RESEARCH ARTICLE OPEN ACCESS

An Unobservable Secure On-Demand Routing Protocol for Mobile Ad-Hoc Networks

Nagaraj.M [1] , Shivaraja.P [2], Sampath Kumar.R[3], Puneeth.G.J. [4]
Assistant Professor [1], [2], [3] & [4]
Department of Computer Science and Engineering
Rap Bahadur Y. Mahabaleswarappa Engineering College
VTU, Ballari
Karnataka - India

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 USOR to offer complete unlinkability and content unobservability for all types of packets. USOR is efficient as it uses a novel combination of group signature and ID-based encryption for route discovery. Security analysis demonstrates that USOR can well protect user privacy against both inside and outside attackers. We implement USOR on ns2, and evaluate its performance by comparing with AODV and MASK. The simulation results show that USOR not only has satisfactory performance compared to AODV, but also achieves stronger privacy protection than existing schemes like MASK.

Keywords:- Routing protocols, security, privacy, anonymity

I. 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.**

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, exist- ing 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 breaks unlinkability and may lead to source traceback attacks. Meanwhile, unprotected packet type and sequence number also make existing schemes observable to the adversary. Until now, there is no solution being able to achieve complete unlinkability and unobservability.

Unfortunately, unlinkability alone is not enough in hostile environments like battlefields as important information like packet type is still available to attackers. Then a passive attacker can mount traffic analysis based on packet type [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 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 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 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.

II. 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 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 [9] uses one-time public 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 interconnected MANETs, but it has the same problem as ODAR.

MASK [13] is based on a special type of public key crypto system, 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 quite a 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, and public keys is simply unprotected in current proposals, and these can be exploited by a global adversary to obtain useful information. A summary of anonymous routing protocols discussed above is given in Table I.

III. USOR: AN UNOBSERVABLE ROUTING SCHEME

In this section we 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 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, USOR comprises two phases: anonymous trust establishment and unobservable route discovery. The unobservable routing scheme USOR aims to offer the following privacy properties.

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

A. Assumptions, System Setup and Attack Model

Assumptions: Since we use the group signature scheme in [18] and the ID-based encryption scheme in [19], we follow the same assumptions and definitions. We assume solving the elliptic curve discrete log problem (ECDLP) and the bilinear Diffie-Hellman problem (BDH) on the two groups is hard. Both the group signature scheme and the ID-based scheme are based on pairing of elliptic curve groups of order of a large prime (e.g. 170-bit long), so that they have the same security strength as the 1024-bit RSA algorithm [18], [19].

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

addresses like MAC addresses in data frames to avoid being identified by others. Instead, they set their network interfaces in the promiscuous mode to receive all the MAC frames that can be detected in the neighborhood. This is important to prevent traffic analysis based on MAC addresses. Before the ad hoc network starts up, by following the group signature scheme, a key server generates a group public key gpk which is publicly known by everyone, and it also generates a private group signature key gsk_X for each node X. The group signature scheme ensures full-anonymity, which means a signature does not reveal the signer's identity but everyone can verify its validity. The setup of the ID-based encryption scheme is as follows. Let G_1 , G_2 be an elliptic curve group of order q. An admissible bilinear mapping $e : G_1 \times G_1 \rightarrow G_2$ is defined as in [13]. The key server chooses a master secret $s \in Z^*$ and generates the ID-based private key for node X as $K_X = s \cdot H_1(X)$. A random generator P is also selected by the server. The corresponding public key is $q, G_1, G_2, e, P, P_{pub}, H_1$, in which $P_{pub} = s \cdot P$.

