Secure Routing Protocol with Unobservable Identity for MANET

[1]Chanchal G. Gaikwad, [2]Prem A. Nankani, [3]Heena M. Sonawane, [4]Kiran K. Nagrani

Students
Computer Engineering,
SSBT's COET, Bambhori, Jalgoan, India

***Abstract*— Two issues plays the critical role for the Mobile ad hoc network i.e Privacy and Routing. Stronger privacy is needed for mobile ad hoc networks. An unobservable secure on demand routing protocol used to provide complete unlinkability and unobservablitiy for all packets. It uses the combination of ID based encryption and Group signature for route discovery. USOR protocol help attacker to break cipher using repetitions. The objective of work is to develop a secure routing protocol scheme with hashing in session authentication. By implementing a USOR protocol using advanced hashing technique in NS2. USOR provides security against both inside and outside attackers.**

***IndexTerms*— key establishment, unobservability, security, privacy preserving.**

I. INTRODUCTION

Mobile Adhoc Network (MANET) is a collection of independent mobile nodes that can communicate to each other via radio waves. 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 communication. 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.

Mobile ad-hoc networks (MANETs) are rapidly evolving as an important area of mobility. MANETs are infrastructure less and wireless in which there are several routers which are free to move arbitrarily and can manage themselves in same manners. The network topology changes very rapidly and unpredictably in which many mobile nodes moves to and from a wireless network without any fixed access point where routers and hosts move, so topology is dynamic. It has to support multi hop paths for mobile nodes to communicate with each other and can have multiple hops over wireless links; also connection point to the internet may also change. If mobile nodes are within the communication range of each other than source node can send message to the destination node otherwise it can send through intermediate node. Existing schemes fail to protect all content of packets from attackers, so that the attacker can obtain information like packet type and sequence number etc.

Background:

Unobservable Secure On-Demand Routing Protocol achieves content unobservability by employing anonymous key establishment based on group signature [1]. The unobservable routing protocol is 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 [2]. Only valid nodes can distinguish routing packets and data packets from dummy traffic with inexpensive symmetric decryption. A node can establish a key with each of its neighbors, and then uses such a key to encrypt the whole packet for a corresponding neighbor [4]. The receiving neighbor can distinguish whether the encrypted packet is intended for it by trial decryption.

Motivation:

MANETs are vulnerable to various types of attacks on network layer. In specific attacks malicious nodes deliberately disrupt data transmission in the network by sending\ incorrect routing information. These attacks disturb route discovery process and degrade network's performance. Thus it is a challenge to keep the communication route free from such attackers [5].

Contribution:

Unobservable Secure On-Demand Routing Protocol achieves the session key establishment. Session key establishment use nonce concept for random number generation. The source node chooses a random number and uses the identity of destination node to encrypt trapdoor information that only can be opened with destination private ID-based key. Source selects a sequence number for route request and another random number as the route pseudonym. Pseudonym is used as the index to a specific route entry.

Organization:

The paper is organized as follows: section II describes related work of system. Result and Performance of system are presented in Section III and Section IV concludes the work.

II. RELATED WORK

A.Menaka and N.Kumaratharan, in [1], have proposed system USOR: An Unobservable Secure On-Demand Routing Protocol for Mobile Ad Hoc Networks is efficient as it uses a novel combination of group signature and ID-based encryption for route discovery. Security analysis demonstrates that USOR can well protect user privacy against both inside and outside attackers. Zhiguo Wan et. al., in [2], proposed USOR that achieves content unobservability by employing anonymous key establishment based on group signature. Each node only has to obtain a group signature signing key and an ID-based private key from an offline key server 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. USOR is to protect all parts of a packet's content, and it is independent of solutions on traffic pattern unobservability. And it can be used with appropriate traffic padding schemes to achieve truly communication unobservability.

Dr. V. Khanaa and Dr. Krishna Mohanta, in [3], proposed to achieve unobservability, a routing scheme should provide unobservability for both content and traffic pattern. Hence further refine unobservability into two types: 1)*Content Unobservability*, referring to no useful information can be extracted from content of any message;2) *Traffic Pattern Unobservability*, referring to no useful information can be obtained from frequency, length, and source-destination patterns of message traffic.

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. A nonce can be a time stamp, a visit counter on a Web page, or prevent the unauthorized replay or reproduction of a file. An initialization vector (IV) is a nonce used for data encryption. The IV, used only once in any session, prevents repetition of sequences in encrypted text. Identifying such repetitions can help an attacker break a cipher.

In security engineering, nonce is an arbitrary number used only once in a cryptographic communication. It is similar in spirit to a nonce word, hence the name. It is often a random or pseudo-random number issued in an authentication protocol to ensure that old communications cannot be reused in replay attacks. A nonce may be used to ensure security for a stream cipher. 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. Nonces are used in proof of work systems to vary the input to a cryptographic hash function so as to obtain a hash for a certain input that fulfils certain arbitrary conditions. In doing so, it becomes far more difficult to create a "desirable" hash than to verify it, shifting the burden of work onto one side of a transaction or system.

