International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:268
Vol.2, No.3, March 2013 DOI:10.15693/ijaist/2013.v2i3.34-41

Privacy-Preserving Routing Protocol for Mobile Ad Hoc Networks

[1]K. Vinoth Kumar, [2]G.Arunsathish, [3]R.Elamurugan
[1]Assistant professor/ECE, MAR College of engg&Tech, Viralimalai.
[2,3]Students/ECE, MAR College of engg&Tech, Viralimalai.

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, we define stronger privacy requirements regarding privacy-preserving routing in mobile ad hoc networks. Then we propose an unobservable secure routing scheme PPRP to offer complete unlinkability and content unobservability for all types of packets. PPRP is efficient as it uses a novel combination of group signature and ID-based encryption for route discovery. Security analysis demonstrates that PPRP can well protect user privacy against both inside and outside attackers
Keywords-- Privacy-preserving routing, group signature, ID-based encryption.

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 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. 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, we follow the terminology on anonymity, unlinkability, and unobservability discussed in [1]. 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 not is indistinguishable to all unrelated subjects, and subjects related to this IOI are anonymous to all other related subjects.

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 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 [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 linkability. Another drawback of most previous schemes is that they 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 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 atterns of message traffic. This paper will focus on content unobservability, which is orthogonal to traffic attern 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 In this paper, we propose an efficient privacy-preserving routing protocol PPRP that achieves content unobservability by employing anonymous key establishment based on group signature. he setup of PPRP 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 of this paper include:

1) We provide a thorough analysis of existing anonymous routing schemes and demonstrate their vulnerabilities.

2) We propose PPRP, 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 PPRP and other related schemes are presented in the paper.

4) We implemented PPRP on ns2 and evaluated its performance by comparing it with the standard implementation of AODV in ns2. In next section, we discuss related work on anonymous routing schemes for ad hoc networks. After that we analyze the proposed scheme against various attacks. We also compare it with other anonymous routing schemes.

III. RELATED WORK

A number of anonymous routing schemes have been proposed 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 [9] 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 nformation 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 [9] uses one-time pubkic keys and bloom filter to establish multiple routes for MANETs. Besides one-time public/private key pairs, SDAR [10] and ODAR [11] 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 [12] provides a solution for protecting privacy for a group of interconnectedMANETs, but it has the same problem as ODAR. MASK [13] 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 linkability between different RREQ packets with the same destination, which actually violates receiver anonymity as defined in [1]. An anonymous location-aided routing scheme ALARM [14] makes use of public key cryptography and the group signature to preserve privacy. The group signature has a good privacy preserving feature in that everyone can verify a group signature but cannot identify who is the signer. But ALARM still leaks lot sensitive privacy information: network topology, location of every node. Similar to ALARM, PRISM [15] also employs location information and group signature to protect privacy in MANETs. A closely related research direction along this line is anonymous routing in peer-to-peer systems, which has been investigated heavily too. Interested readers are referred to [16], [17] for details.

To summarize, public key cryptosystems have 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 or implemented by now. An obvious drawback in existing schemes is that packets are not protected as a whole. Information like packet types, trapdoor information, public keys is simply unprotected in current proposals, and these can be exploited by a global adversary to obtain useful information.

III. PPRP: PRIVACY-PRESEVING ROUTING PROTOCOL

In this section we present an efficient unobservable routing scheme PPRP 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 pairwise key are needed. As a result, PPRP comprises two phases: anonymous trust establishment and unobservable route discovery. The unobservable routing scheme PPRP 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 linkages 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 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 (also including the source node, the destination node, or any other intermediate nodes).

