International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:8, No:1, 2014

An Anonymity-Based Secure On-Demand Routing for Mobile Ad Hoc Networks

M. Gunasekaran, K. Premalatha

Abstract**—**Privacy and Security have emerged as an important research issue in Mobile Ad Hoc Networks (MANET) due to its unique nature such as scarce of resources and absence of centralized authority. There are number of protocols have been proposed to provide privacy and security for data communication in an adverse environment, but those protocols are compromised in many ways by the attackers. The concept of anonymity (in terms of unlinkability and unobservability) and pseudonymity has been introduced in this paper to ensure privacy and security. In this paper, a Secure Onion Throat (SOT) protocol is proposed to provide complete anonymity in an adverse environment. The SOT protocol is designed based on the combination of group signature and onion routing with ID-based encryption for route discovery. The security analysis demonstrates the performance of SOT protocol against all categories of attacks. The simulation results ensure the necessity and importance of the proposed SOT protocol in achieving such anonymity.

Keywords**—**Routing, anonymity, privacy, security and MANET.

I. Introduction

MANET is a system of wireless mobile nodes that can freely and dynamically self-organize in arbitrary and temporary network topologies without the need of a wired backbone or a centralized administration. The mobile nodes can join into the network or can leave from the network only by interaction with other nodes. The mobile nodes communicate over relatively bandwidth constrained wireless links. The routing functionality will be incorporated into mobile nodes; so that all network activity including discovering the topology and delivering messages must be executed by the node itself. Such perceived advantages elicited immediate interest in the field of military [1], [2] disaster and rescue operation [3].

Generally, there are two types of MANETs exist: open and closed [4]. Closed MANETs don't have cooperation problems, since all nodes work towards a common goal and can easily be controlled. Open MANETs contain nodes that share their resources to ensure global connectivity but they many have different goals. The nodes in open MANETs are operated by multiple users, and they need not be forced to cooperate. However, both types of MANET introduce two main problems which are not commonly faced by traditional fixed network routing protocols. These are the lack of fixed infrastructure support and the frequent changes in network topology. Such features pose serious privacy issues for user's and security threats for the information in an adverse environment. Any user wants to communicate with another user, MANET routing protocols [5], [6] should provide a route the users. There are two categories of routing protocols: reactive and proactive. Most of these routing protocols rely on cooperation between nodes due to the lack of a centralized administration and also assumes that all nodes are genuine and trustworthy. These features of MANET provide an opportunity for malicious user to introduce different kinds of attacks [7] at network layer with respect to routing. A malicious user, may falsely advertise good paths to destination node during route discovery process, may drops the packets selectively, may leak confidential or important information to unauthorized nodes in the network, may consume away resources of other nodes present in the network and may disrupt the routing operation of the network. Such malicious features degrade the routing performance of the protocols. There are various secure routing protocols [8]-[10] have been proposed to secure ad hoc networks from security threats and to improve routing performance, but these protocols are compromised in many ways and most of these mechanisms discuss about only reliability not for anonymity.

To protect user privacy and information security in MANETs, complete anonymity is the most requiring feature. Anonymity in terms of unlinkability, unobservability, and pseudonymity discussed in [11], are based on Item of Interest (IOI) including sender, receiver, content etc. These terms are discussed as follows:

(i) **Unlinkability:** Unlinkability of two or more IOI means that within the system from the attackers perspective, these IOI no more and no less related after his/her observation than they are related concerning his/her a priori-knowledge.
(ii) **Unobservability:** Unobservability is the state of IOI being indistinguishable from any IOI at all.
(iii) **Pseudonymity:** A pseudonym is an identifier of a subject other than one of the subject's real names.

Anonymity features ensures that any user may use a resource or service without disclosing the user's identity. Suppose a covert mission is launched, which includes swarms of reconnaissance, surveillance, and attack task forces. The ad hoc network must provide routes between command post and swarms as well as routes between swarms. In this situation, providing anonymity allow the users to communicate by hiding their identities from one another and also from third parties. The demands of such anonymity is required for MANET in order to provide user privacy and information

M. Gunasekaran is with the Bannari Amman Institute of Technology, Sathyamangalam, Erode District, Tamil Nadu, India (phone: +91 9486564226; e-mail: sangraghav@gmail.com).
K. Premalatha is with the Bannari Amman Institute of Technology, Sathyamangalam, Erode District, Tamil Nadu, India (e-mail: kpl_barath@yahoo.co.in)

security. A number of anonymous routing schemes [12]-[14] have been proposed for MANET, in which most of them following on-demand routing approaches. These approaches use various cryptographic operations to anonymize the route discovery and data forwarding processes, but none of the approach provides a complete anonymity in terms of unlinkability, unobservability, and pseudonymity.

Among these requirements, first one is unlinkability: to achieve this, routing scheme should provide unlinkability for both content and communicating parties. The content unlinkability refers that the content of a message is not linkable and user unlinkability refers that it is untraceable who communicates with whom. The second one is unobservability: to achieve this, routing scheme should provide unobservability for both message and traffic pattern. The content unobservability means that no useful information can be extracted from any content and traffic pattern unobservability means that no useful information can be obtained from traffic analyses. The third one is pseudonimity: to provide anonymity for the sender and receiver. The sender anonymity is defined as the sender being anonymous and the receiver anonymity is defined as the recipient being anonymous.

In this paper, a Secure Onion Throat (SOT) protocol is proposed to provide user privacy and information security through complete anonymity in an adverse environment. This is the first protocol that supports for complete anonymity. The SOT protocol adapts group signature scheme [15] and ID-based encryption scheme [16]. In group signature each group member can sign documents on behalf of the whole group. The receiver of a signed document can verify the signature to ensure that the document is signed by a group member. However, no one except the Offline Central Manager (OCM) can recover the exact identity of the signer. The ID-based encryption scheme adapts the concepts of bilinear pairing to generate private and public keys for each user in the network. The SOT protocol has two phases: first one is initial setup and the then anonymous routing phase. In the first phase, each user obtains a group public key and ID-based private key from an OCM. An anonymous routing scheme comprises of three subsections such as anonymous key establishment, anonymous route discovery and anonymous data forwarding. During anonymous key establishment phase, every node communicates with its direct neighbor within its proximity and obtains the session key anonymously. The anonymous route discovery phase establishes random route pseudonym for an on-demand route by using cryptographic trapdoor boomerang onion [17]. Then the sender forwards the data packets anonymously by using outgoing route pseudonym.

