Frothy Privacy-Preserving and Safe Fax Procedure for Cross Ad Hoc Wireless Networks

S.Jagadeesan MCA.,M.Phil.,ME., C.Ramya
Assistant Professor, Final MCA
Department of Computer Application, Nandha Engineering College,
Erode, Tamil Nadu, India.

Abstract*—We planfrothyprocedure for gettingfax and preserving users' anonymity and location privacy in cross ad hoc networks. Symmetric-key-cryptography plus and expense system are used to safe route find and data transmission. To reduce the overhead, the expense can be safed without submitting or processing expense proofs (receipts). To preserve users' anonymity with low overhead, we develop efficient pseudonym generation and trapdoor skills that do not use the resource-consuming asymmetric-key cryptography. Pseudonyms do not require large storage area or frequently contacting a central unit for refilling. Our trapdoor technique uses only frothy hashing plus. This is important because trapdoors may be processed by a large number of nodes. Developing low-overhead safe and privacy-preserving procedure is a real challenge due to the inherent contradictions: 1) getting the procedure requires each node to use one real identity, but a permanent identity should not be used for privacy preservation; and 2) the low overhead requirement contradicts with the large overhead frequently needed for preserving privacy and getting the fax. Our analysis and simulation results demonstrate that our procedure can preserve privacy and safe the fax with low overhead.*

1 INTRODUCTION

Hybrid ad hoc wireless network is a promising network architecture that incorporates ad hoc network with an infrastructure network including base stations [1]. The uplink mobile nodes may relay a source node's packets to the cell's base station, and the downlink mobile nodes may relay the packets to the destination node. This multihop packet relay can extend the base station's coverage area by enabling the nodes outside the coverage area to use the network. Multihop packet relay can increase throughput due to using the available bandwidth more efficiently. This is because the transmission interference area can be reduced by transmitting packets over shorter hops. However, involving autonomous and self-interested nodes in packet relay and the broadcast nature of radio transmission make the network highly vulnerable to serious security and privacy violation attacks.

Attackers may analyze the network transmissions to learn the users' fax activities, e.g., who communicates with whom, when, how long, etc., causing a severe threat for the users' privacy [2], [3]. The adversaries may try to trace the packets to learn the origin and/or the destination of the faxs. They may also attempt to locate users in number of hops and track their movements. Revealing a user's location or the favorite locations he visits may lead to a physical attack. Attackers will exploit the fact that each node frequently uses permanent identity and key to identify the node's transmissions and link them to a user. However, providing privacy preservation for cross ad hoc network poses many challenges.

Due to the open environment and the shared wireless medium, an attacker can intercept all the transmissions within the reception range of his radio receiver without the need to physically compromise a node. Moreover, multihop packet relay necessitates processing the packets by the mobile nodes to route them. This means that the packets' headers should not be encrypted to enable multihop routing. Unfortunately, attackers can inspect packets' headers to gain sensitive information. These attacks can be launched in an undetectable way by overhearing transmissions without disrupting the procedure.

Moreover, attackers may impersonate users or manipulate route establishment packets. For example, attackers may advertise false routing information to involve themselves in routes to collect sensitive information such as the pair of nodes that communicate and the nodes' locations in number of hops. Although the proper network operation requires the mobile nodes' cooperation in relaying others' packets, the selfish nodes will not cooperate without sufficient incentive to save their resources such as battery energy. This selfish behavior degrades the network performance significantly, which may cause the multihop fax to fail [4].

Developing low-overhead safe and privacy-preserving faxprocedure is a real challenge due to the inherent contradictions. First, getting the

procedurefrequently requires each node to use one real identity, but a permanent identity should not be used to preserve the node's privacy. Second, reducing the procedure's overhead is necessary because the nodes are constrained by limited battery energy and computing power. However, the lowoverhead requirement contradicts with the large overhead frequently needed for preserving privacy and getting the fax, as we will discussed in Section 2.

In this paper, we plan a frothyprocedure for getting route establishment and data transmission, and preserving users' privacy in cross ad hoc wireless networks. To preserve users' anonymity, each node uses pseudonyms and one-time session key. Thus, if an adversary captures a packet, he cannot infer the real identities of the source, destination, or intermediate nodes. Our procedure enables the nodes to establish routes and send/relay packets without revealing their real identities or the identity of the destination node. A node's pseudonyms can authenticate it to the intended nodes without revealing its real identity. Packet tracing is prevented by changing the packet's appearance (bits) at each hop and using packet mixers. Therefore, even if an attacker eavesdrops on both the source and destination nodes, he cannot correlate their packets. To safe the procedure and preserve privacy, the intermediate nodes can ensure that the packets are sent by legitimate nodes without revealing the real identities of the source and destination nodes.

To safe the fax, we use hashing and symmetric-key-cryptography plus and a expense (or incentive) system. The system uses credits (or microexpense) to charge the nodes that send packets and reward those relaying them. The system can stimulate the nodes to relay others' packets to earn credits. Since the nodes pay for relaying their packets, the system can regulate packet transmission. Integrating privacy preservation with the expense system is essential to gain acceptance from the users to relay others' packets. Although the expense can make packet relay beneficial, most users will not sacrifice their privacy for earning credits.

To reduce the overhead, our procedure avoids the asymmetric-key cryptography because it consumes much resource, increases the packet delivery delay and degrades the packet delivery ratio [5]. We develop efficient pseudonym generation technique that uses hashing plus. The low overhead of the hashing plus will facilitate reducing the lifetime of each pseudonym and thus boosting the users' privacy. The end-to-end packet delay can be reduced because pseudonyms are fast to compute and can be pre-computed before receiving the packets. The pseudonyms are real and always synchronized and do not require large storage area or frequently contacting a central unit for refilling.

