International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 4, April - 2013

Unobservable Packet Transmission For Mobile Adhoc Network

[1]S.Kamalakannan, [2]Shanthi.M, [3]Shalini.M, [4]Vijayalakshmi.M
[1]Assistant Professor, SNS College of Engineering, Coimbatore
[2,3,4]Final year ECE, SNS College of Engineering, Coimbatore

Abstract:- Mobile ad hoc networks is a self organised,self controlled and self resourceful network.Privacy-preserving routing is crucial for some ad hoc networks that require stronger privacy protection. A number of schemes have been proposed to protect privacy in ad hoc networks. However, none of these schemes offer complete unlinkability or unobservability property since data packets and control packets are still linkable and distinguishable in these schemes. In this paper, stronger privacy requirements regarding privacy-preserving routing in mobile ad hoc networks is defined. Then an unobservable secure routing scheme USOR is proposed to offer complete unlinkability and content unobservability for all types of packets. USOR 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. USOR is implemented on ns2, and evaluated its performance by comparing with AODV. The simulation results show that USOR not only has satisfactory performance compared to AODV, but also achieves stronger privacy protection than existing schemes like MASK.

Key-words: *USOR (Unobservable Secure On-DemandRouting Protocol), MANET (Mobile Ad-hoc Network)*

1. 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 movement pattern, while this sensitive information should be kept private from adversaries in wireless environments. Otherwise, an adversary is able to profile users according to their behaviors, and endanger or harm users based on such information. Lastly, providing privacy protection for ad hoc networks with low-power wireless devices and low-bandwidth network connection is a very challenging task. With regard to privacy-related notions in communication networks, followed the terminology on anonymity, unlinkability, and unobservability discussed in . These notions are defined with regard to item of interest (IOI, including senders, receivers, messages, etc.) as follows:

• Anonymity is the state of being not identifiable within a set of subjects,the anonymity set.

• Unlinkability of two or more IOIs means these IOIs are no more or no less related from the attacker's view.

• Unobservability of an IOI is the state that whether it exists or notis indistinguishable to all unrelated subjects, and subjects related tothis IOI are anonymous to all other related subjects.

In above definitions, related and unrelated subjects refer to subjects involved or not involved in network operations like routing or message forwarding. Privacy protection in routing of MANET has interested a lot of research efforts. A number of privacy-preserving routing schemes have been brought forward. However, existing anonymous routing protocols mainly consider anonymity and partial unlinkability in MANET, most of them exploit asymmetric features of public key cryptosystems to achieve their goals. Complete unlinkability and unobservability are not guaranteed due to incomplete content protection.

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. This information can be used to relate two packets, which breaks unlinkability and may lead to source traceback attacks. Meanwhile, unprotected packet type and sequence number also make existing schemes observable to the adversary. Until now, there is no solution being able to achieve complete unlinkability and unobservability. Unfortunately, unlinkability alone is not enough in hostile environments like battlefields as important information like packet type is still available to attackers. Then a passive attacker can mount traffic analysis based on packet type.

In this case, it is preferable to make the traffic content completely unobservable to outside attackers so that a passive attacker only overhears some random noises. However, this is far from an easy task because it is extremely difficult to hide information on packet type and node identity. Furthermore, a hint on using which key for decryption should be provided in each encrypted packet, which demands careful design to remove linkability.

The most of previous schemes rely heavily on public key cryptography, and thus incur a very high computation overhead. Among these requirements unobservability is the strongest one in that it implies not only anonymity but also unlinkability. To achieve unobservability, a routing scheme should provide unobservability for both content and traffic pattern.

Hence it is further refine unobservability into two types:

- Content Unobservability, referring to no useful information can be extracted from content of any message;
- Traffic Pattern Unobservability, referring to no useful information can be obtained from frequency, length, and source-destination patterns of message traffic.

The content unobservability, which is orthogonal to traffic pattern unobservability will be focussed and it can be combined with mechanisms offering traffic pattern unobservability to achieve truly unobservable communication.

An efficient privacy-preserving routing protocol USOR that achieves content unobservability by employing anonymous key establishment based on group signature is proposed . The setup of USOR is simple: each node only has to obtain a group signature signing key and an ID-based private key from an offline key server or by a key management scheme like [4]. 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.

