International Journal of MC Square Scientific Research Vol.5, No.1 Nov 2013

Preserving Privacy Using an Unobservable Secure Routing Protocol for MANETs

R. Anto Pravin, R
P.G Scholar, Department of CSE, National College of Engineering, Tirunelveli
Email: antovpravin@gmail.com

Uma Mageswari
Assistant Professor, Department of CSE, National College of Engineering, Tirunelveli,
Email: uma_tigi@yahoo.co.in

Abstract - Privacy preserving routing is crucial for some ad-hoc networks. Numbers of schemes have been proposed to protect privacy in ad-hoc networks. 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 project, stronger privacy requirements are defined regarding privacy-preserving routing in mobile ad-hoc networks. Then an unobservable secure routing scheme is proposed to offer complete unlinkability and content unobservability for all types of packets. This protocol is efficient as it uses a combination of group signature and ID-based encryption for route discovery. Security analysis demonstrates that Unobservable Secure Routing (USR) protocol can protect user privacy against both inside and outside attackers. USR is implemented on ns2, and its performance is evaluated by comparing with the existing schemes. The simulation results show that this protocol achieves stronger privacy protection than existing schemes.

Keywords - unlinkability, unobservability, mobile ad-hoc networks, group signature.

1. Introduction

Privacy protection of Mobile Ad-hoc Networks (MANETs) is more demanding than that of wired networks due to the open nature and mobility of wireless media. In wired networks there is no need to protect users' mobility behavior or movement pattern, while the sensitive information should be kept private from adversaries in wireless environments. With regard to privacy-related notions in communication networks, the terminology is followed on anonymity, unlinkability, and unobservability.

Privacy protection in routing of MANET has interested a lot of research efforts. However, existing anonymous routing protocols mainly consider anonymity and partial unlinkability in MANET. Complete unlinkability and unobservability are not guaranteed due to incomplete content protection. Earlier schemes failed to protect all content of packets from attackers, so that the attacker would obtain information like packet type and sequence number. Meanwhile, unprotected packet type and sequence number also make existing schemes observable to the adversary. 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. In this case, it is preferable to make the traffic content completely unobservable to outside attackers. However, this is far from an easy task because it is extremely difficult to hide information on packet type and node identity. Another drawback of most previous schemes is that they rely heavily on public key cryptography.

Unobservability is further refined into two types: 1) Content Unobservability, refers to no useful information can be extracted from content of any message; 2) Traffic Pattern Unobservability, refers to no useful information can be obtained from source-destination patterns of message traffic. This project will focus on content unobservability. In this project, an efficient privacy-preserving routing protocol is proposed so that it achieves content unobservability by employing anonymous key establishment based on group signature. The unobservable routing protocol is then executed in two phases. First, a key generation process is performed to construct session keys. Then an unobservable route discovery process is executed to find a route to the destination. The contributions of this project include: 1) a thorough analysis of existing anonymous routing schemes is provided and demonstrated their vulnerabilities. 2) a routing protocol is proposed, (ie) the first unobservable routing protocol for ad-hoc networks, which achieved stronger privacy protection over network communications. 3) detailed security analysis and comparison between this scheme and other related schemes are presented in the project. 4) The project is implemented on ns2 and evaluated its performance by comparing it with the standard implementation of AODV in ns2.

2. Related Work

A number of anonymous routing schemes have been proposed for ad hoc networks, and they provide different level of privacy protection.

ANODR [1] was the first one to provide anonymity and unlinkability for routing in ad-hoc networks. Based on onion routing for route discovery, ANODR used one-time public/private key pairs to achieve anonymity and unlinkability, but unobservability of routing messages was not considered in its design. ASR [2], ARM [3], AnonDSR [4] and ARMR [5] also used one-time public/private key pairs to achieve anonymity and unlinkability. ASR was designed to achieve stronger location privacy than ANODR, which ensured nodes on route have no information on their distance to the source/destination node. ARM was considered to reduce computation burden on one-time public/private key pair generation. ARMR used one-time pubkic keys and bloom filter to establish multiple routes for MANETs.