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 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 shown in fig 1

(1) S generates a random number rS =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 _rSP, SIGgskS (rSP)_ 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 rXP. X also computes

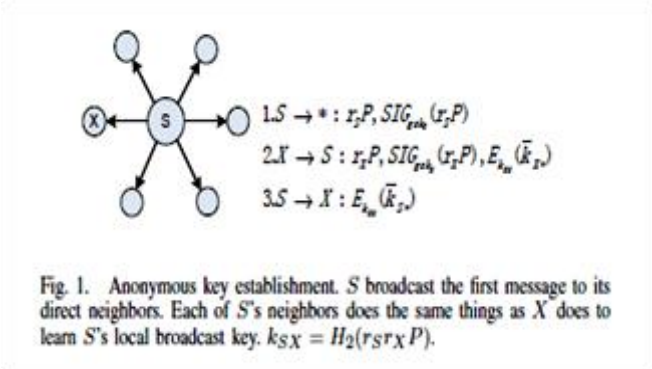

Fig. 1. Anonymous key establishment. S broadcast the first message to its direct neighbors. Each of S's neighbors does the same things as X does to learn S's local broadcast key. $k_{SX} = H_2(r_S r_X P)$.

(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 S also generates a local broadcast key and sends to its neighbor X to inform X about the established local broadcast key. Fig.2 shows the Route Discovery

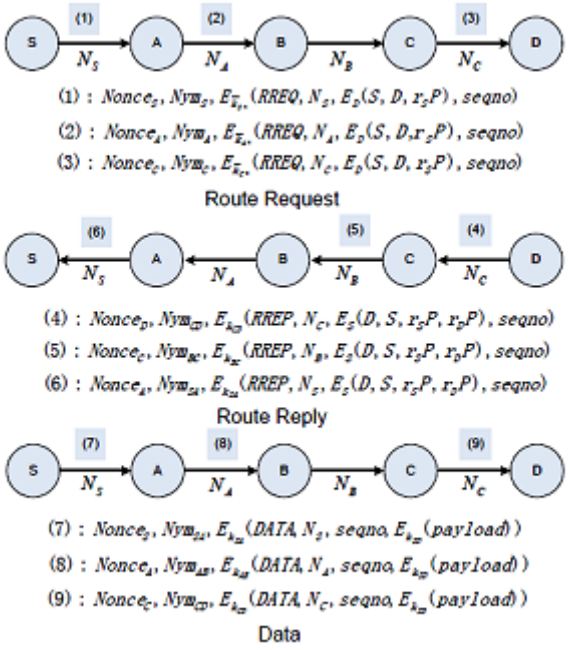

Fig.2 Route Discovery

(4) X receives the message from S and computes the same session key. It then decrypts the message to get the local broadcast key. Figure 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 is 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 , 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 [21], 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. 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, we assume three intermediate nodes between S and D, as illustrated in Fig. 2.

The route discovery process executes as follows:

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

IDbased 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, which is used as the index to a specific route entry. To achieve unobservability, after that, S encrypts these items using its local broadcast key. Finally, S broadcast the following unobservable route request to its neighbors

(1) Upon receiving the route request message from S, A tries all his session keys shared with all neighbors. Then A would find out ¯kS∗ satisfies NymS = H3 (¯kS∗|NonceS), so he uses ¯kS∗ to decrypt the ciphertext. After finding out this is a route request packet, a tries to decrypt using his private IDbased key to see whether he is the destination node. To avoid RREQ broadcasting storm, A will check if he has received the same request before by looking up in his cache, which includes a list of NS and seqno. If it is not a duplicate RREQ, A caches NS and seqno for a given time to detect multiple receipt of the same RREQ packet. 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. He then calculates a pseudonym NymA = H3 (¯kA∗|NonceA). 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 _seqno, NS,NA, S, −_. At the end, A prepares and broadcast the following message to all its neighbors: NonceA, NymA, E¯kA∗ (RREQ, NA, ED(S, D, and rSP), and seqno).

(2) Other intermediate nodes do the same as a does. Finally, the destination node D receives the following message from C: NonceC, NymC, E¯kC∗ (RREQ, NC, ED(S, D, and rSP), and seqno).

(3) Likewise, D finds out the correct key ¯kC∗ according to the equation NymC = H3 (¯kC∗|NonceC). After decrypting the ciphertext using ¯kC∗, 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. 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. The route table entry recorded by D is _seqno, NC,−, C.