The rest of the paper is organized as follows. The related works are discussed in Section II. The proposed routing protocol is discussed in Section III. Privacy and security analysis is discussed in Section IV. Simulation setup and results are discussed in Section V. The proposed work is concluded in Section VI.

II. Related Works

The main focus of this chapter is to discuss the anonymous communication protocols that have been proposed already for MANETs. Most of the works are based on onion routing protocol [18] proposed by Reed et al. in which data is wrapped in a series of encrypted layers to form an onion by a series of proxies communicating over encrypted channels.

Kong and Hong [17] propose an Anonymous On-Demand Routing (ANODR) Protocol, is the first one to provide anonymity and unlinkability for routing in MANET. ANODR uses one-time public/private key pairs to achieve anonymity and unlinkability but fail to guarantee content unobservability. Kong et al. [19] proposed an efficient anonymous routing for MANET, which provides add on advantages for ANODR protocol is that routing performance changes significantly when different cryptosystems are used to implement the same function (i.e., per hop pairwise key agreement). After this work, Seys and Preneel [20] proposed an Anonymous Routing Protocol (ARM) which uses one-time public/private key pairs and follows only anonymity in route discovery and data forwarding. Liu et al. [21] propose a Hierarchical Anonymous Routing Scheme to provide Inter-group and Intra-group anonymity in Mobile Ad-Hoc Networks. This protocol controls the computational overhead using the hierarchical routing scheme and preserves routing anonymity. Yang et al. [22] propose Discount ANODR, achieves substantially lower computation and communication complexities at the cost of a slight reduction of privacy guarantees, but provides only source anonymity and routing privacy. Qin et al. [23] proposed an On-Demand Lightweight Anonymous Routing (OLAR) scheme which applies the secret sharing scheme based on the properties of polynomial interpolation mechanism to achieve anonymous message transfer without per-hop encryptions and decryptions. The only task for a forwarder is to perform additions and multiplications, which cost much less than traditional cryptographic operations.

Pan and Li [24] proposed an Efficient Strong Anonymous Routing (MASR) Protocol which uses onion routing scheme to achieve anonymity but suffers from routing overhead and computation cost. Li et al. [25] propose An Efficient Anonymous Routing Protocol for Mobile Ad Hoc Networks which adapts onion routing algorithm to achieve anonymity. In this protocol, a node that participates in the protocol encrypts entire message with trust key and says Hello to its ancestor within expiration time. This approach detects the malicious node sand isolate from the network. Nezhad et al. [26] proposed a V-routing based on proactive routing protocol which conceals the location and identity of the communication parties, but it provides weaker security for the data. Chen et al. [27] propose a Trusted Anonymous Routing (TARo) Protocol which also adapts onion routing scheme to provide improved anonymity and security but it does not provide any experimental analyses.

Apart from onion routing there are other routing protocols have been proposed for anonymous communication. Ciszkowski and Kotulski [28] propose an Anonymous Authentication Protocol for Mobile Ad Hoc Networks is based

on public and symmetric key cryptography. The proposed protocol consists of two modules, anonymous authentication and monitoring activity and suffers from computational overhead. Zhang et al. [29] proposed Anonymous On-Demand Routing (MASK) which enables anonymous on-demand routing protocols with high routing efficiency by comparing with ANODR, which is very sensitive to node mobility that may lower routing efficiency. Sy et al. [30] propose On-Demand Anonymous Routing (ODAR) using public key cryptosystems for secure anonymous routing, but they assume that long-term public/private key pairs have been set up on each node for anonymous communication. Lin et al. [31] propose An Anonymous Secure Routing Protocol with Authenticated Key Exchange for Wireless Ad Hoc Networks (ASRPAKE) to provide anonymity from all the intermediate nodes and also integrates the authenticated key exchange mechanisms into the routing algorithm design. The proposed protocol uses an efficient ring signature scheme based on ECC to achieve anonymous authenticated key agreement among mobile nodes in the network. This scheme suffers from route message flooding. Chou et al. [32] propose An Efficient Anonymous Communication Protocol for Peer-to-Peer Applications over Mobile Ad-hoc Networks that adopts probabilistic-based flooding control to establish multiple anonymous paths between communication peers. Shokri et al. [33] propose a Chain-based Anonymous Routing (CAR) scheme to improve privacy of the user. The proposed scheme uses unicast-based broadcast data transfer to fulfill anonymous communication in wireless ad hoc networks. Through hiding identifiers of nodes inside the chain, CAR realizes sender, receiver, and relationship anonymity in addition to untraceability in the network. But there is a chance of high potential of interference in the network in high mobility.

Dong et al. [34] propose Anonymous routing protocol with multiple routes (ARMR) for communications in mobile ad hoc networks and Choi et al. [35] anonymous and secure reporting (ASR) of traffic forwarding activity in mobile ad hoc networks, make use of one-time public/private key pairs to achieve anonymity and unlinkability. ARMR uses one-time public-keys and bloom filter to establish multiple routes for mobile ad hoc networks and ASR is designed to achieve stronger location privacy, which ensures nodes on route have no information on their distance to the source/destination node. Defrawy and Tsudik [36] propose an Anonymous Location-Aided Routing in Suspicious MANETs uses group signature, but this protocols does not suitable for viable and practical approach to routing in mission-critical location-based environment because no analyses on protocol performance for privacy and security. Wan et al. [37] propose An Unobservable Secure On-Demand Routing (USOR) Protocol uses the combination of group signature and ID-based encryption for route discovery. The protocol offers complete unlinkability and content unobservability, but it suffers from various attacks.

III. The SOT Protocol

The system model for SOT protocol is depicted in Fig. 1, which consists of two phases such as initial setup and anonymous routing phase. The proposed protocol use the group signature scheme and onion routing with ID-based encryption scheme. Both the schemes are based upon the pairing of elliptic curve cryptography group of order of a large prime (e.g. 160-bit long), which is equivalent to the same security strength as the 1024-bit RSA algorithm.

