iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** IV **Month of publication:** April 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Secure Privacy-Preserving and Low Overhead Communication Protocol for Hybrid Ad Hoc Wireless Networks

A.Rama Krishna[1], D.Durga Prasad[2]
[1]PG Student, Baba Institute of Technology and Sciences, Vishakapatnam, A.P.INDIA.
[2]Assistant Professor, Baba Institute of Technology and Sciences, Vishakapatnam, A.P.INDIA.

Abstract*—In hybrid adhoc networks for securing communication and preserving users anonymity and location privacy we propose light weight protocol. To secure route discovery and data transmission symmetric-key-cryptography operations and payment system are used. The payment can be secured without submitting or processing payment proofs to reduce the overhead.With low overhead, to preserve user's anonymity, 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 trapdoor may be processed by a large number of nodes. The development of low-overhead secure and privacy-preserving protocol is a real challengefor its inherent contradictionsi.e. for securing the protocol requires each node to use one authenticated identity, but a permanent identity should not be used for privacy preservation and for the low overhead requirement contradicts with the large overhead usually needed for preserving privacy and securing the communication. The analysis and simulation results states with low overhead our protocol can preserve privacy and secure the communication.

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

I. INTRODUCTION

The network architecture that incorporates ad hoc network with an infrastructure network including base stations [1] is said to be the hybrid ad hoc wireless network. 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. By enabling the nodes outside the coverage area this multihop packet relay can extend the base station's coverage area to use the network and this can increase throughput since the available bandwidth is used more efficiently. This is because the transmission interference area can be reduced by transmitting packets over shorter hops.

Analyzing the network transmissions by the attackers to learn the users' communication activities, e.g., who communicates with whom, when, how long, etc., causing a severe threat for the users' privacy [2], [3]. The attackers may try to trace the packets to trace the origin and the communication destination. They may also attempt to locate users in number of hops and track their move-ments. There may be a physical attack by revealing a user's location or the favorite locations he visits. 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. Providing privacy preservation for hybrid ad hoc network poses many challenges.An attacker can intercept all the transmissions within the reception range of his radio receiver without the need to physically compromise a node due to the open environment and the shared wireless medium. The packets headers should not be encrypted to enable multihop routing. Unfortunately, to gain sensitive information attackers can inspect packets' headers. By overhearing transmissions without disrupting the protocol, these attacks can be launched in an undetectable way.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. A robust network operation requires the mobile nodescooperation in relaying others packets. Without sufficient incentive to save their resources such as battery energy the selfish nodes will not cooperate. This selfish behavior degrades the network performance significantly, leads to failure inmultihop communication [4].

Due to inherent contradictions, developing low-overhead secureand privacy- preserving communication protocol is a real challenge. In this paper, we propose a lightweight protocol for securing route establishment and data transmission, and preserving usersprivacy

in hybrid ad hoc wireless networks. To preserve users anonymity, each node uses pseudonyms and one-time session key. The proposed protocol enables the nodes to establish routes and send 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 bits at each hop and using packet mixers. Thus, if an attacker eavesdrops on both the source and destination nodes, he cannot correlate their packets. 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 protocol and preserve privacy.

We use hashing and symmetric-key-cryptography operations and a payment system to secure the communication. The system uses credits to charge the nodes that send packets and reward those relaying them. To relay others packets and to earn credits the system can stimulate the nodes.The system can regulate packet transmission since the nodes pay for relaying their packets. Integrating privacy preservation with the payment system is essential to gain acceptance from the users to relay others' packets. The payment can make packet relay beneficial,even though most users will not sacrifice their privacy for earning credits.Our protocol avoids the asymmetric-key cryptography because it consumes much resource, increases the packet delivery delay and degrades the packet delivery ratio [5] to reduce the overhead. 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. Since pseudonyms are fast to compute and can be pre-computed before receiving the packets the end-to-end packet delay can be reduced.The pseudonyms are authenticated and always synchronized and do not require large storage area or frequently contacting a central unit for refilling.To anonymously inform the destination node about the source node's call request we use a token called Trapdoor. In any anonymous communication protocol it is a key component. The token 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. But, much overhead is usually consumed in submit-ting/processing payment proofs to secure the payment systems [6]. Without submitting/processing receipts the payment system can be secured. The analysis and simulation results demonstrate that the proposed protocol can preserve the users privacy and secure the communication with low overhead.

II. THE PROPOSED PROTOCOL

A. 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, hecannot 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.