Trapdoor is a special token used to anonymously inform the destination node about the source node's call request. It is a key component in any anonymous faxprocedure. The token (instead of the destination's identifier) is appended to the route request packet, where only the intended destination node can recognize it. A trapdoor may be broadcasted throughout the network and processed by a large number of nodes. The cost of creating and processing trapdoors should be minimized. We develop efficient trapdoor technique that does not require symmetrickey plus, but only frothy hashing plus. Moreover, much overhead is frequently consumed in submitting/processing expense proofs (or receipts) to safe the expense systems [6]. Our expense system can be safed without submitting/processing receipts. Our analysis and simulation results demonstrate that the planedprocedure can preserve the users' privacy and safe the fax with low overhead.

The remainder of this paper is organized as follows. Section 2 reviews the related works. Section 3 discusses the system models. We describe our procedure in Section 4. Security and privacy analyses and performance evaluation are given in Sections 5 and 6, respectively, followed by conclusion in Section 7.

2 R ELATED WORKS

In [7], incentive mechanism has been planed to stimulate cooperation in multi-hop wireless networks. Instead of using extensive cryptography to safe the expense, a cheating detection system is used to reduce the overhead of submitting/processing. Instead of generating a receipt per message or a group of messages, PIS [6], [11] aims to reduce the receipts' submitting/processing overhead by generating a fixed-size receipt per session. ESIP [5] plans a faxprocedure that can be used for a expense system with limited use of asymmetric-key cryptography. The source and destination nodes generate signatures for only one packet and the efficient hashing plus are used in the other packets. Salem et al. [4] plan a expense system for cross ad hoc networks, where both the uplink and downlink packet relay can be multihop. When a route is broken, the nodes that receive the last packet should submit receipts to the base station to safe the expense.

Different from [1], [4], [5], [6], [7], our procedure can preserve the users' privacy and safe the fax. It can also safe the expense without submitting receipts

or using asymmetric-key cryptography to reduce the overhead.

Capkun et al. [8] planed a privacy-preserving faxprocedure for cross ad hoc network. Each node stores a set of public/private key pairs and certificates with different pseudonyms signed by a trusted party. The node uses a key pair to authenticate itself and to share symmetric keys with its neighbours It periodically changes its public/ private key pair and shares new symmetric keys with its neighbours to protect its anonymity. The nodes should contact the trusted party to refill their certified keys before they are exhausted. Each node also stores a routing table which contains the neighbours pseudonyms and their distances to the base station in number of hops. Different from this procedure, our procedure is on-demand one that establishes routes only when needed. This can boost users' privacy because it does not send out unneeded routing advertisements.

In ANODR [9], the trapdoor is the encryption of the destination node's real identity and a random value by using the shared key with the destination node. However, the trapdoor technique is resource consuming because each node has to try to open the trapdoor with every key it shares with other nodes due to hiding the identities of the source and destination nodes to preserve their anonymity. Moreover, eavesdroppers can trace the packets along the route because their content does not change at each hop, and they can also know if a pair of nodes currently communicates.

In SDAR [10], the trapdoor is the encryption of the destination node's real identity and a one-time session key using the destination node's public key. Each node tries to open the trapdoor with its private key, and if it is not the destination, it uses the source node's one-time public key to add the encryption of its real identity, a one-time symmetric key, and a signature. However, the procedure is very resource consuming as it extensively use asymmetric-key cryptography plus. Moreover, the destination node learns the real identities and locations (in number of hops) of the intermediate nodes, and the location of the destination node is disclosed to the source node.

Ren et al. [13], [14] plan a procedure to enforce user access control and offer user privacy protection. The proposal is presented as a suite of authentication and key agreement procedures built upon a planed short group signature variation. Mahmoud et al. [12], [15] plan a scheme for protecting source nodes' location privacy in sensor networks. SATS [19] is a safe data-forwarding scheme for delay-tolerant wireless networks. SATS uses microexpense to stimulate the nodes' cooperation and a trust system to assign a trust value for each node. The highly trusted nodes are preferable in data forwarding to avoid the Black-Hole attackers. However, since these networks use different network and adversary models, they cannot be applicable for cross ad hoc networks effectively.

Zhang et al. [16] plan a safefaxprocedure for ad hoc network using a combination of identity-based cryptography and threshold cryptography. In ARAN [17], the source node attaches its certificate, a signature, and the identity of the destination node to the route request (RREQ) packet. Each node verifies the signature, signs it, and forwards the packet to its neighbours The destination node signs the route reply (RREP) packet and transmits it to the source node along the reverse path.

In Ariadne [18], the RREQ packet has the identities of the source and destination nodes, a randomly generated request identifier, and a message authentication code (MAC) computed over these elements with the key shared with the destination node. Each intermediate node attaches a MAC computed with the key shared with the destination node. The purpose of the per-hop MAC plus is to prevent the removal of identities from the packet. The destination node verifies the MAC, and sends RREP packet containing the list of identities obtained from the RREQ packet.

3 SYSTEM MODELS

3.1 Network Models

The considered cross ad hoc wireless network consists of mobile nodes, a trusted party (Tp), a set of base stations connected with each other and with Tp. The network is deployed for civilian applications, its lifetime is long, and the nodes have long relations with the network. Tp manages the nodes' credit accounts and maintains their symmetric keys. Each mobile node N_A should register with Tp to get a unique and long-term symmetric key K_A and identity ID_A. Without a valid key, the node cannot act as source, destination, or intermediate node.

A cell is the geographical area that is controlled by a base station. The transmission range of the base station is smaller than the radius of the cell. Thus, some mobile nodes will need to use the other nodes to relay their packets to communicate with the base station. The source base station (Bs) is the base station of the source node's cell, and the destination base station (Bd) is the base station of the destination node's cell. The source node ðN$_S$Þ sends packets to Bs (in multihops if necessary), Bs forwards the packets to Bd if the destination node ðN$_D$Þ resides in a different cell, and the packets are sent to N_D,

possibly in multiple hops. The part of the route between N_S and Bs is called uplink, and the part of the route between Bd and N_D is called downlink.

