Encrypted Receipt with Session Management in Multihop Wireless Network for Secure Payment

M. Durga[1], V. Mareeswari[2], Logesh R[3],K. Bharathi kannamma [4]
[1,3,4]PG Scholars, [2]Assistant Professor, , Sri Manakula Vinayagar Engineering College, *Puducherry.*

Abstract

Receipt-based payment schemes impose significant processing and communication overhead and implementation complexity. A trusted party may not be involved in communication sessions, the nodes compose proofs of others' packets is called receipts, and present them to an offline accounting center (AC) to clear the payment. In this paper, we aim RACE, a Report-based payment scheme for MWNs. The nodes state lightweight payment reports (instead of receipts) to the AC to update their credit accounts, and temporarily store undisputable security tokens called Evidences. For security reason the report can be encrypted using RSA algorithm and send to AC. The AC verifies the payment by investigating the consistency of the reports, and authorizes the payment of the fair reports. For cheating reports, the Evidences are requested to identify and evict the cheating nodes that submit faulty reports, e.g., to steal credits or pay less. In otherwise, the Evidences are used to resolve disputes when the nodes disagree about the payment. Rather requesting the Evidences from all the nodes participating in the cheating reports, RACE can describe the cheating nodes with submitting and processing few Evidences.

Keywords— TP (Trusted Party) , RACE(Report based pAyment sChemE) , payment schemes, AC (Accounting Center) , RSA algorithm

1. Introduction

In multihop wireless networks (MWNs), the traffic originated from a node is usually relayed through the other nodes to the destination for enabling new applications and enhancing the network performance and deployment [1]. Multihop packet relay can extend the network coverage using limited transmit power, better area spectral efficiency, and increase the network throughput and capacity. MWNs can be implemented readily at low cost in developing and rural areas [2]. For example Users is in one area (residential neighborhood, university campus, etc.) having unlike wireless-enabled devices, e.g., laptops, tablets, cell phones, etc., can demonstrate a network to communicate, distribute files, and contribute information. selfish nodes do not relay others packets, because it have their imagination without benefits of the cooperative nodes to relay their packets, which has a damaging effect on the network fairness and may cause multihop communications to fail [3].

1.1 Payment Scheme

Payment (or incentive) schemes [4] use credits (or micropayment) to motivate the nodes to cooperate in relaying others' packets by making cooperation more beneficial than selfishness. Multihop network such as mobile adhoc network selfish or misbehaving nodes cab disrupt the whole network and degrade the network performance. For security reason the report can be encrypted using RSA algorithm and send to the accounting center. The payment scheme regulate packet transmission and discourage Message flooding attacks where the attackers send bogus message to resource intermediate node [5]. Fairness can be enforced by rewarding the nodes that relay more packets and charging the nodes that send more packets. For example, the nodes located at the network center relay more packets than the other nodes because they are more frequently selected by the routing protocol. Without contacting distant home location register the payment scheme will charge the node to different foreign network.

RACE can clear the payment nearly without applying cryptographic operations and with submitting lightweight reports when Evidences are not often requested. Widespread cheating actions are not expected in civilian applications because the common users do not have the technical knowledge to tamper with their devices. Cheating nodes are evicted once they commit one cheating action and it is neither easy nor cheap to change identities. Our analytical and simulation results establish that RACE requires much less communication and processing overhead than the existing receipt-based schemes with acceptable payment clearance delay and Evidences' storage area, which is necessity to make the practical implementation of the payment scheme effective. RACE can secure the payment and precisely identify the cheating nodes without false accusations or stealing credits.

2. Related works

The existing payment scheme can be divided into two types, Tamper-proof-device (TPD)-based and receipt-based scheme. In TPD-based payment scheme [6], [7], a Tamper Proof Device is installed in each node to store and manage the credit account and secure its operation. For receipt-based payment scheme [8], [9], [10], [11], an offline central unit called accounting centre store and manage the nodes' credit account. In order to eliminate the need for TPDs, an offline central bank called the AC is used to store and manage the nodes' credit accounts. The source node signs the identities of the nodes in the route and the message, and sends the signature as a proof for sending a message. The intermediate nodes verify the signature, compose receipts containing the identities of the nodes in the route and the source node's signature, and present the receipts to the AC to claim the payment. The AC verifies the source node's signature to make sure that the payment is correct.

