ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

# On-Demand Routing in Mobile Ad Hoc Network

Buvana.P[1], Arun Sebastian[2], Deepika.K.S[3], Keerthivasan.S[4]

Asst. Prof., Department of Computer Science and Engineering, K.S.Rangasamy College of Technology, KSR Kalvi Nagar, Tiruchengode, Namakkal-637 215, Tamilnadu, India[1]

Student, Department of Computer Science and Engineering, K.S.Rangasamy College of Technology, KSR Kalvi Nagar, Tiruchengode, Namakkal-637 215, Tamilnadu, India[2, 3, 4]

**ABSTRACT**- Ad-hoc networks don't have any Pre-established Network infrastructure or topology. An ad-hoc network in terms of wireless is a small LAN network in which each wireless have a ability to directly communicate with the other peer, especially in some wireless connections, in which some of the network nodes are part of the network only for the duration of a session or, in the case of mobile or portable devices, while in some close proximity to the rest of the network.

Mobile Ad-hoc Network (MANET-Self configurable infrastructure less network) is a collection of independent nodes within the network that can communicate using radio waves as medium. The mobile devices that are in range can directly communicate, whereas others make use of intermediate nodes to route their packets. It uses the combination of ID based encryption and Group signature for route discovery. USOR provides security against both inside and outside attackers.

**KEYWORDS —** Routing protocols, security, privacy, anonymity

## I. INTRODUCTION

The goal of mobile ad hoc security is to safeguard the nodes' operation and ensure the availability of communication in spite of adversary nodes. The node operations can be divided into two phases. The first phase is to discover the route (s) path. The second phase is to forward the data on the available discovered routes. Both stages need to protect from attacks; so many protocols have been proposed to secure the routing and data forwarding.

MOBILE AD HOC NETWORK

Mobile Ad hoc Network (MANET) is defined as a network without infrastructure, meaning a network without the usual routing infrastructure like fixed routers and routing backbones. It composes of a number of nodes that connect on wireless medium with each other in a specified range zone. Since the wireless medium zone is limited the node forwards a packet either by one hop or using multiple hops when the destination out of the zone as illustrated in Fig. 1. There are many applications depending on using MANET such as military mission, relief disaster and meeting.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

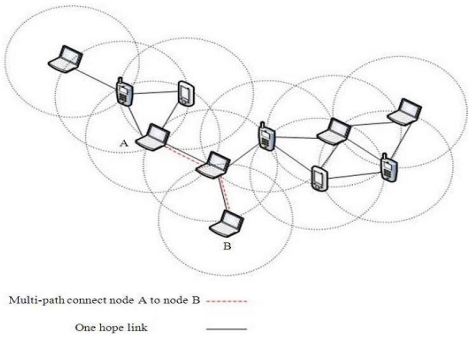
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014




Route request message is flood throughout the whole network (broadcast). Route reply message send to source node only (unicast).

Here Nonce (random number) is used to provide the unobservability. Nonce means number used once, once the number is used for communication it will not be reused again. Each route request contains sequence number (unique) and route pseudonym. 'A' chooses a Nonce and calculates a route pseudonym Nym = H (k*|Nonce).

ROUTING

Data transfer is performed by using the route request and route reply.

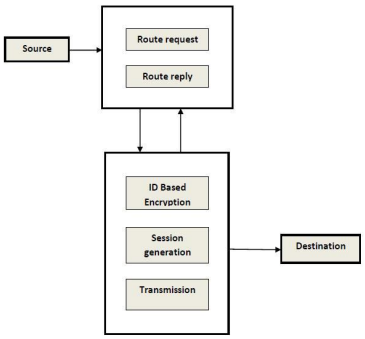



Figure.1.2 Routing

EXISTING SYSTEM

PROCESS OF UNOBSERVABLE ROUTING SCHEME

1. ANONYMOUS KEY ESTABLISHMENT

In this phase, every node in the ad hoc network communicates with its direct neighbors within its range for anonymous key establishment. Each node uses anonymous key establishment to anonymously construct a set of session keys with each of its neighbors. There are two parts