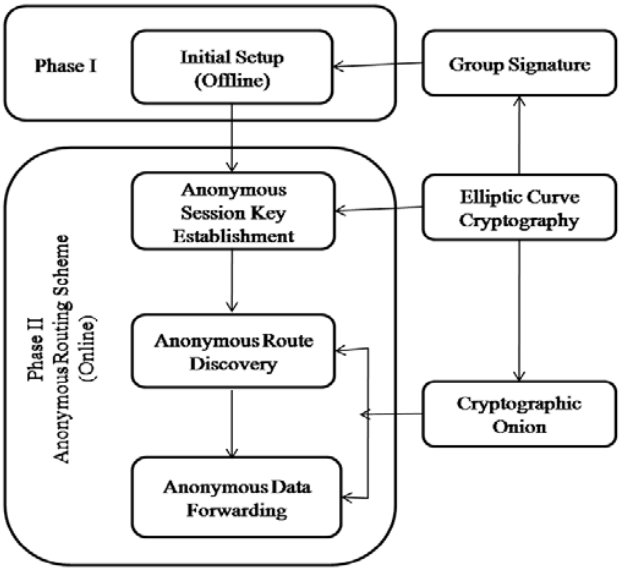

Fig. 1 System Model for SOT

A. Initial Setup (Offline)

The proposed SOT protocol assumes an ad hoc network with two entities i.e., an OCM and the users. In this paper, the mobile node or user has been used alternatively. It is assumed that all the mobile nodes have the same communication range. A mobile node can communicate with other mobile node if it is in the same proximity otherwise, communication happen through multi-hop connection.

Before the mobile ad hoc network starts the anonymous communication, OCM generates a group key (public/secret key pair) based on group signature scheme. The group public key g_{pk} is publicly known by everyone, the group private key g_{sk} is only known to the respective mobile node and the private key of the OCM is gm_{sk} used to trace the signature. The combination of group signature and onion routing with pseudonym based encryption scheme ensures complete anonymity, which means that the signature does not reveal the signer's identity but everyone can verify its validity.

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 $e: G_1 \times G_2 \rightarrow G_2$ is defined in [29]. On input a security parameter 1^k, the Bilinear Pairing Instance Generator

generates a tuple (p, G_1, G_T, e, P). The OCM selects $P_0, H \in_U G_1, \gamma \in_\cup Z_p^*$, and sets $P_{pub} = \gamma P$ and $\Delta = e(P, P)$. Then generates ID-based private key for node X as $PR_X = \gamma . H(X)$ and the corresponding public key is $PU_X = (P, P_{pub}, P_0, H, \Delta)$.

B. Anonymous Routing Scheme (Online)

The anonymous routing scheme consists of three phases: The first one is anonymous session key establishment phase and the second one is anonymous route discovery phase. During the first phase each user establishes a session key anonymously with its neighbors. Then by employing onion routing scheme the source node initiates the route discovery process to find out a path to the destination node anonymously. After establishing the route between the source node and destination node the data will be sent to the destination anonymously. Table I describes the notations which have been used in this routing scheme.

TABLE I
NOTATIONS

OCM	Key server
g_{pk}	Group public key
g_{sk}	Private group signature key only knows to the respective user
gm_{sk}	OCM's private key used to trace the signature of users
PR_X	ID-based private key based on bilinear pairing
PU_X	ID-based public key based on bilinear pairing
γ	Master secret key owned by OCM
$E_{PU_D}(*)$	ID-based encryption using nodes public key
P	Generator of elliptic curve group G_1
p	160-bit prime number
$\overline{sk}_{S*}$	Local broadcast key of node S
sk_{SX}	Pairwise session key shared between S and X
$H(m)$	Secure one way hash function
$SIGN_{g_{sk_S}}(*)$	Signature generation using node S group public key
$Rnym_{SX}$	Random route pseudonym shared between S and X

1. Anonymous Session Key Establishment

During this phase, every node communicates with its direct neighbor within its proximity. Fig. 2 illustrates the anonymous key establishment process. Suppose a mobile node S with a private group signing key g_{sk_S} and the ID-based private key of the user S is PR_S in ad hoc network and it is surrounded by a number of neighboring nodes within its proximity.

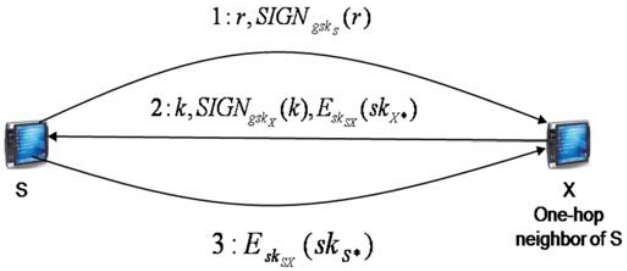

Fig. 2 Anonymous Session Key Establishment

The following procedure shows the mechanism for anonymous session key establishment:

Node S - generates a signature and sends to a neighbor node X

Step 1. S generates a random number $d_S \in Z_p^*$ and calculates $d_S P$, where P is the generator of G_1.

Step 2. It then calculates $r = d_S P.x_1 \mod n$, where $d_S P.x_1$ denotes x_1 coordinate of $d_S P$.

Step 3. Then creates a signature of r using its group private signing key g_{sk_S} to obtain $SIGN_{g_{sk_S}}(r) = k^{-1}(H(m) + xr)(\mod n)$, where H a secure hash function $SHA1$. Any one can verify this signature using group public key g_{pk}.

Step 4. Then broadcasts $< r, SIGN_{g_{sk_S}}(r) >$ to its neighborhood.

Neighbor Node X - verifies a signature received from node S. Generates its own signature and sends to node S

Step 5. X receives the message from S and verify the signature in that message. If the verification is successful, X chooses a random number $d_X \in Z_p^*$ and computes $d_X P$.

Step 6. It then calculates $k = d_X P.x_2 \mod n$ where $d_X P.x_2$ denotes x_2 coordinate of $d_X P$.

Step 7. Then creates a signature $SIGN_{g_{sk_X}}(r \mid k)$ using its own group signing key g_{sk_X}.

