ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department Of CSE, JayaShriram Group Of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

A Trust Based Payment Scheme for Multihop Wireless Networks

S.Suganya,S.Dhivya,Y.Jenifer

PG Scholar, Department of CSE , Kathir College of Engineering, Neelambur,Coimbatore, India

PG Scholar, Department of CSE , Kathir College of Engineering, Neelambur,Coimbatore, India

PG Scholar, Department of CSE , Kathir College of Engineering, Neelambur,Coimbatore, India

ABSTRACT: In a multihop wireless networks a trust based payment scheme is proposed for motivating node collaboration and for regulation of packetbroadcast. Every node submits align weight payment reports to the Accounting Center(AC) and stores an acceptable security tokens called Evidences. For every successful packet,diffusion would report a payment to the AC automatically. There by reports stability are verified to evaluate the payment,and clearsall the successful payment report without any cryptographic operations. For every cheatingreport, submitted evidence is used to identify the occurrence of cheating in the payment reports. Insteadof reporting for every node transmission to the AC, a trust based payment scheme would provide a trust value to be fixed for every node. A higher trust value routes must be chosen for performing the packet transmission. Moreover, trust aggregation technique is used to reduce the trust packing area. This trust value entails very less communication and processing overhead than the existing report-based schemes. Thus the usage of micropayment is an actual execution of a payment scheme. Moreover,for every node,trust based scheme reduces the cheating node with an identification of abrupt trust value.

I. INTRODUCTION

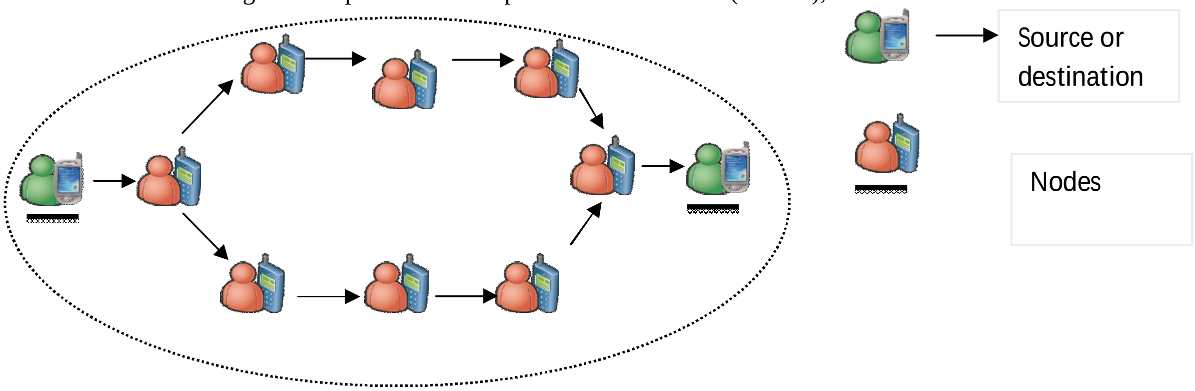
Wireless network are consistent and employed without any physical connection beyond the certain of physical network cabling. Communications are initially installed at low cost and commonlybroadcasted to many locations. Routing is the process of deciding where to send signals in a network. Multi-hop routing involves sending signals through multiple stations instead of one long way. Multi-hop indicates the several routers that were (Fig.1) crossed to reach destination. Wireless networks use two or more wireless hops to convey information fromsource to destination. In Multi-hop networks system are conventionally employed with single hops between mobile units and the base stations. As the node is evolved from one packet to another packet, throughput is a main and becoming a significant concern. Hence the usage of relay can improve the coverage and throughput. Every nodes in the network fall under the centralized Wireless Networks which are also called as last-hop networks.

Wireless nodes communicating with each other using fixed infrastructure (Base Station)here the Base station acts as an interface to the wire line networks as downlink transmission is broadcast to all nodes in the BS coverage can hear all of the transmission and uplink transmission are shared among nodes. Thereby Multihop packet relay can extend the network coverage using very limited transmitting power, improves efficiency, and enhances the throughput capacity. In multihop wireless networks (MWNs), there exit traffic for every node that are relayed through the other nodes to the destination for permitting new uses and enhances the overall network. MWNs can be deployed at

very low cost over developing areas and rural areas. MWNs can also implement many useful applications such as data sharing and data transmission. For example, person in one area (residential neighborhood, university campus, etc.)Have different wireless-enabled devices such as PDAs, laptops, tablets, cell phones, etc., where it can establish effective networks to be able to communicate, distribute files, and shares information. Hence assumption are made tospendthe scarce resources,such asbattery energy, CPU cycles, with available network bandwidth, to relay other packets without any payment for civilian applications where the nodes are autonomous and aim to maximize their safety. Such assumptions is reasonable for military applications because the nodes belong to a single authority and pursue certain common goal, although the proper network operation requires the nodes to collaborate, such a collaboration consumes their valuable resource which would stimulates the nodes to behave selfishly.

Therefore, in civilian applications, selfish nodes are not willingly interested in cooperation without sufficient incentive and make use of the cooperative nodes to relay their packets, which has negative effect on the network fairness, performance, and security. Fairness issue arises when selfish nodes take advantage from the cooperative nodes without any contribution to the network and the cooperative nodes are unequally overloaded because the traffic is focused over them. Hence, the selfish behavior degrades the network performance significantly, which may result in failure of the multi-hop communication [1, 2]

Fig. 1 Example of a multihop wireless networks (MWNs),



II. RELATED WORKS

In multi-hop wireless networks, packet loss will be occurred due to node mobility, packet collision, channel impairment,etc. mostly whenever a packet is about to transfer the node will receive a unique reward which eventually allows the packet to reach its destination. However, it's difficultto correlate an intermediate node while forwarding particular action in a trustable and distributed manner without involving a complex design. The existing payment schemescanbeclassified into tamper-proof-device(TPD)-based and receipt-based schemes.InTPD-basedpaymentschemes[1],[2],[3],[4], foreach nodea scheme with tamper proof device is been made available to stock and achieve its trust account and safe those operation. For receipt-based payment schemes [5],[6],[7],[8],[9],[10],[11],[12], [13],[14],an offline vital repository called the accounting center stores and manages the nodes credit account. The node would always submit an acceptable proof for communicating other packets, called receipts, to the AC to update their credit accounts.

InSprite [5],contains an active research area for several years. It's a simple, cheat-proof, credit based system for motivatingnode collaboration among selfish nodes in mobile ad hoc networks. Here the system provides an incentive for mobile nodes to cooperate and report the actions reliably. And there also it spontaneously generates the sign to be attached as a proof, IN intermediate node checks for accessibility and convey to the accounting center with the corresponding receipt for demanding a payment report. To solve certain issues like before receiving,it just report that they have receivedand never ever forward the received reports.

Furthermore, a reward is given to the entire (IN) intermediate node for performing their works by transmission of received packets. Hence the reports that are received to CCS Credit Clearance Service determine a lack of reliability. Here, mobile nodes can cooperate and forward each other's messages, unless the resource of each node was enormouslylow. In this paper foreachmessage,thesource node signs the identitiesofthe nodes inthe route and certain related message, and sends the norm signature as a proof for sending message. The intermediate nodes verify the signature, comprise receipts containing the identities of the nodes in the route and the source node's signature, and submit the receipts to the AC to claim the payment. The AC verifies the source node signature to make the payment is correct. However,thereceipts overcomethenetwork because thescheme producesareceipt permessage.

Unlike Sprite that charges only the source node, FESCIM [6] adopts fair charging policy by charging both the source and destination nodes and distinguishing the features does not want tamper-proof hardware at any node when both of them are interested in the communication. In PIS [7], In multi-hop wireless networks, the mobile nodes usually act as routers to transmit other nodes packets for enabling new applications and enhancing the network performance and deployment. However, selfish nodes may not cooperate to transmit the packet, which has adverse effect on the network fairness, safety. However, micropayment schemes have been originally planned for web-based applications, so everyday incentive system should reflect the differences between web-based and collaborationand motivation applications. In this paper, the differences are examined and payment model is established for well-organized implementation of micropayment in multi-hop wireless networks,based on the developed payment model, an incentive system is proposed to stimulate the nodescollaborationin multi-hop wireless networks and here reactive receipt submission mechanism is proposed to reduce the number of submitted receipts (or payment data), and protect against conspiracy attacks.

In order to resolve this by reducing the receipt number, fixed size receipts are provided for every session to safe the payment, and reduce the overhead of storing, submitting, and processing the payment data considerably, which can improve the system's practicality due to the high frequency of low-value payment transactions. Herethesourcenode attaches a signature to each message and the destination node replies with a signedACKpacket.PIS can reduce the receipts number by producing a fixed-size receipt per session regardless of the number of messages instead of generating a receipt per message in Sprite In order to reduce the communication and processing overhead, CDS [8] uses statistical methods to identify the cheating node that submit incorrect payment. However, the nature of the numerical methods, the planning nodes may manage to steal credits, and some honest nodes may be incorrectly faulted because cheating which is called false accusations. Moreover, some cheating nodes may not be identified which is called missed recognitions, and it may take long time to identify the cheating nodes.

In[9],a hybrid ad hoc network is a structure-based network that is extended using multi-hop communications. Indeed, the presence of a communication link between the mobile station and the base station is not required; a mobile station that has no direct connection with a base station can use other mobile stations as transmits. Compared with conventional (single-hop) structure-based networks, this new generation can lead abetter use of the vacantband and to a reduction of an arrangement costs. However, these benefits would disappear if the mobile nodes did not properly collaborate and forwards packets for other nodes. In this paper, a charging and rewarding scheme is followed to encourage the most important operation, namely packet forwarding. Here they have used a concept named "MAC layering"for communication to reduce the space overhead in the packets and a stream cipher contains encryption mechanism to provide "implicit authentication" of the nodes. Hence malicious

attacks can be easily detected for all of the selfish nodes. Here 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, corrupted messages are relayed to the base stations before they are dropped because the intermediate nodes cannot verify the authenticity and the integrity of the messages.

In An Identity-Based Broadcast Encryption Scheme for Mobile Ad Hoc Networks [10]A Mobile Ad-hoc Network (MANET) is an autonomous collection of mobile users that link over relatively bandwidth controlled wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. The network is distributed, where all network activity includes by discovering the topology and delivers the message that is in need to be executed by them, i.e., routing functionality will be combined into mobile nodes. Such networks are more vulnerable to safety attacks than conventional wireless networks. In order to handle such a situation, a safe identity-based ad hoc protocol for mobile devices are used to construct a group key for a setup of a secure communication network in an efficient way and propose a collision-free method for computing such keys. Unlike group key management protocols, an identity-based keys that do not require certificates which simplify key management. In contrast to other interactive protocols, one broadcast is needed to setup the group key.

In ESIP [11] proposes a communication protocol that can be used for a payment scheme. ESIP transfers messages from the source to the destination nodes with limited number of public key cryptography operations by integrating public key cryptography, identity-based cryptography, and hash function. Public key cryptography and hash function are used to ensure message integrity and payment non repudiation to secure the payment. 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 computes and sends a keyed hash value for each intermediate node to verify the message integrity. Comparing to PIS, ESIP requires fewer public key cryptography operations but with larger receipts size. Unlike ESIP that aims to transfer messages efficiently from the source to the destination nodes, Trust Based Scheme aims to reduce the overhead of submitting the payment data to the AC and processing them. Although the communication protocol proposed in ESIP can also use with Trust Based Scheme,thus asimple protocol is used forspace limitationandfocuseson the influences.

Reputation-based and incentive systems [3, 4] have been proposed to enforce and motivate node collaboration, respectively. In reputation-based systems, each network node usually monitors the transmissions of its neighbors to make sure that the neighbors forward others traffic, and thus selfish nodes can be reproved. In incentive systems, forwarding other nodes packets is a service not aresponsibility, so the communicating nodes pay credits (or virtual currency) to the intermediate nodes to transmit their packets. However, reputation-based systems [5, 6] suffer from essential problems that may discourage implementing them practically. First, to monitor the transmission of its neighbors, a network node usually works in the promiscuous mode that is not efficient because the node uses the full power transmission instead of adapting the transmission power according to the distance separating the transmitter and the receiver [7]. Furthermore, the directional antennas [8, 9] that can improve the network capacity due to reducing the interference area make monitoring difficult. Second, reputation-based systems achieve non-fairness because the high-contribution nodes are not rewarded, and the nodes are punished when they do not cooperate no matter how they have previously contributed to the network. For example, although the nodes situated in the network center transmit more packets than the packets are transmitting in the edge, they are not compensated. Incentive systems are more appropriate for multi-hop wireless networks because in addition to cooperation stimulation, the systems can achieve fairness by charging or rewarding credits to balance between a node' s contributions and benefits. A node thusinfluence can be relayed over other node packets or paying credits, whereas a nodecan benefit itstransmission powerfor the packets or earns credit value. Moreover, since the network nodes pay for transmitting their packets, incentive systems can discourage resource exhaustion attack where malicious nodes exchange false packets to use the intermediate nodes resources. Incentive systems can also be used for charging future services of mobile networks [11, 12] because communication sessions may occur without involving an infrastructure and mobile nodes may roam among different foreign networks. In other words, by using incentive system, the network nodes can pay all parties involved in its communication without contacting distant home location registers. However, the practicality of the existing incentive systems is questionable because they impose significant overhead cost. Micropayment schemes [13, 14] are electronic payment schemes for frequent and low-value payments. The schemes were originally designed for the Internet electronic commerce applications to take advantage of the high volume of viewers by offering content for low price. Examples of the applications include buying data or news, listening to a song, playing an online game, and reading an article in a journal [14]. In order to implement such scheme in multi-hop wireless networks efficiently, the differences between web-based and cooperation stimulation applications should be taken into account.

Symbol	Description
,	Concatenation.
SR(C)	A session receipt for C packets.
H^x	The hash value resulted from hash X
$h^{(0)}$	The hash value resulted from hash 0
IDS and IDD	The identities of the source and the destination nodes, respectively.
ID_i	The identity of intermediate node i, or node with identity IDi.
n	The number of intermediate nodes.
M_x	The message sent in the ith data packet in a session.
P_x	The probability of submitting a receipt.
R	The concatenation of identities of session nodes.
SigS(X) and SigD(X)	The signatures of the source and the destination nodes for X, respectively.
T_s	A session's establishment time stamp.

In [14]Pi: A Practical Incentive Protocol for Delay Tolerant Networks Delay Tolerant Networks (DTNs) are a class of networks categorized by lack of definite connectivity, with low frequency of meets between DTN nodes and long propagation delays within the network. As a result, the message propagation process in DTNs follows a store carry and forward manner, and the in-transit bundle messages can be opportunistically routed towards the destinations through intermittent connections under the hypothesis that each individual DTN node is willing to help with forwarding. Unfortunately, there mightensure some selfish nodes, especially in a supportive network like DTN, and the presence of selfish DTN nodes could cause terrible damage to any well designed flexible routing scheme and compromise the whole network.In DTNs delays would addresses the selfishproblem, hence theinfluences of Pi's are performed when a source node sends a bundle message; it attaches incentive on the bundle, which is not only striking but also fair to all sharing DTN nodes. With the reasonableincentive, then the selfish DTN nodes could be stimulated to help with forwarding bundles to achieve better packet delivery performance. In addition when compared to Pi protocol trust based scheme gains certain trust value to each node while they have received the intended packets else reputations would be gained. Hence the value of the Pi protocol determines less delivery ratio and lower average delay when compared to trust based scheme.

In [15]RACE, in the case of cheating evidences are submitted and the AC applies cryptographic operations to verify them, but the nodes always submit safety tokens, e.g., names, and the AC always apply some of the cryptographic operations to verify the payment when compared to the existing receipt based schemes. RACE would clear all the payment with almost no cryptographic operations andwhen evidences are infrequently requested, lightweight reports are generated. Extensive cheating actions are not estimated inCivilian applications because the common users do not have the technical knowledge to tamper with their devices. Moreover, cheating nodes are evicted once they commit one cheating action and it is neither easy nor cheap to change identities. RACE is the first payment scheme that can verify the payment by investigating the consistency of the nodes reports without systematically submitting and processing security tokens and without false accusations. RACE is the first

scheme that uses the concept of Evidence to secure the payment and requires cryptographic operations in clearing the payment. Here (Fig. 2) in Trust based -Payment Scheme each time the node need to determine the consistency of a node handler, here in the proposed trust based payment scheme such an overlay is been prevented by the allocation of trust values for every successful node transmission. Hence the cheaters may not widely attack any packets.

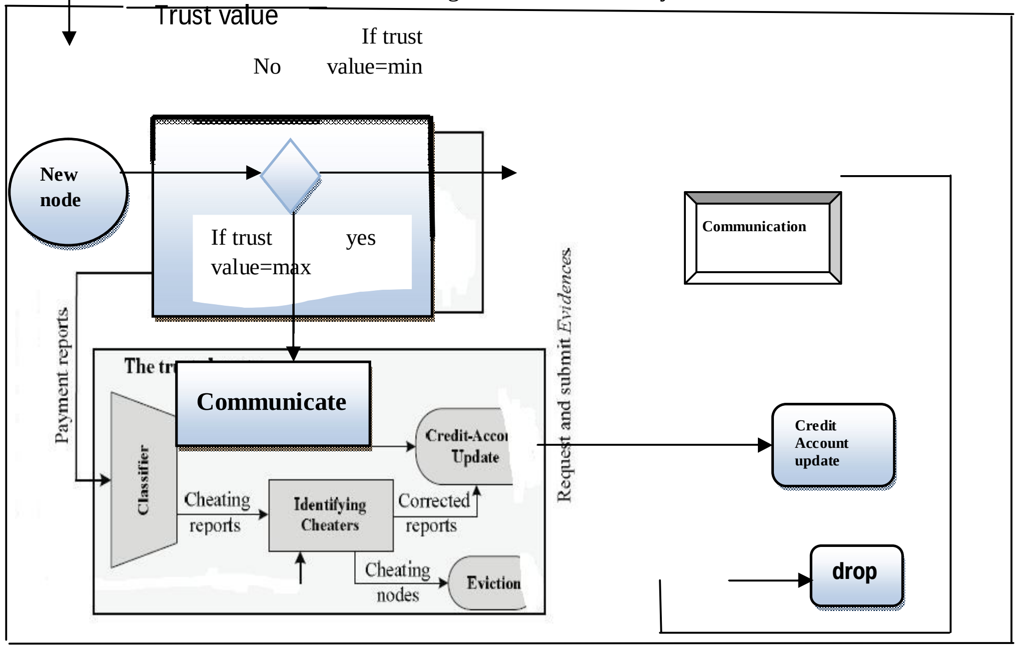
```
 //$n_i$ is the source, intermediate or destination node
    that is running the algorithm
    Step 1: if(c==max)     //c credit
    Step 2: if$n_i$ is the source node then
                $P_x \leftarrow$ [R,X,$T_s$,$M_X$,signs( R,X,$T_s$,H( $M_X$));
                 Send ($P_x$);
    else

    Step 3: if (( R,X,$T_s$are correct) and verify (signs (R,X,$T_s$
    H( $M_X$)));===true) then
    if ( $n_i$  is an intermediate node) then
    relay the packet;
    store signs (R,X,$T_s$ H ($M_X$));
    end if
    if($n_i$  is an destination node) then
                  send ($h^x$);
    end if
    else
    drop the packet
    send error packet to the source node;
    end if
    end if
    Step 4: if ($P_x$ is last packet) then Evidence= {R,X,$T_s$H ($M_X$),
             $h^{(o)}$,$h^{(X)}$,h((R,X,$T_s$ H( $M_X$) $signs_D$(R,$T_s$ $h^{(0)}$));
       report= {R;,$T_s$ ,F,X}
    store report and evidence;
    end if
    Step 5: if sent correctly
c ++ ;
    else repeat step 2 to 5;
    end if;
```

III. THE PROPOSED TRUST BASED SCHEME

Trust based scheme contains routeextraction, data transmission and Evidencecomposition, report submission and trust value updating

Fig. 2 Trust based -Payment Scheme



.ROUTEEXTRACTION

Routes would establish an node-to-node packets, the source node sends the request packet to each of the routes that are established and also they contain certain identification of the source and the destination nodes, time stamp(Ts),and Time-To-Live (TTL),time to exit etc.TTListherepresentation that is used to depict the total number of intermediate nodes. When a node receives the route request packet, it appends the identity and transmits the packet if the number of intermediate nodes is less when compared with the TTL. The destination node comprises the Route Reply packet for the node it transmits the first received request packet, and sends the packet back to the source node. The destination node createsa hash cable for every packet transmissionin an iterative manner over a randomvalue

TRANSMISSION AND EVIDENCECOMPOSITION

Thesource node sends data packets tothe destinationnode throughthe establishedroute and thedestination node replies with ACKpackets. For the Xth data packet, the source node appends the message MX and its signature to R,X,Ts, and the hash value of the message and sends the packet to the first node in the route. Before relaying the packet, each intermediate node verifies the signature to ensure the message's authenticity and integrity, and verifies R and X to secure the payment. Each node stores only the last signature for composing the Evidence, which is enough to prove transmitting X messages, Evidence is defined as information that is used to establish proof about the occurrence of an event, 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. Reducing the storage area of the Evidences is important because they stores until the AC clears the 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. Whenever a packet is been transferred from one end to another respective report is in need to be transposed to the accounting center which is an offline bank.

TRUST VALUE UPDATING

A trust value indicates the successful transformations of packets from source todestination node. Such a trust value would be updated for every transformation of packets which would precisely determine the routes are not accompanied by any cheateres.so that an effective transformation can be manually performed with less time.Whenever node has transferred the packets trust value would be made available and sets the trust value for each of the nodes.

IV . CONCLUSIONS

Thus in the multihop wireless networks atrust based payment scheme is been proposed for motivatingnodecollaboration and for instruction of packetbroadcast. Every node submits align weight payment reports to the Accounting Center(AC)and stores an acceptable security tokens called evidences. For every successful packet transmission node would reports a payment to the AC accordingly. There by report consistency is also verified to evaluate the payment,and clearsall the successful payment report without any cryptographic operations. For everycheatingreport,the evidencesare submitted to identify the occurrence of cheating in the payment reports. Insteadof reporting for every node transmission to the AC, a trust based payment scheme would provide a trust value to be fixed for every node. A higher trust value routes must be chosen for performing the packet transmission. Moreover, trust aggregation technique is used to reduce the trust storage area. This trust value entails an overall communication and processing overhead.

REFERENCES

[1] L. Buttyan and J. Hubaux, "Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks," Mobile Networks and Applications, vol. 8, no. 5, pp. 579-592, Oct. 2004.

[2] 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.

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

[4] A. Weyland, T. Staub, and T. Braun, "Comparison of Motivation Based Cooperation Mechanisms for Hybrid Wireless Networks,"J. Computer Comm., vol. 29, pp. 2661-2670, 2006.

[5] S. Zhong, J. Chen, and R. Yang, "Sprite: A Simple, Cheat-Proof, Credit Based System for Mobile Ad-Hoc Networks," Proc. IEEEINFOCOM '03, vol. 3, pp. 1987-1997, Mar. Apr. 2003

[6] 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.

[7] 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.

[8] M. Mahmoud and X. Shen, `"Stimulating Cooperation in Multihop Wireless Networks Using Cheating Detection System," Proc.IEEE INFOCOM '10, 2010.

[9] N. Salem, L. Buttyan, J. Hubaux, and M. Jakobsson, "Node Cooperation in Hybrid Ad Hoc Networks," IEEE Trans. MobileComputing, vol. 5, no. 4, pp. 365-376, Apr. 2006.

[10] J. Pan, L. CAI, X. Shen, and J. Mark, "Identity-Based Secure Collaboration in Wireless Ad Hoc Networks," Computer Networks,vol. 51, no. 3, pp., 2007.

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

[12] M. Mahmoud and X. Shen, "An Integrated Stimulation and Punishment Mechanism for Thwarting Packet Drop in MultihopWireless Networks," IEEE Trans. Vehicular Technology, vol. 60, no. 8, pp. 3947-3962, Oct. 2011.

[13] H. Zhu, X. Lin, R. Lu, Y. Fan, and X. Shen, "SMART: A Secure Multilayer Credit Based Incentive Scheme for Delay-TolerantNetworks," IEEE Trans. Vehicular Technology, vol. 58, no. 8, pp. 4628-4639, Oct. 2009.

[14] R. Lu, X. Lin, H. Zhu, X. Shen, and B.R. Preiss, "Pi: A Practical Incentive Protocol for Delay Tolerant Networks," IEEE Trans. Wireless Comm., vol. 9, no. 4, pp. 1483-1493, Apr. 2010.

[15 Mohamed M.E.A. Mahmoud and Xuemin (Sherman) Shen" A Secure Payment Scheme with LowCommunication and Processing Overheadfor Multihop Wireless Networks"published in , IEEE Transactions on Parallel and Distributed Systems, VOL. 24, NO. 2, FEBRUARY 2013