Besides one-time public/private key pairs, SDAR [6] and ODAR [7] used long-term public/private key pairs at each node for anonymous communication. Those schemes are more scalable to network size, but required more computation effort.

MASK [8] was based on a special type of public key cryptosystem, to achieve anonymous communication in MANET. MASK required a trusted authority to generate sufficient pairs of secret points and corresponding pseudonyms as well as cryptographic parameters. The ALARM [9] used public key cryptography and the group signature to preserve privacy. The group signature had a good privacy preserving feature in that everyone can verify a group signature but cannot identify who is the signer. But ALARM still leaked out lot sensitive privacy information. Similar to ALARM, PRISM [10] also employs location information and group signature to protect privacy in MANETs.

To summarize, public key cryptosystems had a preferable asymmetric feature, and it is well-suited for privacy protection in MANET. As a result, most anonymous routing schemes proposed for MANET make use of public key cryptosystems to protect privacy. However, existing schemes provide only anonymity and unlinkability, while unobservability is never considered.

3. An Unobservable Routing Scheme

In this section, an efficient unobservable routing scheme is presented for ad-hoc networks. In this protocol, both control packets and data packets look random and indistinguishable from dummy packets for outside adversaries. In order to support both broadcast and unicast, a group key and a pair wise key are needed. As a result, the protocol comprised of two phases: anonymous trust establishment and unobservable route discovery.

3.1Assumptions, System Setup and Attack Model

Assumptions: The group signature scheme in [11] and the ID-based encryption scheme in [12] are used in implementing this protocol. 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.

System Setup: An ad hoc network consists of 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.

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 size of each packet sent over the network, and analyzes them to obtain information on who is the source or the destination of packets, who is communicating with whom etc. However, the adversary cannot launch wormhole attacks [13] to attract a large amount of network traffic. As a result, the adversary intends to break the privacy properties.

3.2 The 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, each node employs 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 is listed in the Table I.

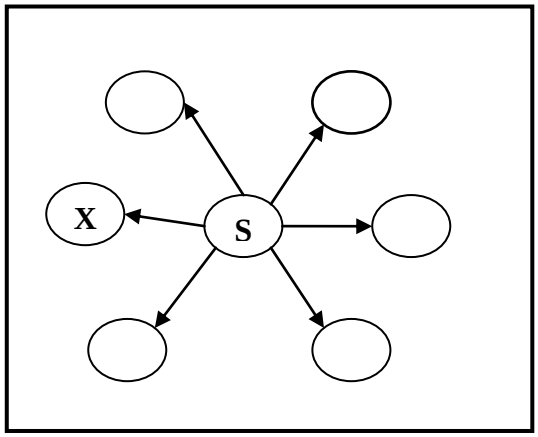

Figure 1: Anonymous key establishment

1) **Anonymous Key Establishment:** Suppose there is a node S with a private signing key $gskS$ and 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:

(1) S generates a random number $rS \in Z^*q$ and computes rSP, where P is the generator of G1. It 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.

(2) 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 rX ∈ Z*q and computes XP. X also computes a signature using its own signing key $gskX$. X computes the session key, and replies to S with message $(rXP, SIGgskX(rSP|rXP), EkSX(\bar{k}^*|rSP|rXP))$, where $\bar{k}X^*$ is X's local broadcast key.

(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 kSX = H2(rSrXP). S also generates a local broadcast key $\bar{k}S^*$, and sends to its neighbor X to inform X about the established local broadcast key.

(4) X receives the message from S and computes the same session. It then decrypts the message to get the local broadcast key $\bar{k}S^*$.

Figure 1 illustrates the anonymous key establishment process. As a result of this phase, a pairwise session key kSX is constructed anonymously, which means the two nodes establish the key without knowing who the other party is. Meanwhile, node S establishes a local broadcast key *kS**, and transmits it to all its neighbors.