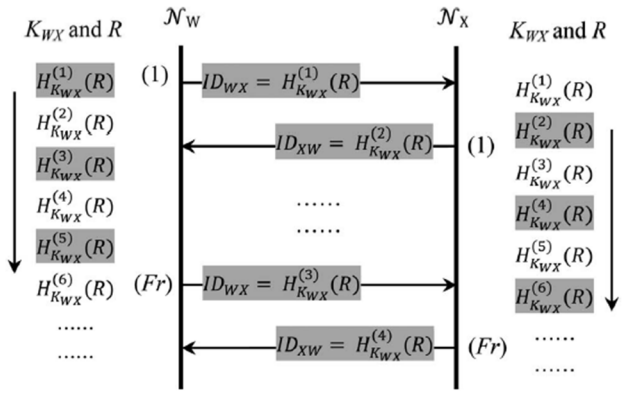


Fig. 1 Pseudonym Generation Technique

From Fig. 1, if nodes $N_w$and $N_X$share a secret key K_{wx}*(=* K_{xw}*)*and a public random seed value R, they can generate shared

pseudonyms by iteratively hashing R withK_{wx}.$H^{n}_{Kwx}(R)$refers to the keyed hash value resulted fromiteratively hashing R n times with Kw_X.The pseudonyms generated from hashing R odd times (ID $_{wx}$= $H_{kwx}^{(2*i-1)}$(R)= {$H^{(1)}_{kwx}$(R), $H^{(3)}_{kwx}$(R),….}) are used byNw,and those generated from hashing R even times(ID $_{xw}$= $H_{kwx}^{(2*i)}$(R)= {$H^{(2)}_{kwx}$(R), $H^{(4)}_{kwx}$(R),….}) are used by N_X where i=1,2,….etc. A one-way hash function, H, maps an input of any length to a fixed-length bit string. The function H is simple to compute yet computationally infeasible to invert. An example for a secure hash function is SHA-1 [20].To maintain pseudonym synchronization between Nwand N_X, each node matches the other node's expected pseudonym with the current and next pseudonyms. Each node does not change its pseudonym more than once before the other node changes its pseudonym. By this way, if the packet containing new pseudonym e.g., $H^{(3)}_{kwx}$(R) is lost, the nodes do not lose synchronization because N_W will not use $H^{(5)}_{kwx}$(R) before N_X releases $H^{(4)}_{kwx}$(R) and shifts the window of expected pseudonyms from N_W to $H^{(3)}_{kwx}$(R) to $H^{(5)}_{kwx}$(R).

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> 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 (Fr) is the number of packets that use one pseudonym. Higher privacy level is obtained when Fr decreases.

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

Fig. 2.Authentication phase.

The highest privacy level can be obtained whenFr = 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 (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 authenticated because no one can compute them except the owner of the secret key.

B. 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:

Each node, e.g., N_X, and Tp share a longterm key K_X. By using this key, they can generate a long-term pseudonym chain named ID_{XTp} and ID_{TpX}.

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 authenticationprocess 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 basestation 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 throughmultihopping. AREQ packet has a fresh pseudonym shared with Tp(ID_{XTp}) and the encryption of ID_{XTp} and its real identity (ID_X), where (ID_{XTp}; ID_X)K_X refers to the ciphertext resulted from encrypting ''ID_{XTp},ID_X'' with K_X.

AREQ packet authenticates N_X to Tp because the secret key K_X is required to compose valid packet. Without knowing K_X, it is infeasible to compute valid ($ID_{XTp,}ID_X$)K_X and fresh ID_{XTp}. The base station (Bs) forwards the request to Tp which checks whether the pseudonym is for a registered user and replieswith the node's real identity, the shared key between N_X andBs(K_{XBs} =K_{BsX}), and

Volume 3 Issue IV, April 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

the seed of the pseudonym

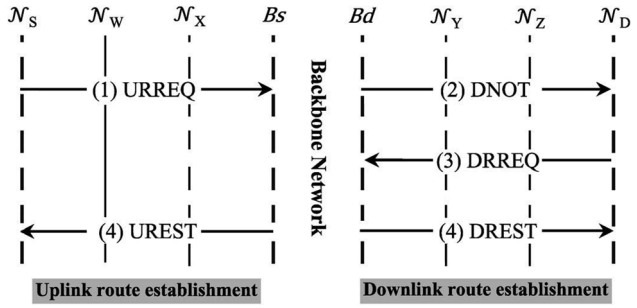


Fig. 3.Route discovery packets.

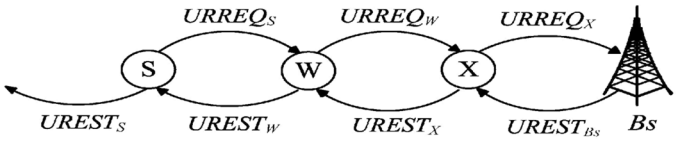
chain(R). With this packet, Tp authenticates N_X to the base station. R and K_{XBs} are used to generate pseudonyms shared between N_X and Bs.base station sends Authentication Reply (AREP) packet to N_X. N_X can ensure that the packet is sent from Tp because it is infeasible to compute ID_{TpX} and (K_{XBs},ID_{TpX}; R)K_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.