Our expense model adopts a fair charging policy by supporting a cost sharing between the source and the destination nodes when both of them are interested in the fax. The expense-splitting ratio is adjustable and service-dependent, e.g., a DNS server should not pay for name resolution. The source and destination nodes are charged and the uplink intermediate nodes are rewarded when the source base station receives the source node's packets. The downlink intermediate nodes are rewarded when the destination base station receives acknowledgements of packet delivery. In Section 5, we will discuss that this expense model can stimulate packet relay and safe the expense without submitting receipts.

3.2 Adversary Model

The mobile nodes are potential attackers because they are autonomous, self-interested, and motivated to misbehave to increase their welfare. The network infrastructure including Tp and the base stations are safe. They are operated by a single operator that is interested to ensure the network security. The adversaries can be legitimate nodes which have valid keys to access the network, or external adversaries who are not members in the network. They may also work individually or collude with each other to launch sophisticated attacks.

We consider two different types of attackers. The first type of attackers would target the faxprocedures including the expenses system, the authentication procedure, and the route establishment and data transmission procedures. These attackers try to steal credits, pay less, and communicate freely. They can also attack the authentication procedure to impersonate other nodes and get an unauthorized use of the network, and manipulate/ fabricate route establishment and data packets. The second type of attackers would target the users' privacy to know the users' fax activities, e.g., who is communicating to whom.

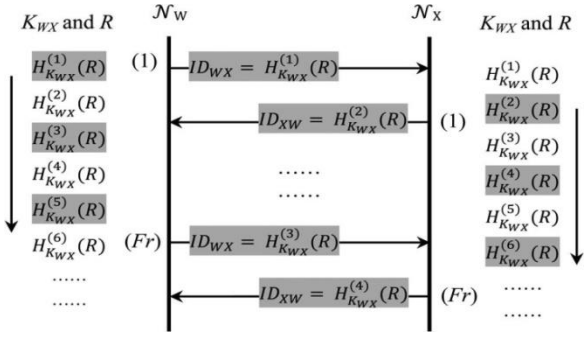

Fig. 1. Pseudonym generation technique.

The base stations and Tp are trusted in performing auditing correctly and in preserving the nodes' location and identity privacy, but only Tp is trusted regarding the nodes' long-term keys. A node's identity and location should be known to the base stations to route the packets accordingly, but the long-term secret key is known only to Tp. The source and destination nodes do not know the location of each other or the real identities of the intermediate nodes. The intermediate nodes do not know the real identities or the locations of the source and destination nodes.

Our objective is to fully protect the expense system against colluding attackers. We also aim to protect the users' privacy against single and small-scale colluding attackers, and make the attacks launched by global eavesdroppers less effective. Global eavesdroppers can eavesdrop on every radio transmission on every fax link in the network at all time. In our procedure, global eavesdroppers may infer a fax route if there are few active sessions in the network, but they cannot link the nodes' pseudonyms to the real identities.

4 THE PLANEDPROCEDURE

4.1 Pseudonym Generation Technique

The explicit use of a long-term identity or a permanent group of pseudonyms can violate users' privacy. Attackers can link the identity or the pseudonyms to the user, e.g., by analyzing the associated activities. To preserve users' anonymity, each pseudonym is used for short time in such a way that only the intended node can link the pseudonyms to each other. By this way, even if an attacker could link a pseudonym to the user in one occasion, he cannot violate the user's privacy for a long time and will not benefit from this conclusion in the future due to pseudonyms' periodic change and unlikability. Using a pseudonym for a long time enables attackers to collect much information about the visited locations by the anonymous user. Then, by analyzing this information, the attackers may identify the users and gain much information about their past visited locations.

The requirement that a node should not change its pseudonym more than once before the other node changes its pseudonym, can work well if the two nodes exchange packets regularly. However, in some cases, such as route request packets, a node may send multiple packets before receiving a packet from the other node. This requirement can be relaxed if each

node matches the other node's pseudonym against a window of L expected pseudonyms, where L 9 2. The node should advance the window when it receives a pseudonym, where the last released pseudonym is always on top of the window. Each node can release up to L pseudonyms before receiving a packet from the other node without losing synchronization.

Since privacy is a user-specific concept, our pseudonym generation technique allows users to trade off the privacy level and the computational overhead. Pseudonym change can be arbitrarily triggered by any of the two nodes without losing synchronization. The frequency of pseudonym change ðFrÞ is the number of packets that use one pseudonym. Higher privacy level is obtained when Fr decreases. The highest privacy level can be obtained when

$$\mathcal{N}_X \rightarrow Bs \rightarrow Tp: <AREQ, ID_{XTp}, (ID_{XTp}, ID_X)K_X>$$
$$Tp \rightarrow Bs: <(ID_X, K_{BsX}, R, ID_{TpX}, (K_{XBs}, ID_{TpX}, R)K_X)K_{TpBs}>$$
$$Bs \rightarrow \mathcal{N}_X: <AREP, ID_{TpX}, (K_{XBs}, ID_{TpX}, R)K_X>$$

Fig. 2. Authentication phase.

Fr ¼ 1, i.e., a pseudonym is used for only one packet. Another advantage in our technique is that pseudonyms are computed by frothy hashing plus and do not require large storage area or pseudonym refilling (unlike [8]). This means that Fr can be few (to boost nodes' privacy) with an acceptable overhead. Pseudonyms can also be computed before receiving a packet to avoid delaying the packet relay. Pseudonyms are not linkable to the real identity because the real identity is not used in computing them. An attacker cannot link the pseudonyms of a chain without knowing the secret key used in computations. Moreover, pseudonyms are real because no one can compute them except the owner of the secret key.

