A Secured On-Demand Routing Protocol for Mobile Ad-Hoc Network - A Literature Survey

K.Vinayakan[1], Dr.M.V.Srinath[2]
[1] Assistant Professor, Department of Computer Applications, STET Womens College, Mannargudi.
[2]Director, Department of Computer Applications, STET Womens College, Mannargudi

E-mail Id: k.vinayakan@gmail.com[1], sri_induja@rediffmail.com[2]

Abstract: The essential feature for Ad-hoc networks is security in-terms of communication. It is the major requirement for a network. Due to mobility and wireless nature of nodes, this secure communication becomes critical. In Mobile Ad-hoc Networks, for the purpose of stronger privacy protection various schemes were introduced. The security features provided by MANET to the mobile users are authentication, confidentiality, integrity, anonymity and availability. In this paper, we have made a detailed theoretical study on efficient unobservable routing scheme that provides complete unlinkability and content observability for data packets and control packets. We have also analyzed some existing routing scheme and proved the unobservable routing scheme is very efficient. It ensures high packet delivery ratio and average packet delivery latency.

Keywords: MANET,On demand Routing Protocols, Review Analysis, Optimization, Performance Metrics.

1.INTRODUCTION

Mobile ad-hoc networks - A MANET is a specific type of ad hoc network which can change the locations and configure itself. It is also known as wireless mesh network in which the mobiles are connected by wireless link shown in Fig 1. The independent mobile nodes communicate to each other directly or indirectly through radio waves.

Fig 1. Mobile Adhoc Network

The essential feature in MANET is secrecy preserving, compared with wired environment because of its both static and dynamic topologies with enhanced dynamics due to node motion or other factors. Comparing with wired networks it is hard to gain the access of the cable and there is no mobility in the network. Providing secrecy preservation in MANET is a very challenging task.

In mobile ad-hoc networks, preserving the secret during the communication of nodes in the network are emphasized through three terms. They are as follows[1]

1.Anonymity

2.Unlinkability

3.Unobservability

ANONYMITY: In the network, the node that are not identified in a network refers to anonymity. The sender, receiver and intermediate nodes are not known to other neighbouring nodes.

UNLINKABILITY: The nodes available in the MANET are secured from the intruder.

UNOBSERVABILITY: During Transmission from sender to receiver in MANET, all the packets are similar to other nodes and are difficult to distinguish the data packets from other packets[14].

Secured routing in MANET is accomplished by implementing the above factor in all the nodes of the network. In MANET, all the nodes perform both the activities like host and routers. These nodes are always independent to each other. Therefore, while designing the structure of MANET, the major factor namely secured routing has to be considered.

2. Related Works

J. Kong and X. Hong, [3] described Anonymous On Demand Routing (ANODR) protocol for MANET deployed in military environments.For route anonymity, the protocol prevents strong enemies from tracking the transmission of packets in the network.,the protocol ensures that enemies cannot identify the identities of transmitters. S. Seys and B. Preneel, [5] suggest a novel ANODR scheme for MANETs and propose aanonymity solution for a stronger adversary model. Y. Dong, T. W. Chim, [6] focus on the needs of securing and robustness, an ideal routing protocol should not present the identity information of the nodes in the route. Due to broken links and to increase the complexity of traffic analysis Multiple routes should be established.The protocol has the ability to create fake routes to

confuse the enemies, thus increasing the level of anonymity. A. Boukerche, K. El-Khatib, [7] describes a distributed routing protocol which ensures the high reliability, securityand anonymity of the discovered route in MANET, by encrypting routing packet header. D. Sy, R. Chen, and L. Bao, [8] suggest an On Demand Anonymous Routing (ODAR) protocol based on bloom filters for wireless ad hoc networks to enable complete anonymity of nodes.It provides node, link and path anonymities in ad hoc networks based on Bloom filters. The use of Bloom filters additionally gives ODAR the storage, processing and communication efficiencies, making it suitable in the ad hoc network environments with mechanisms to efficiently store source routes anonymously, and to forward data packets anonymously. A key management mechanism is described in order to provide strong anonymity for end-to-end communications.

