www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 2 Issue 3 March 2013 Page No. 551-557

An Unlinkable and Unobservable Secure Routing with Symmetric Approach for MANETS

Dr.V.Khanaa, Dr.Krishna Mohanta

Dean Info. Bharath University Chennai 600 073
Sri Lakshmi Ammal Engineering College Chennai 73
Department of Computer Sci.&Engg.

Mail:drvkannan62@yahoo.com

Abstract—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, define stronger privacy requirements regarding privacy-preserving routing in mobile ad hoc networks. Then propose an unobservable secure routing scheme to offer complete unlinkability and content unobservability for all types of packets. It is efficient as it uses a novel combination of group signature and ID-based encryption for route discovery. Security analysis demonstrates that can well protect user privacy against both inside and outside attackers. Implement it on ns2, and evaluate its performance by comparing with AODV and MASK. The simulation results show that not only has satisfactory performance compared to AODV, but also achieves stronger privacy protection than existing schemes like MASK.

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 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. Otherwise, an adversary is able to profile users according to their behaviors, and endanger or harm users based on such information.

- **Anonymity is the state of being not identifiable within a set of subjects, the anonymity set**.
- **Unlinkability of two or more means these are no more or no less related from the attacker's view.**
- **Unobservability is the state that whether it exists or not is indistinguishable to all unrelated subjects, and subjects related 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 feature 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 break unlinkability and may lead to source trace back 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[2]. 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 unlinkability. Another drawback of most previous schemes is that they rely heavily on public key cryptography, and thus incur a very high computation overhead.

Hence we 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. This paper will focus on content unobservability, which is orthogonal to traffic pattern unobservability, and it can be combined with mechanisms offering traffic pattern unobservability to achieve truly unobservable communication. The major mechanisms to achieve traffic pattern unobservability include MIXes [3] and traffic padding [2].

In this paper, we propose an efficient privacy-preserving routing protocol USOR that achieves content unobservability by employing anonymous key establishment based on group signature. 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 unob- servable route discovery process is executed to find a route to the destination. The contributions of this paper include: 1) we provide a thorough analysis of existing anonymous routing schemes and demonstrate their vulnerabilities. 2) we propose USOR, to our best knowledge, the *first* unobservable routing protocol for ad hoc networks, which achieves stronger privacy protection over network communications. 3) detailed security analysis and comparison between USOR and other related schemes are presented in the paper. 4) we implemented USOR on ns2 and evaluated its performance by comparing it with the standard implementation of AODV in ns2.

We emphasize that our scheme 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.

The rest of the paper is organized as follows. In next section, we discuss related work on anonymous routing schemes for ad hoc networks. Then we describe our unobservable routing scheme in Section III. After that we analyze the proposed scheme against various attacks. We also compare it with other anonymous routing schemes. In Section V, we implement and evaluate performance of USOR. Finally, we summarize and conclude the paper.

RELATED WORK

A number of anonymous routing schemes have been pro- posed for ad hoc networks in recent years, and they provide different level of privacy protection at different cost. Most of them rely on public key cryptosystems (PKC) to achieve anonymity and unlinkability in routing. Although asymmetry of PKC can provide better support for privacy protection, expensive PKC operations also bring significant computation overhead.

Most schemes are PKC-based and the ANODR scheme proposed by Kong et al. [5] is the first one to provide anonymity and unlinkability for routing in ad hoc networks.

Based on onion routing for route discovery, ANODR uses one-time public/private key pairs to achieve anonymity and unlinkability, but unobservability of routing messages is not considered in its design. During the route discovery process, each intermediate node creates a one-time public/private key pair to encrypt/decrypt the routing onion, so as to break the linkage between incoming packets and corresponding outgoing packets. However, packets are publicly labeled and the attacker is able to distinguish different packet types, which fails to guarantee unobservability as discussed.

Meanwhile, both generation of one-time PKC key pairs (this can be done during idle time) and PKC encryption/decryption present significant computation burden for mobile nodes in ad hoc networks.