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 kSD = H2 (rSrDP|S|D) is computed for data protection. Then he generates a new pairwise pseudonym NymCD = H3(kCD|NonceD) between

C and him. At the end, using the pairwise session key kCD, he computes and sends the following message to C

(4) When C receives the above message from D, he identifies Who the sender of the message is by evaluating the equation NymCD = H3(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 At the end, C chooses a new nonce NonceC, computes NymBC = H3(kBC|NonceC), and sends the following message

(5) Other intermediate nodes perform the same operations as C does. Finally, the following route reply is sent back to the source node S by A in our example illustrated in the Fig. 2:

(6) S decrypts the ciphertext using the right key kSA and verifies that 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 The final route table for each node is as in Table III, and Fig. 2 illustrates the detailed routing messages.

(7) 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.

(8) The data packet is further forwarded by other intermediate nodes until it reaches the destination node D. At the end, the following data packet is received by D.

(9) By looking up in his route table, D knows himself is the destination of this packet. So he is able to decrypt the encrypted payload with the session key kSD. Fig. 2 illustrates data transmission in PPRP.

IV. SECURITY AND PRIVACY ANALYSIS

In this section, we introduce an information theoretic metric to quantify privacy in anonymous routing protocols, and then we employ it to evaluate privacy of PPRP and other existing schemes. Next, we discuss issues on anonymity, unlinkability, and unobservability against the global adversary who can continuously monitor the whole network. A. Privacy Metric and Analysis We adopt an information theoretic approach [22] to measure network privacy provided by PPRP and MASK (or ANODR). The entropy-based privacy metric is obtained according to the probability distribution of a node being the sender (resp. the receiver). Specifically, we consider the sender anonymity of RREQ packets in our analysis. The sender anonymity is computed by Hk = −_pi log2 pi, where pi is the probability of node i being the sender of a packet RREQk. If the anonymity set, i.e., the set of nodes that are the possible sender, is AS, and nodes in AS are equally possible to be the sender, then the sender anonymity is Hk = _ 1 |AS| log2 |AS| = log2 |AS|. This metric represents the bits of information that an attacker needs to identify the sender of the packet RREQk.

When the anonymity set is the whole network, the sender anonymity gets the maximum value. In the following analysis, we always assume nodes in the anonymity set have the same probability to be the sender. For schemes like ANODR or MASK, RREQ tags are publicly known and RREQ packets with the same ID belong to the same session. A node nearer to the source node receives the RREQ packet earlier than a farther node. Based on this observation, a simple but effective attack to reduce the anonymity set can be launched. Suppose there are m eavesdropping nodes controlled by the attacker, and t of them, labeled as ni1, ni2,

nit, receive RREQ packets with the same sequence number in subsequent time. Then the possible source of the RREQ packet is the one whose coordinate (x, y) satisfies the following condition:

$$\sqrt{(x-\hat{x_{i_r}})^2+(y-\hat{y_{i_r}})^2} < \sqrt{(x-\hat{x_{i_s}})^2+(y-\hat{y_{i_s}})^2}, \quad \text{--------- (A)}$$

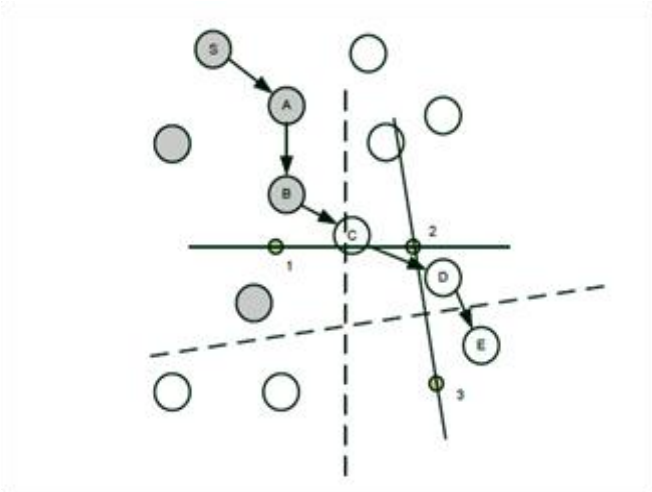

Fig. 3. A Simple Example on Sender Anonymity Reduction: Source node S initiates a route discovery process to the destination node E. There are three eavesdropping nodes (1-3) controlled by the attacker. The two dash lines are mid-perpendiculars between node 1 and node 2, node 2 and node 3, respectively. According to the RREQ packet forwarding time, the attacker can reduce the possible source of the RREQ to the grey nodes.