In SIP [6], after receiving a data packet, the destination node sends out a RECEIPT packet to the source node to issue a REWARD packet to increment the credit accounts of the intermediate nodes. In CASHnet [7], the credit account of the source node is charged and a signature is attached to each data packet. Finding the packet, the credit account of the destination node is also charged, and a digitally signed acknowledgement (ACK) packet is sent back to the source node.

In Sprite [8], for each message, the source node signs the identities of the nodes in the route and the message, and sends the signature as a proof for sending a message. The intermediate nodes verify the signature, compose receipts containing the identities of the nodes in the route and the source node's signature, and present the receipts to the AC to claim the payment. The AC verifies the source node's signature to make sure that the payment is correct. However, the receipts overwhelm the network because the scheme generates a receipt per message.

Unlike the SPRITE charge only to the source node, FESCIM [9] adopts fair charging policy by charging both the source and the destination node in which both of the nodes are interested to communication. In PIS, the signature will be attached to each source node and the destination node replies the sign with an ack. In a payment scheme has been proposed for hybrid ad-hoc networks, but involving the base stations in every communication session may lead to suboptimal routes when the source and destination nodes reside in the same cell. In addition the intermediate nodes cannot verify the authenticity and the integrity of the messages because corrupted messages are relayed to the base stations before they are dropped and it create a bottleneck.

In SPRITE, PIS [10] can reduce the receipt number by generating the fixed-size receipt per session regardless of the number of message instead of generating a receipt message. CDS is used to reduce communication and processing overhead to identify the cheating nodes that submit incorrect report. Due to the nature of the statistical method some honest nodes are treated as a false node, these nodes may be falsely accused of cheating which is called false accusation illustrated in fig 1. Sometime it takes a long time to identify the cheating nodes.

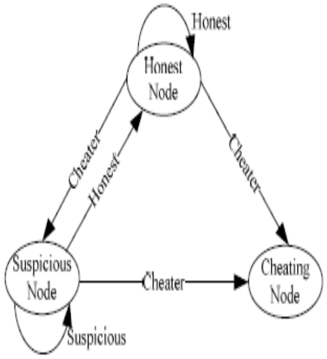
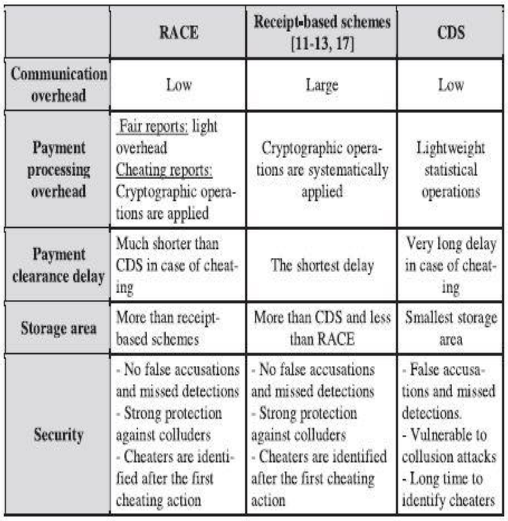


Fig. 1.State transition diagram of a node

In ESIP [11] proposes a communication protocol that can be used for payment scheme. In ESIP the message can be transfer from source node to the destination node with limited number of public key cryptography operation. Identity based cryptography is used to efficiently compute a shared symmetric key between the source node and each node in the route. Using these keys, the source node calculates and sends a keyed hash value for each intermediate node to verify the message integrity. Equating to PIS, ESIP requires fewer public key cryptography operations but with larger receipts' size. Unlike ESIP objective is to transfer messages efficiently from the source to the destination nodes, RACE objective to reduce the overhead of submitting the payment data to the AC and working them. Although the communication protocol proposed in ESIP can be used with RACE, we use a simple protocol due to space limitation and to focus on our contributions.