Step 8. Finally X computes a session key $sk_{SX} = H(d_S d_X P)$ and replies to S with a message $< k, SIGN_{g_{sk_X}}(r \mid k), E_{sk_{SX}}(\overline{sk}_{X*} \mid r \mid k) >$, where $\overline{sk}_{X*}$ is $X's$ local broadcast key.

Node S - verifies a signature received from node X and computes its own session key.

Step 9. Upon receiving a reply from X, S verifies the signature. If the signature is valid, S proceeds to

compute session key between X and itself as $sk_{SX} =< d_S d_X P >$, S also generates a local broadcast key $\overline{sk}_{S*}$, and sends $E_{sk_{SX}}(\overline{sk}_{S*} | \overline{sk}_{X*} | r | k) >$ to its neighbor X to inform X about the established local broadcast key.

Step 10. X receives the message from S and computes the same session key as $sk_{SX} = H(d_S d_X P)$ and decrypts the message to get the local broadcast key $\overline{sk}_{S*}$.

The anonymous session key establishment protocol is designed based on the combination of Elliptic Curve Diffie-Hellman (ECDH) [38] - Elliptic Curve Digital Signature Algorithm (ECDSA) [39] because the ECDH standard alone not provide authentication. Therefore, the combination of ECDH - ECDSA has been used in this paper to provide authentication through certificates verification using ECDSA. This combination inherits the security and implementation properties of the elliptic curve cryptosystems and offers the highest cryptographic strength than all other existing public-key cryptosystems. The smaller key sizes result in smaller system parameters, smaller public-key certificates, bandwidth savings, faster implementations, lower power requirements, and smaller hardware processors.

2. Anonymous Route Discovery

Anonymous route discovery establishes a privacy-preserving route based on the session key established in previous phase and cryptographic onion for an on-demand route. The route discovery process consists of anonymous route request and anonymous route reply. The anonymous route request messages broadcast to the whole network, while the anonymous route reply message is unicast in nature and sent back to the source node only. Suppose there is a node S wants to find a route to the destination node D as shown in Fig. 3, then the route discovery process executes as follows:

Anonymous Route Request: The source node S initiates the route discovery procedure and broadcast the anonymous route request packet locally which is shown here:

$$\langle ARREQ \quad , seqno \quad , tr_{dest} \ , TBO \ \rangle$$

where $ARREQ$ denotes anonymous route request packet, $seqno$ is a globally unique random route pseudonym which is used as index to a specific route entry. tr_{dest} is a cryptographic global trapdoor that can only be opened with D's private pseudonym-based key, which yields $E_{PU_D}(D, K_{commit})$ and $K_{commit}(D)$ where D is the tag for destination and K_{commit} is a trapdoor commitment key. Here the concept of "trapdoor commitment" is one-way functions are collision resistant – given a message digest $K_{commit}(D)$, it is computationally hard to find the preimage of the digest, or another preimage collision that can produce the same digest. TBO is a cryptographic Trapdoor Boomerang Onion shown in Fig. 5.

Upon receiving the route request message from S, the node X tries to open the trapdoor information using its private pseudonym-based key to see whether it is the destination node. To avoid $ARREQ$ broadcasting storm, the node X checks if it has received the same request before by looking up $seqno$ in its cache. If it is not a duplicate $ARREQ$, X caches $seqno$ for a given time to detect multiple receipt of the same $ARREQ$ packet. In this paper, the node X is not the destination and its trial fails, so it acts as an intermediate forwarding node. When an intermediate forwarding node X sees an $ARREQ$, it embeds a random nonce N_X (this random nonce achieves unobservability) to the boomerang onion, encrypts the result then broadcasts the $ARREQ$ locally and all the other intermediate nodes Y and Z do the same as X.

Finally, the $ARREQ$ reach the destination node D and it successfully decrypts the trapdoor information using its private pseudonym-based key to find out it is the destination node. If the destination node D receives more than one $ARREQ$ then only it replies to the first arrived message and drops the following ones.

Anonymous Route Reply: After node D finds out it is the destination, then it starts to prepare a reply message to the source node. The anonymous route reply message is shown here:

$$\langle ARREP \quad , Rnym \ , sk_{ij}(pr_{dest} \ , TBO \ ) \rangle$$

where $ARREP$ denotes a label that specifies the anonymous route reply packet, $Rnym$ is a locally random route pseudonym which has been used for data forwarding, sk_{ij} denotes session keys such as $sk_{ZD}, sk_{YZ}, sk_{XY}, sk_{SX}$ etc. respectively, pr_{dest} is the anonymous proof of global trapdoor opening which yields K_{ckey} created by the destination. Any forwarding node can verify the anonymous proof of trapdoor opening by checking $K_{commit}(D) \stackrel{?}{=} K_{ckey}(D)$.

The destination node D transmits the $ARREP$ packet with the above field. The node that receives the route reply packet will try to open the boomerang onion. Only the correct node (which is the previous node during route request phase) can open the boomerang onion using the anonymous session key as shown in Fig. 3. Such a node selects another random route pseudonym and opens the layer of the onion, replaces the older pseudonym with newer one and stores the mapping between them in its forwarding table. All the intermediate

forwarding nodes repeating the same until the source receives the route reply packet. The source node verifies the proof of global trapdoor opening, if it is found correct then the source node communicates with the intended destination.

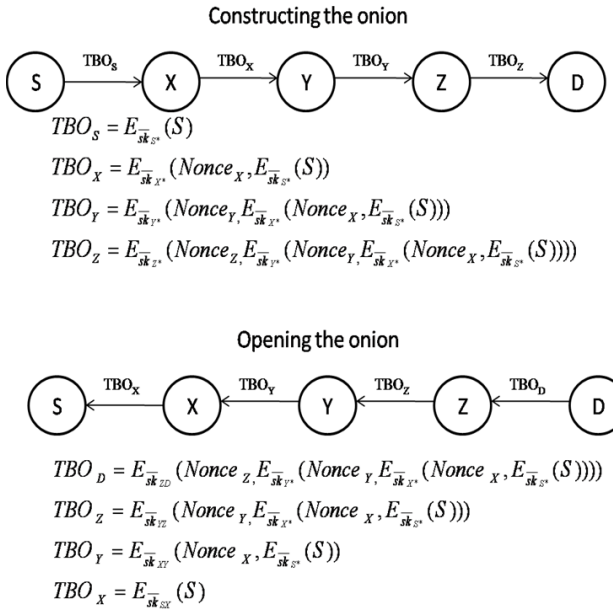

Fig. 3 TBO Construction and Opening

3. Anonymous Data Forwarding

Once the anonymous route discovery process is over a locally unique route pseudonym is setup between the source node and the destination node. This route can be used for forwarding packets. After the source receives anonymous route reply message, it encapsulates the data packets using outgoing route pseudonym in its forwarding table and then broadcasts locally. All the other local users must look up the route pseudonym in their forwarding tables and the user discards the packet if no match is found. Otherwise, it changes the route pseudonym to the matched outgoing route pseudonym and then broadcasts locally. The procedure is repeated until the data packet arrives at the destination. The general format of the data packet is shown here:

$$< Rnym , sk_{ij}(TData , E_{PU_D}(payload)) >$$

where $Rnym$ is the random route pseudonym, $TData$ denotes the packet type and $payload$ is the data that needs to be transmitted.

Suppose the source node S correctly finds out a route to the destination node D, then the source node S can start anonymous data transmission using random route pseudonyms and keys. The data packets from the source node S have to travel through X, Y and Z to D as illustrated in Fig. 4.

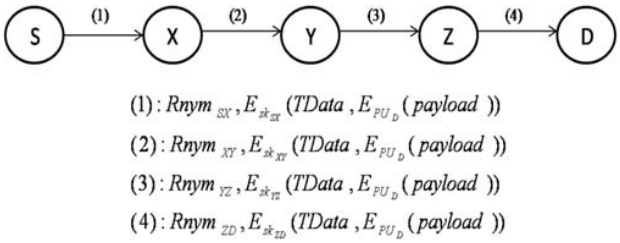

Fig. 4 Anonymous Data Forwarding

IV. Privacy and Security Analysis

This section provides an informal analysis on the privacy and security related goals achieved by SOT protocol and compared with MASK.

A. Privacy Analysis

The main difference between SOT protocol and MASK is that SOT relies on established keys between per-hop nodes to achieve privacy and security, while SOT protocol uses one-time pairing-based keys for preserving privacy. In SOT protocol, per-hop protection provides complete anonymity in terms of unlinkability and unobservability, where as in MASK one-time pairing-based keys are generated by a trusted party in advance, thus it has to face the problem of one-time depletion. Moreover, the identity information is well protected in SOT protocol using random route pseudonymity, but MASK leaks identity information of the recipient during route discovery process

Anonymity: The concept of pseudonymity used in this paper, which assigns pseudonyms as IDs for the mobile nodes. The anonymity is achieved through group signature by using pseudonyms without disclosing the user's real identity. Group signature is used to establish session keys anonymously between per-hop nodes. The route discovery process uses session keys for route establishment. Hence SOT protocol satisfies anonymity requirement as long as the group signature is secure.

Unlinkability: In this work, cryptographic onion production is implemented by using session key encryption function which ensures that the cryptanalysts cannot understand the relation between the input onion and the output onion. Only the forwarding mobile node knows that the onion which has been received by it is produced by the respective predecessor. It is very hard for the cryptanalysis to discover the relation between the producer and recipient of the particular onion. It is proved that the cryptanalysts cannot correlate the route pseudonyms established by cryptographic onions.

Unobservability: In SOT protocol, the mobile nodes involved in routing procedure are anonymous to the other nodes. A mobile node chooses the nonce randomly and uses it only once; there is no relation between pseudonyms which are computed from nonces. Because, the mobile nodes with valid session keys can recognize the respective pseudonyms and obtains the plain text by decrypting the corresponding cipher text. Moreover, a mobile node establishes the session key anonymously with its previous or next mobile node. So, no

one can know the real identities of the intermediate nodes on en-route. So, SOT protocol preserves the content unobservability.

B. Security Analysis

This section provides the security issues and countermeasures that SOT protocol achieves through anonymity during per-hop authentication, route discovery and data forwarding.

Timing and Data Analysis: Data transmission is assumed to be observable, and the adversary can monitor the traffic based-on timing information which is recorded during its transmission.

Let X and Y are sets of explicit attributes of a temporal relation schema, R. A temporal functional dependency, denoted $X \rightarrow Y$, exists on R if, for all instances r of R, all snapshots of r satisfy the functional dependency $X \rightarrow Y$. Based on the definition, the adversary can use temporal dependency between transmissions to trace the victim message's forwarding path.

In SOT protocol, the forwarding mobile node uses random pseudonyms while forwarding the data packets. To prevent timing and data analysis, the forwarding mobile node forwards dummy packets associated with pseudonyms in addition to the original data packets. The pseudonyms associated with original data packets are different from the pseudonyms associated with dummy packets. When the traffic is high all the transmissions mix together, it is very difficult to the adversary for timing and data analysis. However, when the traffic is less then more number of dummy packets needs to be generated that consume significant communication and energy resources.

Node Compromise: In compromised node attack, firstly the attacker can secretly enter in to the network and compromise individual nodes. Then the attackers can extract cryptographic secrets such as private signing key and ID-based encryption key and establish key with neighboring nodes. This kind of privacy information leakage is unavoidable due to the nature of mobile ad hoc networks.

In the proposed SOT protocol, even though the private signing key and ID-based encryption key is compromised by adversary, it cannot get useful privacy information from the compromised node. The privacy information only contains the cryptographic secrets of compromised nodes one-hop neighbor. SOT protocol implements per-hop authentication and onion routing scheme during route discovery and data forwarding phase. So, the compromised node cannot extract location and real identities of the source/destination node of the relaying packets.

Collusion Attack: The proposed SOT protocol implements per-hop authentication and key establishment using group signature. In addition to that the forwarding mobile node generates meaning full dummy packets depending on the load of the network. The proposed protocol also supports for unobservability as discussed earlier. So, it is impossible for the colluding insiders/outsiders to infer any useful information from the compromised node.

Sybil Attack: Mobile Ad Hoc Network consists of autonomous mobile nodes which forms a decentralized network. Due to its decentralization the mobile nodes in ad hoc network is prone to Sybil attack. In Sybil attack, a mobile node can create multiple fake identities to the other nodes in the network. The proposed SOT protocol uses centralized key server OCM to generate group signature signing key and ID-based private key for the mobile nodes. So, it is impossible for the adversary to obtain the real identities except the compromised nodes.