The contributions include:

- Provide a thorough analysis of existing anonymous routing schemes and demonstrate their vulnerabilities.
- Proposed USOR to our best knowledge, the first unobservable Routing protocol for ad hoc networks, which achieves stronger privacy protection over network communications.
- Detailed security analysis and comparison between USOR and other related schemes are presented in the paper.
- Implemented USOR on ns2 and evaluated its performance by comparing it with the standard implementation of AODV in ns2.

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

2. AN UNOBSERVABLE ROUTING SCHEME

In this section presented an efficient unobservable routing scheme USOR for ad hoc networks. 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 pair wise key are needed. As a result, USOR comprises two phases: anonymous trust establishment and unobservable route discovery.

The unobservable routing scheme USOR aims to offer the following privacy properties.

- **Anonymity**: The senders, receivers, and intermediate nodes are not identifiable within the whole network, the largest anonymity set.
- **Unlinkability**: The linkage between any two or more IOIs from the senders, the receivers, the intermediate nodes, and the messages is protected from outsiders. Note-linkage between any two messages, e.g., whether they are from the same source node, is also protected.
- **Unobservability**: Any meaningful packet in the routing scheme is indistinguishable from other packets to an outside attacker. Not only are the content of the packet, but also the packet header like packet type protected from eavesdroppers. And any node involved in route discovery or packet forwarding, including the source node, destination node, and any intermediate node, is not aware of the identity of other involved nodes.

2.1 ASSUMPTIONS, SYSTEM SETUP AND ATTACK MODEL

2.1.1 Assumptions

Since it uses the group signature scheme and follow the same assumptions and definitions of ID-based encryption scheme. Solving the ECDLP and the BDH on the two groups is hard. Both the group signature scheme and the ID-based scheme are based on pairing of elliptic curve groups of order of a large prime, so that they have the same security strength as the 1024-bit RSA algorithm.

2.1.2 System Setup

Consider an ad hoc network consisting n nodes. In this network, all nodes have the same communication range, and each node can move around within the network. A node can communicate with other nodes within its transmission range, and these nodes are called its neighbors. For nodes outside of one's transmission range, one has to communicate via a multi-hop path. Assume the ad hoc network is all connected, and each node has at least one neighbor. Nodes do not use physical addresses like MAC

addresses in data frames to avoid being identified by others. Instead, they set their network interfaces in the promiscuous mode to receive all the MAC frames that can be detected in the neighborhood. This is important to prevent traffic analysis based on MAC addresses.

Before the ad hoc network starts up, by following the group signature scheme, a key server generates a group public key gpkwhich is publicly known by everyone, and it also generates a private group signature key gskXfor each node X. The group signature scheme ensures full-anonymity, which means a signature does not reveal the signer's identity but everyone can verify its validity

2.1.3 Attack Model

With regard to the adversary model, assume a global adversary that is capable of monitoring traffic of the entire ad hoc network. The adversary can monitor and record content, time, and size of each packet sent over the network, and analyze them to obtain information on who is the source or the destination of packets, who is communicating with whom etc. Meanwhile, the adversary can mount active attacks afar or nearby, e.g., injecting, modifying, dropping packets within the network. However, the adversary cannot launch wormhole attacks to attract a large amount of network traffic. The adversary is able to compromise one or more nodes to make his attack more successfully, but each node has at least one legitimate (uncompromised) neighbor after node compromise attack. As a result, the adversary intends to break the aforementioned privacy properties, i.e., anonymity, unlinkability and unobservability.

2.2 PHASE OF UNOBSERVABLE ROUTING SCHEME

The unobservable routing scheme comprises of two phases: anonymous key establishment as the first phase and the route discovery process as the second phase. In the first phase of the scheme, each node employs anonymous key establishment to anonymously construct a set of session keys with each of its neighbors. Then under protection of these session keys, the route discovery process can be initiated by the source node to discover a route to the destination node. Notations used in the description of the scheme are listed in the Table 3.2.