Table 1 summarizes the main features of RACE and the existing payment schemes. RACE is more secure than CDS because it does not suffer from false charge, missed detections, and delay in identifying attackers, and it can thwart collusion attacks. Moreover, RACE requires much less communication and processing overhead comparing to receipt-based schemes [8], [9], [10], yet with more and acceptable storage area and payment clearance delay.

TABLE 1
Comparison between RACE and the Existing Payment Schemes



	RACE	Receipt-based schemes [11-13, 17]	CDS
Communication overhead	Low	Large	Low
Payment processing overhead	Fair reports: light overhead Cheating reports: Cryptographic operations are applied	Cryptographic operations are systematically applied	Lightweight statistical operations
Payment clearance delay	Much shorter than CDS in case of cheating	The shortest delay	Very long delay in case of cheating
Storage area	More than receipt-based schemes	More than CDS and less than RACE	Smallest storage area
Security	- No false accusations and missed detections - Strong protection against colluders - Cheaters are identified after the first cheating action	- No false accusations and missed detections - Strong protection against colluders - Cheaters are identified after the first cheating action	- False accusations and missed detections. - Vulnerable to collusion attacks - Long time to identify cheaters

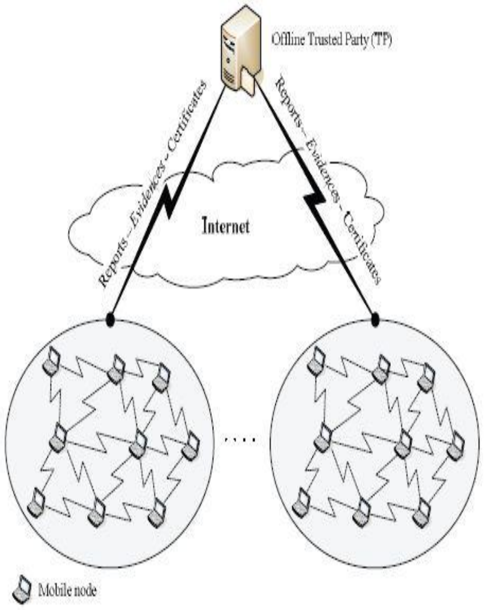

Offline Trusted Party (TP)
Reports – Evidences – Certificates
Reports – Evidences – Certificates
Internet
....
Mobile node

Fig. 2. Architecture of the network

3. System design

3.1 Network and Communication Models

MWN includes AC, mobile nodes, and base stations in some types of MWNs. The AC stores and manages the nodes' credit accounts and generates private/public key pair and certificate with unique identity for each node to participate in the network. Once the AC receives a receipt (proof of payment), it updates the relevant nodes' accounts and identifies and revokes the misbehaving nodes. An on-demand routing protocol, such as dynamic source routing [12] and ad hoc on-demand distance vector (AODV) [13], is implemented to establish an end-to-end communication session between the source and the destination nodes. The source node's packets may be relayed in several hops by the intermediate nodes to the destination. The network nodes can contact with the AC at least once during a time interval, which can be in the range of a few days. This connection can occur via base stations, Wi-Fi hotspots, or wired networks (e.g., Internet). During this connection, a network node renews or revokes its certificate, submits the payment receipts, and purchases credits by real money.

Each node A has to register with the trusted party to receive a symmetric key KA, private/public key pair, and certificate. The symmetric key is used to present the payment reports and the private/public keys are required to act as source or destination node. We assume that the clocks of the nodes are synchronized. The details of this synchronization process are out of the scope of the paper, but several mechanisms have been proposed to synchronize the nodes' clocks [14]. Once the AC receives the payment reports of a session and verifies them, it clears the payment if the reports are fair; else, it requests the Evidences to identify the cheating nodes. The CA evicts the cheating nodes by denying renewing their certificates illustrated in fig2. RACE can be used with any source routing protocol, such as DSR [15], which establishes end-to-end routes before transmitting data. Source nodes' packets may be relayed several hops by intermediate nodes to their destinations. The nodes can contact the TP at least once during a period of few days.

