymous on demand routing for mobile ad hoc networks", in *Proc. Int. Conf. SECURECOMM*, pp. 1–10, Aug. 2006.
[12] Tomasz Ciszkowski and Zbigniew Kotulski, "ANAP: Anonymous Authentication Protocol in Mobile Ad hoc Networks", Warsaw University of Technology, 2006.
[13] J. Paik, B. Kim, and D. Lee, "A3RP: Anonymous and authenticated ad hoc routing protocol", in *Proc. Int. Conf. ISA*, pp. 67–72, Apr. 2008.
[14] S. Seys and B. Preneel, "ARM: Anonymous routing protocol for mobile ad hoc networks", *Int. J. Wireless Mobile Comput.*, vol. 3, no. 3, pp. 145– 155, Oct. 2009.
[15] R. Song and L. Korba, "A robust anonymous ad hoc on-demand routing," in *Proc. IEEE MILCOM*, pp. 1–7, Oct. 2009.
[16] Z.Wan, K. Ren, and M. Gu, "USOR: An unobservable secure on-demand routing protocol for mobile ad hoc networks", *IEEE Trans. Wireless Commun.*, vol. 11, no. 5, pp. 1922–1932, May 2012.