Attack Model: With regard to the adversary model,we assume a global adversary that is capable of monitoring traffic of the entire ad hoc network. The adversary can monitor and record content, time, and size of each packet sent over the network, and analyzes them to obtain information on who is the source or the destination of packets, who is communicating with whom etc. Meanwhile, the adversary can mount active attacks afar or nearby, e.g., injecting, modifying, dropping packets within the network. However, the adversary *cannot* launch wormhole attacks [20] to attract a large amount of network traffic. The adversary is able to compromise one or more nodes to make his attack more successfully, but each node has at least one legitimate(uncompromised) neighbor after node compromise attack. As a result, the adversary intends to break the aforementioned privacy properties, i.e., anonymity, unlinkability and unobservability.

We assume the adversary has only bounded computation capability, and is not capable of breaking the aforementioned pairing-based cryptosystem as well as symmetric cryptosystems with appropriate key length.

B. 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 of the scheme, each node employs anonymous key establishment to anonymously construct a set of session keys with each of its neighbors. Then under protection of these session keys, the route discovery process can be initiated by the source node to discover a route to the destination node. Notations used in the description of the scheme are listed in the Table 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 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 and computes $r_S P$ where P *is* the generator of G_1. It then computes a signature of $r_S P$ *using* its private signing key gsk_S to obtain $SIG_{gsk_S}(r_S P)$. Anyone can verify this signature using the group public key gpk. It broadcast $r_S P, SIG_{gsk_S}(r_S P)$ 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∗and computes rX P . X also computes a signature SI GgskX (rS P |rX P) using its own signing key gskX . X computes the session key kSX = H2 (rS rX P), and replies to S with message rX P, SI GgskX (rS P |rX P), EkSX (k¯X ∗|rS P |rX P) , where 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 $k_{SX} = H_2(r_S r_X P)$. S also generates a local broad- cast key k_{S*}, and sends $E_{k_{SX}}(k_{S*} // k_{X*} // r_S P // r_X P)$ 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 key as $k_{SX} = H_2(r_S r_X P)$. It then decrypts the message to get the local broadcast key $\bar{k}_{S*}$.

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 k_{SX} 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 $\bar{k}_{S*}$, 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 DiffieHellman 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.

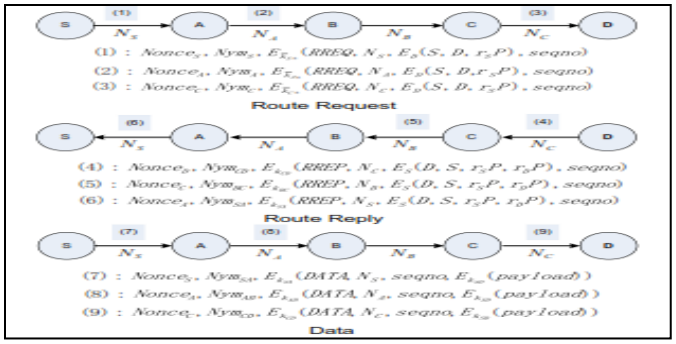

Fig. 2. USOR route request, route reply and data packet transmission

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 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. To achieve unobservability, S chooses a nonce $Nonce_S$ and calculates a pseudonym as $\mathrm{Nym}_S = H_3(\bar{k}_{S*} / Nonce_S)$.

Table 1
Comparison of Anonymous Routing Protocol

	Cryptosystems	Sender Anonymity	Receiver Anonymity	Observable Info.
ANODR	One-time PKC	Yes	Yes	Sequence no., trapdoor info., RREQ/RREP tag
ASR	One-time PKC	Yes	Yes	Sequence no., trapdoor info., RREQ/RREP tag
ARM	One-time PKC	Yes	Yes	Trapdoor info., RREQ/RREP tag
AnonDSR	One-time PKC	Yes	Yes	Trapdoor info., RREQ/RREP tag
ARMR	One-time PKC	Yes	Yes	RREQ/RREP tag
SDAR	Long-term & One-time PKC	Yes	Yes	Trapdoor info., RREQ/RREP tag
ODAR	Long-term & One-time PKC	Yes	Yes	Trapdoor info., RREQ/RREP tag
ALARM	Long-term PKC	Yes	Yes	RREQ/RREP tag, Location
PRISM	Long-term PKC	Yes	Yes	RREQ/RREP tag, Location
MASK	One-time Pairing	Yes	No	RREQ ID, Dest. ID