3.2 Charging and Rewarding Policy

In most existing incentive systems [17], [18], [19]–[20], only the source node is charged. We argue that a more fair charging policy is to support cost sharing between the source and the destination nodes because both of them benefit from their communication.

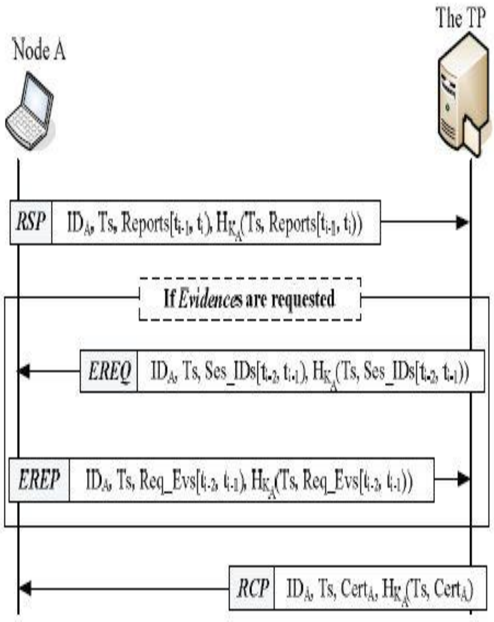
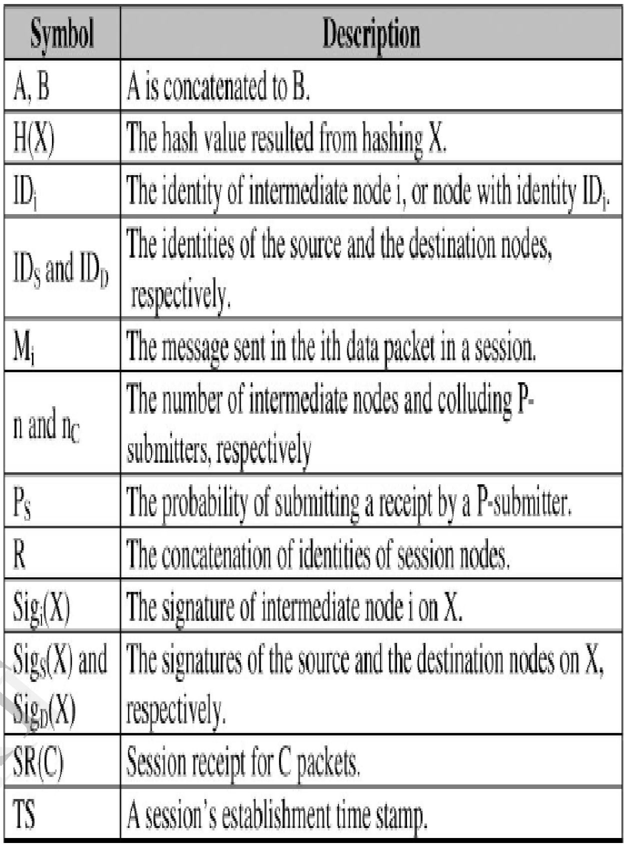

The TP
Node A
RSP
ID_A, Ts, Reports[t_{i-1}, t_i), H_{K_A}(Ts, Reports[t_{i-1}, t_i))
If Evidences are requested
EREQ
ID_A, Ts, Ses_IDs[t_{i-2}, t_{i-1}), H_{K_A}(Ts, Ses_IDs[t_{i-2}, t_{i-1}))
EREP
ID_A, Ts, Req_Evs[t_{i-2}, t_{i-1}), H_{K_A}(Ts, Req_Evs[t_{i-2}, t_{i-1}))
RCP
ID_A, Ts, Cert_A, H_{K_A}(Ts, Cert_A)

Figure 3. Submission of reports and evidence

The payment ratio is adaptable and can be negotiated during the session establishment phase. To simplify our presentation, we suppose the source and the destination nodes agreed to halve the packet-relaying expense, although any other payment splitting ratio can be used. For rewarding policy, some motivator systems [21], [22] consider a different packet-relaying cost that corresponds to the incurred energy in packet relay. This rewarding policy is difficult to be implemented in practice without involving complicated route-discovery process and calculation of en route individual payments.

Therefore, similar to [16], [18], [19], and [20], we use a fixed rewarding rate, e.g., λ credits per unit-sized packet. In MWNs, packet loss may occur normally due to node mobility, packet collision, channel damage, or other reasons. Ideally, any node that has ever tried to forward a packet should be rewarded no matter if the packet eventually reaches its destination or not because forwarding a packet consumes the node's resources. Table 2 gives the description of the used symbols. A payment report contains the session identifier, a flag bit (F), and the number of messages (X). The session identifier is the concatenation of the identities of the nodes in the session and the time stamp. The flag bit is zero if the last obtained packet is data and one if it is ACK. The submission of reports and Evidences are illustrated in Fig. 3.

TABLE II
Description of the Used Symbols



Symbol	Description
A, B	A is concatenated to B.
H(X)	The hash value resulted from hashing X.
ID_i	The identity of intermediate node i, or node with identity ID_i.
ID_S and ID_D	The identities of the source and the destination nodes, respectively.
M_i	The message sent in the ith data packet in a session.
n and n_C	The number of intermediate nodes and colluding P-submitters, respectively
P_S	The probability of submitting a receipt by a P-submitter.
R	The concatenation of identities of session nodes.
$Sig_i(X)$	The signature of intermediate node i on X.
$Sig_S(X)$ and $Sig_D(X)$	The signatures of the source and the destination nodes on X, respectively.
SR(C)	Session receipt for C packets.
TS	A session's establishment time stamp.

4. Proposed Work

RACE illustrated in fig 4 has four phase. In Communication phase, the nodes are involved in communication sessions and Evidences and payment reports are composed and temporarily stored. The nodes collect the payment reports and submit them in batch to the TP. For the Classifier phase, the TP classifies the reports into fair and cheating. For Identifying Cheaters phase, the TP requests the Evidences from the nodes that are involved in cheating reports to identify the cheating nodes. The cheating nodes are forced out and the payment reports are corrected. Finally, in Credit-Account Update phase, the AC clears the payment reports.

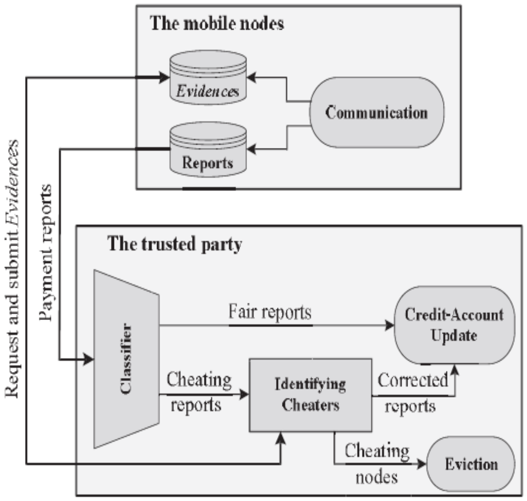


Fig. 4. The Architecture of RACE.

4.1 Network Formation

In this module we form the network for secure payment scheme. The network contains number of mobile nods and Trusted Party. The TP contains the AC and the certificate authority (CA). The AC maintains the nodes' credit accounts and the CA renews and revokes the nodes' certificates. Each node A has to show with the trusted party to receive a symmetric key KA, private/public key pair, and certificate. The symmetric key is used to present the payment reports and the private/public keys are required to act as source or destination node.

4.2 Communication Phase

The Communication module has four processes: route establishment, data transmission, Evidence composition, and payment report composition/submission.

4.2.1 Route Establishment

In this process an end to end route will be established. The source node broadcasts the Route Request (RREQ) packet containing the identities of the source (IDS) and the destination (IDD) nodes, time stamp (Ts), and Time-To-Live (TTL). The destination node composes the Route Reply (RREP) packet for the nodes broadcasted the first received RREQ packet, and sends the packet back to the source node.

4.2.2 Data transmission

The source node sends data packets to the destination node through the established route and the destination node replies with ACK packets.

4.2.3 Evidence composition

Evidence is defined as information that is used to establish proof about the occurrence of an event or action, the time of occurrence, the parties involved in the event, and the outcome of the event. The purpose of Evidence is to resolve a dispute about the amount of the payment resulted from data transmission.

4.2.4 Payment report submission

A payment report contains the session identifier, a flag bit (F), and the number of messages (X). The session identifier is the concatenation of the identities of the nodes in the session and the time stamp. The flag bit is zero if the last received packet is data and one if it is ACK.

4.3 Classifier Phase

The Trusted Party verifies them by investigating the consistency of the reports, and sort them into fair or cheating. For fair reports, the nodes present correct payment reports, just for cheating reports, at least one node does not submit the reports or submits incorrect reports, e.g., to steal credits. Fair reports can be for accomplished or broken sessions.

4.4 Cheaters Identification

The TP processes the cheating reports to identify the cheating nodes and correct the financial data. Our aim is to secure the payment is preventing the attackers (singular of collusive) from stealing credits or paying less. The AC requests the Evidence only from the node that submits report with more payment instead of all the nodes in the route because it should have the necessary and undeniable proofs (signatures and hash chain elements) for identifying the cheating node(s). In this way, the AC can exactly identify the cheating nodes with requesting few Evidences. To verify Evidence, the TP composes the PROOF by generating the nodes' signatures and hashing them. The Evidence is reasonable if the computed PROOF is similar to the Evidence's PROOF.

4.5 Credit Account Phase

The Credit-Account Update phase receives fair and corrected payment reports to update the nodes‟ credit accounts. The payment reports are authorized using the charging and rewarding policy and get the payment rightly. Upon registration the trusted party will give A Public & Private key pair, a symmetric key and a certificate. The public and private key pair is used in communication are required to act as source or destination node. The symmetric key is used to submit the payment reports.

5. Conclusion

Based on these trust values, we will propose a trust-based routing protocol to route messages through the highly trusted nodes (which performed packet relay more successfully in the past) to minimize the probability of dropping the messages, and thus improve the network execution in terms of throughput and packet delivery ratio. However, the trust system should be secure against singular and collusive attacks, and the routing protocol should make smart decisions regarding node selection with low overhead. By introducing RSA algorithm and the cluster algorithm overhead also reduced in RACE we can able to resist many attacks and the report is fair

6. References

[1] G. Shen, J. Liu, D. Wang, J. Wang, and S. Jin, “Multi-Hop Relay for Next-Generation Wireless Access Networks,” Bell Labs Technical J., vol. 13, no. 4, pp. 175-193, 2009.

[2] C. Chou, D. Wei, C. Kuo, and K. Naik, “An Efficient Anonymous Communication Protocol for Peer-to-Peer Applications Over Mobile Ad-Hoc Networks,” IEEE J. Selected Areas in Comm., vol. 25, no. 1, pp. 192-203, Jan. 2007.

[3] S. Marti, T. Giuli, K. Lai, and M. Baker, “Mitigating Routing Misbehavior in Mobile Ad Hoc Networks,” Proc. MobiCom ’00, pp. 255-265, Aug. 2000.

[4] G. Marias, P. Georgiadis, D. Flitzanis, and K. Mandalas, “Cooperation Enforcement Schemes for MANETs: A Survey,” Wiley’s J. Wireless Comm. and Mobile Computing, vol. 6, no. 3, pp. 319-332, 2006.

[5] Y. Zhang and Y. Fang, “A Secure Authentication and Billing Architecture for Wireless Mesh Networks,” ACM Wireless Networks, vol. 13, no. 5, pp. 663-678, Oct. 2007.

[6] Y. Zhang, W. Lou, and Y. Fang, “A Secure Incentive Protocol for Mobile Ad Hoc Networks,” ACM Wireless Networks, vol. 13, no. 5, pp. 569-582, Oct. 2007.

[7] A. Weyland, “Cooperation and Accounting in Multi-Hop Cellular Networks,” PhD thesis, Univ. of Bern, Nov. 2005.

[8] S. Zhong, J. Chen, and R. Yang, “Sprite: A Simple, Cheat-Proof, Credit Based System for Mobile Ad-Hoc Networks,” Proc. IEEE INFOCOM ’03, vol. 3, pp. 1987-1997, Mar./Apr. 2003.

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

[10] M. Mahmoud and X. Shen, “PIS: A Practical Incentive System for Multi-Hop Wireless Networks,” IEEE Trans. Vehicular Technology, vol. 59, no. 8, pp. 4012-4025, Oct. 2010.

[11] M. Mahmoud and X. Shen, “ESIP: Secure Incentive Protocol with Limited Use of Public-Key Cryptography for Multi-Hop Wireless Networks,” IEEE Trans. Mobile Computing, vol. 10, no. 7, pp. 997- 1010, July 2011.

[12] D. Johnson and D. Maltz, “Dynamic source routing in ad hoc wireless networks,” in *Mobile Computing*. Norwell, MA: Kluwer, 1996, ch. 5, pp. 153–181.

[13] C. Perkins and E. Royer, “Ad-hoc on-demand distance vector routing,” in *Proc. IEEE Workshop Mobile Comput. Syst. Appl.*, New Orleans, LA, Feb. 1999, pp. 90–100.

[14] B. Wehbi, A. Laouiti, and A. Cavalli, “Efficient Time Synchronization Mechanism for Wireless Multi Hop Networks,” Proc. IEEE Personal, Indoor and Mobile Radio Comm. (PIMRC), 2008.

[15] D. Johnson and D. Maltz, “Dynamic Source Routing in Ad Hoc Wireless Networks,” Mobile Computing, Chapter 5, pp. 153-181, Kluwer Academic Publishers, 1996.

[16] M. Mahmoud and X. Shen, “ESIP: Secure Incentive Protocol with Limited Use of Public-Key Cryptography for Multi-Hop Wireless Networks,” IEEE Trans. Mobile Computing, vol. 10, no. 7, pp. 997- 1010, July 2011.

[17] C. Perkins and E. Royer, “Ad-hoc on-demand distance vector routing,” in *Proc. IEEE Workshop Mobile Comput. Syst. Appl.*, New Orleans, LA, Feb. 1999, pp. 90–100.

[18] M. Mahmoud and X. Shen, “DSC: Cooperation incentive mechanism for multi-hop cellular networks,” in *Proc. IEEE ICC*, Dresden, Germany, Jun. 14–18, 2009, pp. 569–574.

[19] L. Buttyan and J. Hubaux, “Stimulating cooperation in self-organizing mobile ad hoc networks,” *Mobile Netw. Appl.*, vol. 8, no. 5, pp. 579–592, Oct. 2004.

[20] Y. Zhang, W. Lou, and Y. Fang, “A secure incentive protocol for mobile ad hoc networks,” *ACM Wireless Netw.*, vol. 13, no. 5, pp. 569–582,

[21] S. Zhong, J. Chen, and R. Yang, “Sprite: A simple, cheat-proof, credit based system for mobile ad-hoc networks,” in *Proc. IEEE INFOCOM*, San Francisco, CA, Mar. 30–Apr. 3, 2003, vol. 3, pp. 1987–1997.

[22] H. Janzadeh, K. Fayazbakhsh, M. Dehghan, and M. Fallah, “A secure credit-based cooperation stimulating mechanism for MANETs using hash chains,” *Future Gener. Comput. Syst.*, vol. 25, no. 8, pp. 926–934, Sep. 2009.