V. Performance Evaluations

Firstly, this section provides the computation cost and network scenario parameters for the implementation of the SOT protocol. Then analyze the routing performance and effectiveness of the SOT protocol in providing complete anonymity with the existing schemes through simulation results.

A. Simulation Setup

The proposed SOT protocol is for MANET is implemented on ns2 simulator version 2.32. The network scenario parameters used for simulation are listed in Table II. In the simulation scenario an ad hoc network of size 700m × 700m consists of 100 mobile nodes and the node in blue color is OGM and the nod red color is an adversary. Simulation is done with the benchmarks on a 2-GHz Pentium Dual Core platform. The mobile nodes are moving in the field according to the random waypoint model, and their average speeds range from 0 to 10 m/s. The bidirectional Constant Bit Rate (CBR) traffic is generated and the radio range of mobile node is 250 meters.

TABLE II
Scenario Parameters

Parameter	Value
Simulation Time	700s
Scenario Dimension	700m X 700m
Wireless Radio Range	250m
Mobile Nodes	100
Node Speed	0 – 10 m/s
Traffic Type	CBR 512-byte packet
Mobility Model	Random Way Point Model

The proposed SOT protocol implements the group signature scheme and onion routing with ID-based encryption scheme. Both of the scheme are based upon the pairing of elliptic curve cryptography group of order of a large prime (e.g. 160-bit long), which is equivalent to the same security strength as the 1024-bit RSA algorithm. The SOT protocol use SHA-1 as the hash function as the encryption method during route discovery and data forwarding phase. The computational cost is as shown in Table III.

TABLE III
COMPUTATIONAL COST

Techniques	Value
Group Signature generation	60ms
Group Signature verification	80ms
ID-based Encryption	50ms
ID-based Decryption	40ms
SHA-1	10ms

The SOT protocol is evaluated in terms of: (1) packet delivery ratio – data packets successfully delivered to the destination / data packets generated by the source, (2) packet delivery latency – the time that the data packet takes to reach from the source to destination, (3) routing packet overhead - the total number of control packets transmitted for each delivered data packet and (4) throughput – the average number of data packets transmitted per unit of time.

B. Simulation Results

The performance of SOT protocol is analyzed and the observations are made with respect to the parameters of packet delivery ratio, packet delivery latency, routing packet overhead and throughput. Fig. 5 demonstrates the performance of SOT protocol and MASK at different moving speeds of mobile node with the traffic load of 4 packets/second.

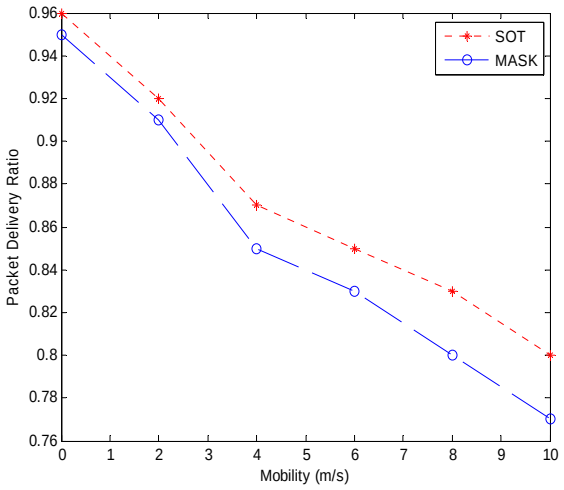

Fig. 5 (a) Packet Delivery Ratio Vs Mobility

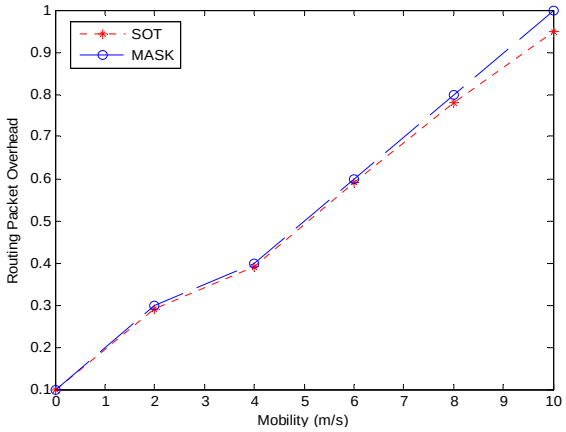

Fig. 5 (b) Routing Packet Overhead Vs Mobility

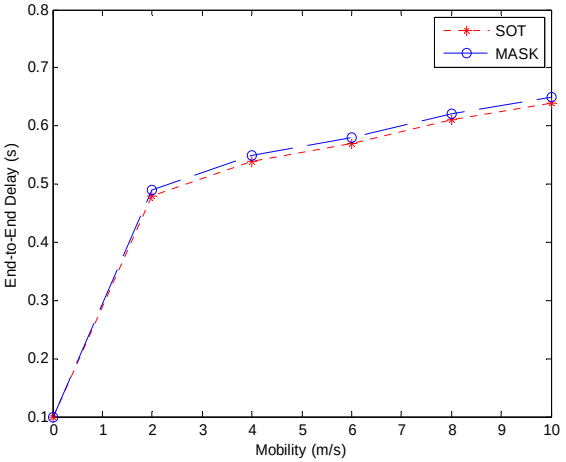

Fig. 5 (c) End-to-End Delay Vs Mobility

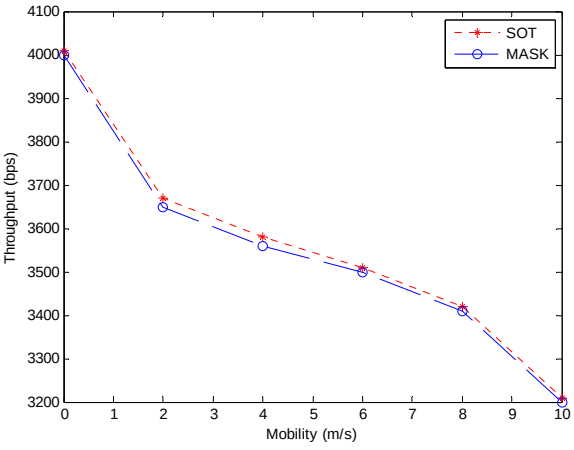

Fig. 5 (d) Throughput Vs Mobility

According to Fig. 5 (a), SOT has the better packet delivery ratio than MASK under different mobile speed such as 0, 2, 4, 6, 8 and 10 m/s. The packet delivery ratio of SOT protocol is around 96% and for MASK is about 95% when there is no mobility. In case of MASK, as the mobility increases the

packet delivery ratio is decreased significantly about 77% when the mobile speed is 10 m/s. On the other hand, under the same scenario and mobile speed the packet delivery ratio of SOT protocol is about 80%. The biggest difference between SOT protocol and MASK 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. Fig. 5 (b) illustrates the routing cost for delivering a unit of data payload. There is a very small strange that MASK have to send more control packets than SOT protocol, but there is no much deviation when the mobile nodes are in stable state.