ASR [6], ARM [7], AnonDSR [8] and ARMR [5] also make use of one-time public/private key pairs to achieve anonymity and unlinkability. ASR is designed to achieve stronger location privacy than ANODR, which ensures nodes on route have no information on their distance to the source/destination node. As the routing onion used in ANODR exposes distance information to intermediate nodes, ASR abandons the onion routing technique while still make use of one-time public/private key pair for privacy protection. ARM [7] considered to reduce computation burden on one-time public/private key pair generation. Different from the above schemes, ARMR [5] uses one-time public keys and bloom filter to establish multiple routes for MANETs.

Besides one-time public/private key pairs, SDAR [3] and ODAR [8] use long-term public/private key pairs at each node for anonymous communication. These schemes are more scalable to network size, but require more computation effort. For example, SDAR is similar to ARM except ARM uses shared secrets between source and destination for verification. Unfortunately, ODAR provides only identity anonymity but not unlinkability for MANET, since the entire RREQ/RREP packets are not protected with session keys. A more recent scheme [7] provides a solution for protecting privacy for a group of interconnected MANETs, but it has the same problem as ODAR.

MASK [4] is based on a special type of public key cryptosystem, the pairing-based cryptosystem, to achieve anonymous communication in MANET. MASK requires a trusted authority to generate sufficient pairs of secret points and corresponding pseudonyms as well as cryptographic parameters. Hence the setup of MASK is quite expensive and may be vulnerable to key pair depletion attacks. The RREQ flag is not protected and this enables a passive adversary to locate the source node. Moreover, the destination node's identity is in clear in route request packets. Though this would not disclose where and who the destination node is, an adversary can easily recover unlinkability between different RREQ packets with the same destination, which actually violates receiver anonymity as defined in [1].

USOR: The Unobservable Routing Scheme

In this section present 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

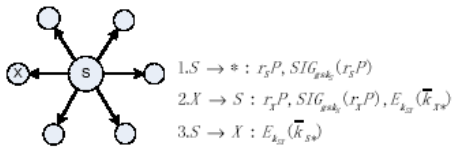

Fig. 1. Anonymous key establishment. S broadcast the first message to its direct neighbors. Each of S's neighbors does the same things as X does to learn S's local broadcast key. $k_{SX} = H_2(r_S r_X P)$.

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.

1) Anonymity: the senders, receivers, and intermediate nodes are not identifiable within the whole network, the largest anonymity set.
2) 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, are also protected.
3) Unobservability: any meaningful packet in the routing
scheme is indistinguishable from other packets to an outside attacker. Not only the content of the packet but also the packet header like packet type are 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 (also including the source node, the destination node, or any other intermediate nodes).

The 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

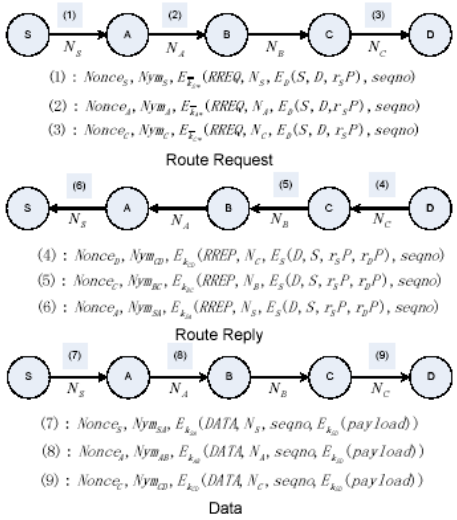

Fig. 2. USOR route request, route reply and data packet transmission.

the description of the scheme is listed in the Table II.

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 gsk_S and a private ID-based key K_S 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:

(1) *S* generates a random number $r_S \in Z^*$

(2) A neighbor X of S receives the message from S and verifies the signature in that message.

(3) 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 $k_{SX} = H_2 (r_S r_X P)$.
(4) X receives the message from S and computes the same session key as $k_{SX} = H_2 (r_S r_X P)$. It then decrypts the message to get the local broadcast key k_{S*}.

Route Request (RREQ): *S* chooses a random number r_S, and uses the identity of node *D* to encrypt a trapdoor information that only can be opened with *D*'s private ID- based key, which yields E_D (*S, D,* r_S *P*). *S* then selects a sequence number *seqno* for this route request, and another random number N_S as the route pseudonym, which is used as the index to a specific route entry.