In route discovery 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 (K_{WX}= K_{XW}) 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 neighbors. By this way, routes can be identified by pseudonym chains, which is necessary for successful packet routing.

C. Anonymous Route Discovery

From 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 broadcastsDestination 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 Establish-ment Packet (DREST), respectively to establish the route

*1) Uplink Route Request Packet (URREQ):*As shown in Fig. 4, the source node initiates route discovery by



$\boldsymbol{URREQ_S}$: $<Un_i, TTL, (Un_i, ID_S, ID_D, P_L, Pad)K_{SBs}>$

$\boldsymbol{URREQ_W}$: $<Un_i, \boldsymbol{TTL-1}, \boldsymbol{ID_{WBs}}, ((Un_i, ID_S, ID_D, P_L, Pad)K_{SBs})\boldsymbol{K_{WBs}}>$

$\boldsymbol{URREQ_X}$: $<Un_i, \boldsymbol{TTL-2}, \boldsymbol{ID_{XBs}}, ((ID_{WBs}, ((Un_i, ID_S, ID_D, P_L, Pad)K_{SBs})K_{WBs}))\boldsymbol{K_{XBs}}>$

$\boldsymbol{UREST_{Bs}}$: $<ID_{BsX}, (Un_i, K_{XBs}, ID_{BsW}, (Un_i, K_{WX}, ID_{BsS}, (Un_i, K_{SW}, Pad)K_{BsS})K_{BsW})K_{BsX}>$

$\boldsymbol{UREST_X}$: $<ID_{BsW}, (Un_i, K_{WX}, ID_{BsS}, (Un_i, K_{SW}, Pad)K_{BsS})K_{BsW}>$

$\boldsymbol{UREST_W}$: $<ID_{BsS}, (Un_i, K_{SW}, Pad)K_{BsS}>$

$\boldsymbol{UREST_S}$: $<Pad>$

Fig. 4. Anonymous uplink route establishment

broadcasting URREQ packet containing a unique request identifier (Un_i), time to live (TTL), and the encryption of Un_i, the source

and the destination nodes' real identities, dummy bits called padding (Pad), and the padding length (P_L). Un_i is the pseudonym shared with Bs(ID_{SBs}) and time stamp. Each node and the base station process only the first received URREQ packet and discard all further packets having the identifier Un_i. Using this identifier is necessary to avoid routing loops and broadcastexplosion that causes broadcasting the same packet each time it is received from a neighbor. This identifier does not reveal much information because the packets are broad-casted. ID_{SBs} and the encrypted part authenticate N_S 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 N_D resides in a different cell. Since the packet length grows with fixed amount of data as it is relayed, the attackers may try to locate the source node's location either from TTL or the packet size. To protect the location privacy of N_S and to confuse its neighbors whether the packet is originated from or relayed by N_S, a random-length padding is added and the initial TTL is variable value. Since Un_i 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. This can thwart fingerprint recording attack as will be discussed in Section 5.

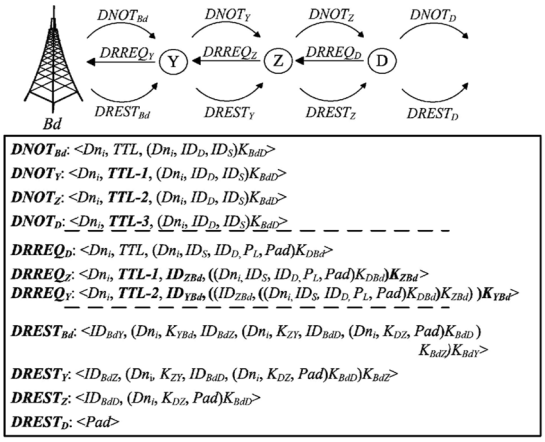


Fig. 5. Anonymous downlink route establishment

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 ðDn$_i$Þ that has the pseudo-nym shared with N_D and time stamp. The packet also contains Time-to-Live (TTL), and the encryption of Dn_i and the destination and source nodes' identities with using the shared key with N_D. 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.
3) *Downlink Route Request Packet (DRREQ):*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) *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 Un_i and its pseudonym and key. The node hashes this

