www.ijiarec.com

ISSN:2348-2079

Volume-5 Issue-2

International Journal of Intellectual Advancements and Research in Engineering Computations

Session based low overhead privacy- preserving and secure communication protocol in adhoc network

[1]Ms N.Zahira Jahan MCA.,M.Phil., Associate Professor,
[2]Ms M.Sri soundharyaa Final M.C.A,
Department Of M.C.A, Nandha Engineering College (Autonomous), Erode-52.
E-Mail ID: zahirajahan1977@gmail.com, sri.soundharyaa@rediffmail.com

Abstract — We propose lightweight protocol for securing communication and preserving users' anonymity and location privacy in hybrid adhoc networks. Symmetric-key-cryptography operations and payment system are used to secure route discovery and data transmission. To reduce the overhead, the payment can be secured without submitting or processing payment proofs (receipts). To preserve users' anonymity with low overhead, we develop efficient pseudonym generation and trapdoor techniques 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 lightweight hashing operations. This is important because trapdoors may be processed by a large number of nodes. Developing low-overhead secure and privacy-preserving protocol is a real challenge due to the inherent contradictions: 1) securing the protocol requires each node to use one authenticated identity, but a permanent identity should not be used for privacy preservation; and 2) the low overhead requirement contradicts with the large overhead usually needed for preserving privacy and securing the communication. Our analysis and simulation results demonstrate that our protocol can preserve privacy and secure the communication with low overhead.

Index Terms—Anonymous and secure routing protocols, hybrid ad-hoc networks, privacy-preserving protocols, payment systems

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' communication activities, e.g., who communicates with whom, when, how long, etc., causing a severe threat for the users' privacy [3].

The adversariesmay try to trace the packets to learn the origin and/or the destination of the communications. 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 usually uses permanent identity and key to identify the node's transmissions and link them to a user. However, providing privacy preservation for hybrid 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 protocol. 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 communication to fail [4].

Developing low-overhead secure and privacy-preserving communication protocol is a real challenge due to the inherent contradictions. First, securing the protocol usually requires each node to use one authenticated identity, but a permanent identity should not be used to preserve the node's privacy. Second, reducing the protocol'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 usually needed for preserving privacy and securing the communication, as we will discussed in Section 2.

We propose a lightweight protocol for securing route establishment and data transmission, and preserving users' privacy in hybrid 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 protocol 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 secure the protocol 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 secure the communication, we use hashing and symmetric-key-cryptography operations and a payment (or incentive) system. The system uses credits (or micropayment) 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 thepayment system is essential to gain acceptance from theusers to relay others' packets. Although the payment can make packet relay beneficial, most users will not sacrifice their privacy for earning credits.

To reduce the overhead, our protocol 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 operations. The low overhead of the hashing operations 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 authenticated 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 communication protocol. 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 symmetric key operations, but only lightweight hashing operations. Moreover, much overhead is usually

consumed in submitting/processing payment proofs (or receipts) to secure the payment systems [6]. Our payment system can be secured without submitting/processing receipts. Our analysis and simulation results demonstrate that the proposed protocol can preserve the users' privacy and secure the communication 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 protocol 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 RELATED WORKS

In [7], incentive mechanism has been proposed to stimulate cooperation in multi-hop wireless networks. Instead of using extensive cryptography to secure the payment, 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], [2] aims to reduce the receipts' submitting/processing overhead by generating a fixed-size receipt per session. ESIP [5] proposes a communication protocol that can be used for a payment system with limited use of asymmetric-key cryptography. The source and destination nodes generate signatures for only one packet and the efficient hashing operations are used in the other packets. Salem et al. [4] propose a payment system for hybrid 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 secure the payment. Different from [1], [4], [5], [6], [7], our protocol can preserve the users' privacy and secure the communication. It can also secure the payment without submitting receipts or using asymmetric-key cryptography to reduce the overhead. Capkun et al. [8] proposed a privacy-preserving communication protocol for hybrid 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 neighbors. It periodically changes its public/ private key pair and shares new symmetric keys with its neighbors 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 neighbors' pseudonyms and their distances to the base station in number of hops. Different from this protocol, our protocol is on-demand one that establishes routes only when needed. This can boost users' privacy because it does not send out unneeded routing advertisements.