Each node also maintains a temporary entry in his routing table $\langle seqno, Prev\_RNym, Next\_RNym, Prev\_hop, Next\_hop \rangle$, where *seqno* is the route request sequence number, $Prev\_RNym$ denotes the route pseudonym of previous hop, $Next\_RNym$ is the route pseudonym of next hop, $Prev\_hop$ is the upstream node and $Next\_hop$ is the downstream node along the route.

A generates a $Nonce_A$ a new route pseudonym N_A for this route. He then calculates a pseudonym $\text{Nym}_A = H_3(\bar{k}_A * | Nonce_A)$. He also records the route pseudonyms and sequence number in his routing table for purpose of routing, and the corresponding table entry he maintained is $\langle seqno, N_S, N_A, S, - \rangle$. At the end, *A* prepares and broadcast the following message to all its neighbors:

$$Nonce_A, \text{Nym}_A, E_{\bar{k}_A}(RREQ, N_A, E_D(S, D, r_S P) * seqno). \quad (2)$$

Other intermediate nodes do the same as *A* does. Finally, the destination node *D* receives the following message from *C*

Likewise, *D* finds out the correct key $\bar{k}_{C\_} *$ according to the equation $\text{Nym}_C = H_3(\bar{k}_C * | Nonce_C)$. After decrypting the cipher text using $\bar{k}_C *$, *D* records route pseudonyms and the
Sequence number into his route table. Then *D successfully* decrypts E_D (*S, D,* r_S *P*) to find out he is the destination node. *D may* receive more than one route request messages that originate from the same source and have the same destination *D*, but he just replies to the first arrived message and drops the following ones.

Route Reply (RREP): After node *D* finds out he is the destination node, he starts to prepare a reply message to the source node. For route reply messages, unicast instead of broadcast is used to save communication cost. *D* chooses a random number r_D and computes a cipher text E_S (*D, S,* r_S *P,* r_D *P*) showing that he is the valid destination capable of opening the trapdoor information. A session key $k_{SD} = H_2(r_S r_D P | S | D)$ computed for data protection. Then he generates a new pair wise pseudonym $\text{Nym}_{CD} = H_3(k_{CD} | Nonce_D)$.

The fundamental difference between USOR and ANODR or AnonDSR 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 AnonDSR fail to protect unlinkability or unobservability 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.

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 cipher text 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 nonce. Only those mobile nodes with valid session keys can recognize valid pseudonyms and decrypt the corresponding cipher texts 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 according to the definition in [1].

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. As discussed in Section II, 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.

Node Compromise. 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.

Collusion Attacks. 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: 1) a target node is involved in a route discovery procedure since it is broadcasting a RREQ packet; 2) 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. According to the design of USOR, authentication and key establishment is achieved by group signature, which perfectly protects user identity from disclosure. Consequently, unobservability is guaranteed by USOR under colluding insider attacks according to the definition of unobservability.

Sybil Attacks. In the Sybil attack [11], 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. 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.

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. This traffic load is half of the light traffic (2 packets/s and 512 bytes/packet). 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.

Finally, compare USOR with MASK in terms of privacy protection. We make use of the information theoretic privacy metric discussed in Section IV. We alter the number of eavesdropping nodes in the network and compute the sender anonymity of RREQ packets. The sender anonymity is the obtained by calculating entropy of probability distribution of possible sender of RREQ packets. It can be seen from Fig. 5 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. This is reasonable since the anonymity set of possible senders cannot be reduced any more by introducing more eavesdroppers.

Conclusion and future work

In this paper, proposed an 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.

REFERENCES

[1] A. Pfitzmann and M. Hansen, "Anonymity, unobservability, and pseudonymity: a consolidated proposal for terminology," draft, July 2000.

[2] Y. Zhu, X. Fu, B. Graham, R. Bettati, and W. Zhao, "On flow correlation attacks and countermeasures in mix networks," in *PET04, LNCS 3424*, 2004, pp. 207–225.

[3] D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Commun. of the ACM*, vol. 4, no. 2, Feb. 1981.

[4] 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. 2003.

[5] J. Kong and X. Hong, "ANODR: aonymous on demand routing with untraceable routes for mobile ad-hoc networks," in *Proc. ACM MOBI- HOC'03*, pp. 291–302.

[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.