2.2.1 Anonymous Key Establishment

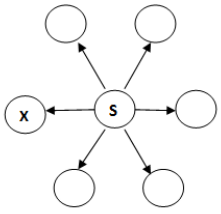
In this phase, every node in the ad hoc network communicates with its direct neighbors within its radio range for anonymous key establishment. Suppose there is a node S with a private signing key gskSand a private ID-based key KS in the ad hoc network and it is surrounded by a number of neighbors within its power range. Following the anonymous key establishment procedure, S does the following:

- S generates a random number rS €q and computes rSP, where P is the generator of G1. It then computes a signature of rSPusing its private signing key gskSto obtain SIGgskS(rSP). Anyone can verify this signature using the group public key gpk. It broadcast _rSP, SIGgskS(rSP)within its neighborhood.

- A neighbor X of S receives the message from S and verifies the signature in that message. If the verification is successful, X chooses a random number rXΣZ S broadcast the first message to its direct neighbors. Each of S's neighbors does the same things as X does to learn S's local broadcast key. kSX= H2(rSrXP). a signature SIGgskX(rSP|rXP) using its own signing key gskX. Computes the session key kSX= H2(rSrXP), and replies to S with message _rXP,
SIGgskX(rSP|rXP),EkSX(¯kX|rSP|rXP)_,
where ¯kXis X's local broadcast key.

- Upon 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 EkSX(¯kS|¯kX|rSP|rXP) to its neighbor X to inform X about the established local broadcast key.

- X receives the message from S and computes the same session key as kSX= H2(rSrXP). It then decrypts the message to get the local broadcast key ¯kS.



1.S→rsP, SIGgsks (rsP)

2.X→S : rxP,SIGgskx (rxP), Eksx (kx*)

3.S→ X : Eksx (ks*)

Fig. 2.1. Anonymous key establishment

Figure 2.1 illustrates the anonymous key establishment process. Note that the messages exchanged in this phase are not unobservable, but this would not leak any private information like node identities. As a result of this phase, a pairwise session key kSXis constructed anonymously, which means the two nodes establish this key without knowing who the other party is. Meanwhile, node S establishes a local broadcast key ¯kS, and transmits it to all its neighbors.

It is used for per-hop protection for subsequent route discovery.

The key establishment protocol is designed following the principal of KAM , which employs Diffie-Hellman key exchange and secure MAC code. It can effectively prevent replay attacks and session key disclosure attack, and meanwhile, it achieves key confirmation for established session keys. KAM has been proved to be secure under the oracle Diffie-Hellman assumption and the hash Diffie-Hellman assumption. Our key establishment protocol uses elliptic curve Diffie- Hellman (ECDH) key exchange to replace Diffie-Hellman key exchange, and uses group signature to replace MAC code. Consequently, the security of our protocol can be derived using the same proof technique of KAM.

2.2.2 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. The route request messages flood throughout the whole network, while the route reply messages are sent backward to the source node only. Suppose there is a node S (source) intending to find a route to a node D (destination), and S knows the identity of the destination node D. Without loss of generality, assume three intermediate nodes between S and D.

2.3 FEATURES

The fundamental feature difference between USOR and ANODR or Anon DSR is that USOR relies on established keys between neighboring nodes to achieve privacy protection, while the other two schemes depend on onion encryption and end-to-end security. Consequently, per-hop protection in USOR can provide complete unlinkability and unobservability efficiently, but ANODR and Anon DSR fail to protect likability or observability of messages. Another advantage of USOR over ANODR is the constant size of routing packets. This makes USOR more advantageous as the attacker cannot obtain private information from packet size, while ANODR has to deal with this issue by padding packets to the same size.

The neighboring nodes authentication in USOR makes use of group signatures, while MASK uses one-time pairing-based keys for preserving privacy. Because these one-time pairing based keys are generated by a trusted party beforehand, thus MASK has to face the problem of one-time key depletion. Moreover, MASK leaks identity information of the destination node during routing discovery, not to mention the disclosure of packet types. However, all these information is well-protected in USOR.

Anonymity

User anonymity is implemented by group signature which can be verified without disclosing one's identity. Group signature is used to establish session keys between neighboring nodes, so that they can authenticate each other anonymously. Subsequent routing discovery procedure is built on top of these session keys. Hence it is easy to see that USOR fulfills the anonymity requirement under both passive and active attacks, as long as the group signature is secure.