3. Classification of on Demand Routing Protocol.

Classification of on demand routing protocols is based on routing strategy and network structure. On demand routing protocol are source initiated protocols. When the node needs a route to destination, source will initiate a route discovery process and establish the route. Once the route is established route discovery process is completed and the routine for route maintenance keeps track on the authentic nodes and false nodes. The route remains valid in the routing table till the route is no longer needed or the destination is reachable.

The classification of on demand routing protocol is depicted in Fig 2 are based on the routes created which broadcast the packets. A few on demand routing protocols are Dynamic Source Routing Protocol (DSR),Cluster Based Routing Protocol(CBRP), Ad hoc On-demand Distance Vector Routing (AODV), The Temporally Ordered Routing Algorithm (TORA) and Associativity Based Routing (ABR).

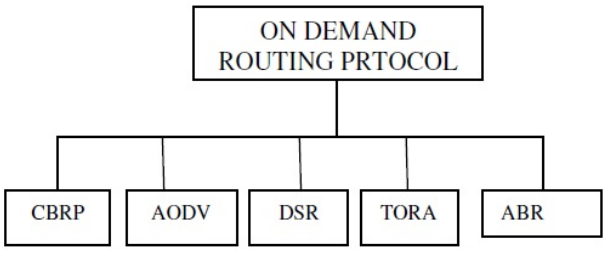

Fig 2: Classification of Routing Protocols

3.1 Cluster based Routing Protocols

The nodes are divided into clusters. Based on the algorithm shown in Fig 3, the clusters are formed and one of the node will be assigned as the cluster-head. A cluster-head maintains information about the nodes of its cluster and also holds a cluster adjacency table to maintain information about the neighbouring clusters. When the node enters the cluster it starts its timer and it broadcasts the messages.

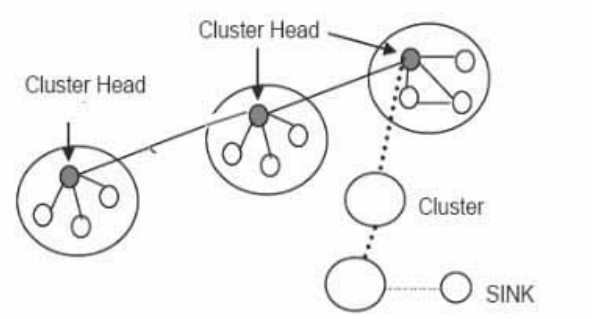

Fig 3. Cluster Based Routing Protocol

Source Routing is used for routing the packets using CBRP. Route shortening is also used in CBRP. The node will try to find its neighbor which is the farthest node in the network, while receiving a source packet. To reduce the route, the packet will be send to that node. When a broken link is found by the node, when forwarding the packet, an error message will be send back to the source node, and then it uses local repair mechanism. In this mechanism, the node will try to find whether next hop is reachable or not. If it is unreachable, then it checks for any neighbor node to reach next hop or any hop after next hop to reach the destination through any other of its neighbor. The packet will be sent over the path if any of the above two works fine

3.2 Ad hoc On-demand Distance Vector Routing (AODV)

It is a reactive routing protocol; a route is established to a destination only when the source node demands for a route. In contrast, the proactive approach is most commonly used routing protocols in the network; they determine the path irrespective of their usage. AODV (distance-vector routing protocol) is a routing protocol for ad hoc mobile networks with large numbers of mobile nodes depicted in Fig 4. The algorithm creates the routes between the source and destination only when the source nodes requests a route to the destination nodes, giving the network the flexibility to allow nodes to enter into or exit from the network. Routes remain active between the nodes only as long as data packets are routed along the paths from the source node to the sink node. When the source node stops transmitting the packet, the path will expire and the route will be closed. AODV supports both unicast and multicast.