Table I: Notations

A- A node in the ad hoc network, and its real identity
s- The master secret key owned by the key server
q- A 170-bit prime number
P- Generator of the elliptic curve group G1
Hi(*)- Secure one-way hash functions, *i* = 1, 2.
gskA- Node *A*'s private group signature key
Gpk-The public group signature verification key
KA- Node *A*'s private ID-based key which is $s \cdot H1(A)$
EA(*)-ID-based encryption using *A*'s public key
kA*- A local broadcast key within *A*'s neighborhood
kAX- A pairwise session key shared between *A* and *X*
Nym*A*- The pseudonym only valid within *A*'s neighborhood
Nym*AX*- The pseudonym shared between *A* and X

2) **Privacy-Preserving Route Discovery:** This phase is a privacy-preserving route discovery process based on the keys established in previous phase. 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.

Route Request (RREQ): S chooses a random number rS, 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 *ED*(*S,D, rSP*). S then selects a sequence number seqno for this route request, and another random number NS as the route pseudonym. To achieve unobservability, S chooses a nonce NonceS and calculates a pseudonym as NymS = H3(¯kS*|NonceS). Each node also maintains a temporary entry in his routing table, 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. As any node does not know the real identity of its upstream or downstream node the entry maintained by S is (*seqno,*−*,NS,*−*,* −*)*.

Upon receiving the route request message from S, A tries all his session keys shared with all neighbors to see which one matches the received Nym*S*. In this example, A is not the destination and his trial fails, so he acts as an intermediate node. A generates a nonce NonceA and a new route pseudonym NA for this route. At the end, A prepares and broadcast the message to all its neighbors. Other intermediate nodes do the same as A does.

Likewise, D finds out the correct key. After decrypting the ciphertext, D records route pseudonyms and the sequence number into his route table. Then D successfully decrypts *ED*(*S,D, rSP*) to find out he is the destination node.

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 rD and computes a ciphertext *ES*(*D, S, rSP, rDP*) 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, using the pair wise session key kCD, he computes and sends the following message to C:

When C receives the above message from D, he identifies who is the sender of the message by evaluating the equation Nym*CD* = *H*3(*kCD*|*NonceD*). So he uses the right key kCD to decrypts the ciphertext, then he finds out which route this RREP is related to according to the route pseudonym NC and seqno. C then searches his route table and modifies the temporary entry (seqno,NB,NC,B,−) into (seqno,NB,NC,B,D). At the end, C chooses a new nonce NonceC, computes NymBC = H3(kBC|NonceC), and sends the message to B. Other intermediate nodes perform the same operations as C does.

S decrypts the ciphertext using the right key kSA *a*nd verifies that *ES*(*D, S, rSP, rDP*) is composed faultlessly. Now S is ensured that D has successfully opened the route request packet, and the route reply is really originated from the destination node D. S also computes the same session key as D does. Till now, S has successfully found a route to the destination node D, and the route discovery process is finished with success. S then finds and modifies his temporary route table entry.

3) Unobservable Data Packet Transmission:

After the source node S successfully finds out a route to the destination node D, S can start unobservable data transmission under the protection of pseudonyms and keys. Data packets from S must traverse A, B, and C to reach D. The data packets sent by S take the following format (DATA denotes the packet type):

Upon receiving the above message from S, A knows that this message is for him according to the pseudonym NymSA. After decryption using the right key, A knows this message is a data packet and should be forwarded to B according to route pseudonym NS. Hence he composes and forwards the following packet to B. The data packet is again forwarded by other intermediate nodes until it reaches the destination node D. At the end, the following data packet is received by D:

4. Security And Privacy Analysis

In this section, issues on anonymity, unlinkability, and unobservability against the global adversary are discussed who can continuously monitor the whole network.

Anonymity: User anonymity is implemented by group signature which can be verified without disclosing one's identity.

Unlinkability: The nonces 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 RREQ, 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.

Unobservability: In USRM, 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.

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 this routing protocol can protect user privacy against serious node compromise.

Collusion Attacks: For the colluding insiders, this protocol still offers unobservability. The attackers are able to know: 1) a target node is involved in a route discovery procedure; 2) a target node is the previous hop or the next hop on a path.

Sybil Attacks: In the Sybil attack [14], 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.

5. Implementation And Performance Evaluation

USR protocol 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.

The protocol is implemented on ns2, and evaluates their performance by comparing with AODV. In the simulation, 50 nodes are randomly distributed within a network. Mobile nodes are moving in the field according to the random way point model. The local session keys are updated every 40 seconds in the simulation. The performance is evaluated in terms of packet delivery ratio, packet delivery latency, and normalized control bytes.