Unlinkability

Let's consider the three types of packets. In these packets, they are identified by pseudonyms which are generated from random nonces and secret session keys. The nonce are only used once and never reused, and so are the pseudonyms. Except the random nonce and the pseudonym, the remaining part of the message, including the trapdoor information in the route request, is decrypted and encrypted at each hop. Hence even for a global adversary who can eavesdrop every transmission within the network, it is impossible for him to find linkage between messages without knowing any encryption key. He even has no idea of the type of the packet being transmitted in the network, and he cannot relate different packets in terms of packet type. The only way to gain information on relationship between transmissions is that the attacker has access to some encryption keys, i.e., he has compromised one or more valid nodes.

Unobservability

In USOR, RREQ, RREP and data packets are indistinguishable from dummy packets to a global outside adversary. Meanwhile, nodes involved in the routing procedure are anonymous to other valid nodes. Consequently, USOR provides unobservability as defined for ad hoc networks. First of all, a global adversary cannot distinguish different packet types, and neither can he distinguish a meaningful ciphertext from random noise. Moreover, a node chooses the nonce randomly and never reuses it. The nonce is updated each time after it is used, so there is no linkage between the pseudonyms which are computed from nonces. Only those mobile nodes with valid session keys can recognize valid pseudonyms and decrypt the corresponding ciphertexts to obtain meaningful plaintexts from them. Secondly, a node and its next-hop node or previous-hop node on route establish a session key anonymously, hence no one is able to know real identities of its next-hop node or previous-hop node. Even the source and the destination node do not know real identities of the intermediate nodes on route. As a result, USOR offers content unobservability for ad hoc networks.

Based on the content unobservability provided by USOR, traffic padding can be introduced into the network to thwart traffic analysis and provide traffic

pattern unobservability. Privacy-preserving routing problem is orthogonal to countermeasures against traffic analysis, and appropriate countermeasures against traffic analysis can be applied to make USOR unobservable in terms of traffic pattern.

2.4 NODECOMPROMISE

Node compromise is easy for the adversary and highly possible in ad hoc networks hence it is crucial for a privacy-preserving routing protocol to withstand security attacks due to node capture. In this case, privacy information leakage is unavoidable due to secret exposure, while our routing protocol can protect user privacy against serious node compromise. Suppose a node is compromised by an attacker, his private signing key and ID-based encryption key are disclosed to the attacker.

The attacker has now been able to establish keys with neighboring nodes, but only the following information can be obtained by the attacker:

- The type of a received packet;
- Data/RREP packets sent to/via the compromised node;
- Headers of packets relayed by the compromised node;
- RREQ packets sent from the compromised node's neighbors.

The attacker is not able to gain more beyond this information. From this information, he cannot infer:

- The location of the source/destination node;
- Real identities of source/destination node of the relaying packets;
- Source/Destination node of the RREQ packets.

2.5 COLLUSIONATTACKS

For the colluding outsiders, privacy information is perfectly protected with USOR. As the attacker is unable to distinguish a meaningful packet from a dummy packet, USOR can provide complete protection for privacy with an appropriate traffic padding scheme. Even if the target node is surrounded by more than one attack node, given the assumption that no node is totally surrounded by compromised nodes, the attacker is unable to perceive anything except some random dummy packets. If appropriate dummy traffic is injected into the network, the colluding outsiders cannot gain any privacy information about the network at all.

For the colluding insiders, USOR still offers unobservability as promised. Though information disclosure is unavoidable for colluding insiders, and the adversary knows some keys, the information that the colluding insiders can obtain is largely restricted by USOR.

The attackers are able to know:

- A target node is involved in a route discovery procedure since it is broadcasting a RREQ packet;
- A target node is the previous hop or the next hop on a path. However, the colluding insiders are not able to know identity of the target node or other intermediate nodes on route.