TABLE II 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 G_1
$H_i(*)$	Secure one-way hash functions, $i = 1, 2, 3$ †
gsk_A	Node A's private group signature key
gpk	The public group signature verification key
K_A	Node A's private ID-based key which is $s \cdot H_1(A)$
$E_A(*)$	ID-based encryption using A's public key
k_{A*}	A local broadcast key within A's neighborhood
k_{AX}	A pairwise session key shared between A and X
Nym_A	The pseudonym only valid within A's
Nym_{AX}	The pseudonym shared between A and X

Consequently, the security of our protocol can be derived using the same proof technique of KAM. Due to space limit, we do not elaborate proof details here, but interested readers are referred to [21].

2) Privacy-Preserving Route Discovery: This phase is a privacy-preserving route discovery process based on the keys established in previous phase. Similar to normal route discovery process, our discovery process also comprises of route request and route reply. The route request messages flood throughout the whole network, while the route reply messages are sent backward to the source node only.

Suppose there is a node S (source) intending to find a route to a node D (destination), and S knows the identity of the

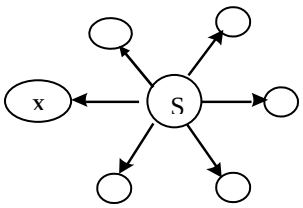

Fig. 1. Anonymous key establishment. S broadcast the first message to its direct neighbors. Each of S's neighbors does the same things as X does to learn S's local broadcast key. $k_{SX} = H_2(r_S r_X P)$.

Each node also maintains a temporary entry in his routing table seqno, P rev RNym, Next RNym, P rev hop, N ext hop , where seqno is the route request sequence number, P rev RNym denotes the route pseudonym of previous hop, N ext RN ym is the route pseudonym of next hop, P rev hop is the upstream node and N ext 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 temporarily is seqno, , NS , After that, S encrypts these items using its local broad- Cast Key K_S to obtain $E_{k_S}(RREQ, N_S, E_D(S, D, r_S P))$. In this example, A is not the destination and his trial fails, so he acts as an intermediate node. A generates a nonce $Nonce_A$ and a new route pseudonym N_A for this route. He then calculates a pseudonym $\mathrm{Nym}_A = H_3(\bar{k}_{A*} / Nonce_A)$. 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 $seqno, N_S, N_A, S$ At the end, A *prepares* and broadcast the following message to all its neighbors:

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

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

$Nonce_C$, Nym_C , $E_{\bar{k}_C}$(*RREQ*, N_C , $E_D(S, D, r_S P)$, *seqno*).

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 ciphertext using $\bar{k}_{C*}$, D records route pseudonyms and the sequence number into his route table. Then D successfully decrypts ED (S, D, rS 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. 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 r_D *and* computes a ciphertext $E_S(D, S, r_S P, r_D P)$ showing that he is the valid destination capable of opening the trapdoor information. A session key $k_{SD} = H_2(r_S r_D P / S / D)$ is computed for data protection. Then he generates a new

TABLE
III
ROUTE TABLE FOR ALL NODES IN THE EXAMPLE: EACH NODE HAS ONLY ONE ROW OF THE TABLE.

	Seqno	P_RNym	N_RNym	Prev Hop	Next Hop
S	seqno	-	N_S	-	$\bar{*}_A$
A	seqno	N_S	N_A	$\bar{*}_S$	$\bar{*}_B$
B	seqno	N_A	N_B	$\bar{*}_A$	$\bar{*}_C$
C	seqno	N_B	N_C	$\bar{*}_B$	$\bar{*}_D$
D	seqno	N_C	-	$\bar{*}_C$	-

C and him. At the end, using the pairwise session key k_{CD}, he computes and sends the following message to C:

$Nonce_D$, Nym_{CD} , $E_{k_{CD}}$ (*RREP*, N_C , E_S (D,S,$r_S P$, $r_D P$), *seqno*).