Volume 3 Issue IV, April 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

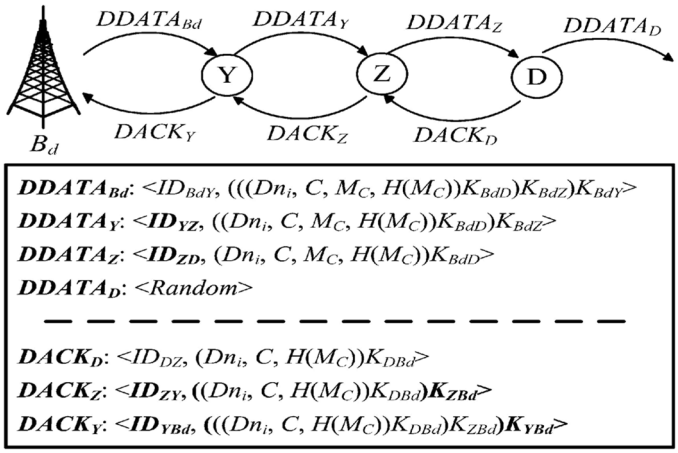


Fig. 6. Anonymous uplink data transmission

key to compute the key shared with the other neighbor, e.g., node N $_W$ usesK$_{WX}$ to communicate with N $_X$ and K$_{WS}$-H$_{KwBs}$(K$_{WX}$,1),H$_{KwBs}$(K$_{WX}$,1.2) . . . etc, to communicate with N $_S$. Obviously,K$_{WS}$ should be similar to K$_{SW}$ 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.

5) Downlink Route Establishment Packet (DREST) :This packet informs the downlink intermediate nodes to act as relays and distributes the session keys shared betweeneach two neighboring nodes. The packet's format is similar to that of UREST packet. By the route discovery packets, the base station and the nodes mutually authenticate each other, and each two neighboring nodes mutually authenticate each other with the assistance of the base station. These authentication processes are necessary to secure the routing protocol and the payment.

6) 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 (ID$_{SW}$), and the encryption of Un$_i$, the message's number (C), and the message M$_C$ and its hash value (H (M$_C$))). 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

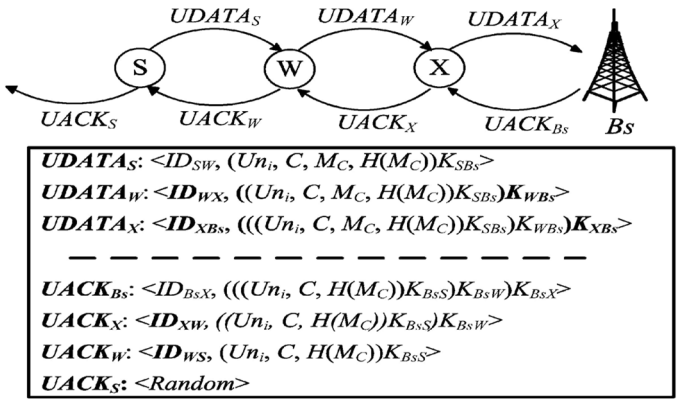


Fig. 7.Anonymous downlink data transmission

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.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 (N_Y). Each intermediate node removes one encryption layer and replaces the pseudonym with the one shared with the next node. The destination node decrypts the packet and verifies the hash value to ensurethe message's integrity and authenticity. For reliable communication, the destination node sends back an acknowledgement packet when it receives a correct message.Note that the session keys are used only for generating one-time pseudonyms, but the keys shared with the base station are used in encryption to prevent manipulating the messages and secure the payment by thwarting free riding attack, as will be discussed in Section 4. Moreover, the time element in Un_i can guarantee that the packets look different if the same message is sent at different times. As will be discussed in Section 4, this can protect the nodes' anonymity against fingerprint recording attack. To reduce the overhead on the mobile nodes, each node performs one encryption/decryption operation, but the base station performs more operations. To simplify our description, we focus on unidirectional data transmission, but the protocol can also be used for bidirectional communication.

A route is broken when two neighboring nodes in the route cannot communicate, e.g., because they are no longer in transmission range due to node mobility. When a node forwards a packet to its neighbor, it can confirm that the neighbor received the packet by link-layer acknowledgment. A route isconsidered broken if a node does not receive an acknowledgment after a limited number of packet retransmissions. In this case, the node should send an error packet to the base station to reestablish the route. Moreover, the base station can determine route breakage by re-starting a timer each time it receives a data or acknowledgement packet, and the route is considered broken if the timer expires. To reduce the overhead of reconnecting the broken routes, the base station can cache the routing information when it receives route discovery packets and uses this information when it needs to establish a route by unicasting a DREST packet.

7) *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 interme-diate 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 payment model can do that without using receipts as will be discussed in Section 5. To manage the payment without instantaneously contacting Tp in each session, the base stations can manage the payment 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.

III. SECURITY AND PRIVACY ANALYSES

A. Communication Security

The existing payment systems can guarantee the rationality of packet relaying by rewarding the nodes for every relayed packet even if it does not reach the destination. However, this requires submitting payment receipts when a route is broken to identify the last node that relayed the packet. The nodes can collude to earn credits with consuming low resource by relaying only the security token (e.g., signature) to compose valid receipt instead of relaying the whole packet. Our payment system can guarantee the rationality of packet relaying, encourage the nodes' cooperation, and counteract rational cheating actions without the overhead of storing, submitting, and processing receipts, as follows:

1) 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.