3 SYSTEM MODELS

3.1 Network Models

The considered hybrid 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 NA should register with Tp to get a unique and long-term symmetric key KA and identity IDA. Without a valid key, the node cannot act as source, destination, or intermediate node.

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 secure. 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.

4 THE PROPOSED PROTOCOL

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.

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

Fig. 2. Authentication phase.

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 Fr ¼ 1, i.e., a pseudonym is used for only one packet.

Another advantage in our technique is that pseudonyms are computed by lightweight hashing operations and do not require large storage area or pseudonym refilling . 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 authenticated because no one can compute them except the owner of the secret key.

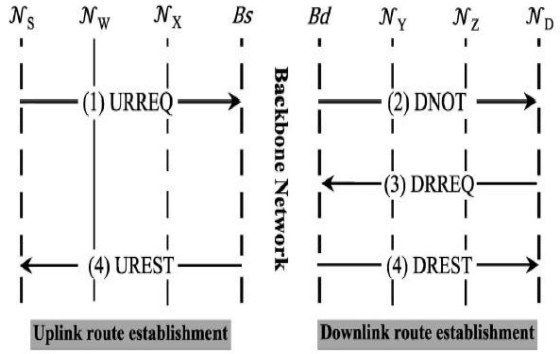

Fig. 3. Route discovery packets.

4.2 Shared Keys and Authentication

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

1. Each node, e.g., NX, and Tp share a long-term key KX. By using this key, they can generate a long-term pseudonym chain named IDXTp and IDTpX.

2. Each node, e.g., NX, shares a symmetric key and apseudonym 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 NX 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, NX 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 TpðIDXTpÞ and the encryption of IDXTp and its real identity ðIDXÞ, where ðIDXTp; IDXÞKX refers to the ciphertext resulted from encrypting ''IDXTp; IDX'' with KX. AREQ packet

authenticates NX to Tp because the secret key KX is required to compose valid packet. Without knowingKX, it is infeasible to compute valid ðIDXTp; IDXÞKX and fresh IDXTp. The base station (Bs) forwards the request to Tp which checks whether the pseudonym is for a registered user and replies with the node's real identity, the shared key between NX and BsðKXBs ¼ KBsXÞ, and the seed of the pseudonym chain ðRÞ. With this packet, Tp authenticates NX to the base station. R and KXBs are used to generate pseudonyms shared betweenNX and Bs. The base station sends Authentication Reply (AREP) packet to NX. NX can ensure that the packet is sent from Tp because it is infeasible to compute IDTpX and (KXBs; IDTpX; RÞKX without knowing the secret key KX. By this way, Tp mutually authenticates NX and Bs without revealing the node's long-term secret key.

3. In route discovery phase, the base station mutually authenticates each two neighboring nodes, e.g., NW and NX, and distributes a one-time/one-route shared key ðKWX ¼ KXWÞ to generate pseudonym chain IDWX and IDXW. 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 neighbors. By this way, routes can be identified by pseudonym chains, which is necessary for successful packet routing.

4.3 Anonymous Route Discovery

From Fig. 3, when a source node NS wants to communicate with another node ND, two routes should be established: 1) uplink route between Ns and the source node's base station (Bs); and 2) downlink route between the destination node's base station (Bd) and ND. To establish end-to-end route, NS broadcasts the Uplink Route Request Packet (URREQ) and Bs forwards a call request to the destination node's base station if ND resides in a different cell. Bd broadcasts Destination Notification Packet (DNOT) if it does not know a route to ND to inform the node about the call request. ND 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.

4.3.1 Uplink Route Request Packet (URREQ)

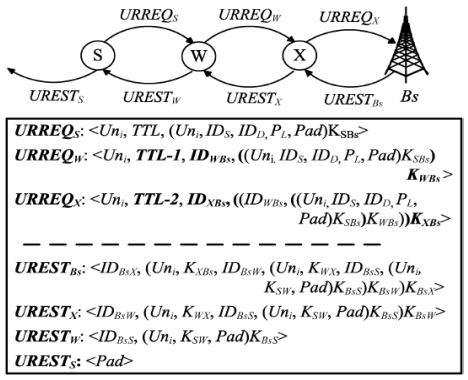

Fig. 4. Anonymous uplink route establishment.