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:

IV. IMPLEMENTATION AND PERFORMANCE EVALUATION

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

USOR requires a signature generation and two point multiplications in the first process. In the route discovery process, each node except the source node and destination node needs one ID-based decryption, while the source node and destination node have to do two ID-based encryption/decryption and two point multiplications.

A detailed comparison on computation cost of existing schemes and USOR is showed in Table 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 USOR can achieve unobservability without too much computation cost. We implement both USOR 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 crypto- graphic benchmarks on 1GHz Pentium III.

In the simulation, 50 nodes are randomly distributed within a network field of size 1500mx300m as such a rectangle field can make the number of hops between two nodes larger. Mobile nodes are moving in the field according to the random way point model, and we adopt the speed ranges used in [13] so that the average speeds range from 0 to 10m/s. Two different CBR traffic loads are generated for each of the 20 pairs selected from the 50 nodes: 2 packets/s as the light traffic load and 4 packets/s as the heavy traffic load. The local session keys are updated every 40 seconds in the simulation, and each update involves a complete anonymous key establishment procedure. To simulate cryptographic operations on each node, we force each node to delay for some time according to the benchmarks given in table V. The period a node needs to wait is determined by cryptographic operations the node performs. We evaluate the performance of USOR in terms of *packet delivery ratio*, *packet delivery latency*, and *normalized control bytes*. With Fig. 4 we demonstrate performance of USOR, MASK and AODV at different moving speeds for two different traffic loads. Two traffic loads are selected according to performance of the standard AODV implementation of ns2. According to Fig. 4(a), AODV has the highest packet delivery ratio for both types of traffic loads, and MASK's performance is between AODV and USOR. The packet delivery ratio decreases as nodal speed increases and traffic load becomes heavier. Under the light traffic load (2 packets/s), USOR has more than 90% packet delivery ratio at high node speeds, only slightly lower than MASK and AODV. Under the heavy traffic load (4 packets/s), performance of all three proto- cols has downgraded greatly. The biggest difference between USOR and AODV

on packet delivery ratio is less than 10%. Apparently, the performance drop of both protocols when node speed goes up due to more frequent route disruption at higher speeds. Route disruption leads to packet drop and retransmission, and a new route has to be constructed before remaining packets can be sent out. Lower packer delivery ratio of USOR is due to the following reasons: 1) In USOR 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 USOR; 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 USOR 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 USOR, but the packet delivery latency difference between USOR and MASK is less than 100ms. Under the light traffic load USOR's latency increases from 50ms to 90ms when node speed increases from 0m/s to 10m/s. Under the heavy traffic load, USOR'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 USOR than AODV.

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

We also examine impact of packet padding on USOR's performance with Fig. 4. 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, we 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.

V. CONCLUSION AND FUTURE WORK

In this paper, we 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 protection—completes unlinkability and content unobservability—for ad hoc networks. The security analysis demonstrates that USOR not only provides strong privacy protection, it is also more resistant against attacks due to node compromise. We implemented the protocol on ns2 and examined performance of USOR, which shows that USOR has satisfactory performance in terms of packet delivery ratio, latency and normalized control bytes.

Future work along this direction is to study how to defend against wormhole attacks, which cannot be prevented with USOR. Also how to make the unobservable routing scheme resistant against DoS attacks is a challenging task that demands in-depth investigation.

ACKNOWLEDGMENTS

The authors would like to thank the anonymous reviewers for their valuable comments. Zhiguo Wan's research is sup- ported in part by Scientific Foundation for Returned Overseas Chinese Scholars, MOE, and the NSFC project under Grant No. 61003223. Kui Ren's research is supported in part by the US National Science Foundation under grants CNS-0831963 and CNS-1117811.