2) Relaying the route discovery 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.
3) If the source and destination nodes are charged only for delivered packets, they can communicate freely if thedestination 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 communication time. Most of the existing payment systems [1], [5], [6], [7] are vulnerable to this attack because they use post-paid payment policy, where the nodes communicate first and pay later. In our payment system, the base stations can thwart this attack because they can know the

nodes' total credits at the communication time.Our protocol 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 protocol 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 fabrication of route discovery packets, an attacker tries to fabricate route discovery packets to impersonate a source or a destination node or a base station. This is infeasible in our protocol because the nodes' secret keys should be used to compose valid packets. In our protocol, the attackers cannot compose URREQ packet with valid timestamp and fresh pseudonym without knowing the secret keys of the victim nodes.For packet modification attack, if an attacker manipulates a packet in our protocol, 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.

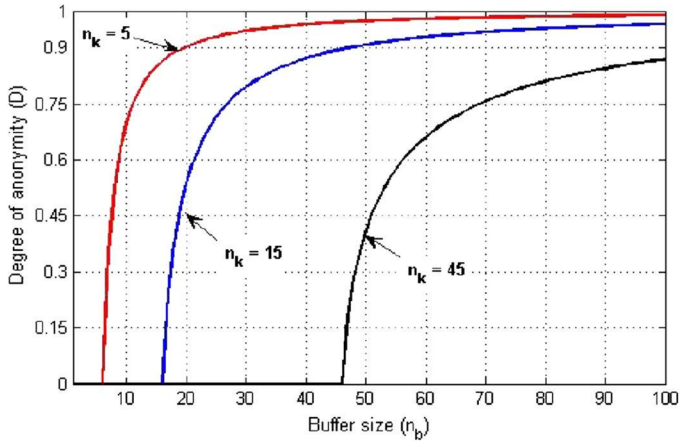


Fig. 8.Degree of anonymity versus n_b.

In session-hijacking attack, 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.

We use information-theoretic metric, called entropy [21], to

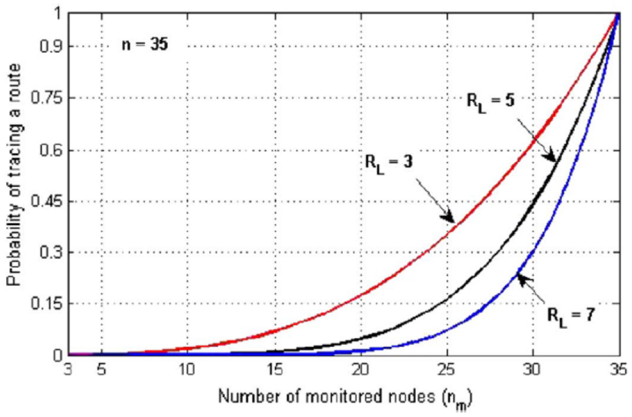


Fig. 9. Probability of tracing a route versus n_m

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. Themaximum entropy (H_{max}) is given in Eq. (2), and the anonymity degree (D) is given in Eq. (3)

Volume 3 Issue IV, April 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

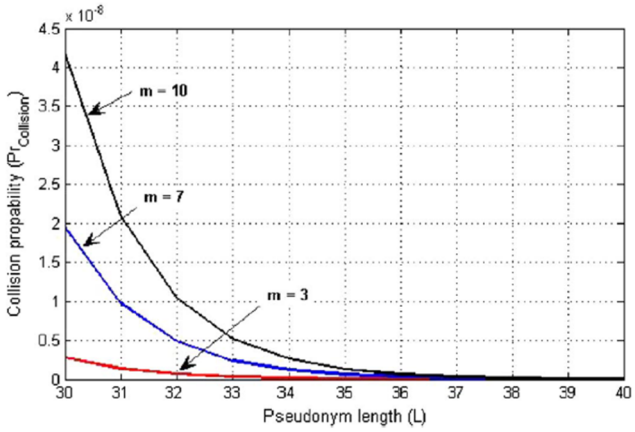


Fig. 10. Collision Probability versus pseudonym length

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, 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, communication activities, and locations.

$$H(X) = -\sum_{i=1}^{n_b - n_k} P_i \cdot \log_2(P_i) \quad (1)$$

$$H'_{\max} = -\sum_{i=1}^{n_b - n_k} \frac{1}{n_b - n_k} \cdot \log_2\left(\frac{1}{n_b - n_k}\right) = \log_2(n_b - n_k) \quad (2)$$

$$D = 1 - \frac{H_{\max} - H'_{\max}}{H_{\max}} = \frac{H'_{\max}}{H_{\max}} = \frac{\log_2(n_b - n_k)}{\log_2 n_b}$$

$$Where: \; H_{\max} = -\sum_{i=1}^{n_b} \frac{1}{n_b} \cdot \log_2\left(\frac{1}{n_b}\right) = \log_2(n_b). \quad (3)$$