Routing protocol:

Anonymous Key Establishment:

Every node in the network communicates with its direct neighbors within its radio range for anonymous key establishment. Suppose there is a node *S* with a private signing key *gskS* and a private ID based key *KS* in the adhoc network and it is surrounded by a number of neighbors within its power range. The messages are exchanged in this phase are not unobservable but this would not leak any private information like node identities. The result of this phase, a pair wise session key

kSX is constructed anonymously; the two nodes establish this key without knowing who the other party is. Node *S* establishes a local broadcast key ¯ *kS**, and transmits it to all its neighbors. It is used for per-hop protection for route discovery [7].

Steps involved for generating a group signature:

i. S generates a random number rS∈Zq* and computes rSp, where P is the generator of G1. Then computes a signature of rSP using its private signing key gsks to obtain *SIGgsks*(*rSp*). Anyone can verify this signature

using the group public key *gpk*. It broadcast within its neighborhood.

ii. A neighbor X of S receives the message from Sand verifies the signature in that message. If theverification is successful, X chooses a random number rX∈Zq * and computes rXP. X also computes a signature

using its own signing key gskX. X computes the session key kSX = H2(rSrXP), and replies to S with message<rXP, SIGgskX (rSP|rXP),EkSX(¯ kX*|rSP|rXP)>.

iii. Receiving the reply from X, S verifies the signature inside the message. If the signature is valid, S proceeds to compute the session key between X and itself as kSX =H2(rSrXP). S also generates a local broadcast key ¯Ks*,

and sends to its neighbor X to inform X about the established local broadcast key.iv. X receives the message from S and computes the same session key as kSX =H2(rSrXP). Then it decrypts the message to get the local broadcast key.

Route Discovery:

The route discovery process can be initiated by the source node to discover a route to the destination node. In this process each node except the source node and the destination node needs one ID based decryption. The route discovery process also comprises of route request and route reply. The route request messages can be flood throughout the whole network, then the corresponding route reply messages are sent backward to the source node only [6]. Each node maintain the routing table,

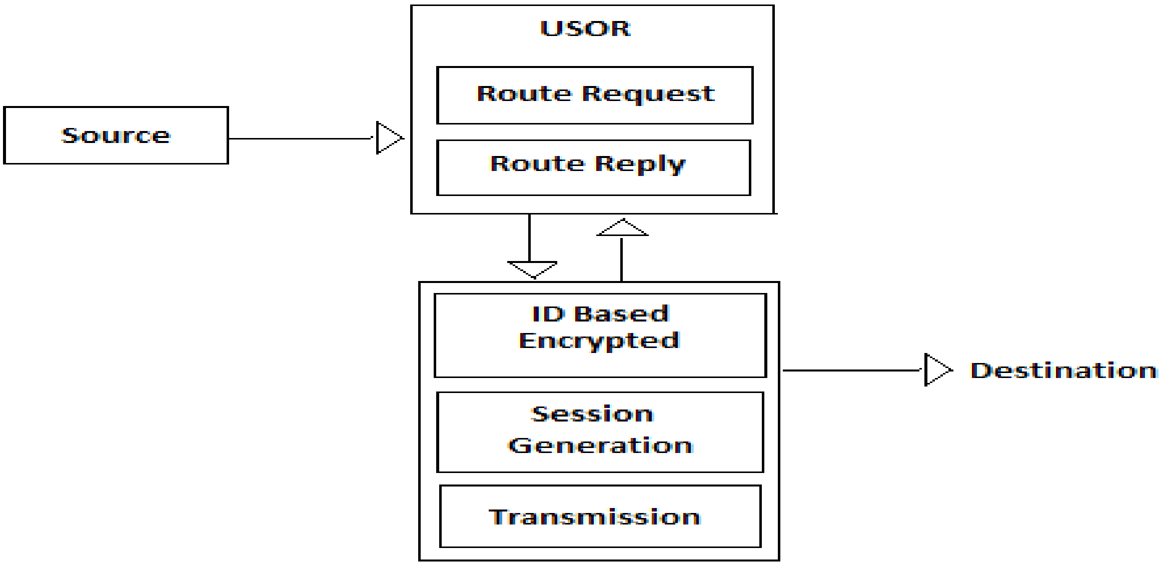

Fig: Process of USOR scheme

and updates the content while receiving a routing message. When a originator needs to send data to a destination, if in the originator's routing table, the path toward the destination is out of date, or there is simply no path toward the destination, the originator would broadcast an RREQ to all nodes [8].

The sender broadcasts the route request initially and hence the RREQ message is broadcasted to all other nodes. The node which decrypts the message with its own session key constructed in the earlier phase. It is widely used to authenticate the neighbors with a valid session key. After receiving the RREQ message then the receiver sends the route reply to the source node. The secure route is constructed between the source the destination.

Packet Data Transmission:

The source node *S* successfully finds a route to the destination node *D*, node *S* can starts data transmission under the protection of pseudonyms and keys. The data packets from

source node *S* must traverse nodes *A*, *B*, and *C* to reach destination node *D*. The data packets sent by source node *S*. Receiving the message from source node *S*, node *A* knows that this message according to the pseudonym Nym*SA*. After decryption key, node *A* knows this message is a data packet should be forwarded to node *B* according to route pseudonym *NS*. Hence node S composes and forwards the packet to node *B*. Data packet is forwarded by other intermediate nodes until it reaches the destination node *D*.