2.6 SYBIL ATTACKS

On the Sybil attack, a single node presents multiple fake identities to other nodes in the network. Sybil attacks pose a great threat to decentralized systems like peer-to-peer networks and geographic routing protocols. In USOR, the centralized key server generates group signature signing keys and ID-based keys for network nodes. Thus, it is impossible for the adversary to obtain other valid identities except the compromised ones. Nevertheless, the anonymity feature of USOR allows the adversary to launch Sybil attacks which are similar to collusion attacks discussed above. As discussed in the collusion attack part, USOR is able to count such attacks effectively.

3. RESULTS AND DISCUSSIONS

In this paper, analysed the resultsof USOR, and compare it with existing schemes. USOR requires a signature generation and two point multiplications in the first process. 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 and two point multiplications.

A detailed comparison on computation cost of existing schemes and USOR is showed in Table 3.1 .

TABLE 3.1: Computation cost of USOR and existing system

	COMPUTATION COST		
PROTOCOL	SOURCE	DESTINATION	INTERMEDIATE
ANODR	*KG+1P(1P)*	*1P*	*KG+2P(2P)*
ASR	*KG+1P(1P)*	*1P*	*KG+2P(2P)*
ARM	*KG+1P(1P)*	*L*P*	*1P*
Anon DSR	*KG+1P(1P)*	*(L+1)*P*	*1P*
SDAR	*KG+2P(2P)*	*(L+1)*P*	*KG+1P(1P)*
ODAR	*KG+1P(1P)*	*1P*	*0*
ARMR	*KG+3P(3P)*	*3P*	*4P*
PRISM	*KG+3P(3P)*	*3P*	*0*
ALARM	*KG+2P(2P)*	*2P*	*0*
USOR	*4P(3P)*	*4P(3P)*	*P*

In this table, ignored the symmetric operations as they are negligible compared to PKC operations. MASK is not listed in the table as they do not need public key operations during the route discovery process. However, MASK does not offer sender anonymity or receiver anonymity. From the table, USOR can achieve unobservability without too much computation cost. In this paper both USOR and MASK on ns2 is implemented, and evaluate their performance by comparing with AODV. In simulation, the scenario

parameters are listed as in table1, and use the cryptographic benchmarks on 1GHz Pentium. In the simulation, 50 nodes are randomly distributed within a network field of size 1500mx300m as such a rectangle field can make the number of hops between two nodes larger. Mobile nodes are moving in the field according to the random way point model, and adopt the speed ranges used. So that the average speeds range from 0 to 10m/s.

Mobile nodes are moving in the field according to the random way point model, and adopt the speed ranges used. So that the average speeds range from 0 to 10m/s. Two different CBR traffic loads are generated for each of the 20 pairs selected from the 50 nodes and 4 packets/s as the heavy traffic load. The local session keys are updated every 40 seconds in the simulation, and each update involves a complete anonymous key establishment procedure. The period a node needs to wait is determined by cryptographic operations the node performs. To simulate cryptographic operations on each node, force each node to delay for some time according to the benchmarks given in table 3.2.

TABLE 3.2: Parameter on cryptographic operationsand experiment scenarios

1024-bit ID based Enc 1024-bitd based Dec Group signature generation Group signature Verification	22ms 17ms 24ms 26ms
Simulation time Scenario dimension Wireless Radio Range Mobile nodes number Average node speed	600s 1500m ×300m 250m 50 0-10m/s

Fig 3.2 Packet Delivery Ratio

USOR has more than 90% packet delivery ratio at high node speeds, only slightly lower than MASK and AODV. Under the heavy traffic load(4 packets/s), performance of all three protocols has downgraded greatly. The biggest difference between USOR and AODV on packet delivery ratio is less than 10%. Apparently, the performance drop of both protocols when node speed goes up due to more frequent route disruption at higher speeds. Route disruption leads to packet drop and retransmission, and a new route has to be constructed before remaining packets can be sent out. Lower packet delivery ratio of USOR is due to the following reasons:

Local key update and node mobility lead to trust lost between one and its neighbors. Before neighboring nodes establish shared local keys, no traffic can be passed between them, which results in transmission delay in USOR; Route repair in AODV is not applicable in the protocol for the sake of privacy protection, as route repair requires identity information about the destination.