As shown in Fig. 4, the source node initiates route discovery by broadcasting URREQ packet containing a unique request identifier ðUniÞ, time to live (TTL), and the encryption of Uni, the source and the destination nodes' real identities, dummy bits called padding (Pad), and the padding length ðPLÞ. Uni is the pseudonym shared with BsðIDSBsÞ and time stamp. Each node and the base station process only the first received URREQ packet and discard all further packets having the identifier Uni. Using this identifier is necessary to avoid routing loops and broadcast explosion that causes broadcasting the same packet each time it is received from a neighbour.

This identifier does not reveal much information because the packets are broadcasted. IDSBs and the encrypted part authenticate NS to Bs, which is necessary for authorizing the network access and securing the payment. TTL is used to bind the request propagation area. Each node decrements TTL, and once it is zero the request is no longer broadcasted. Each node adds the pseudonym shared with Bs, encrypts the previous node's pseudonym and the encrypted part with the shared key with Bs, and broadcasts the request. As the packet moves towards the base station, it stores the pseudonyms of the nodes in the route. For the first received URREQ packet, Bs decrypts the encryption layers to tell the identities of the source, intermediate, and destination nodes. Then, it sends call request to Bd if ND resides in a different cell. Since the packet length grows with fixed amount of data as it is relayed, the attackersmay try to locate the source node's location either from TTL or the packet size. To protect the location privacy of NS and to confuse its neighbors whether the packet is originated from or relayed by NS, a random-length

padding is added and the initial TTL is variable value. Since Uni varies over time, each time a node sends URREQ packet to the same destination, the packet looks different in spite of using the same key.

4.3.2 Destination Notification Packet (DNOT)

From Fig. 5, after the destination base station (Bd) receives a call request for a node in its cell, it notifies the node by broadcasting Destination Notification Packet (DNOT). The packet contains a unique identifier ðDniÞ that has the pseudonym shared with ND and time stamp. The packet also contains Time-to-Live (TTL), and the encryption of Dni and the destination and source nodes' identities with using the shared key with ND. Padding is not needed because preserving the base station's location privacy is not important. After receiving the packet, each node first checks whether it is the intended destination by checking if the attached pseudonym is in the list of expected pseudonyms.

If so, the node decrypts the encryption to tell the identity of the source node, and sends DRREQ packet. If it is not the destination and TTL is greater than zero, the node decrements TTL and broadcasts the packet. Each node processes each notification once and drops any further packets with the same identifier. The destination node broadcasts the DNOT packet as well to deprive its neighbors from inferring that the destination is a one hop neighbor. Thus, all DNOT packets are transmitted for TTL hops regardless of the location of the destination node to preserve its location privacy.

4.3.3 Downlink Route Request Packet (DRREQ)

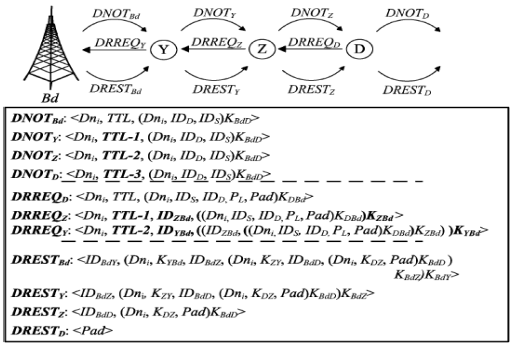

Fig. 5. Anonymous downlink route establishment.

Fig. 5 shows that the destination node composes and broadcasts the DRREQ packet. Processing the packet is similar to that of the URREQ packet.

4.3.4 Uplink Route Establishment Packet (UREST)

The objective of the UREST packet is to inform the uplink intermediate nodes to act as relays and to distribute the session keys shared between each two neighboring nodes.

From Fig. 4, each intermediate node removes one encryption layer by using the key shared with Bs, stores the session key shared with the previous neighbor in the route, and relays the packet after removing Uni and its pseudonym and key. The node hashes this key to compute the key shared with the other neighbor,Obviously,KWS should be similar to KSW distributed by Bs. By this way, the number of distributed keys can be nearly halved to reduce the packet overhead. Padding is added to make it infeasible to infer the source node's location from the packet size. The source node relays the packet as well to protect its location privacy from its neighbors.