where $1 \le r < s \le t$, and (x^{ir}, y^{ir}),(x^{is}, y^{is}) are coordinates of node nir, nis . The nodes that satisfy condition (10) form the anonymity set AS. This method is effective as long as the network has no extraordinary congestion. An example is illustrated in Fig. 3, the anonymity set is composed of the four grey nodes. As a result, the sender anonymity of the RREQ packet can be computed as H = log24 = 2. That is, the attacker needs 2-bit information to identify who is the real sender. It can be seen that if the attacker can control more eavesdropping nodes then he is able to obtain more information on who might be the sender.

The fundamental difference between PPRP and ANODR or AnonDSR is that PPRP 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 PPRP can provide complete unlinkability and unobservability efficiently, but ANODR and AnonDSR fail to protect linkability or observability of messages. Another advantage of PPRP over ANODR is the constant size of routing packets. This makes PPRP 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 PPRP makes use of group signatures, while MASK uses one-time pairing-based keys for preserving privacy. Because these one-time pairingbased 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 PPRP.

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. And subsequent routing discovery procedure is built on top of these session keys. Hence it is easy to see that PPRP 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 defined in Section III-B2. In these packets, they are identified by pseudonyms which are generated from random nonces and secret session keys. 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 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 PPRP, 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, PPRP 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, PPRP offers content unobservability for ad hoc networks according to the definition in [1].

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. Suppose a node is compromised by an attacker, his private signing key and ID-based encryption key are disclosed to the attacker. The attacker now is able to establish keys with neighboring nodes, but only the following information can be obtained by the attacker: 1) the type of a received packet;

2) data/RREP packets sent to/via the compromised node;

3) Headers of packets relayed by the compromised node;

4) RREQ packets sent from the compromised node's neighbors. The attacker is not able to gain more beyond this information.

Even if the global attack exploits the compromised node's secret credential for a global attack, PPRP's resilience against privacy leakage can still offer satisfactory protection, due to its per-hop protection of packets. As described in (4) and (7), RREP and data packets are encrypted hop-by-hop, and onetime nonces and pseudonyms are used to provide unlinkability and unobservability. Only if the RREP or data packets pass through the compromised node can the attacker know the packet type. Even if the compromised node happens to be on the route, as an intermediate node, the attacker has no clue on where the source node or the destination node is. If the attacker tries to impersonate as the source node to request a route to a specific node, the attacker is still not certain where the destination node is in any case.

Collusion Attacks. For the colluding outsiders, privacy information is perfectly protected with PPRP. As the attacker is unable to distinguish a meaningful packet from a dummy packet, PPRP 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, PPRP 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 PPRP. 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 PPRP, authentication and key establishment is achieved by group signature, which perfectly protects user identity from disclosure. Consequently, unobservability is guaranteed by PPRP under colluding insider attacks according to the definition of unobservability.

V. SIMULATION AND PERFORMANCE EVALUATION

In this section, we analyze computation cost of PPRP, and compare it with existing schemes. We then describe the implementation and performance evaluation of our protocol.

PPRP 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 PPRP is showed in Table IV. In this table, we ignore 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, we can see that PPRP can achieve unobservability without too much computation cost. We implement both PPRP and MASK on ns2, and evaluate their performance by comparing with AODV (the standard implementation of ns-2.31). In our simulation, the scenario parameters are listed as in table V, and we use the cryptographic benchmarks on 1GHz Pentium III according to [24], [25]. Table.1 shows the simulation parameters.