4.2 Shared Keys and Authentication

In our procedure, each node uses three symmetric keys and pseudonym chains shared with Tp, base stations, and other nodes, as follows:

1. Each node, e.g., N_X, and Tp share a long-term key K_X. By using this key, they can generate a long-term pseudonym chain named ID_{XTp} and ID_{TpX}.
2. Each node, e.g., N_X, shares a symmetric key and a pseudonym chain with its cell's base station. When the node handovers, the old base station sends the key and the pseudonyms to the new base station so that the key and pseudonym chain do not change and authentication process will not be needed. However, when N_X first joins the network or handover fails to keep the keep the keys and the pseudonyms, Tp mutually authenticates the node and the base station and distributes shared key to be used in generating pseudonyms. Tp should be involved because the base station does not know the node's long-term key. As shown in Fig. 2, N_X initiates the authentication process by sending an Authentication Request (AREQ) packet to the base station, probably through multihopping. AREQ packet has a fresh pseudonym shared with TpðID$_{XTp}$Þ and the encryption of ID_{XTp} and its real identity ðID$_X$Þ, where ðID$_{XTp}$;ID$_X$ÞK$_X$ refers to the ciphertext resulted from encrypting''ID$_{XTp}$;ID$_X$'' with K_X.

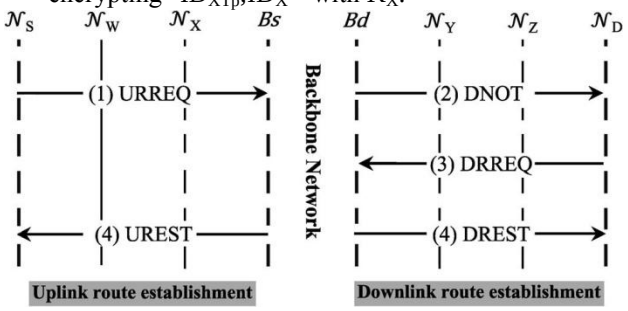

Fig. 3. Route discovery packets.

The base station sends Authentication Reply (AREP) packet to N_X. N_X can ensure that the packet is sent from Tp because it is infeasible to computeID$_{TpX}$ and (K$_{XBs}$;ID$_{TpX}$;RÞK$_X$ without knowing the secret key K_X. By this way, Tp mutually authenticates N_X and Bs without revealing the node's long-term secret key.

3. In route find phase, the base station mutually authenticates each two neighboring nodes, e.g., N $_W$ and N_X, and distributes a one-time/one-route shared key ðK$_{WX}$ ¼ K$_{XW}$Þ to generate pseudonym chain ID$_{WX}$ and ID$_{XW}$. If two nodes are neighbors in different active routes, they will have a different key and pseudonym chain per route, i.e., each key and pseudonym chain are unique for each route and two neighbours By this way, routes can be identified by pseudonym chains, which is necessary for successful packet routing.

4.3 Anonymous Route Discovery

FindFrom Fig. 3, when a source node N_S wants to communicate with another node N_D, two routes should be established: 1) uplink route between N_s and the source node's base station (Bs); and 2) downlink

route between the destination node's base station (Bd) and N_D. To establish end-to-end route, N_S broadcasts the Uplink Route Request Packet (URREQ) and Bs forwards a call request to the destination node's base station if N_D resides in a different cell. Bd broadcasts Destination Notification Packet (DNOT) if it does not know a route to N_D to inform the node about the call request. N_D replies with Downlink Route Request Packet (DRREQ) to enable Bd to know the identities of the intermediate nodes in the route. Finally, Bs and Bd send Uplink Route Establishment Packet (UREST) and Downlink Route Establishment Packet (DREST), respectively to establish the route.

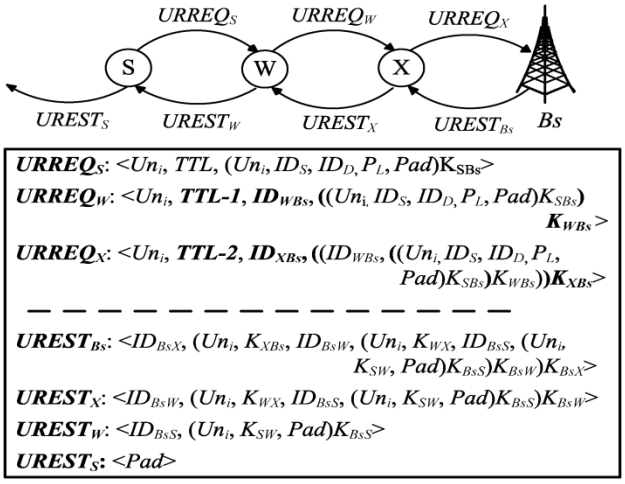

Fig. 4. Anonymous uplink route establishment.

4.4 Data Transmission

After receiving the UREST packet, N_S starts transmitting data to the destination through the established route. As shown in Fig. 6, the data packet at the source node has the shared pseudonym with the next node in the route ðID$_{SW}$Þ, and the encryption of Un_i, the message's number ðCÞ, and the message ðM$_C$Þ and its hash value ðHðM$_C$ÞÞ. If a node simultaneously participates in different routes, it stores each route's pseudonyms and keys in memory, so that it can quickly verify whether a packet is targeted at it or not and which pseudonym/key it has to use. From Fig. 6, each intermediate node replaces the incoming pseudonym with the outgoing one shared with the next node, and encrypts the iteratively-encrypted part with the key shared with base station. Thus, when the packet reaches the source base station, it should have a layered-encrypted ciphertext that is computed by all the nodes in the uplink route. The source base station removes the encryption layers by iteratively decrypting the packet with the keys shared with the nodes in the route. It also verifies the attached hash value to make sure that the message has not been modified during transmission. If this verification fails, the base station sends a negative acknowledgement to the source node to retransmit the message, otherwise, it forwards the message to the destination base station if the destination node resides in a different cell.