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

i) Node Authentication

ii) Session key Generation

1.1 Node Authentication

Each node creates its own signing key and generates the signature and send to its neighbor, that neighbor node checks, if the key is valid or not. If the key appears to be valid then it generates the session key and its own signing key and sends to the reply. For example, 'A' wants to communicate with 'B', then 'A' send its own signing key to 'B'. 'B' checks the key if the key is valid, then it creates the own signing key and session key replied to 'A'.

1.2 Session Key Generation

Once the keys are valid, 'B' sends its signature and generates the session key and it end the reply to 'A'. 'A' checks the key; if it is valid it generates the session key. Both the session keys are matched then it has to do the data transfer. If the session keys are not same, attacker can be identified.

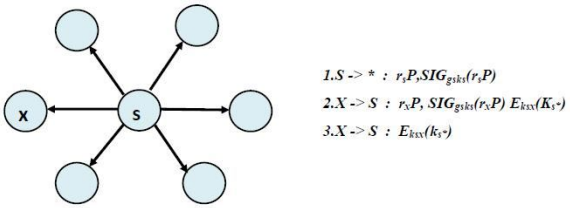



Figure.1.2.1.Anonymous Key Establishment

## II. PRIVACY PRESERVING ROUTE DISCOVERY

This phase is a privacy-preserving route discovery process based on the keys established in the previous phase. Similar to normal route discovery process, the 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.

2.1. Route Request

The source node S chooses a random number and uses the identity of destination node D to encrypt trapdoor information that only can be opened with D's private ID-based key. S selects a sequence number for this route request and another random number as the route pseudonym. It is used as the index to a specific route entry.

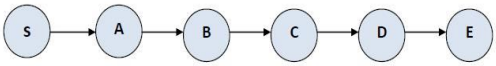



Figure.2.1.1. Route Request

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

2.2. Route Reply

After node D finds out it is the destination node, it starts to prepare a reply message to the source node. D chooses a random number and computes a cipher text showing that he is the valid destination capable of opening the trapdoor information. A session key is computed for data protection. Then he generates a new pair wise pseudonym between C and him. At the end, the pair wise session key is used. It computes and sends the following message to C

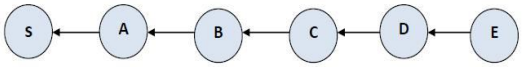



Figure.2.2.1.Route Reply

2.3. Unobservable Data Packet Transmission

The source node S successfully finds out a route to the destination node D, S can start unobservable data transmission under the protection of psuedonyms. The data packets sent by S.A receiving the message from S, A knows that this message is for him according to the pseudonym. After decryption using the right key, A knows this message is a data packet and should be forwarded to B according to route pseudonym. Finally data packet reached a node D. This is depends upon route table entry D knows himself is the destination of this packet.

2.4. Unobservability Scheme using Nonce:

A nonce, in information technology, is a number generated for a specific use, such as session authentication. In this context, "nonce" stands for "number used once" or "number once". It is some value that varies with time, although a very large random number is sometimes used. Where the same key is used for more than one message then a different nonce is used to ensure that the key stream is different for different messages encrypted with that key. Often the message number is used.

To ensure that a nonce is used only once, it should be time-variant, or generated with enough random bits to ensure a probabilistically insignificant chance of repeating a previously generated value. Some authors define pseudo randomness (or unpredictability) as a requirement for a nonce.

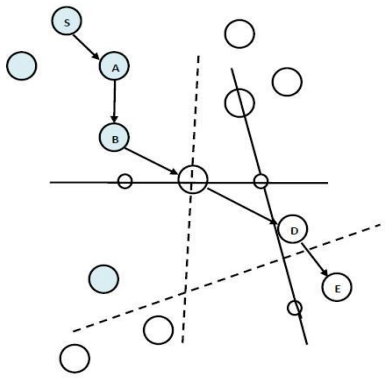



Figure 2.4.1. Sender Anonymity Reduction

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

DRAWBACKS

1. The existing system is not able to prevent wormhole attacks.

2. Unobservable routing scheme floods the route request messages throughout the whole network.

## III. PROPOSED SYSTEM

The proposed system in addition with existing system implementation, also proposes a wormhole attack resistant secure neighbor discovery (SND) scheme, which establishes the communications with signature-based authentication techniques, and achieves SND by utilizing the information of antenna direction, local time information and carefully designed length of the broadcast message.

Second, it introduces a random delay multiple access (RDMA) protocol to solve the transmission collision problem in the response/authentication phase when each node in the same sector does not have information of others and cannot listen to the others transmissions due to the limitation of directional antenna.

Third, it conducts extensive secure analysis and neighbor discovers time analysis to demonstrate the effectiveness and efficiency of the proposed wormhole attack resistant SND scheme.

MODULE DESCRIPTION

The project contains following are the module description as follows,

1. Route Request
2. Route Reply
3. Unobservable Data Packet Transmission
4. Unobservability Scheme using Nonce

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

ADVANTAGES

- The suspicious node can be tracked easily since it does not satisfy the node behaviors of neighbor nodes.
- The proposed SND scheme can effectively prevent and detect wormhole attack.

## IV. FUTURE WORK

Future work along this direction is to study how to defend against wormhole attacks, which cannot be prevented with USOR. Also how to make the unobservable routing scheme resistant against DoS attacks is a challenging task that demands in-depth investigation. USOR requires a signature generation and two point multiplications in the first process.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

In the route discovery process, each node except the source node and destination node needs one ID-based decryption, while the source node and destination Node has to do two ID-based encryption/decryption and two point multiplications.

## V. CONCLUSION

In this paper, to propose an unobservable routing protocol USOR based on group signature and ID-based cryptosystem for ad hoc networks. The design of USOR offers strong privacy protection-complete unlinkability and content unobservability for ad hoc networks.

The security analysis demonstrates that USOR not only provides strong privacy protection, it is also more resistant against attacks due to node compromise. To implement the protocol on ns2 and examined performance of USOR, this shows that USOR has satisfactory performance in terms of packet delivery ratio, latency and normalized control bytes.

Future work along this direction is to study how to defend against wormhole attacks, which cannot be prevented with USOR. Also how to make the unobservable routing scheme resistant against DoS attacks is a challenging task that demands in-depth investigation.

## REFERENCES

[1] 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. 2012.

[2] B. Zhu, Z. Wan, F. Bao, R. H. Deng, and M.

KankanHalli, "Anonymous secure routing in mobile ad-hoc networks," in Proc. 2011 IEEE Conference on Local Computer Networks, pp. 102–108.

[3] S. Seys and B. Preneel, "ARM: anonymous routing protocol for mobile ad hoc networks," in

Proc. 2010 IEEE International Conference on Advanced Information Networking and Applications, pp. 133–137.

[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. 2012 IEEE LCN, pp. 618–624.

[5]. D. Sy, R. Chen, and L. Bao, "ODAR: on-demand anonymous routing in ad hoc networks," in 2011 IEEE Conference on Mobile Ad-hoc and Sensor Systems.

[6]. J. Ren, Y. Li, and T. Li, "Providing source privacy in mobile ad hoc networks," in Proc. IEEE

MASS'09, pp. 332–341.

[7]. Y. Zhang, W. Liu, and W. Lou, "Anonymous communications in mobile Ad hoc networks," in 2009 IEEE INFOCOM.

[8]. K. E. Defrawy and G. Tsudik, "ALARM: anonymous location-aided routing in suspicious MANETs," IEEE Trans. Mobile Comput., vol. 10, no. 9, pp. 1345–1358