4.3.5 Downlink Route Establishment Packet (DREST)

This packet informs the downlink intermediate nodes to act as relays and distributes the session keys shared between each two neighboring nodes. The packet's format is similar to that of UREST packet.

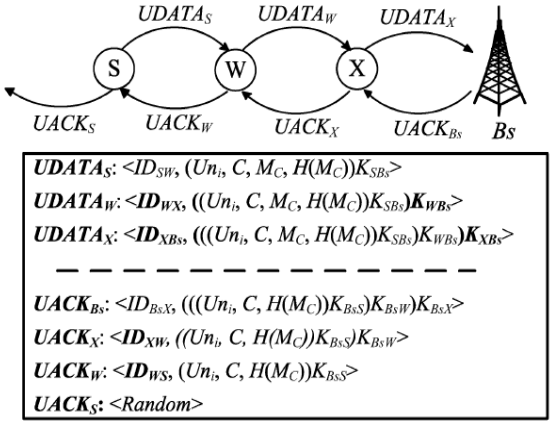

Fig. 6. Anonymous uplink data transmission.

4.4 Data Transmission

After receiving the UREST packet, NS 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 ðIDSWÞ, and the encryption of Uni, the message's number ðCÞ, and the message ðMCÞ and its hash value ðHðMCÞÞ. 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.

5 SECURITY AND PRIVACY ANALYSES

5.1 Communication Security

The per-hop encryption/decryption operations 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.

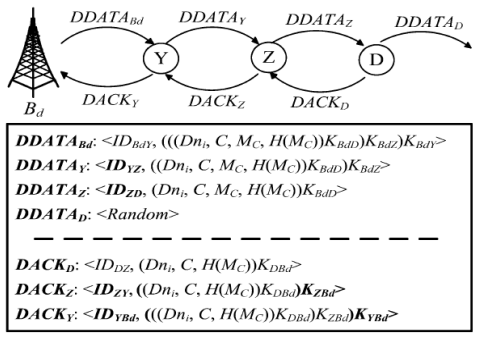

Fig. 7. Anonymous downlink data transmission.

For URREQ and DRREQ packets, the per-hop encryption operations can secure the routing by preventing manipulating the routing information including the identities of the nodes in the route.

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:

a) Packet-content correlation:
b) Packet-length correlation:

6 PERFORMANCE EVALUATION

To measure the computational times of the cryptographic operations required for our protocol, we have implemented AES (128 bit key) symmetric key cryptosystem and SHA-1 (160 bit) hash function using the Crypto++5 library and 1.6 GHZ processor. Accordingly the secure key size should be at least 128 bits. The measurement results indicate that a hashing operation requires 16.79 Mbytes/s and encryption/decryption operations require 9.66 Mbytes/s. For the energy consumption, the measurements 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 operations require low overhead.

TABLE 1
Cryptographic Operations Required by Our Protocol

	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

7 CONCLUSION

We have proposed a lightweight secure and privacy preserving protocol for hybrid ad hoc wireless network. Short-life pseudonyms, one-time session keys, and per-hop encryption/decryption operations are used to preserve users' privacy. Cryptographic operations and payment system are used to secure the communication. To reduce the overhead, lightweight cryptographic operations are used,

efficient trapdoor technique is developed, and the payment can be secured without storing, submitting, or processing receipts. In addition, our pseudonym generation technique requires only lightweight hashing operations and does not require large storage area or frequently refilling pseudonyms from a trusted party. The pseudonyms are authenticated and can be pre-computed which can reduce the packet delay. Our evaluations and simulation results demonstrate that the proposed protocol can preserve the nodes' privacy with low overhead and secure the payment, route establishment, and data transmission.

REFERENCES

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

[2] 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.

[3] M. Mahmoud and X. Shen, ''Anonymous and Authenticated 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 inHybridAdHocNetworks,'' IEEE Trans. on Mobile Computing, vol. 5, no. 4, pp. 365-376, Apr. 2006.

[5] M.Mahmoud and X. Shen, ''ESIP: Secure Incentive Protocol with Limited Use of Public-Key Cryptography forMulti-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 Multi-Hop Wireless Networks Using Cheating Detection System,'' in Proc. IEEE Conf. Information Comm. (IEEE INFOCOM'10), San Diego, CA, USA, Mar. 20