In AODV or MASK, intermediate nodes can reply to a route request if they know a route to the requested destination, while USOR cannot do this as any intermediate node is not supposed to know either the source node or the destination node. From (Fig. 3.2) shows that AODV has the least delivery latency and MASK is between AODV and USOR, but the packet delivery latency difference between USOR and MASK is less than 100ms. It is not strange that USOR and MASK have to send more control packets than AODV. In AODV, only three types of routing control packets, namely routing a request packet, routing reply packet, and routing error packet.

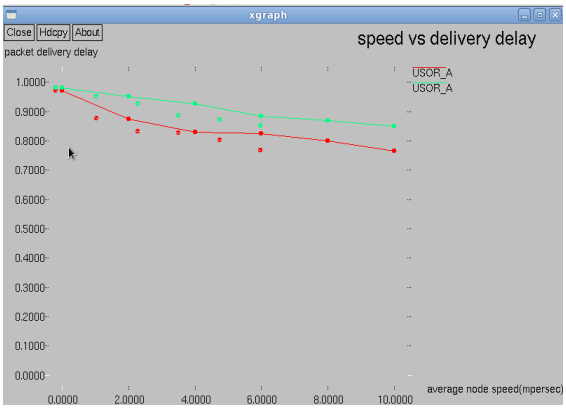


Fig. 3.3 Packet delivery Latency

However, USOR needs more control packets to maintain anonymous routing information. Since MASK and USOR exploit similar key management and route discovery approach, their normalized control bytes are very close. Examine impact of packet padding on USOR's performance with (Fig. 3.3). In the experiment CBR traffic packet size is set to 128 bytes, and CBR traffic frequency is set to 4 packets/s in the experiment. In the padded USOR, all packets including RREQ, RREP packets and other control packets (e.g. Beacon packets) are padded to 128 bytes. Due to the packet padding, performance of the

padded USOR is obviously downgraded, but the padded USOR still achieves satisfactory performance: more than 85% delivery success and about 250ms delivery latency.

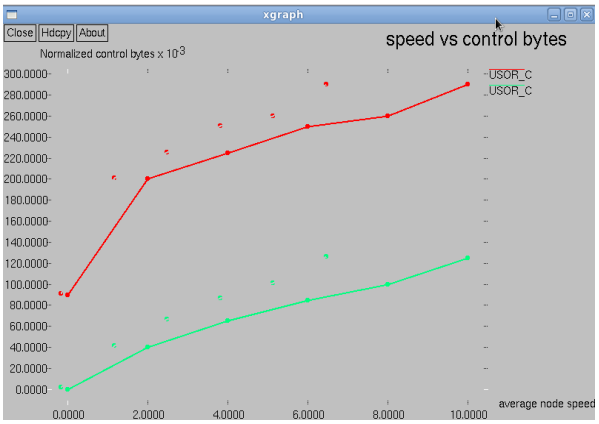


Fig. 3.4 Packet delivery Latency

Finally, USOR with MASK in terms of privacy protection is compared. The number of eavesdropping nodes in the network and compute the sender anonymity of RREQ packets is altered. The sender anonymity is then obtained by calculating entropy of a probability distribution of possible sender of RREQ packets. It can be seen from (Fig. 3.4) that USOR provides best privacy protection regardless of the number of eavesdroppers, while MASK provides better privacy for less eavesdropping nodes. However, when the number of eavesdropper increases to 8 or larger, the privacy entropy does not decrease significantly.

4. CONCLUSION AND FUTURE WORK

This paper proposes 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 completes 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. The protocol is implemented on ns2 and examined performance of USOR, which 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.

REFERENCE

[1] Boneh,D., Boyen,X and Shacham,H (2004). 'Short group signatures inAdvances in Cryptology–Crypto', Lecture Notes in Computer Science,vol. 3152, ,pp. 41–55.

[2] Boneh,D and Franklin,M. (2001) 'Identity-baseencryption from the Weil pairing,'inAdvances in Cryptology–Crypto', Lecture Notes inComputerScience.

[3] Boukerche, A,.Khatib,A., Xu, L., and Korba, L. (2004) 'SDAR: a securedistributed anonymous routing protocol for wireless and mobile ad hocnetworks,' in IEEE LCN, pp. 618–624.