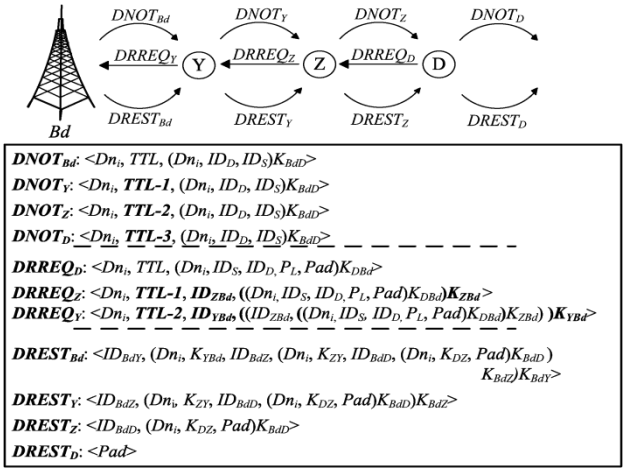

Fig. 5. Anonymous downlink route establishment.

As shown in Fig. 7, the destination base station iteratively encrypts the message with the keys shared with the nodes in the route, and sends the packet to the first node in the route ðN$_Y$Þ. Each intermediate node removes one encryption layer andreplaces the pseudonym with the one shared with the next node. The destination node decrypts the packet and verifies the hash value to ensure the message's integrity and authenticity. For reliable fax, the destination node sends back an acknowledgement packet whenit receives a correct message.

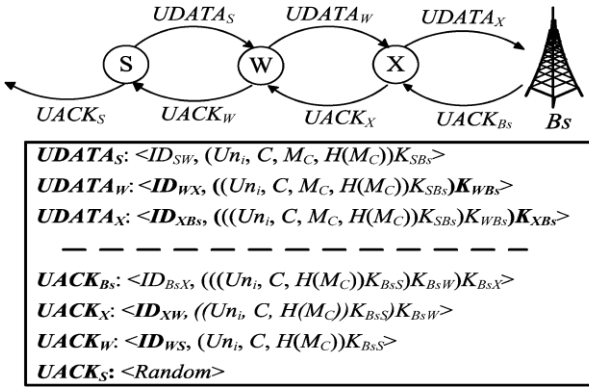

Fig.6. Anonymous uplink data transmission.

4.5 Accounting and Auditing

When the source base station receives a data packet, the source and destination nodes are charged and the uplink intermediate nodes are rewarded. The downlink intermediate nodes are rewarded when the destination base station receives acknowledgement for packet delivery. Unlike [4] that uses receipts to make packet relay rational action for the nodes, our expense model can do that without using receipts as will be discussed in Section 5. To manage the expense without instantaneously contacting Tp in each session, the base stations can manage the expense of the nodes in their cells and update the nodes' accounts stored in Tp. The base stations can also enforce access control by rejecting a node's call request if it does not have sufficient credits.

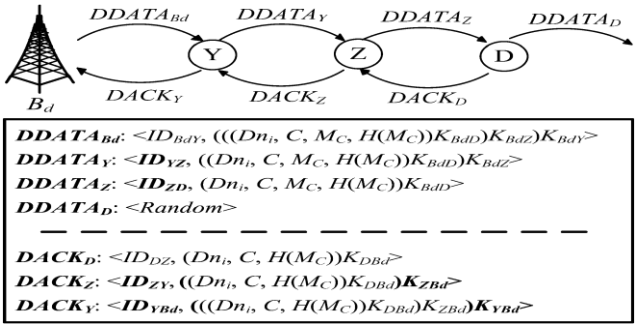

Fig .7. Anonymous downlink data transmission.

5 SECURITY AND PRIVACY ANALYSES

5.1 Fax Security

The per-hop encryption/decryption plus can thwart several attacks. Removing the encryptions and verifying the correctness of the message implicitly authenticates the intermediate nodes, verifies the hop count, and ensures that the packet is relayed through the route it was supposed to take. For URREQ and DRREQ packets, the per-hop encryption plus can safe the routing by preventing manipulating the routing information including the identities of the nodes in the route. Moreover, the hop-by-hop encryption/decryption plusmake the packets look different as they are relayed, which can boost privacy preservation, as will be discussed in Section 5.2.

In free-riding attack, two colluding nodes, e.g., N_{C1} and N_{C2}, in a legitimate session manipulate the packets to piggyback their data to communicate freely. The planedexpense systems in [1], [6], [7] use asymmetric-key cryptography to thwart this attack by signing the messages and verifying the signatures by intermediate nodes, so that manipulated packets can be detected and dropped. However, the asymmetric-key cryptography is resource consuming and frequently inefficient in preserving users' privacy. In our procedure, the per-hop encryption/decryption plus can thwart this attack because the data sent by N_{C1} cannot be interpreted by N_{C2} due to encrypting (or decrypting) it by at least one intermediate node. The nodes should use the keys shared with the base station in the encryption/decryption plus because using the session keys cannot thwart the attack if there is only one intermediate node between colluders: N_{C1} can piggyback data and encrypt the packet with the session key K_{C1V} shared with the victim node N_V; N_V encrypts the packet with the key $\eth K_{VC2}Þ$ shared with the next node N_{C2}; the colluding nodes can retrieve the data because they knowKC1V and KVC2.

The uplink and downlink intermediate nodes are motivated to relay the data packets because they are rewarded only when the source base station and destination node receive the packets, and thus packet dropping is an irrational action.

Relaying the route find packets is beneficial for the nodes to participate in routes and thus earn credits. Relaying UACK packets can trigger the source node to generate more packets, and thus the nodes can earn more credits. Relaying DACK packets is beneficial for the downlink nodes because they are rewarded when the packets reach the base station.

If the source and destination nodes are charged only for delivered packets, they can communicate freely if the destination node denies receiving the packets or a colluding intermediate node claims route breakage. To prevent this, the source and destination nodes are charged for all sent packets.

For credit-overspending attack, the nodes may spend more than the amount of credits they have at the fax time. Most of the existing expense systems [1], [5], [6], [7] are vulnerable to this attack because they use post-paid expense policy, where the nodes communicate first and pay later. In our expense system, the base stations can thwart this attack because they can know the nodes' total credits at the fax time.