According to Figure 2, USR has the highest packet delivery ratio for both types of traffic load compared to AODV. The packet delivery ratio decreases as nodal speed increases and traffic load becomes heavier. From Figure 3, it is clear that USR has the least average delay compared to existing AODV. Figure 4 illustrates the packet loss rate where USR has lesser packet loss compared to that of AODV.

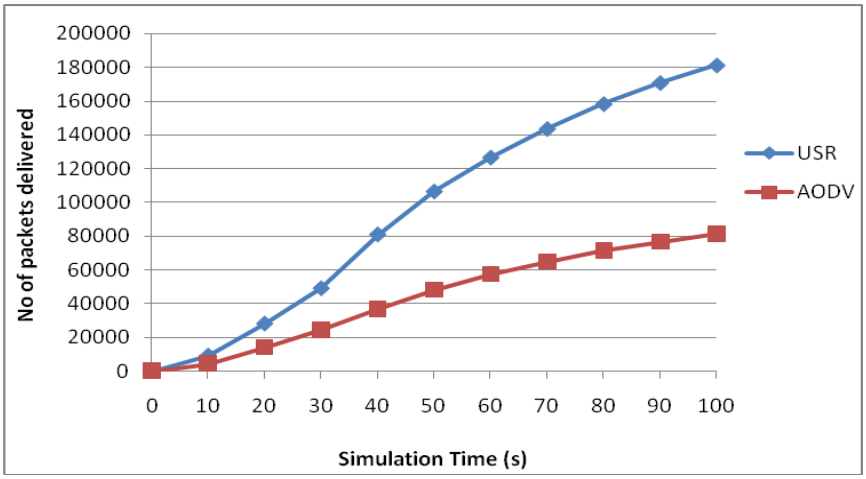

Figure 2: Packet delivery rate

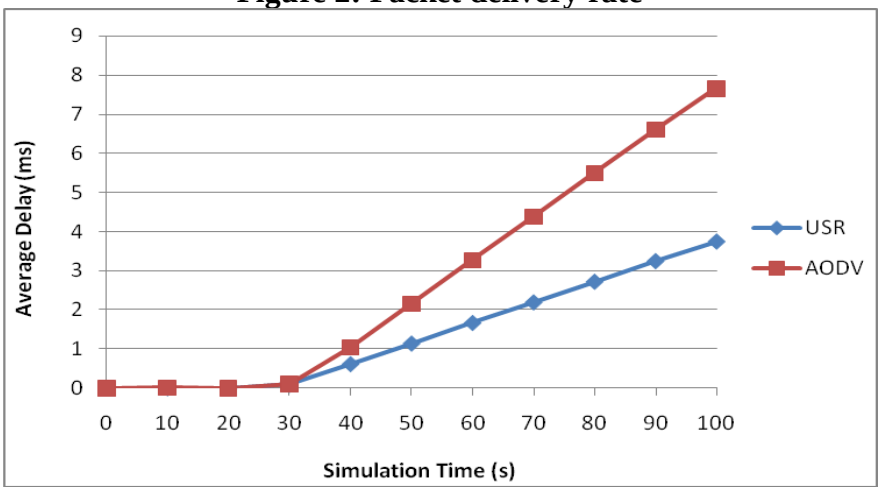

Figure 3: Average delay

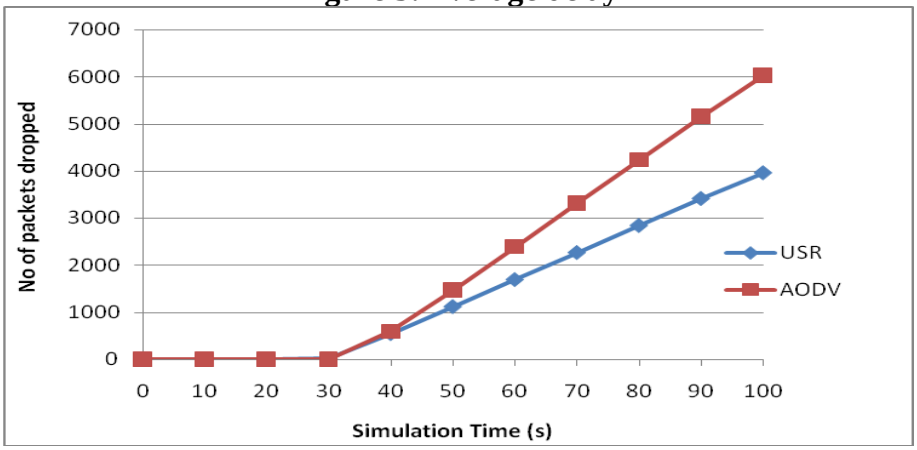

Figure 4: Packet Loss rate

6. Conclusion

In this project, an unobservable routing protocol is proposed based on group signature and ID-based cryptosystem for ad hoc networks. The design offers strong privacy protection complete unlinkability and content unobservability for ad hoc networks. The security analysis demonstrates that this protocol 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 the performance of USR, which shows that USR has satisfactory performance in terms of packet delivery ratio, latency and normalized control bytes.

REFERENCES

[1] Kong, J., Hong, X., "ANODR: anonymous on demand routing with untraceable routes for mobile ad-hoc networks" In Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing, p 291-302, 2003.

[2] Zhu, B., Wan, Z., Kankanhalli, M.S., Bao, F., Deng, R. H., "Anonymous secure routing in mobile ad-hoc networks" In Local Computer Networks, 29th Annual IEEE International Conference on, pp. 102-108, 2004.

[3] Seys, S., Preneel, B., "ARM: Anonymous routing protocol for mobile ad hoc networks" International Journal of Wireless and Mobile Computing, Vol. 3, No. 3, p 145-155, 2009.

[4] Song, R., Korba, L., Yee, G., "AnonDSR: efficient anonymous dynamic source routing for mobile ad-hoc networks" 2005.

