ISSN: 2395-7639

International Journal of Multidisciplinary Research in Science, Engineering, Technology & Management (IJMRSETM)

Visit: www.ijmrsetm.com

Volume 1, Issue 1, October 2014

A Study on Unidentified Routing Protocols in MANETs

N.Saravana Selvam[1], R.T.Nivetha[2], S.S.Nevatha[3]

Dept. of CSE, Sri Eshwar College of Engineering, Anna University, Coimbatore, India[1]

Dept. of CSE, Sri Eshwar College of Engineering, Anna University, Coimbatore, India[2]

Dept. of CSE, Sri Eshwar College of Engineering, Anna University, Coimbatore, India[3]

ABSTRACT: This survey on anonymous routing protocols identifies various routing schemes for finding the source node, destination node and their relationship in the mobile adhoc network which is an infrastructureless network. A passive attacker perform traffic analysis and find all the necessary details. To overcome this problem, an efficient routing scheme must be proposed. The protocols such as (MASK) Anonymous on demand routing in mobile ad hoc networks, Anonymous On-Demand Routing (ANODR), Anonymous Dynamic Source Routing (AnonDSR), A Secure Distributed Anonymous Routing Protocol for Wireless and Mobile Ad Hoc Networks (SDAR) and On-Demand Lightweight Anonymous Routing in MANETs (OLAR) uses unique anonymous routing protocols by hiding the details of nodes.

KEYWORDS: Mobile ad hoc networks, Statistical traffic analysis, RREQ, RREP, Anonymity

I. INTRODUCTION

MANET is an infrastructure less network with many number of mobile nodes connected in a wireless manner. Each mobile node can serve as both a host and router. The nodes move in any direction at any speed. Also it is a kind of wireless ad hoc network that has a routable networking environment. It is a self-forming and self-healing network and may contain multiple transceivers between nodes. The issues related are it is difficult to find source, destination of the network and also difficult to identify the end to end Communication relation. There are different protocols such as proactive, reactive and hybrid routing protocols. In proactive routing protocol, the path between individual nodes is found before they plan to communicate. In reactive routing protocol, the path is found only after they plan to communicate. In hybrid routing protocol both are satisfied.

II. RELATED WORK

In paper [1] two communication methods such as network layer and MAC layer communications are accomplished without disclosing the real ID's of nodes. Each node follows three tables such as forwarding routing table, reverse routing table and target link ID table. In paper [2] two design principles such as identity free routing and on-demand routing are used where it relies on one time cryptographic trapdoor. It follows three phases such as anonymous route discovery, anonymous route maintenance and anonymous route forwarding. In paper [3] security parameter establishment, anonymous route discovery and data transfer protocols are used. It follows two phases such as RREQ phase and RREP phase. In paper [4] it follows novel distributed routing protocol which allows trustworthy intermediate nodes to participate in path construction. Here the phases followed are the path discovery phase, the path reverse phase and the data transfer phase. In the paper [5] Shamir's secret sharing scheme is followed which is based on the properties of polynomial interpolation.Route discovery and message transfer are the two phases followed in this protocol.

III. MASK

The paper [1] provides a novel anonymous on-demand routing protocol, termed MASK to avoid passive eavesdropping on data communications.It accomplish both MAC-layer and network-layer communications without disclosing real IDs

ISSN: 2395-7639

International Journal of Multidisciplinary Research in Science, Engineering, Technology & Management (IJMRSETM)

Visit: www.ijmrsetm.com

Volume 1, Issue 1, October 2014

of the participating nodes. MASK provides anonymity of sender, receiver and their relationship. Simulation shows that MASK is effective and efficient.