For man-in-the-middle attack, an attacker residing between a victim node and the base station (or Tp) may attempt to obtain the key shared between the node and the base station. The attacker can use the key to establish sessions that are payable by the victim node or launch attacks under its name. Our procedure is not vulnerable to this attack because the shared key between a node and a base station is encrypted with the node's long-term key, and thus no one can obtain this key except the intended node. For

impersonation attack, attackers attempt to impersonate Tp, base stations, or other nodes, e.g., to unfairly obtain free service or implicate victim nodes in malicious actions. This attack is infeasible in our procedure because the nodes have to authenticate themselves using the long-term keys shared with Tp to share a key with a base station. Without knowing this secret key, attackers cannot send valid packets under the name of others.

For packet modification attack, if an attacker manipulates a packet in our procedure, the packet integrity check fails at the base station and destination node. The attackers cannot manipulate the route request packets successfully, e.g., by adding or removing nodes' identities, because they do not know the nodes' secret keys. In session-hijacking attack,

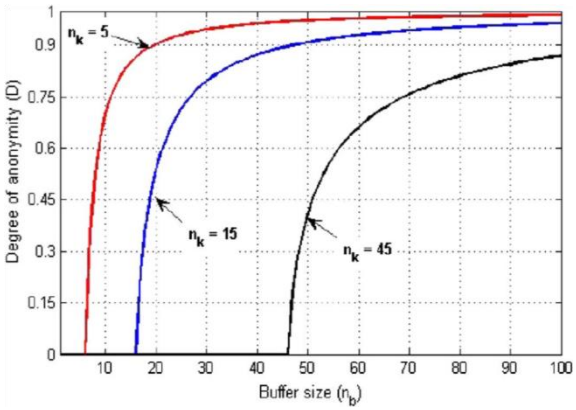

Fig. 8. Degree of anonymity versus n_b.

attackers try to hijack a session after it is established by legitimate nodes to communicate for free. Since the source node's encryption is required in each data packet, the attacker cannot compose valid packets without knowing the node's secret key and thus invalid packets can be detected and dropped.

For access control, our procedure ensures that only legitimate users can access the network to prevent unauthorized use. Only legitimate nodes can share keys with base stations and the nodes cannot communicate without these keys. For real packet forwarding, although an intermediate node should not know the identity of the other nodes in a route, it should ensure that it relays packets for legitimate nodes to prevent unauthorized use of the network and to ensure that it will be rewarded for relaying packets. In our procedure, Tp mutually authenticates the nodes and base stations, and a base station authenticates each node to its neighbors in the route. With these authentications, each node can ensure that it relays packets sent from legitimate nodes.

5.2 Privacy Preservation

For packet correlation, attackers try to correlate the packets sent in one route at different hops by finding information that indicate that the packets belong to the same traffic flow. Attackers will try to correlate packets as follows:

Packet-content correlation: In our procedure, the encryption/decryption plus and changing pseudonyms at each intermediate node guarantee that a packet looks quite different as it is relayed from the source to the destination node. Actually, we make use of the diffusion property of the encryption scheme, i.e., encrypting a message M with different keys produces different ciphetexts, e.g., although the ciphertexts E_{KA}ðMÞ and E_{KB}ðMÞ are for the same message, they look completely different. Moreover, with using safe symmetric-key cryptosystem such as AES [20], it is computationally infeasible to correlate the ciphertexts E_{KA}ðMÞ and E_{KB}ðMÞ without knowing the secret keys K_A and K_B.

Packet-length correlation: The packets of a flow can be correlated if they have distinguishable length. One of the following two skills can be used to prevent this correlation: 1) fixed-length packets: all packets have the same length and random padding is appended if a packet's length is short; or 2) random-length packets: a random-length padding is added by a node and replaced by the next node so that a packet's length is variable at each hop.

Packet-transmission-time correlation: Attackers may try to correlate a packet as it is relayed by observing the transmission time at a node and its neighbours The attackers make use of the fact that the nodes frequently relay packets after a short processing delay and based on firstreceived-first-relayed basis. Changing the packets' appearance at each hop cannot prevent this correlation because it depends on the packets' sending time and not the content. A common approach to obfuscate the temporal relationship between the incoming and outgoing packets is to use mixing technique. A mixer buffers a sequence of incoming packets and shuffles them before transmission such that correlating the incoming and outgoing packets is difficult. It can also add dummy packets to the buffer if necessary. The base stations and some mobile nodes can act as mixers.

We use information-theoretic metric, called entropy [21], to quantify the privacy protection provided by mixers. The entropy of the probability that an attacker can correlate an ingoing packet of interest with the corresponding outgoing packet is given in Eq. (1). P_i is the probability assigned by the attacker for the outgoing packet number i to be the

corresponding for the ingoing packet of interest. P ^{n}i¼^{b}1 ^{nk} P$_i$ ¼ 1, where n_b and n_k are the buffer size of the mixer and the number of ingoing packets the attacker sent to ease correlating packets, respectively. If the attacker can know that n_k packets are uncorrelated to the packet of interest, he can shrink the anonymity set from n_b to n_b n_k. The maximum entropy (or the maximum privacy protection) can be achieved when the probabilities P$_i$ (for 1 i n_b n_k) pursue uniform distribution or

P$_i$ ¼ 1=ðn$_b$ n_kÞ. In this case, the attacker believes that all the outgoing packets have the same probability to be the correspondent of the packet of interest, and thus the input packet is perfectly hidden in the buffer's packets. The maximum entropy ðH$_{max}$^{0} Þ is given in Eq. (2), and the anonymity degree ðDÞ is given in Eq. (3)

$$H(X) = -\sum_{i=1}^{nb-nk} Pi.log2(Pi) \quad (1)$$

$$H_{max} = -\sum_{i=1}^{Nb-Nk} \frac{1}{Nb-Nk}.Log2\frac{1}{Nb-Nk} \quad (2)$$

$$H_{max} = -\sum_{i=1}^{Nb} \frac{1}{Nb}.Log2\frac{1}{Nb} = log2(Nb) \quad (3)$$

Fig. 8 shows the degree of anonymity versus n_b at different values of n_k. It can be seen that the increase of n_b increases the degree of anonymity. For n_k ¼ 5, increasing n_b above 20 has little impact on the degree of anonymity, but certainly increases the packet relaying delay. It can also be seen that the increase of n_k decreases the degree of anonymity for the same buffer size, however, this can be alleviated by increasing the buffer size.