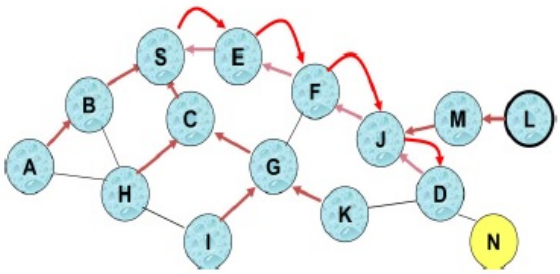

Fig 4: Adhoc On-Demand Distance Vector Routing

When a route request packet is forwarded from a node to its neighbours, the node will record the first copy of the request in

its table. For route reply packet, this information will be useful for the construction of reverse path. As this packet traverse back to the source, the nodes that are present along the path will follow forward route in their tables. The route discovery can be reinitiated to the destination when the source trying to move along the route. If the intermediate node finds any link failure during the movement of neighbour nodes then it sends the notification to the upstream neighbours till it reaches the source so that it can reinitiate the route discovery when needed.

3.3 Dynamic Source Routing Protocol

The DSR Protocol is also called as Source-routed on-demand routing protocol is shown in fig 5. A node maintains a routing table to maintain the route cache. When a new route is identified, then the node will update the entries in the routing table. DSR protocol has two major phases they are route discovery and route maintenance. When the source node wants to transmit the data to the destination, it will check the route cache entry to find any existing route available to reach to the destination.

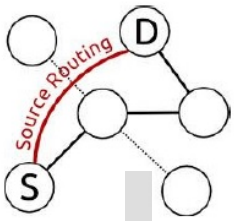

Fig 5. Dynamic Source Routing

If unexpired route is found in the route cache, then it uses that route to send the packet. If there is no route available in the routing table, then the source node will initiates the route discovery process to establish a route to the destination. The route discovery process will broadcast a route request packet to all neighboring nodes. The route request packets contains the source address, the destination address and unique identification number. Each intermediate node will check whether there is a path to the destination, if it is not available, it appends its address and forward the route request packet to the neighbouring nodes. Johnson [15] describes the destination node or the intermediate node which contains the current information to reach the destination that will generate a route reply packet and send back to the source node. A route request packet contains route record, the hops sequence accepted from the source to that particular node.

3.4 Associativity Based Routing

A new metric is used for routing the packets in ABR are known as degree of association stability. This metric avoids forming deadlock, loops and also packet duplicates. ABR will establish the route depending on associativity state of nodes. The routes which are selected by ABR routing will be a long-lived. In general, all nodes available in the network will produce beacon signal. This beacon signal when it reaches the neighbouring node, it will automatically update the associativity tables. The associativity tick will be increased by the node for every received beacon with respect to the node from which the beacon is received. The connection stability of a node will depend on another node based on time and space which is referred as Association stability. When associativity tick is high value, it indicates a low state of node mobility, where as when it is low value, it indicates high state of node mobility. When the node moves out of the network then the corresponding associative tick will also be removed. The aim of ABR is to determine a stable route for Adhoc networks.

ABR consists of three phases, they are (i) Route discovery, (ii) Route Reconstruction and (iii) Route deletion. The first phase is mainly used for (BQ-REPLY) broadcast query and await-reply cycle. During the search of node that holds a route to the destination by broadcasting the BQ message from source node. Each node is capable of broadcasting BQ request not more than once. When the intermediate node receives a BQ message, it adds its address along with associativity to the packet.

4. Analysis of Secured Efficient On Demand Routing Protocols

A survey is made on several on demand routing protocols of MANETs and analyzed them for its fast delivery rate and secured transmission. Due to the nodes mobility in the network the security is important for each individual nodes. In order to improve the security in MANET, many researchers developed and implemented new protocols. Some of the protocols are analyzed not only to improve the fast transmission and also to increase the speed in the packet transmission.

4.1 Various On Demand Routing Protocols

In this section, we analyse a brief description of secured on demand routing protocols in MANET. The following protocol uses Public key cryptosystem [2] for providing security in the nodes and data packets.

4.1.1 Anonymous On Demand Routing (ANODR) Protocol:

ANODR protocol [13] in mobile adhoc networks works to deploy the hostile environments. This protocol is proposed for two problems (i) Route anonymity and (ii)Location privacy. The design of this protocol is based on the broadcasting and trapdoor information. These two design approaches are mainly used for existing network and security mechanism. The protocol provides unlinkability and partial unobservability. The route anonymity is implemented for untraceable route discovery. This is implemented for anonymous route discovery and different approach for route anonymity is discussed. The location privacy is designed for unlinkability. The nodes identity and its location are not identified by other nodes.