Fig. 5 (c) shows that the proposed SOT protocol and MASK has got the same end-to-end delay when there is no movement of mobile nodes. There is negligible latency between both of the protocols when there is a mobility that is the end-to-end delay of SOT is quite lesser than the MASK. According to Fig. 5 (d), SOT performs slightly better throughput than MASK. The throughput of the both protocols decreases as the node speed increases.

VI. Conclusion and Future Work

In this paper, Secure Onion Throat protocol provides privacy and security for data communication through complete anonymity in mobile ad hoc networks. To achieve complete anonymity, the SOT protocol implements the combination of group signature and onion routing with ID-based encryption for route discovery which prevents the different kinds of attacks which have been posed by adversaries. Based on a pseudonymity approach, SOT prevents strong eavesdroppers, from exposing local wireless transmitters' identities. Through anonymity the protocol achieves untraceability and unlinkability that is tracing ad hoc network packet flows and the relationship among them is prevented. The simulation results ensure the necessity and effectiveness of the SOT protocol.

Future work: The SOT protocol provides anonymity only during route discovery and data forwarding. Besides route discovery and data forwarding anonymity is also required during event reporting i.e., informant anonymity (an informant who identifies and reports anonymously the misbehavior of the users in the mobile ad network). This feature needs to be incorporated in to the SOT protocol to provide strong privacy and security.

References

[1] B. Epstein, C. Weinstein, and R. Cunningham, "System Adaptation as a System Response in a Tactical Ad Hoc Networks," in *Proc. IEEE International Conference on Military Communication Conference*, USA, 2003, pp. 209-214.

[2] J. L. Burbank, P. F. Chimento, B. K. Haberman, and W. Kasch, "Key Challenges of Military Tactical Networking and the Elusive Promise of MANET Technology," *IEEE Communications Magazine*, Vol. 44, No. 11, pp. 39-45, Nov. 2006.

[3] H. Jang, Y. Lien, and T. Tsai, "Rescue Information System for Earthquake Disasters Based on MANET Emergency Communication Platform," in *Proc. of International Conference on Wireless Communications and Mobile Computing*, New York, 2009, pp. 623-627.

[4] H. Miranda, and L. Rodrigues, "Preventing Selfishness in Open Mobile Ad Hoc Networks," in *Proc. 7th CaberNet Radicals Workshop*, Portugal, 2002, pp. 440-445.

[5] S. Buruhanudeen, M. Othman, and B. M. Ali, "Existing MANET routing protocols and metrics used towards the efficiency and reliability- an overview," in *Proc. IEEE International Conference on Telecommunications and Malaysia International Conference on Communications*, Malaysia, 2007, pp. 231-236.

[6] F. Maan, "MANET Routing Protocols Vs Mobility Models: A performance evaluation," in *Proc. 3rd International Conference on Ubiquitous and Future Networks*, Dalian, 2011, pp. 179-184.

[7] B. Kannhavong, Y. Nemoto, and N. Kato, "A Survey of Routing Attacks in Mobile Ad Hoc Networks," *IEEE Wireless Communications*, Vol. 14, No. 5, pp. 85-91, Dec. 2007.

[8] L. Abusalah, Khokhar, and M. Guizani, "A Survey of Secure Mobile Ad Hoc Routing Protocols," *IEEE Communications Surveys and Tutorials*, Vol. 10, No. 4, pp. 78-93, Jan. 2008.

[9] P. G. Argyroudis, and D. O'Mahony, "Secure Routing for Mobile Ad Hoc Networks," *IEEE Communications Surveys and Tutorials*, Vol. 7, No. 3, pp. 2-21, Mar. 2005.

[10] T. R. Andel, and A. Yasinsac, "Surveying Security Analysis Techniques in MANET Routing Protocols," *IEEE Communications Surveys and Tutorials*, Vol. 9, No. 4, pp. 70-84, Feb. 2007.

[11] A. Pfitzmann, and M. Hansen, "Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology," Draft, February 2008.

[12] J. Liu, J. Kong, X. Hong, M. Gerla, "Performance Evaluation of Anonymous Routing Protocols in MANETs", in *Proc. IEEE International Conference on Wireless Communications and Networking Conference*, Las Vegas, 2006, pp. 646-651, 2006.

[13] J. Kong, X. Hong, and M. Gerla, "An Identity-free and On Demand Routing Scheme against Anonymity Threats in Mobile Ad-hoc Networks," *IEEE Trans. on Mobile Computing*, Vol. 6, No. 8, pp. 888-902, Aug. 2007.

[14] D. Kelly, R. Raines, R. Baldwin, M. Grimaila, and B. Mullins, "Exploring Extant and Emerging Issues in Anonymous Networks: A Taxonomy and Survey of Protocols and Metrics," *IEEE Communications Surveys and Tutorials*, Vol. 14, No. 2, pp. 579-606, Jun. 2012.

[15] D. Boneh, X. Boyen, and H. Shacham, "Short Group Signatures," in *Proc. Advances in Cryptology*, Lecture Notes in Computer Science, Springer-Verlag, Vol. 3152, pp. 41-55, Aug. 2004.

[16] D. Boneh, and M. Frankliny, "Identity-Based Encryption from the Weil Pairing," in *Proc. Advances in Cryptology, Lecture Notes in Computer Science*, Springer-Verlag, Vol. 2139, pp. 586-615, Aug. 2001.