Location privacy is defined as the ability to prevent attackers from deducing a user's current or past locations whether the exact physical locations or the relative locations in number of hops.For Source-destination pair unlink ability, although attackers may know that a pair of nodes participates in communication activity, they cannot ensure that the pair communicates with each other. In our protocol, every time a source and destination pair communicates, the route discovery packets look different, so linking a packet to a source-. Moreover, if an attacker eavesdrops on the source and destination nodes and their base stations, he cannot make sure that they currently communicate. For source node and base station unlink ability, if an adversary eavesdrops on a source node and its base station, linking the packets is infeasible. For a transmission and source node unlink ability, 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. Anonymity of a subject means that the subject is not uniquely characterized within a set of subjects that is called the anonymity set. Identity anonymity means that the real identity of a node that participates in a route either as source, intermediate or destination cannot be identified by attackers. Sender anonymity means that an adversary cannot identify the source node in a particular communication session. In our protocol, a particular transmission is unlikable to a source node, and any transmission is unlinkable to a particular source node. Similarly, recipient anonymity means that an adversary cannot identify the destination node of a particular session.

Route anonymity means that attackers cannot infer the nodes participating in the route. For Neighbor anonymity, a long-time

relation between a node and its neighbors enables the attackers to collect much information that will severely violate theneighbor's anonymity if the attackers could link a neighbor to a user. 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 protocol can use one pseudonym per packet. In the protocols that do not use per-hop encryption/decryption operations, 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 eaves-dropper 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 is more probable to trace the shorter routes than the longer ones.

$$P_r = \frac{n_m! \times (n - R_L)!}{(n_m - R_L)! \times n!}. \qquad (4)$$

In fingerprint recording attack, the attackers record a list of plaintexts and the corresponding ciphertexts computed by a node so that they are used as a fingerprint for the node. Each time the attackers observe a plaintext-ciphertext pair, they can identify the node. In our protocol, the session keys are used only for one session and all the packets have a variable part (time stamp or a fresh pseudonym) so that the same plaintext-ciphertext pair cannot be produced at different occasions. Thus, even if an attacker could link a plaintext-ciphertext pair to a node in one occasion, he cannot benefit from this conclusion in the future. We call this property forward privacy-preservation, i.e., if an attacker could violate a user's privacy in one occasion, this privacy violation should not help violate the user's privacy in the future. For pseudonym unlinkability, attackers should not be able to link the pseudonyms of one chain. Pseudonym collision means that more than one node have identical pseudonyms because the hash function may generate the same hash value from hashing different inputs. Pseudonym collision may result in losing pseudonym synchronization, or forwarding packets to a wrong direction because pseudonyms are used as routes' identifiers. Using birthday paradox [20], the pseudonym collision probability is $2^{-k/2}$, where K is the number of bits of a pseudonym. For example, if K = 64 bits, the pseudonym collision probability is 2.3×10^{-10}, which implies one pseudonym collision every $4.2\text{-}10^{+9}$ pseudonyms. As studied in [22], the probability of pseudonym collision is given in Eq. (5) when m pseudonyms are selected and L is the pseudonym length in bits.

$$Pr_{Collision} = 1 - \frac{\prod_{i=0}^{m-1}(2^L - i)}{(2^L)^m}. \qquad (5)$$

Fig. 10 shows that the linear increase of L decreases the pseudonym collision probability exponentially and the increase of m can increase the collision probability. To reduce the packet overhead, pseudonyms can be truncated to shorter bit string without significantly increasing the probability of pseudonym collision as shown in Fig. 10.

In fake route discovery attack, the attackers initiate route discovery packets with the intention of collecting information about the nodes in the network.

The attackers may make use of this fact by initiating fake URREQ packets and analyzing the packets sent by neighbors to learn whether a user is still in the neighborhood

To do this, the proposed protocol for establishing uplink routes explained in Fig. 5 can be used, and the padding can be a pre-defined value to inform the base station that the packet is for updating the pseudonym window and not for communication call. The base station replies with UREST packet with a fresh pseudonym.In pseudonym de-synchronization attack, the attackers try to damage the pseudonym synchronization between a node and the base station.