Drawbacks

The performance of ANODR protocol is low when compared to other protocols due to the mobility of nodes in the network. This protocol ensures unlinkability and partial unobservaility. The node intrusion is avoided but the nodes and intermediate nodes are viewed by eavesdropper.

4.1.2Anonymous Secure Routing (ASR) protocol

ASR protocol define the need for the anonymity and security characteristics of the routing protocol in MANET. ASR [10] provides additional security by implementing the anonymous node identity and secured route discovery from both the active

and passive attacks. From the analysis it shows ASR provides anonymity and satisfies the requirement of security in the mobile ad-hoc networks. The identity privacy, location privacy and anonymous route discovery are the approaches to design the anonymous secure routing. The nodes identity and the location of the nodes are unknown to other nodes and the location of the nodes is also not known to other nodes. Anonymous Route discovery is based on traffic analysis. This protocol ensures the anonymity and security mechanism are achieved and efficiency in performance is achieved compared to the previous protocols.

Drawbacks

These methods use some security mechanism which are sometimes having Denial Of Service (DOS) in hop by hop. The wormhole attacks [9] are possible when there are temporal leashes or the geographical leashes occur. The performance of the routing protocols should be improved when the route changes since it is anonymous. It can have extended functionality in anonymity and security.

4.1.3 Anonymous Routing Protocol with Multiple Routes (ARMR):

ARMR protocol establishes multiple route using bloom filter in order to decrease the overhead of traffic analysis and to overcome broken paths due to node movements. It also creates some fake path to confuse the adversaries and to increase the level of anonymity. This protocol is implemented to anonymity in the mobile ad- hoc network. The anonymity is designed using cryptographic key exchange algorithm and the hash function algorithm. They are implemented as key exchange between the nodes. In addition to the anonymous route discovery which includes route request and route reply, Anonymous fake routes are also made to confuse he intruders in the network. The approach described here are Node identity ,Location identity and route identity to identify from fake route. ARMR protocol ensures the anonymity and security in the routes of the network.

Drawbacks

The ARMR are vulnerable to DOS attacks. These protocols needs authenticated Route Request to each node. Sometimes a redundant transmission may occur in fake route which will flood the network even though it cannot be obtained by intruders. Hence there is no unlinkability and no unobservability is achieved. The analyzes shows security features does affect the communication and hence it enhanced.

4.1.4 A Secure Distributed Anonymous Routing (SDAR) Protocol

SDAR protocol proposes a novel distributed routing protocols that assures the security, anonymity, reliability in route establishment. This protocol uses one time private/public key for nodes key exchange. The Protocol works on the trustworthiness of the intermediate nodes for anonymous route establishment with its neighbouring nodes. This protocol proposes three phases (i) Path discovery phase (ii) Path reverse Phase and (iii) Data transfer phase. The main features of this protocol are Non-Source based routing, Non-Source control over route length and Resilience against Path Hijacking. SDAR is secured from passive and active attacks. It can easily identify the malicious code and the trust requirement for a node to qualify the trust value between the nodes. Hence the security is achieved.

Drawbacks

SDAR protocol has DOS attack. This protocol achieves security and anonymity and it does not support unlinkability and unobservablity.

4.1.5 On-Demand Anonymous Routing (ODAR) protocol

ODAR protocol proposes anonymity and complete unlinkablity. This protocol approach defines the network, anonymity and bloom filter. It uses diffie-Hellmann algorithm to generate a long term public key. Key Server that generates the public key. The key is distributed between the nodes and the route is discovered with shared key. The node identity, forwarding node identity and route identity are anonymous. Hence the different level of anonymity is made. The performance of ODAR compared with AODV and a control overhead is achieved with public key exchange system.

Drawbacks

The protocol achieves the anonymity and complete unlinkablity but not the unobservablity. It is vulnerable to Man in the middle attack.

4.1.6 MASK protocol

MASK protocol is proposed for anonymous communication based on the cryptographic key exchange.. The phases of protocol are anonymous neighborhood authentication, anonymous route discovery and anonymous data forwarding. It provides strong sender and receiver anonymity. It serves as lightweight routing protocol. The performance of MASK protocol proves a secure anonymous communication compared to AODV.

Drawbacks:

MASK protocol provides a anonymity, unlinkabilitiy and partial unobservability. The analysis on the protocol shows that security is achieved but it has DOS attack and timing analysis attack.

4.1.7 Unobservable Secured On demand Routing Protocol (USOR) Protocol

Unobservable Secured On demand Routing Protocol[12] satisfies all the features such as anonymity, unlinkability and unobservability. It uses public key cryptosystem for secure key exchange. The algorithm used for key generation is Elliptic

Curve Discrete Log Problem (ECDLP) and the Bilinear Diffie-Hellman problem (BDH).

It uses group signature scheme and ID based scheme for pairing. It has security strength as same of 1024 bit RSA algorithm. The phases of protocol are Anonymous key establishment, Privacy-preserving route discovery and unobservable data packet transmission. This protocol avoids the collision attack and Sybil attack. From the brief analysis the USOR protocol has a strong security, complete unlinkability and content unobservablity.

5. RESULTS AND DISCUSSION

Various on demand routing protocols have been analyzed and metrics that have been used to determine efficient secure routing. The results of the survey are illustrated in Table 1 The main aim is to find a route which is not directly noticeable; or based on secured node"s trust level. The communication between the source to destination should maintain the property of Anonymity, Unlinkability, and Unobservability.

Table 1: Optimisation of Routing Protocol

Techniques	Author & Reference	Year	Metrics	Performance
User Behavior Analysis				
ANODR: ANonymous On Demand Routing with Untraceable Routes for Mobile Adhoc Networks	Jiejun Kong, Xiaoyan Hong [3]	2003	Traceable ratio, Average end to end delay	Increased Normalized control bytes
Anonymous secure routing in mobile ad-hoc networks	B. Zhu, F. Bao, R. H. Deng,Z. Wan, and M. KankanHalli [4]	2004	Traffic Analysis	Increased Anonymity
ARMR: Anonymous routing protocol with multiple routes for communications in mobile ad hoc networks	Y. Dong, S.-M.Yiu, T. W. Chim, V. O. K. Li, and C. K. Hui [6]	2009	Number of Nodes flow	Increased Communication Efficiency
SDAR: a secure distributed anonymous routing protocol or wireless and mobile ad hoc networks	A. Boukerche, K. El-Khatib, L. Xu, and L. Korba[7]	2004	Trustworthy Anonymity	Increased Security Reliable path selection
ODAR: on-demand anonymous routing in ad hoc networks	D. Sy, R. Chen, and L. Bao[8]	2006	Delivery ratio, Number of Control Packets	Improved Control Overhead Reliable
"MASK: Anonymous On-Demand Routing in Mobile Ad Hoc Networks" IEEE transactions on wireless communications	Yanchao Zhang, Wei Liu, Wenjing Lou, and Yuguang Fang [11]	2006	Normalized Routing load Packet Delivery Ratio Average packet delay	Improved packet delivery Partial delay

6. SUMMARY

Privacy-preserving routing techniques have been analysed for MANET. The following drawbacks found in existing anonymous routing protocols. They are

1. In MANET, the anonymous routing protocols which exists concentrates on partial unlinkability and anonymity.
2. Due to partial content protection, there is no guarantee for unlinkability and unobservability.
3. Information such as Packet type and sequence number can be attacked by the attacker, thereby it breaks unlinkability.
4. Information about the key for decryption technique should be furnished in all cipher packet, which requires for efficient design to eliminate linkabilty

7. PROPOSED WORK

In the proposed system, we focus on high packet delivery ratio and average packet delivery latency. With the help of Content Unobservability, no useful information can be extracted from content of any message. It is attained by employing anonymous key establishment based on group signature. Traffic Pattern Unobservability, no useful information can be obtained from frequency, length, and source-destination patterns of message traffic. USOR is an Unobservable Secure On-demand Routing protocol for mobile ad hoc network that achieves unlinkability and unobservability by employing anonymous key establishment based on group signature. The security analysis demonstrates that USOR not only provides strong privacy protection, but it is also resistant against attacks due to malicious node and its performance is almost equivalent to AODV.