[17] J. Kong, and X. Hong, "ANODR: ANonymous On Demand Routing with Untraceable Routes for Mobile Adhoc Networks," in *Proc. 4th International Symposium on Mobile Ad Hoc Networking & Computing*, New York, 2003, pp. 291-302.

[18] M. G. Reed, P. F. Syverson, and D. M. Goldschlag, "Anonymous Connections and Onion Routing," *IEEE Journal on Selected Areas in Communications*, 16(4), pp. 482-494. Aug. 1998.

[19] K. Jiejun, H. Xiaoyan, M. Y. Sanadidiy, and G. Mario, "Mobility Changes Anonymity: Mobile Ad Hoc Networks Need Efficient Anonymous Routing," in *Proc. of 10th IEEE Symposium on Computers and Communications*, Los Angeles, 2005, pp. 57-62.

[20] S. Seys, and B. Preneel, "ARM: Anonymous Routing Protocol for Mobile Ad hoc Networks," in *Proc. of the International Conference on Advanced Information Networking and Applications*, Vienna, 2006, pp. 133-137.

[21] L. Jun, H. Xiaoyan, K. Jiejun, Z. Qunwei, H. Ning, and G. B. Phillip, "A Hierarchical Anonymous Routing Scheme for Mobile Ad-Hoc Networks," in *Proc. International Conference on Military Communication*, Washington, 2006, pp. 1-7.

[22] Y. Liu, J. Markus, and W. Susanne, "Discount Anonymous On Demand Routing for Mobile Ad hoc Networks," in *Proc. 2nd International Conference on Security and Privacy in Communication Networks*, Baltimore, 2006, pp. 1-10.

[23] Q. Yang, H. Dijiang, and K. Vinayak, "OLAR: On-demand Lightweight Anonymous Routing in MANETs," in *Proc. 4th International*

Conference on Mobile Computing and Ubiquitous Networking, Tokyo, 2008, pp. 72-79.
[24] P. Jun, and L. Jianhua, "MASR: An Efficient Strong Anonymous Routing Protocol for Mobile Ad Hoc Network," in *Proc. International Conference on Management and Service Science*, Wuhan, 2009, pp. 1-6.
[25] L. Xiaoqing, L. Hui, M. Jianfeng, and Z. Weidong, "An Efficient Anonymous Routing Protocol for Mobile Ad Hoc Networks," in *Proc. 5th International Conference on Information Assurance and Security*, Xian, 2009, pp. 287-290.
[26] N. Alireza, M. Ali, M. Dimitris, and O. B. Luis, "Privacy within Pervasive Communications," *Springer Journal on Telecommunication Systems*, 40(4-3), pp. 101-116, Oct. 2009.
[27] Jiefeng, B. Roksana, and S. Vijay, "TARo: Trusted Anonymous Routing for MANETs", in *Proc. 8th IEEE International Conference on Embedded and Ubiquitous Computing*, Hong Kong, 2010, pp. 756-762.
[28] Tomasz, and K. Zbigniew, "ANAP: Anonymous Authentication Protocol in Mobile Ad hoc Networks," 2006.
[29] Z. Yanchao, L. Wei, L. Wenjing, and F. Yuguang, "MASK: Anonymous On-Demand Routing in Mobile Ad Hoc Networks," *IEEE Trans. On Wireless Communications*, 5(9), pp. 2376 – 2385, Sep. 2006.
[30] S. Denh, C. Rex, and B. Lichun, "ODAR: On-Demand Anonymous Routing in Ad Hoc Networks," in *Proc. 3rd IEEE International Conference on Mobile Ad-hoc and Sensor Systems*, 2006, pp. 267-276.
[31] L. Xiaodong, L. Rongxing, Z. Haojin, H. Pin-Han, S. Xuemin, and C. Zhenfu, "ASRPAKE: An Anonymous Secure Routing Protocol with Authenticated Key Exchange for Wireless Ad Hoc Networks," in *Proc. IEEE International Conference on Communications*, Glasgow, 2007, pp. 1247-1253.
[32] C. Chao-Chin, S. L. W. David, K. Jay Kuo, and N. Kshirasagar, "An Efficient Anonymous Communication Protocol for Peer-to-Peer Applications over Mobile Ad-hoc Networks," *IEEE Journal on Selected Areas in Communications*, 25(1), pp. 192-203, Jan. 2007.
[33] S. Reza, Y. Nasser and K. Ahmad, "Chain-based Anonymous Routing for Wireless Ad Hoc Networks," in *Proc. 4th IEEE International Conference on Consumer Communications and Networking Conference*, Las Vegas, 2007, pp. 297-302.
[34] D. Ying, W. C. Tat, O. K. L. Victor, S. M. Yiu, and C. K. Hui, "ARMR: Anonymous Routing Protocol with Multiple Routes for Communications in Mobile Ad Hoc Networks," *Elsevier Journal on Ad Hoc Networks*, 7(8), pp. 1536-1550, Apr. 2009.
[35] C. Heesook, E. William, S. Jaesheungn, D. M. Patrick, and F. L. P. Thomas, "ASR: Anonymous and Secure Reporting of Traffic Forwarding Activity in Mobile Ad Hoc Networks," *Wireless Networks*, pp. 525-539, May. 2009.
[36] E. D. Karim, and T. Gene, "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs," in *IEEE Trans. on Mobile Computing*, 10(9), pp. 1345-1358, Jul 2011.
[37] W. Zhiguo, R. Kui, and G. Ming, "USOR: An Unobservable Secure On-Demand Routing Protocol for Mobile Ad Hoc Networks," in *IEEE Trans. on Wireless Communications*, 11(5), pp. 1922-1932, Mar. 2012.
[38] R. J. Ik, O. K. Jeong, and H. L. Dang, "A Diffie-Hellman Key Exchange Protocol without Random Oracles," in *Proc. 5th International Conference on Cryptology and Network Security*, Springer-Verlag Berlin, pp. 37-54, 2006.
[39] D. Johnson, and A. Menezes, "The Elliptic Curve Digital Signature Algorithm (ECDSA)", Technical Report CORR 99-34, Centre for Applied Cryptographic Research (CACR), University of Waterloo, 1999.