TABLE 2 PERFORMANCE EVALUATION

		RREQ	*DNOT*	*REST*	Data packet
Delay (ms)	**Min**	Route establishment		97.61	41.68
	Avg.			101.32	42.76
	Max			105.03	43.84
Avg. packet length (bytes)	**Min**	70.585	91.88	161.76	534.3
	Avg.	73.68	95.31	170.27	548
	Max	76.775	98.74	178.78	561.7

Table 2 gives the simulation results of the proposed protocol. Route establishment delay is the average time interval between sending an URREQ packet by a source node and receiving the UREST packet. The data packet delay is the average time interval between sending a data packet by a source node and receiving it by the destination node. These delays include: processing delays at each node, queuing delay atthe interface queue, retransmission delays, and propagation time. The simulation results indicate that the expected route establishment and data transmission delays are acceptable due to using lightweight cryptographic operations and pre-computing the pseudonyms. For the RREQ and REST packets, the packet length varies at each node as the packet is relayed, so the average is computed by dividing the amount of data relayed at all hops by the number of hops. The results also indicate that the overhead of the data packets is 36 bytes that constitute 7 percent of the message size (512 byes). REST packet is large because it carries the nodes' session keys, but being unicated packet and reducing the packet size at each hop can alleviate this. The packet delivery ratio is the number of data packets received by the destination nodes to those sent by the source nodes. Our simulation results indicate that the average packet delivery ratio is 0.95.