Privacy is defined as the protection of data from unauthorized parties. While encryption can protect the content of the messages, traffic analysis may reveal valuable information about the users' relationships, fax activities, and locations.

For a transmission and source node unlinkability, an adversary cannot link a transmission to its source node because the packets sent in different times have no common information or any information that can be linked to a real identity. Moreover, identifying the source or the destination node does not necessarily lead to identifying the other party.

In packet-flow tracing attack, the attackers try to infer a route by tracing packets backward/forward to the source/ destination node. Unlike [10] where each node uses one pseudonym for all the packets of a session, our procedure can use one pseudonym per packet. Eavesdroppers cannot link a session's packets at one node or link a packet at different intermediate nodes of a route. In the procedures that do not use per-hop encryption/decryption plus, such as ANODR [9], if an eavesdropper captures a packet at different intermediate nodes of a route, he can correlate the packets.

Equation (4) gives the probability (Pr) that an eavesdropper can trace a route in ANODR, where R_L is the number of nodes in the route including the source and destination nodes, n denotes the total number of nodes in the network, and n_m denotes the number of nodes that the attacker can overhear their transmissions. The probability of overhearing a node's transmission and the probability of participating in a session are uniformly distributed. Fig. 9 shows that the route tracing probability increases when the attacker can overhear the transmissions of more nodes, and it ismore probable to trace the shorter routes than the longer ones

TABLE 1
Cryptographic Plus Required by Our Procedure

	Route discovery	Data packet	*ACK*
$\mathcal{N}_S$	$2h, e, d$	$2h, e$	h, d
Uplink nodes	$2h, e, d$	h, e	h, d
Bs	$2\alpha h, \alpha e, \alpha d$	$2h, \alpha d$	$h, \alpha e$
Bd	$(2\beta+1)h, (\beta+1)e, \beta d$	$2h, \beta e$	$h, \beta d$
Downlink node	$3h, e, d$	h, d	h, e
$\mathcal{N}_D$	$3h, e, 2d$	$2h, d$	h, e

6 PERFORMANCE EVALUATION

To measure the computational times of the cryptographic plus required for our procedure, we have implemented AES (128 bit key) symmetric key

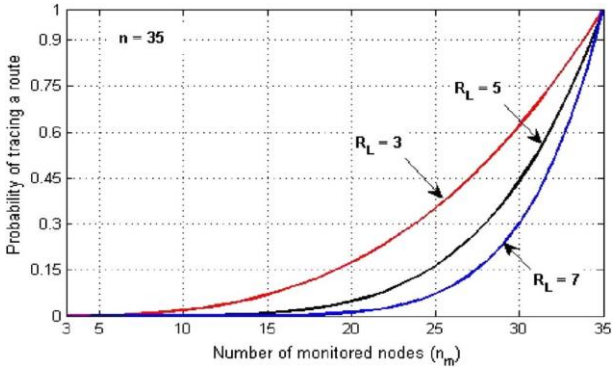

Fig. 9. Probability of tracing a route versus n_m.

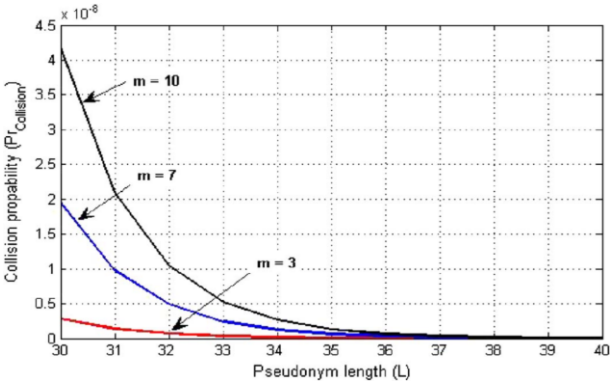

Fig. 10. Collision probability versus pseudonym length.

cryptosystem and SHA-1 (160 bit) hash function using the Crypto++5 [23] library and 1.6 GHZ processor. According to NIST [24], the safe key size should be at least 128 bits. The measurement results indicate that a hashing operation requires 16.79 Mbytes/s and encryption/decryption plus require 9.66 Mbytes/s. For the energy consumption, the measurements given in [25] indicate that a hashing operation and an encryption or decryption operation require 0.76 J=byte and 1.21 J=byte, respectively. These results confirm that hashing and symmetric-key plus require low overhead.

7 CONCLUSION

We have planed a frothysafe and privacypreserving procedure for cross ad hoc wireless network. Short-life pseudonyms, one-time session keys, and per-hop encryption/decryption plus are used to preserve users' privacy. Cryptographic plus and expense system are used to safe the fax. To reduce the overhead, frothy cryptographic plus are used, efficient trapdoor technique is developed, and the expense can be safed without storing, submitting, or processing receipts. In addition, our pseudonym generation technique requires only frothy hashing plus and does not require large storage area or frequently refilling pseudonyms from a trusted party. The pseudonyms are real and can be pre-computed which can reduce the packet delay. Our evaluations and simulation results demonstrate that the planedprocedure can preserve the nodes' privacy with low overhead and safe the expense, route establishment, and data transmission.

REFERENCES

[1] M. Mahmoud and X. Shen, ''FESCIM: Fair, Efficient, Safe Cooperation Incentive Mechanism for Cross Ad Hoc Networks,'' IEEE Trans. Mobile Computer, vol. 11, no. 5, pp. 753-766, May 2012.