1024-bit ID-based Enc	22ms
1024-bit ID-based Dec	17ms
Group Signature Generation	24ms
Group Signature Verification	26ms
Point Multiplication	3ms
1024-bit Pairing	8.6ms
Simulation Time	600s
Scenario Dimension	1500m x 300m
Wireless Radio Range	250m
Mobile Nodes Number	50
Average Node Speed	0-10m/s
Source-Destination Pairs	20 random pairs
Traffic Type	512-byte CBR traffic
Traffic Frequency	2 or 4 packets/s
Wireless Bandwidth	2Mbps
Node Pause Time	0s
Key Update Interval	40s
Average Hops	2.90
Average Neighbors	12.69

Table.1 Simulation Parameters

1) In PPRP only trusted neighbors will forward route packets for each other, otherwise packets are simply dropped

2) 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 PPRP;

3) 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;

4) In AODV or MASK, intermediate nodes can reply to a route request if they know a route to the requested destination, while PPRP cannot do this as any intermediate node is not supposed to know either the source node or the destination node.

From Fig. 4(b), we can also see that AODV has the least delivery latency and MASK is between AODV and PPRP, but the packet delivery latency difference between PPRP and MASK is less than 100ms. Under the light traffic load PPRP's latency increases from 50ms to 90ms when node speed increases from 0m/s to 10m/s. Under the heavy traffic load, PPRP's latency increases from about 100ms to more than 400ms for node speed from 0m/s to 10m/s. Due to the same reasons discussed above, non-optimal paths and local key construction delay result in longer latency of PPRP than AODV.

Figure 4(c) illustrates the routing cost for delivering a unit of data payload. It is not strange that PPRP and MASK have to send more control packets than AODV. In AODV, only three types of routing control packets, namely routing request packet, routing reply packet, and routing error packet. However, PPRP needs more control packets to maintain anonymous routing information. Since MASK and PPRP exploit similar key management and route discovery

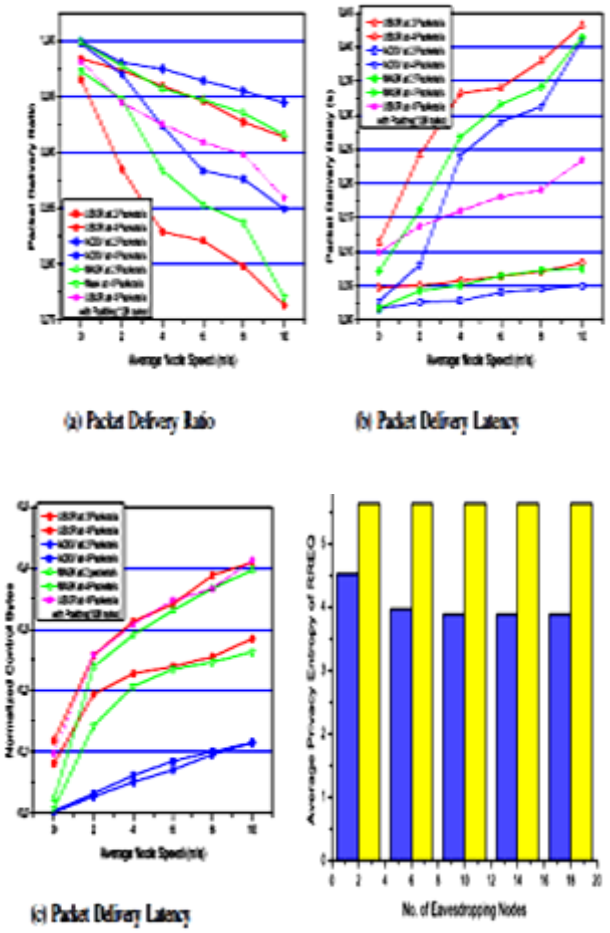

Fig.4 Simulation Results

VI. CONCLUSION

In this paper, we proposed an unobservable routing protocol PPRP based on group signature and ID-based cryptosystem for ad hoc networks. The design of PPRP offers strong privacy protection—completes unlinkability and content unobservability—for ad hoc networks. The security analysis demonstrates that PPRP not only provides strong privacy protection, it is also more resistant against attacks due to node compromise. We implemented the protocol on ns2 and examined performance of PPRP, which shows that PPRP 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 PPRP. Also how to make the unobservable routing scheme resistant against DoS attacks is a challenging task that demands in-depth investigation.

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 MOBIHOC' 03, pp. 291–302.

[6] B. Zhu, Z. Wan, F. Bao, R. H. Deng, and M. KankanHalli, "Anonymous 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.