8. Conclusion

MANET (Mobile Ad-Hoc Network) is a self-forming network with wireless links. Due to moving nature in the network, security is becoming a challenging task in, on demand routing protocols. The protocols designed for secured routing uses several technique and various cryptographic algorithms. In this paper, we analyzed and classified various on demand routing schemes and each has its own features. The analysis show that most of the protocol has its key feature anonymity. Hence the Unlinkability and Unobservability are achieved by few protocols. It is difficult to compare these protocols directly since it has different assumption and different goals. With the three key feature such anonymity, unlinkability, and unobservability a secured communication is provided in on demand routing protocol of Mobile ad-hoc networks.

References

[1] A. Pfitzmann and M. Hansen, "Anonymity, unobservability, and pseudonymity: a consolidated proposal for terminology," draft, July 2000.

[2] S. Capkun, L. Buttyan, and J. Hubaux, "Self-organized public-key management for mobile ad hoc networks," IEEE Trans. Mobile Comput., vol. 2, no. 1, pp. 52-64, Jan.-Mar. 2003.

[3] J. Kong and X. Hong, "ANODR: aonymous on demand routing with untraceable routes for mobile ad-hoc networks," in Proc. ACM MOBIHOC' 03, pp. 291-302.

[4] B. Zhu, F. Bao, R. H. Deng,Z. Wan, and M. KankanHalli, "Anonymous secure routing in mobile ad-hoc networks," in Proc. 2004 IEEE Conference on Local Computer Networks, pp. 102-108.

[5] S. Seys and B. Preneel, "ARM - Anonymous routing protocol for mobile ad hoc networks," in Proc. 2006 IEEE International Conference on Advanced Information Networking and Applications, pp. 133-137.

[6] Y. Dong, S.-M.Yiu, T. W. Chim, V. O. K. Li, and C. K. Hui, "ARMR: Anonymous routing protocol with multiple routes for communications in mobile ad hoc networks," Ad Hoc Networks, vol. 7, no. 8, pp. 1536-1550, 2009.

[7] A. Boukerche, K. El-Khatib, L. Xu, and L. Korba, "SDAR: a secure distributed anonymous routing protocol or wireless and mobile ad hoc networks," in Proc. 2004 IEEE LCN, pp. 618-624.

[8] D. Sy, R. Chen, and L. Bao, "ODAR: on-demand anonymous routing in ad hoc networks," in 2006 IEEE Conference on Mobile Ad-hoc and Sensor Systems.

[9] J. Ren, Y. Li, and T. Li, "Providing source privacy in mobile ad hoc networks," in Proc. IEEE MASS'09, pp. 332-341.

[10] Y. Zhang, W. Liu, and W. Lou, "Anonymous communications in mobile ad hoc networks," in 2005 IEEE INFOCOM.

[11] Yanchao Zhang, Wei Liu, Wenjing Lou, and Yuguang Fang "MASK: Anonymous On-Demand Routing in Mobile Ad Hoc Networks" IEEE transactions on wireless communications, vol. 5, no. 9, september 2006.

[12] Zhiguo Wan, Kui Ren , Ming Gu, "USOR: An unobservable secure on- Demand Routing protocol for mobile adhoc networks" Wireless communication, IEEE transacations vol 11 issue: 5, pp . 1922-1932, 2012

[13] Dr.G.Padmavathi, Dr.P.Subashini, and Ms.D.Devi Aruna "ANODR-ECC Key Management protocol with TELNET to secure Application and Network layer for Mobile Adhoc Networks" International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.1, January 2012

[14] A.Menuka, N. Kumaratharan "Secure Routing Protocol based on unobservable identity in mobile adhoc network" Internation Journal of P2P network trends and Technology – Volume 3 Issue 1 -2013

[15] D. Johnson and D. Maltz. Dynamic Source Routing in Ad Hoc Wireless Networks. In Mobile Computing, edited by Tomasz Emilienski and Hank Korth, Kluwer Academic Publishers, 1996.