[5] Dong, Y., Chim, T.W., Li, V.O., Yiu, S.M., Hui, C.K., "ARMR: anonymous routing protocol with multiple routes for communications in mobile ad hoc networks" Ad Hoc Networks, Vol. 7, No. 8, p 1536-1550, 2009.

[6] Boukerche, A., El-Khatib, K., Xu, L., Korba, L., "SDAR: a secure distributed anonymous routing protocol for wireless and mobile ad hoc networks" In Local Computer Networks, 29th Annual IEEE International Conference on, p 618-624, 2004.

[7] Sy, D., Chen, R., Bao, L., "Odar: On-demand anonymous routing in ad hoc networks" In IEEE International Conference on Mobile Ad Hoc and Sensor Systems, p 267-276, 2006.

[8] Zhang, Y., Liu, W., Lou, W., "Anonymous communications in mobile ad hoc networks", In Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies, Vol. 3, p 1940-1951, 2005.

[9] El-Defrawy, K., Tsudik, G., "ALARM: anonymous location-aided routing in suspicious MANETs", IEEE Transactions on Mobile Computing, Vol. 10, No. 9, p 1345-1358, 2011.

[10] El-Defrawy, K., Tsudik, G., "Privacy-preserving location-based on-demand routing in MANETs", IEEE journal on selected areas in communications, Vol. 29, No. 10, 1926-1934, 2011.

[11] Boneh, D., Boyen, X., Shacham, H., "Short group signatures", In Annual International Cryptology Conference, Springer Berlin Heidelberg, p 41-55, 2004.

[12] Boneh, D., Franklin, M., "Identity-based encryption from the Weil pairing" In Annual International Cryptology Conference, Springer Berlin Heidelberg, p 213-229,2001.

[13] Dong, D., Li, M., Liu, Y., Li, X.Y., Liao, X., "Topological detection on wormholes in wireless ad hoc and sensor networks" IEEE/ACM Transactions on Networking, Vol. 19, No. 6, p 1787-1796, 2011.
[14] Yu, H., Kaminsky, M., Gibbons, P.B., Flaxman, A., "Sybilguard: defending against sybil attacks via social networks", In ACM SIGCOMM Computer Communication Review, Vol. 36, No. 4, p 267-278, 2006.