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

[10] A. Boukerche, K. El-Khatib, L. Xu, and L. Korba, "SDAR: a secure distributed anonymous routing protocol for wireless and mobile ad hoc networks," in Proc. 2004 IEEE LCN, pp. 618–624. [11] D. Sy, R. Chen, and L. Bao, "ODAR: on-demand anonymous routing in ad hoc networks," in *2006 IEEE Conference on Mobile Ad-hoc and Sensor Systems*.

[12] J. Ren, Y. Li, and T. Li, "Providing source privacy in mobile ad hoc networks," in *Proc. IEEE MASS'09*, pp. 332–341.

[13] Y. Zhang, W. Liu, and W. Lou, "Anonymous communications in mobile ad hoc networks," in *2005 IEEE INFOCOM*.

[14] K. E. Defrawy and G. Tsudik, "ALARM: anonymous location-aided routing in suspicious MANETs," *IEEE Trans. Mobile Comput.*, vol. 10,no. 9, pp. 1345–1358, 2011.

[15] G. Tsudik "Privacy-preserving location-based on-demand routing in MANETs," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 10, pp. 1926– 1934, 2011.

[16] J. Han and Y. Liu, "Mutual anonymity for mobile peer-to-peer systems,"*IEEE Trans. Parallel Distrib. Syst.*, vol. 19, no. 8, pp. 1009–1019, Aug.2008.

[17] Y. Liu, J. Han, and J. Wang, "Rumor riding: anonymizing unstructured peer-to-peer systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 22, no. 3,pp. 464–475,

[18] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in*Advances in Cryptology–Crypto'04, Lecture Notes in Computer Science*,vol. 3152, 2004, pp. 41–55.

[19] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in *Advances in Cryptology–Crypto'01, Lecture Notes in ComputerScience*, vol. 2139, 2001, pp. 213–229.

[20] D. Dong, M. Li, Y. Liu, X.-Y. Li, and X. Liao, "Topological detection onwormholes in wireless ad hoc and sensor networks," *IEEE/ACM Trans.Netw.*, vol. 19, no. 6, pp. 1787–1796, Dec. 2011.

[21] I. R. Jeong, J. O. Kwon, and D. H. Lee, "A Diffie-Hellman key exchangeprotocol without random oracles," in *Proc. CANS 2006*, vol. LNCS 4301, pp. 37–54.
[22] A. Serjantov and G. Danezis, "Towards an information theoretic metricfor anonymity," in *Privacy Enhancing Technologies*, 2002, pp. 41–53.
[23] H. Yu, M. Kaminsky, P. B. Gibbons, and A. Flaxman, "Sybilguard:defending against sybil attacks via social networks," in *Proc. 2006SIGCOMM*, pp. 267–278.
[24] M. Brown, D. Hankerson, J. L´opez, and A. Menezes, "Software implementationof the NIST elliptic curves over prime fields," in *Topics in Cryptology – CT-RSA 2001, LNCS*, vol. 2020, 2001, pp. 250–265.
[25] M. Scott, "MIRACL: Multiprecision Integer and Rational Arithmetic C/C++ Library."

Authors Profile

K.Vinoth Kumar received the **B.E.** degree in electronics and communication engineering from the Kurinji College of engineering and technology, Manapparai, Anna University, Chennai, India, in 2009. He received the **M.E.** degree in Applied electronics from the J.J College of engineering and technology, Trichirappalli, India, in 2011. Currently doing **Ph.D.** in communication and Networking in Karpagam University Coimbatore. His research interest includes wireless communication, Mobile Ad hoc networks, Sensor Networks, Communication networks

G.Arunsathish pursuing **B.E.** degree in electronics and communication engineering from the M.A.R College of engineering and technology, Viralimalai, Anna University, Chennai, India. His research interest includes wireless communication, Mobile Ad hoc networks, Sensor Networks

R.Elamurugan pursuing **B.E.** degree in electronics and communication engineering from the M.A.R College of engineering and technology, Viralimalai, Anna University, Chennai, India. His research interest includes wireless communication, Mobile Ad hoc networks, Sensor Networks