[4] Brown,M., Hankerson,D.,Lopez,J. and Menezes,A. (2001) 'Softwareimplementation of the NIST elliptic curves over prime fields,' in Topics inCryptology.

[5] Capkun, S., Buttyan, L, and Hubaux, J.(2003) 'Self-organized public-keymanagement for mobile ad hoc networks,'IEEE Trans. Mobile Comput.,vol. 2, no. 1, pp. 52–64

[6] Chaum, D. (1981) 'Untraceable electronic mail, return addresses,and digital pseudonyms,' Commun. of the ACM, vol. 4, no. 2

[7] Defrawy,E.J., and Tsudik, G. (2011)'ALARM: Anonymous location-aidedrouting in suspicious MANETs,'IEEE Trans. Mobile Comput., vol. 10,no. 9, pp. 1345–1358.

[8] Dong, Y. T. W. Chim, T, W., Yiu, L and C. K. Hui, K,C. (2009) 'ARMR:anonymous routing protocol with multiple routes for communicationsin mobile ad hoc networks,' Ad Hoc Networks, vol. 7, no. 8.

[9] Dong, D.,Li, M.,Liu,Y.,Li,X and Liao,X. (2011) 'Topological detectiononwormholes in wireless ad hoc and sensor networks,'IEEE/ Netw.

[10] Han ,J. and Liu,Y. (2008)'Mutual anonymity for mobil peerto peer systems,' IEEE Trans. Parallel Distrib. Syst., vol. 19, no. 8, p

[11] Jeong, I.R., Kwon,J.O. and Lee,D.H. (2006)'A Diffie-Hellmankey exchange protocol without random oracles,' in Proc. CANS ,vol. LNCS 4301,54.

[12] Kong, J. and Hong, X. (2003) 'ANODR: 'aonymous on demandrouting with untraceable routes for mobile ad-hoc networks' inProc. ACM MOBIHOC

[13] Liu,Y., Han,J.,andWang,J. (2011)'Rumor riding:anonymizing unstructured peer-to-peer systems,' IEEE Trans.

Parallel Distrib.Syst pp.

[14] Pfitzmann, A. and Hansen, M. (2000) 'Anonymity, unobservability,and Pseudonymity': a consolidated proposal for terminology

[15] Ren, J, Li, Y and Li,T (2009) 'Providing source privacy in mobilead hoc networks,' in Proc. IEEE MASS, pp. 332–341

[16] Seys,S. and Preneel, B. (2006) 'ARM: anonymous routing protocolfor mobile ad hoc networks,' in IEEE International Conferenceon Advanced Information.Networking and Applications, pp. 133–137

[17] Song, L., Korba, L and Yee,G. (2005) 'Anon DSR: efficient anonymousdynamic source routing for mobile ad-hoc networks,' in ACMWorkshop on Security of Ad Hoc and Sensor Networks, pp. 33–42.

[18] Sy, D., Chen, R and Bao,L (2006) 'ODAR: on-demand Anonymous routing in ad hoc networks,'in IEEE Conference onMobile Ad-hoc.

[19] Serjantov,A. and Danezis,G. (2002)'Towards an information theoreticmetric for anonymity ,' in Privacy Enhancing Technologies, pp. 41–53.

[20] Scott,M. (2006)'MIRACL: Multiprecision Integer and RationalArithmeticC/C++ Library

[21] Yu,h.,Kaminsky,M., Gibbons,P,B., and Flaxman,A.(2006) 'Sybilguard:defending against sybil attacks via social networks,' in Proc.

[22] Zhu, Y., Fu, X., Graham, B., Bettati, R., and Zhao, W.(2004) 'On flowcorrelation attacks and countermeasures in mix networks', in PET04,

[23] Zhu, B., Wan, Z., Bao, F., Deng,H,R. and M. KankanHalli, M.(2004)' Anonymous secure routing in mobile ad-hoc networks,' in Proc IEEEConference on Local Computer Networks

[24] Zhang, Y.,Liu, W and Lou,W(2005)'Anonymous communicationsin mobile ad hoc networks,'in2005 IEEE INFOCOM.