[2] M. Mahmoud and X. Shen, ''Frothy Privacy-Preserving Routing and Incentive Procedure for Cross Ad Hoc Wireless Networks,'' in Proc. IEEE INFOCOM'11-Int'l Workshop Security Computers, Networking Comm. (SCNC), Shanghai, China, Apr. 2011, pp. 1006-1011.

[3] M. Mahmoud and X. Shen, ''Anonymous and Real Routing in Multi-Hop Cellular Networks,'' in Proc. IEEE Int'l Conf. Comm. (IEEE ICC'09), Dresden, Germany, June 2009, pp. 839-844.

[4] N. Salem, L. Buttyan, J. Hubaux, and M. Jakobsson, ''Node Cooperation in Cross Ad Hoc Networks,'' IEEE Trans. on Mobile Computing, vol. 5, no. 4, pp. 365-376, Apr. 2006.

[5] M. Mahmoud and X. Shen, ''ESIP: Safe Incentive Procedure with Limited Use of Public-Key Cryptography for Multi-Hop Wireless Networks,'' IEEE Trans. on Mobile Computing, vol. 10, no. 7 , pp. 997-1010, July 2011.

[6] M. Mahmoud and X. Shen, ''PIS: A Practical Incentive System for Multihop Wireless Networks,'' IEEE Trans. on Vehicle Technology, vol. 59, no. 8, pp. 4012-4025, Oct. 2010.

[7] M. Mahmoud and X. Shen, ''Stimulating Cooperation in MultiHop Wireless Networks Using Cheating Detection System,'' in Proc. IEEE Conf. Information Comm. (IEEE INFOCOM'10), San Diego, CA, USA, Mar. 2010, pp. 776-784.

[8] S. Capkun, J.P. Hubaux, and M. Jakobsson, ''Safe and PrivacyPreserving Fax in Cross Ad Hoc Networks,'' EPFL-DI-ICA, Laussane, Switzerland, Tech. Rep. IC/2004/10, 2004.

[9] J. Kong, X. Hong, and M. Gerla, ''An Identity-Free and OnDemand Routing Scheme Against Anonymity Threats in Mobile Ad Hoc Networks,'' IEEE Trans. on Mobile Computing, vol. 6 , no. 8, pp. 888-902, Aug. 2007.

[10] M. Mahmoud and X. Shen, ''MYRPA: An Incentive System with Reduced Receipts for Multi-Hop Wireless Networks,'' in Proc. IEEE Vehicular Technology Conf. (IEEE VTC'10-Fall), Ottawa, ON, Canada, Sept. 2010, pp. 1-5.

[11] M. Mahmoud and X. Shen, ''Safe and Efficient Source Location Privacy-Preserving Scheme for Wireless Sensor Networks,'' in Proc. IEEE Int'l Conf. Comm. (IEEE ICC'12), Ottawa, Canada, June 10-15, 2012.

[12] K. Ren, S. Yu, W. Lou, and Y. Zhang, ''PEACE: A Novel PrivacyEnhanced Yet Accountable Security Framework for Metropolitan Wireless Mesh Networks,'' IEEE Trans. on Parallel Distributed Systems, vol. 21, no. 2, pp. 203-215, Feb. 2010.

[13] K. Ren and W. Lou, ''A Sophisticated Privacy-Enhanced Yet Accountable Security Framework for Wireless Mesh Networks,'' in Proc. IEEE ICDCS, Beijing, China, June 2008, pp. 286-294.

[14] M. Mahmoud and X. Shen, ''Cloud-Based Scheme for Protecting Source Location Privacy Against Hotspot-Locating Attack in Wireless Sensor Networks,'' IEEE Trans. on Parallel Distributed Systems, vol. 23, no. 10, pp. 1805-1818, Oct. 2012.

[15] Y. Zhang, W. Liu, W. Lou, and Y. Fang, ''Getting Mobile Ad Hoc Networks with Certificateless Public Keys,'' IEEE Trans. on Dependable Safe Computing, vol. 3, no. 4, pp. 386-399, Oct./Dec. 2006.

[16] S. Yi, P. Naldurg, and R. Kravets, ''Security-Aware Ad Hoc Routing for Wireless Networks,'' in Proc. 2nd ACM Symp. MobiHoc Networking Computing, Long Beach, CA, USA, Oct. 2001, pp. 299-302.

[17] Y.-C. Hu, A. Perrig, and D. Johnson, ''Ariadne: A Safe OnDemand Routing Procedure for Ad Hoc Networks,'' in Proc. ACM Conf. MobiCom Computing and Networking, 2002, pp. 12-23.

[18] M. Mahmoud, M. Barua, and X. Shen, ''SATS: Safe DataForwarding Scheme for Delay-Tolerant Wireless Networks,'' in Proc. IEEE Global Comm. Conf. (IEEE GLOBECOM'11), Houston, TX, USA, Dec. 2011, pp. 1-5.

[19] A.J. Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography. Boca Raton, FL, USA: CRC Press, 1996.

[20] C. DNaz, S. Seys, J. Claessens, and B. Preneel, ''Towards Measuring Anonymity,'' in Proc. Privacy Enhancing Technologies Workshop(PET'02),LNCS2482,R.DingledineandP.Syverson, Eds., Apr. 2002, pp. 54-68.

[21] J. Kong and X. Hong, ''ANODR: Anonymous on Demand Routing with Untraceable Routes for Mobile Ad-Hoc Networks,'' in Proc. MobiHoc, 2003, pp. 291-302.

[22] W. Dai, Crypto++ Library 5.6.0. [Online]. Available: http://www. cryptopp.com/.

[23] Recommendation for Key ManagementVPart 1: General (Revised), NationalInstitute ofStandards and Technology (

NIST),Washington, DC, USA, 2007, Special Publication 800-57 200.

[24] Boukerche, K. El-Khatib, L. Korba, and L. Xu, ‘‘A Safe Distributed Anonymous Routing Procedure for Ad Hoc Wireless Networks,’’ J. Comput. Commun., vol. 28, no. 10, pp. 1193-1203 , 2005.