In MASK, each node is assigned with a pseudonym for real id in communication. Usage of one pseudonym lead to difficult so dynamic pseudonyms are used. Anonymous MAC layer communication can be achieved by anonymous neighborhood authentication protocol which makes the two neighbor nodes to identify each other in the same group. MASK uses a three-stage handshake for key exchanges among a node and its new neighboring nodes. After the handshake, each pair of nodes shares a chain of secret key and locally unique Link ID pair which corresponds to the pseudonyms used during handshake. In anonymous network layer communication, each node maintains the following table,

- Forwarding routing table: This table consists of dest_id, destseq, pre link id list, and next linked list.
- Reverse routing table: It consists of dest_id, destseq, prehoppseudonym where route replies are relayed back to source.
- Target linkID table: It has link ids shared with neighbors.

The route discovery starts by broadcasting route request message when a node needs to send a packet to destination. The format is as follows <ARREQ, ARREQid, destid, destSeq, PSsr>.Here the real ids of source and intermediate nodes are concealed but destination id is exposed. An anonymous route reply is sent back to source at destination or intermediate nodes which has a valid route.ARREP packet is of the format <LinkID, {ARREP, destid, destSeq}Skey>.

In the packet forwarding step, source selects a random link IDs from the list. The packet is then sent to next neighbor that shares the link id.A packet is of format<LinkID, data> where data may be differed based on application.it can be end to end encrypted or use cryptographic method for encryption.

The issues are adversaries might launch active DoS attacks on target nodes by continuously sending a number of bogus authentication requests, routing information is secured against external adversaries only so once they become internal adversaries then no security, implementation of low end devices is a problem.

The simulation results show that MASK has higher probability of colliding and dropping of packets. Also data packets are not routed along shortest path due to random selection of next hops. MASK cannot achieve anonymity without sacrificing efficiency.

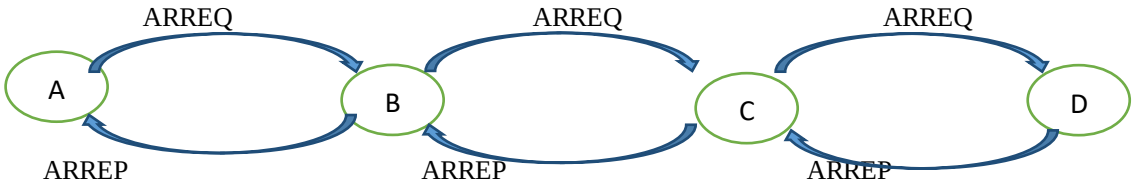

Fig. 1 Example of route discovery

The Fig. 1 represents route discovery process. Node A sends ARREQ (ie) Anonymous Route REQuest to node B. Then node B sends to c and the node C to D which is the destination. Node D sends ARREP (Anonymous Route REPly) to node C. This is followed and node A receives the route reply. Thus the route is discovered successfully.

IV. ANODR

The paper [2] proposed a new anonymous routing protocol ANODR (Anonymous On Demand Routing) where it relies on one-time cryptographic trapdoors.

It is purely on-demand routing (ie) sets up anonymous routes as needed. Also it is an identity-free routing scheme where one-time cryptographic trapdoors are used instead of node identities. So, the adversary has no means to break a mobile node's identity anonymity.ANODR has 3 phases. They are anonymous route discovery, anonymous route maintenance and anonymous route forwarding.

ISSN: 2395-7639

International Journal of Multidisciplinary Research in Science, Engineering, Technology & Management (IJMRSETM)

Visit: www.ijmrsetm.com

Volume 1, Issue 1, October 2014

Anonymous route discovery establishes an on-demand route. A communication source initiates the route discovery procedure by assembling an RREQ (Route request) packet and locally broadcasting it. There are RREQ phase and RREP phase in the route discovery process. The source puts a random nonce as the onion "core." If each RREQ forwarder adds a layer of encryption during the RREQ phase, then only the node itself can peel off this layer during the RREP phase. The onion is formed during RREQ propagation and will be used to set up an anonymous virtual circuit when the RREPs come back. ANODR implements 1) symmetric key agreement between two consecutive RREP forwarders and 2) enforces destination-initiated RREP procedure. The global trapdoor holds secret information for the intended destination and a public commitment for the same destination. RREP proof (or receipt) from the destination is obtained to prevent an adversarial network node to send back fake RREPs to disrupt ANODR.

For anonymous route maintenance, the routing table entries are recycled upon timeout Twin similar to the same parameter used in DSR and AODV. When one or more hop is broken due to mobility or node failures, nodes cannot forward a packet via the broken hops. The one-hop sender can detect such anomalies when the retransmission count exceeds a predefined threshold.
Upon anomaly detection, the node looks up the corresponding entry in its forwarding table, when nodes fail then it finds the other which is associated with the broken hop, and assembles an anonymous route error report packet. Then node recycles the table entry and transmits.
Anonymous data forwarding is the last phase where the source forwards the packet and all receiving nodes check for the pseudonym. If it doesn't match then it discards the packet. This is followed till the packet reaches the destination.
The simulation results show that ANODR is suitable for low end nodes, medium mobility and also has the low packet delay.

V. ANONDSR

The paper [3] consists of three protocols: security parameter establishment, anonymous route discovery, and anonymous data transfer.

The security parameter establishment protocol has two phases: RREQ phase and RREP phase.
The anonymous route discovery protocol establishes an anonymous route between a pair of source and destination nodes that is resistant against traffic analysis attacks launched by any adversaries including the intermediate forwarding nodes. The protocol is used when the source and destination want to create an anonymous path for their communications and they already have a shared secret key and secret key index in their key ring.

The anonymous data transfer protocol builds a cryptographic onion for anonymous communication data protection. The protocol is only used when an anonymous route discovery protocol is completed. Each intermediate forwarding node checks whether the pseudonym of the data packet belongs to it and decrypts one layer of the data onion using its session key if it is on the anonymous route. It then changes the route pseudonym by its forwarding routing table, uses the decrypted onion instead of the received onion, and broadcasts the new packet locally. It discards the packet if it is not on the anonymous route. The procedure is repeated until the data packet arrives at the destination. A reverse anonymous communication data transfer from the destination to the source uses the reverse data onion.
The simulation results show that AnonDSR has no neighbor exposure and is crypto protected for destination.

VI. SDAR

The major objective of the paper [4] is to allow trustworthy intermediate nodes to participate in the path construction protocol without jeopardizing the anonymity of communication nodes.
The process is divided into three phases: the path discovery phase, the path reverse phase and the data transfer phase.
The path discovery phase allows source node to find route path through all intermediate nodes by sending a path discovery message to all nodes within the wireless range. Once a node receives a path discovery message then it does the following,

- Checks whether it is already received from other nodes if so then drop it.
- Checks whether the node is the sender's next hop if so decrypt the message.

ISSN: 2395-7639

International Journal of Multidisciplinary Research in Science, Engineering, Technology & Management (IJMRSETM)

Visit: www.ijmrsetm.com

Volume 1, Issue 1, October 2014

- Checks whether the node is the intended receiver. If not then add the information such as node id, session key, path id, signature and forward it to the neighbor else put all node's id and session key in one message and encrypt several times and sent to source in reverse path.

The data transfer phase is similar to onion routing where each node decrypts one encryption layer and sends to next node based on the id of the next node.
The main features include Non-source-based routing, no source control over route length and resilience against path hijacking. SDAR maintains anonymity of sender, receiver but it is not secured under denial of service attack.

The simulation results show that SDAR has significant degradation delivery ratio, longer end to end latency, have large RREQ and RREP packet sizes for carrying keys, low successful delivery of packets.

VI. **OLAR**

The paper [5] apply the Shamir's secret sharing scheme based on the properties of polynomial interpolation. OLAR is an identity-free routing scheme, which provides source and destination anonymity, end-to-end communication relation anonymity, route anonymity.

The secret sharing mechanism conforms to a (k, n) threshold. The (k, n) threshold means that if the secret M is divided into n parts, then the knowledge of any k parts or more makes M easily computable but knowledge of any k−1 parts or fewer leaves M completely undetermined.
Two phases used in this protocol are Route discovery and message transfer phase. In route discovery phase, the source S broadcasts a route request (RREQ). The initial RREQ has the following format: <RREQ, RP Ksrc, (RP Ksrc, SN)GP Kdest , TPKS>.after the node receives the message it checks whether it has received the RREQ before. If so it discards the request otherwise it tries to open the trapdoor using the private key. When D receives the message it decrypts and compare the RPK_{src} to verify integrity. If they are different then ignores else send a route reply message with the following format < RREP, (SN, ND, KSD)RP Ksrc)T P Kn2>.

In anonymous message transfer phase, based on the path in route discovery phase the message is sent from source to destination. Here addition and multiplication are done instead of encryption and decryption.

OLAR ensures the privacy of messages transmitted. Only source and destination can see the original message. Instead of real identities, one time public key and shared keys are used.it uses distance vector scheme so nodes do not know the entire path also since polynomial interpolation is used, the messages differ at different stage so attacker cannot find path by hacking the message. The source/ destination anonymity and end to end link anonymity is protected and even the intermediate nodes along the path do not know the source and destination. The overhead is low but cost is higher than other protocols.

The simulation results show that OLAR exhibits better performance, average computation time per node is lesser than ANODR as traffic rate increases.

In Fig. 2, the node S sends a route request to node A then that to node B and then to destination node D. This is followed by sending route reply message to source node S. In OLAR, another step is route confirmation message (RCNF) where the source node sends that message to destination node through intermediate nodes.

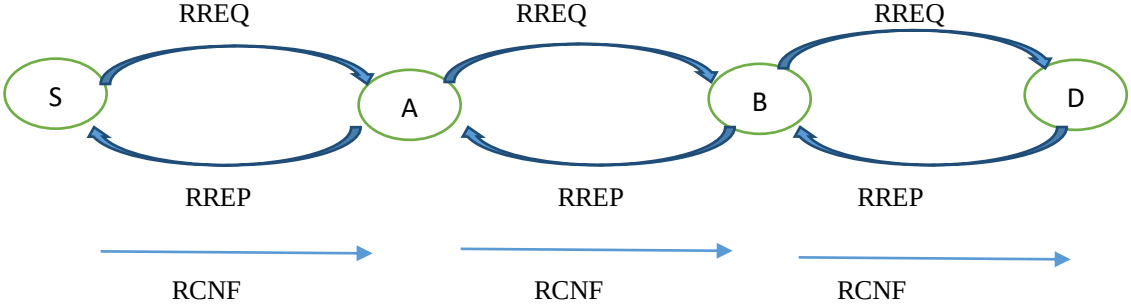

Fig. 2 Example of route discovery in OLAR

ISSN: 2395-7639

International Journal of Multidisciplinary Research in Science, Engineering, Technology & Management (IJMRSETM)

Visit: www.ijmrsetm.com

Volume 1, Issue 1, October 2014

VII. COMPARISON RESULTS

In MASK, network layer and MAC layer communications are used. The drawbacks are higher probability of dropping of packets and lower efficiency for achieving anonymity. In ANODR, two design principles such as identity free routing and on-demand routing are used. The issues are heavy overhead when traffic is higher and less performance if packet size is higher. In AnonDSR, three protocols such as security parameter establishment, anonymous route discovery and anonymous data transfer are used. In SDAR, a novel distributed routing protocol is used. Denial of service attack is the main drawback. In OLAR, the Shamir's secret sharing scheme is used and the issue is high of cost.

VIII. CONCLUSION

The paper describes in detail about the comparison and simulation results of five different anonymous routing protocols which provide source/destination anonymity and end to end path anonymity. In paper [1] two communication methods such as network layer and MAC layer communications are accomplished without disclosing the real ID's of nodes. In paper [2] two design principles such as identity free routing and on-demand routing are used where it relies on one time cryptographic trapdoor. In paper [3] security parameter establishment, anonymous route discovery and data transfer protocols are used. In paper [4] it follows novel distributed routing protocol which allows trustworthy intermediate nodes to participate in path construction. In the paper [5] Shamir's secret sharing scheme is followed which is based on the properties of polynomial interpolation. Each protocol has different type of routing scheme such as proactive, reactive and hybrid. All the five routing protocols ensures source, destination anonymity and end to end anonymity but with some issues in it. The comparison results help to find out the techniques used and the drawbacks found. To overcome these issues AODV protocol can be used which is a reactive routing protocol, where the routes are determined only when needed. In this protocol, to send a message, first a Route Request (RREQ) is send to the nodes and then Route Reply (RREP) is received. Finally the data is transfered. This protocol improves the performance and efficiency

REFERENCES

1. Y. Zhang, W. Liu, W. Lou, and Y. Fang, "MASK: Anonymous On-Demand Routing in Mobile Ad Hoc Networks,"IEEE Trans.Wireless Comm., vol. 5, no. 9, pp. 2376-2385, Sept. 2006.
2. J. Kong and X. Hong, "ANODR: ANonymous on Demand Routing with Untraceable Routes for Mobile Ad-Hoc Networks," Proc. MobiHoc, pp 291-302, 2003.
3. R. Song, L. Korba, and G. Yee, "AnonDSR: Efficient Anonymous Dynamic Source Routing for Mobile Ad-Hoc Networks," Proc. ACM Workshop Security of Ad Hoc and Sensor Networks (SASN '05), 2005.
4. A. Boukerche, K. El-Khatib, L. Xu, and L. Korba, "SDAR: A SecureDistributed Anonymous Routing Protocol for Wireless and Mobile Ad Hoc Networks,"Proc. IEEE 29th Ann. Int'l Conf. Local ComputerNetworks (LCN '04),pp. 618-624, 2004.
5. Y. Qin and D. Huang, "OLAR: On-Demand Lightweight Anonymous Routing in MANETs," Proc. Fourth Int'l Conf. Mobile Computing and Ubiquitous Networking (ICMU '08), pp. 72-79, 2008.
6. Sanzgiri, B. Dahill, B. Levine, C. Shields, and E. Royer, "A secure routing protocol for ad hoc networks," in IEEE ICNP'02, Paris, France, Nov. 2002.
7. Perkins, E. Belding-Royer, and S. Das, "Ad hoc on-demand distance vector (AODV) routing," RFC 3561, July 2003.
8. D. Goldschlag, M. Reed, and P. Syverson. Onionrouting for anonymous and private internet connections. InCommunications of the ACM, 1999.
9. S. Seys and B. Preneel. Arm:Anonymous routing protocol for mobile ad hoc networks. In IEEE AINA , 2006.
10. P. F. Syverson, D. M. Goldschlag, and M. G. Reed: Anonymous connections and onion routing. In Proceedings of the IEEE Symposium on Security and Privacy (Oakland, California, May1997), pp. 44–54
11. J. Kong, X. Hong, and M. Gerla, "An Identity-Free and On-Demand Routing Scheme against Anonymity Threats in Mobile Ad Hoc Networks," IEEE Trans. Mobile Computing, vol. 6, no. 8, pp. 888-902, Aug. 2007.
12. M. Reed, P. Syverson, and D. Goldschlag, "Anonymous Connections and Onion Routing," IEEE J. Selected Areas in Comm.,vol. 16, no. 4, pp. 482-494, May 2002.

13. 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 29th IEEE International Conference on Local Computer Networks (LCN'04), pages 618–624, 2004.
14. Y.-C. Hu, A. Perrig, and D. B. Johnson. Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks. In ACM MOBICOM, pages 12–23, 2002
15. J. Raymond, "Traffic Analysis: Protocols, Attacks, Design Issues,and Open Problems,"Proc. Int'l Workshop Designing Privacy Enhancing Technologies: Design Issues in Anonymity and Unobservability, pp. 10-29, 2001.