III. RESULT

For the simulation of the developed system, latest version2.34 of NS- 2 has been used in this paper. Ns- 2 is a discrete event simulator targeted at networking research. Network Simulator (Version 2), widely known as NS2, is simply an event driven simulation tool that has proved useful in studying the dynamic nature of communication networks. Simulation of wired as well as wireless network functions and protocols (e.g. routing algorithms, TCP,

UDP) can be done using NS2. In general, NS2 provides users with a way of specifying such network protocols and simulating their corresponding behaviors.

USOR requires a signature generation. 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 have to do two ID-based encryption/decryption.

Table 1: parameters on cryptographic operations

PARAMETER	SPECIFICATION
1024-bit ID-based encryption	20ms
1024-bit ID-based decryption	16ms
Group signature generation	22ms
Group signature verification	24ms
1024-bit pairing	8ms

Simulation time	100s
No. of mobile nodes	50
Routing protocol	USOR

In graph, USOR routing protocol performance measures in terms of packet delivery ratio. Performance of USOR is improved using hashing technic. Performance is improved then low power consumption.

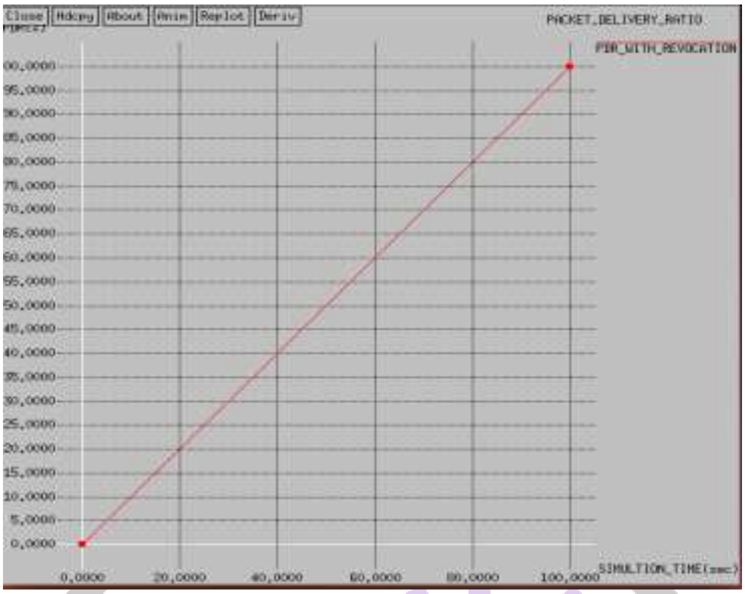

Fig: Packet Delivery Ratio

Ns-2 simulator has two files. These are one is NAM file, and another one is TRACE file. Nam file is used to store the temporary information about nam window, and trace file is used to trace the network environment.

IV. CONCLUSION

Unobservable routing protocol USOR based on group signature and ID-based cryptosystem for ad hoc networks. The design of USOR offers strong privacy 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. USOR Protocol based on advanced hashing technique provides better performance. The implementation of the protocol and its performance shows satisfactory performance in terms of packet delivery ratio.

REFERENCES

[1] A.Menaka, N.Kumaratharan,”*Secure Routing Protocol Based On Unobservable Identity in Mobile Ad-Hoc Networks*”, International Journal of P2P Network Trends and Technology- Volume3 Issue1- 2013.

[2] Zhiguo Wan, KuiRen, and Ming Gu, ”*USOR: An Unobservable Secure On-Demand Routing Protocol for Mobile Ad Hoc Networks*”, In IEEE transactions on wireless communications, vol. 11, no. 5, may 2012.

[3] Dr.V.Khanaa, Dr.KrishnaMohanta,”*An Unlinkable and Unobservable Secure Routing with Symmetric Approach for MANETS*”, International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 2 Issue 3 March 2013 Page No. 551-557.

[4] S. Srikanth, S.Penchala Reddy, V. Jai Kumar,”*Unobservable Secure Proactive Routing Protocol For Fast & Secure Transmission*”,In International Journal of Research in Computer and Communication Technology, Vol 3, Issue 11, November – 2014.

[5] R.Regan, D.Muruganandam, S. Senthil,“*Privacy Preserving USOR Protocol Using Mobile Adhoc Networks*”, In International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-4, April 2013.

[6] B. Zhu, Z. Wan, F. Bao, R. H. Deng, and M. KankanHalli, “Anony- mous secure routing in mobile ad-hoc networks,” in *Proc. 2004 IEEE Conference on Local Computer Networks*, pp. 102–108.

[7] 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.

[8] L. Song, L. Korba, and G. Yee, “AnonDSR: efficient anonymous dynamic source routing for mobile ad-hoc networks,” in *Proc. 2005 ACM Workshop on Security of Ad Hoc and Sensor Networks*, pp. 33– 42.