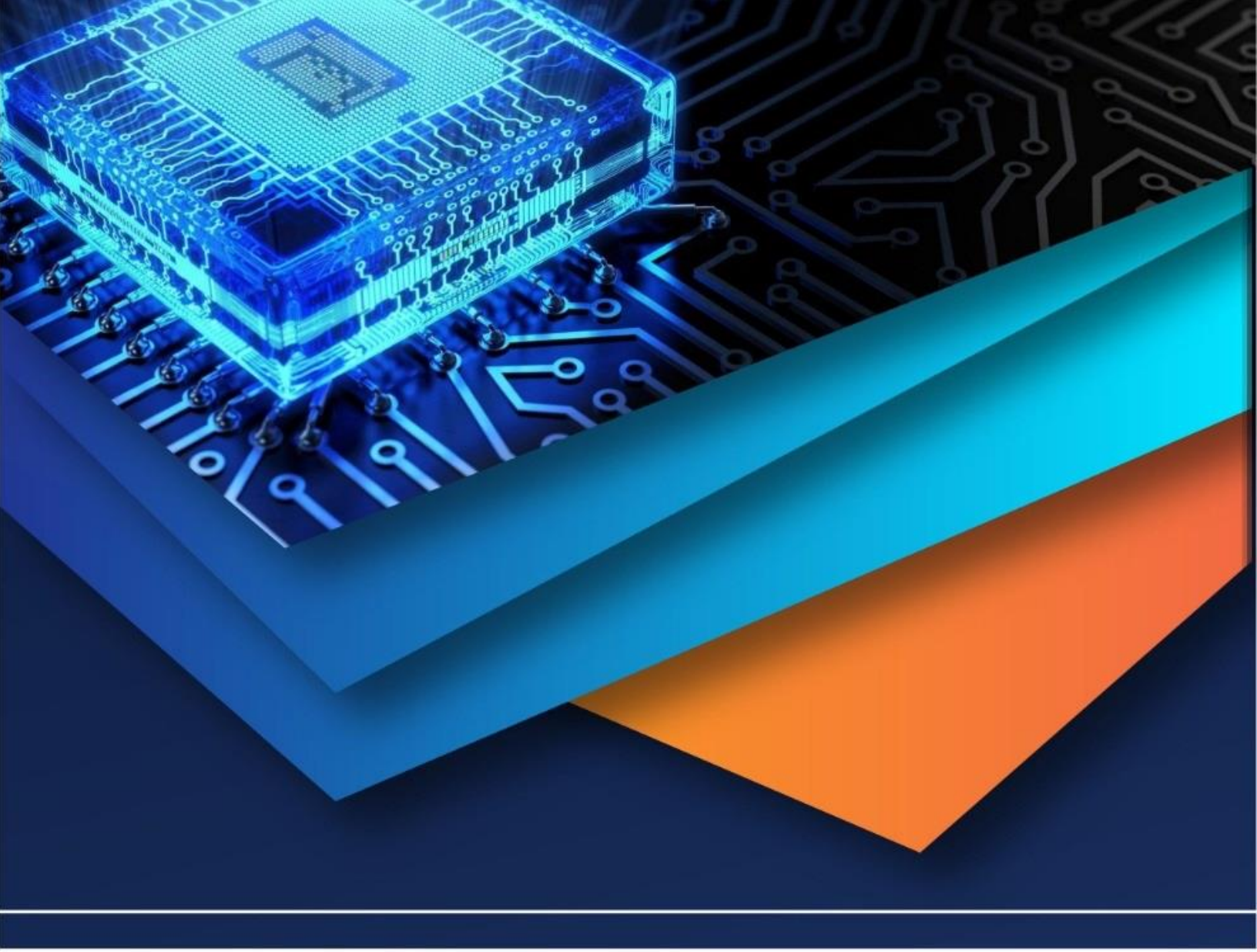
IV. CONCLUSION

The protocol proposed is a lightweight secure and privacy-preserving protocol for hybrid ad hoc wireless network. To preserve users' privacy, short-life pseudonyms, one-time session keys, and per-hop encryption/decryption operations are used. To secure the communication Cryptographic operations and payment system are used. Lightweight cryptographic operations are used, efficient trapdoor technique is developed, and the payment can be secured without storing, submitting, or processing receipts to reduce the overhead. 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. The 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] Mohamed M.E.A. Mahmoud, Sanaa Taha, JelenaMisic, Xuemin (Sherman) Shen "Light Weight Privacy Preserving and Secure Communication Protocol for Hybrid Ad Hoc Wireless Networks" IEEE Trans. on Parallel Distributed Systems, vol. 25, no. 8, pp. 2077-2090,Aug. 2014.
[2] 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.
[3] M. Mahmoud and X. Shen, ''Lightweight Privacy-Preserving Routing and Incentive Protocol for Hybrid Ad Hoc Wireless Networks,'' in Proc. IEEE INFOCOM'11-Int'l Workshop Security Computers, Networking Comm. (SCNC), Shanghai, China, Apr. 2011, pp. 1006-1011.
[4] 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.
[5] N. Salem, L. Buttyan, J. Hubaux, and M. Jakobsson, ''Node Cooperation in Hybrid Ad Hoc Networks,'' IEEE Trans. on Mobile Computing, vol. 5, no. 4, pp. 365-376, Apr. 2006.
[6] M. Mahmoud and X. Shen, ''ESIP: Secure Incentive Protocol 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.
[7] 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.
[8] 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. 2010, pp. 776-784.
[9] S. Capkun, J.P. Hubaux, and M. Jakobsson, ''Secure and Privacy-Preserving Communication in Hybrid Ad Hoc Networks,'' EPFL-DI-ICA, Laussane, Switzerland, Tech. Rep. IC/2004/10, 2004.
[10] 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.
[11] A. Boukerche, K. El-Khatib, L. Korba, and L. Xu, ''A Secure Distributed Anonymous Routing Protocol for Ad Hoc Wireless Networks,'' J. Comput. Commun., vol. 28, no. 10, pp. 1193-1203, 2005.
[12] 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.
[13] M. Mahmoud and X. Shen, ''Secure 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.
[14] K. Ren, S. Yu, W. Lou, and Y. Zhang, ''PEACE: A Novel Privacy-Enhanced Yet Accountable Security Framework for Metropolitan Wireless Mesh Networks,'' IEEE Trans. on Parallel Distributed Systems, vol. 21, no. 2, pp. 203-215, Feb. 2010.

[15] 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.
[16] 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.
[17] Y. Zhang, W. Liu, W. Lou, and Y. Fang, ‘‘Securing Mobile Ad Hoc Networks with Certificateless Public Keys,’’ IEEE Trans. on De-pendable Secure Computing, vol. 3, no. 4, pp. 386-399, Oct./Dec. 2006.
[18] 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.
[19] Y.-C. Hu, A. Perrig, and D. Johnson, ‘‘Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks,’’ in Proc. ACM Conf. MobiCom Computing and Networking, 2002, pp. 12-23.
[20] M. Mahmoud, M. Barua, and X. Shen, ‘‘SATS: Secure Data-Forwarding Scheme for Delay-Tolerant Wireless Networks,’’ in Proc. IEEE Global Comm. Conf. (IEEE GLOBECOM’11), Houston, TX, USA, Dec. 2011, pp. 1-5.
[21] A.J. Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography. Boca Raton, FL, USA: CRC Press, 1996.
[22] C. DNaz, S. Seys, J. Claessens, and B. Preneel, ‘‘Towards Measuring Anonymity,’’ in Proc. Privacy Enhancing Technologies Workshop (PET’02), LNCS 2482, R. Dingledine and P. Syverson, Eds., Apr. 2002, pp. 54-68.
[23] 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.
[24] W. Dai, Crypto++ Library 5.6.0. [Online]. Available: http://www. cryptopp.com/.
[25] Recommendation for Key ManagementVPart 1: General (Revised), National Institute of Standards and Technology (NIST), Washington, DC, USA, 2007, Special Publication 800-57 200.
[26] N. Potlapally, S. Ravi, A. Raghunathan, and N. Jha, ‘‘A Study of the Energy Consumption Characteristics of Cryptographic Algorithms and Security Protocols,’’ IEEE Trans. on Mobile Computing, vol. 5, no. 2, pp. 128-143, Feb. 2006.
[27] J. Yoon, M. Liu, and B. Nobles, ‘‘Sound Mobility Models,’’ in Proc. ACM MobiCom, San Diego, CA, USA, Sept. 2003, pp. 205-216.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY