# Unobservable Privacy-Preserving Routing in MANET

**P. Thamizharasi, D.Vinoth**

***Abstract— Privacy-preserving routing is crucial for some ad hoc networks that require stronger privacy protection. A number of anonymous routing schemes have been proposed for ad hoc networks in recent years, and they provide different level of privacy protection at different cost. These schemes are more scalable to network size, but require more computation effort. However, existing schemes provide only anonymity and unlinkability, while unobservability is never considered or implemented by now. An obvious drawback in existing schemes is that packets are not protected as a whole. An efficient privacy-preserving routing protocol USOR that achieves content unobservability by employing anonymous key establishment based on group signature. USOR is to protect all parts of a packet's content and it is independent of solutions on traffic pattern unobservability. The unobservable routing protocol is then executed in two phases. First, an anonymous key establishment process is performed to construct secret session keys. Then an unobservable route discovery process is executed to find a route to the destination. By using NS-2 the performance analysis such as energy, bandwidth etc., are simulated.***

***Keywords- MANET, Privacy, Public key, Routing, Unobservable***

## I. INTRODUCTION

Privacy protection of mobile ad hoc networks is more demanding than that of wired networks due to the open nature and mobility of wireless media. In wired networks, one has to gain access to wired cables so as to eavesdrop communications. In contrast, the attacker only needs an appropriate transceiver to receive wireless signal without being detected. In wired networks, devices like desktops are always static and do not move from one place to another. Hence in wired networks there is no need to protect users' mobility behavior or movement pattern, while this sensitive information should be kept private from adversaries in wireless environments.

To achieve unobservability, a routing scheme should provide unobservability for both content and traffic pattern. Hence we further refine unobservability into two types one is content Unobservability, referring to no useful information can be extracted from content of any message and another one is Traffic Pattern Unobservability, referring to no useful information can be obtained from frequency, length, and source-destination patterns of message traffic.

USOR is to protect all parts of a packet's content, and it is independent of solutions on traffic pattern unobservability [6]. And it can be used with appropriate traffic padding schemes to achieve truly communication unobservability.

The ANODR, an anonymous on-demand routing protocol for mobile ad hoc networks. From [1] the design of ANODR is based on "broadcast with trapdoor information", a novel network security concept which includes features of two existing network and security mechanisms, namely "broadcast" and "trapdoor information". It only can prevent outside passive attackers is the only drawback. A novel anonymous on-demand routing protocol, termed MASK. From [2] MASK provides the desirable sender and receiver anonymity, as well as the relationship anonymity of the sender and receiver. It is also resistant to a wide range of adversarial attacks. The drawback is there is no destination anonymity.

An On-Demand Anonymous Routing protocol for wireless ad hoc networks to enable complete anonymity of nodes, links and source-routing paths/trees using Bloom filters. From [3] Bloom filter is a space-efficient probabilistic bit vector data structure for starting the elements of a set, and testing whether or not any given element is a member of the set. The drawback –it provide only identity anonymity but not unlinkability for MANET. From [4] ALARM uses nodes' current locations to securely disseminate and construct topology snapshots and forward data. With the aid of advanced cryptographic techniques for an example group signature, ALARM provides both security and privacy features, including: node authentication, data integrity, anonymity and untraceability tracking resistance. It also offers protection against passive and active insider and outsider attacks. It leaks quite a lot sensitive privacy information-network topology, location of every node is the major drawback. From [5] Anonymity is an important part of the overall security architecture for mobile ad hoc networks as it allows users to hide their activities. This enables private communications between users while making it harder for adversaries to focus their attacks. A solution that provides stronger anonymity properties while also solving some of the efficiency problems.

## II. MOBILE AD-HOC NETWORKS

An ad-hoc network is a collection of wireless mobile hosts forming a temporary network without the aid of any stand-alone infrastructure or centralized administration. Mobile Ad-hoc networks are self-organizing and self-configuring multihop wireless networks where, the structure of the network changes dynamically [7]. This is mainly due to the mobility of the nodes. Nodes in these networks utilize the same random access wireless channel, cooperating in a friendly manner to engage themselves in multihop forwarding. The nodes in the network not only act as hosts but also as routers that route data to/from other nodes in network. In mobile ad-hoc networks where there is no infrastructure support as is the case with wireless networks, and since a destination no de might be out of range of a source node transmitting packets; a routing procedure is always needed to find a path so as to forward the packets appropriately between the source and the destination.

**Manuscript received on January, 2013**

**P. Thamizharasi**, Communication Systems, Anna University/ Arunai College of Engineering/ Tiruvannamalai, India.

**D. Vinoth**, Communication Systems, Anna University/ Arunai College of Engineering/ Tiruvannamalai, India.

Within a cell, a base station can reach all mobile nodes without routing via broadcast in common wireless networks. In the case of ad-hoc networks, each node must be able to forward data for other nodes. This creates additional problems along with the problems of dynamic topology which is unpredictable connectivity changes.

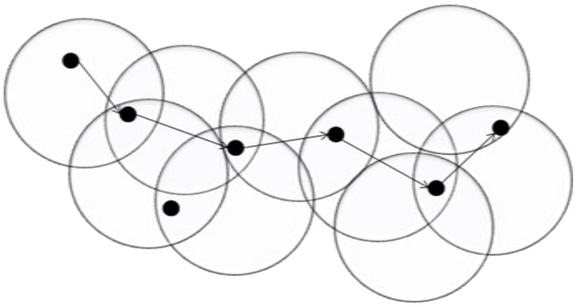

**Fig1.Archicteture of MANET**

## III. CLASSIFICATION OF ROUTING PROTOCOLS IN MANET's

Classification of routing protocols in MANET's can be done in many ways, but most of these are done depending on routing strategy and network structure. According to the routing strategy the routing protocols can be categorized as Table-driven and source initiated, while depending on the network structure these are classified as at routing, hierarchical routing and geographic position assisted routing [8], [9]. Both the Table-driven and source initiated protocols come under the Flat routing.

### A. *Table-Driven routing protocols*

These protocols are also called as proactive protocols since they maintain the routing information even before it is needed. Each and every node in the network maintains routing information to every other node in the network [8], [9]. Routes information is generally kept in the routing tables and is periodically updated as the network topology *changes*. Many of these routing protocols come from the link-state routing. There exist some differences between the protocols that come under this category depending on the routing information being updated in each routing table. Furthermore, these routing protocols maintain different number of tables. The proactive protocols are not suitable for larger networks, as they need to maintain node entries for each and every node in the routing table of every node. This causes more overhead in the routing table leading to consumption of more bandwidth.

### B. *On Demand routing protocols*

These protocols are also called reactive protocols since they don't maintain routing information or routing activity at the network nodes if there is no communication [8], [9]. If a node wants to send a packet to another node then this protocol searches for the route in an on-demand manner and establishes the connection in order to transmit and receive the packet. The route discovery usually occurs by flooding the route request packets throughout the network.

## IV. SYSTEM IMPLEMENTATION

In this protocol, both control packets and data packets look random and indistinguishable from dummy packets for outside adversaries. Only valid nodes can distinguish routing packets and data packets from dummy traffic with inexpensive symmetric decryption. The intuition behind the proposed scheme is that if a node can establish a key with each of its neighbors, then it can use such a key to encrypt the whole packet for a corresponding neighbor. The receiving neighbor can distinguish whether the encrypted packet is intended for itself by trial decryption. In order to support both broadcast and unicast, a group key and a pairwise key are needed. As a result, USOR comprises two phases: anonymous trust establishment and unobservable route discovery.

### A. *Topology Formation & Anonymous Key establishment*

Constructing project design in NS2 should takes place. In this phase, every node in the ad hoc network communicates with its direct neighbors within its radio range for anonymous key establishment. Each node employs anonymous key establishment to anonymously construct a set of session keys with each of its neighbors.

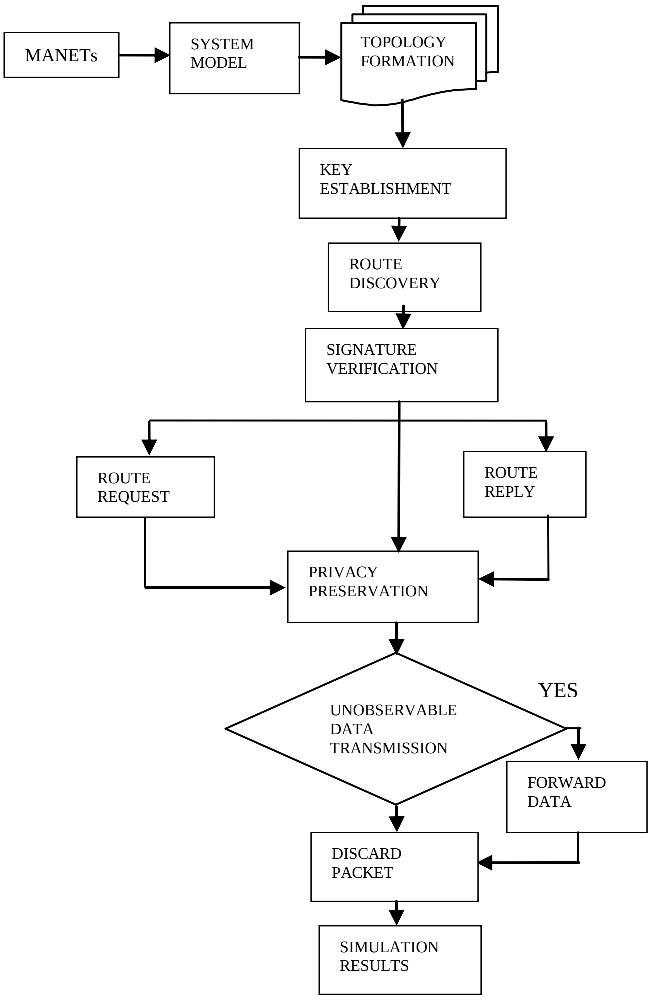

**Fig 2 System Design**

### B. *Privacy-Preserving Route Discovery*

This phase is a privacy-preserving route discovery process based on the keys established in previous phase. Similar to normal route discovery process, our discovery process also comprises of route request and
route reply.

Under the protection of these session keys in the first phase, the route discovery process can be initiated by the source node to discover a route to the destination node.

## V. SIMULATION ENVIRONMENT

This proposed routing protocol has been implemented by the Network Simulator2 (NS2). The Network Simulator is mainly utilized to implement the routing protocols in the networking research. The Main focus of our analysis is security and privacy. The simulation results are shown below.

| | |
|---|---|
| Simulation time | 600 sec |
| Scenario dimension | 1500m X 300m |
| Wireless Radio range | 250m |
| Number of nodes | 50 |
| Average node speed | 0-10m/s |
| Traffic type | 512 byte CBR traffic |
| Traffic frequency | 2or 4 packets/s |
| Wireless bandwidth | 2Mbps |
| 1024-bit ID-based Enc | 22ms |
| 1024-bit ID-based Dec | 17ms |
| Node pass time | 0s |
| Key update interval | 40s |

**Tables 1Simulation environment**

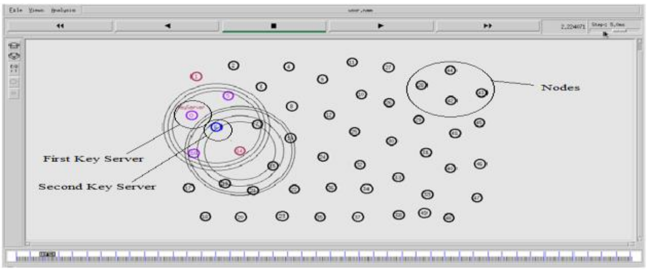

**Fig 3 Topology Formation & Anonymous Key Establishment**

Here Node-0 forwards the Topology Discovery Packet with master key value to its neighbor node 5, node 16 and node 1. The pink color node act as a first key server next it find neighboring nodes and then the blue color node act as a next key server. The process will be continued up to 49th node.

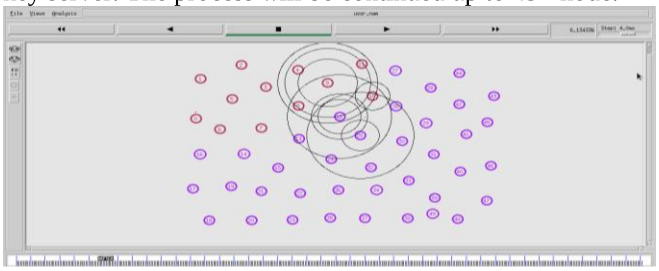

**Fig 4 Privacy- Preserving Route Discovery**

Here node 10 send the Hello message with key values to its neighbor node 12, node 10 send the reply hello key message with session to its neighbor node 12 then node 10 send about the acceptance of session key with broadcast key to its neighbor node 11.

## VI. CONCULSION

In this phase, every node in the ad hoc network communicates with its direct neighbors within its radio range for anonymous key establishment. Each node employs anonymous key establishment to anonymously construct a set of session keys with each of its neighbors. This method is Topology Formation & Anonymous Key establishment. And also a privacy-preserving route discovery process based on the keys established in previous phase. Similar to normal route discovery process, our discovery process also comprises of route request and route reply. Under the protection of these session keys in the first phase, the route discovery process can be initiated by the source node to discover a route to the destination node. This method is Privacy-Preserving Route Discovery.

## FUTURE WORK

After the source node S successfully finds out a route to the destination source node S successfully finds out a route to the destination node D, S can start unobservable data transmission under the protection of pseudonyms and keys. The proposed method should focus on full and full privacy preserved routing in mobile ad hoc networks. Only security has been improved.

## ACKNOWLEDGEMENT

Thanks to Management, Staff of Arunai College of Engineering for their Wonderful Support towards this paper submission.

## REFERENCES

1. J. Kong and X. Hong, “ANODR: anonymous on demand routing with untraceable routs for mobile ad-hoc networks,” in proc. ACM MOBIL-HOC’03,pp, 291-302.
2. B. Zhu, Z. Wan, F. Bao, R. H. Deng, and M. KankanHailli, “Anonymous secure routing in mobile ad-hoc networks,” in proc. 2004 IEEE conference on Local Computer Networks, pp. 102-108.
3. D. Sy, R. Chen, and L. Bao, “ODAR: on-demand anonymous routing ad hoc networks,” in 2006 IEEE Conference on Mobile Ad-hoc and Sensor Systems.
4. K. E. Defrawy and G. Tsudik, “ALARM: anonymous location-aided routing in suspicious MANETs,” IEEE Trans. Mobile Comput., vol. 10, no. 98
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. Zhiguo Wan, Kui Ren, and Ming Gu,” USOR: An Unobservable Secure On-Demand Routing Protocol for Mobile Ad Hoc Networks.
7. http://www.academia.edu/219032/A_Review_of_Broadcasting_Methods _for_Mobile_Ad_Hoc_Network.
8. http://www.ijcse.com/docs/IJCSE10-01-04-61.pdf.
9. http://www.ijopcm.org/Vol/10/IJOPCM(vol.3.5.11.D.10).pdf