International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 2, February - 2014

A Light Weight Payment Report Scheme for Multihop Wireless Networks

S. Suganya,
Department of CSE(PG Scholar),
Kathir College of Engineering,
Neelambur,Coimbatore.

Dr. M. Sadish Sendil,
Head of the Department (CSE),
Kathir College of Engineering,
Neelambur,Coimbatore.

***Abstract*--Most of the wireless networks are applicable for either a single hop or multihop but not both. There exists an awkward gap between the similarity metrics for multihop network. In a multihop wireless networks a trust based payment scheme is proposed for motivating node collaboration and for regulation of packet broadcast. Every node submits a lightweight 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 stable reports are verified to evaluate the payment, and clears all the successful payment report without any cryptographic operations. For every cheating report, submitted evidence is used to identify the occurrence of cheating in the payment reports. Instead of reporting for every node transmission to the AC, a trust based payment scheme would make an alternative path for moving the packets to the respective node and also it provide a trust value to be fixed for every node. A node containing a better route path is chosen for performing an effective packet transmission. Moreover, a trust aggregation technique is used to reduce the overall trust packaging area. This trust value entails very less communication and processing overhead than the existing report-based schemes over multihop wireless network. Thus the usage of micropayment is an actual execution of a payment scheme. Moreover, trust value can secure the payment and precisely identify the cheating nodes without any false accusations.**

Keywords—tokens; reports; forwarding node; selfish node

I. INTRODUCTION

Wireless network are consistent and employed without any physical connection beyond the physical network. Communications are initially installed at low cost and commonly broadcasted to many locations. Routing is the process of deciding where to send signals in a network Wireless networks use two or more wireless hops to convey information from source to destination. Here the end points are fixed in a hierarchical architecture.

Wireless communications have become very pervasive. The number of mobile phones and wireless Internet users has increased significantly in recent years. Wireless networks come in many forms, cover various distances, and provide a range of low to high bandwidth depending on the type installed. In high end connectivity, nodes send a packet to neighboring nodes until it reach at destination. In city area, end connectivity graph can increase delay due to the large number of nodes. Multi-hop wireless network access the network that leverage the overall economies-of-scale that have driven the costs point that is feasible for low-income communities. Multihop is separated by the routers and contains multiple intermediate nodes.

Multihop wireless networks are collection of nodes connected together over a wireless medium. In multihop wireless networks there are one or more intermediate nodes along the path that receive and forward packets via wireless links. Multihop wireless networks (MWNs) composed of two end nodes is carried out through a number of intermediate nodes whose function is to relay information from one point to another, without using any kind of fixed wired infrastructure. Multihop wireless networks utilize multiple wireless nodes to provide coverage to a large area by forwarding and receiving data wirelessly between the nodes. Multihop wireless networks have several benefits that are mostly depends on the comparative networks with single wireless links, multihop wireless networks can extend the coverage of a network and improve connectivity. In multi-hop wireless networks, keeping track of node is a crucial function, such a tracking function can be used for the detection of certain attacks, to secure routing protocols based on the history of encounters, and for the detection of cheating attempts (e.g., in charging mechanisms).

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 area and rural area. 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 an effective network to be able to communicate, distribute files, and shares information. Hence assumption are made to spend the scarce resources, such as battery 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.

II. RELATED WORKS

The existing payment schemes can be classified into Tamper-proof-device (TPD)-based, Receipt-based schemes. In TPD-based payment schemes a TPD is installed in each node to store and manage its credit account and secure its operation. For receipt-based payment schemes an offline central unit called the accounting center (AC) stores and manages the nodes‟ credit accounts. The nodes usually submit undeniable proofs for relaying packets, called receipts, to the AC to update their credit accounts. The nodes at the end are seems to be useless since they can't have the reputed credit values to be maintained. Here the multihop facility may also be not applicable since there is certain violation towards the communication scheme that is maintained for all of the nodes.

Naik.K, [1], here a multiple anonymous path is established between communication peers. Main drawback is that anonymous protocol can't identify cheater node. So there occur high performance delays.

In An Identity-Based Broadcast Encryption Scheme for Mobile Ad Hoc Networks (MANET), is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile node, the network topology may change rapidly and unpredictably over time. In order to handle vulnerability, a secure Identity-based Ad hoc protocol for mobile devices is used to construct a group key for setting up a secure communication network in an efficient way and proposes a collision-free method for computation is the main advantage.

Weyland.A [10], the source node is charged with a certain credit and a signature is attached to each data packet. Upon receiving the packet, the credit account of the destination node is also charged, and a signed acknowledgement (ACK) packet is sent back to the source node to increase the credit accounts of all the intermediate nodes that are placed from the source to the destination node. Security mechanisms are based on public-key cryptography where nodes authenticate themselves using certificates with short lifetime and the transmitted messages are digitally signed ensuring non repudiation (data integrity and data origin authentication).

Mahmoud.M and Shen.X,'FESCIM: Fair, Efficient, and Secure Cooperation Incentive Mechanism for Hybrid Ad Hoc Networks [3]', are interested in communication meanwhile in case of "Mitigation Routing Misbehavior in mobile adhoc network" charges only the source node, but in the FESCIM it charges the source and destination node. In order to securely charge the nodes, a light weight hashing operation is used in the ACK. The advantage is that one small size check would be generated per session. It reduces the public key cryptographic operation. The payments lead a non-repudiation to be achieved using a hash chain at the source node side. Hence FESCIM is a Fair, Efficient, and Secure Cooperation Incentive Mechanism, to stimulate the node cooperation in MWN. In order to efficiently and securely charge the source and destination nodes, the lightweight hashing operations are used

Shen.M has introduced a 'SMART: A Secure Multilayer Credit Based Incentive Scheme for Delay-Tolerant Networks [11]', Here for improving the overall efficiency a unique characteristics of delay tolerant networks is been exploited. Then the selfish or malicious nodes can easily violate the process. Main issue seen in the SMART is that the end to end connectivity is not available.

Marias.G, 'Cooperation Enforcement Schemes for MANETs: A Survey[4]', implemented an employment of adequate trust methods in mobile ad hoc networks (MANET) have increased the attention during the last few years, and several trust and security establishment solutions that rely on cryptographic and hashing schemes have been proposed. These schemes, classified as reputation-based and credit-based, are considered suitable for ad hoc networks, where key or certificate distribution centers are absent or ephemerally present, and for networks that consist of devices with limited processing, battery, and memory resources. Cooperation enforcement methods do not provide strong authentication of entities. Instead, they contribute to the identification of the trustworthiness of peers and to the enforcement cooperation using mutual incentives.

An important issue for the cooperation enforcement models is that the control packets will be always available in the routing protocol; hence the identity of a node should be unique and remain permanent. Another main issue depends on the fairness (e.g., handling the reputation of nodes that are in the edge of the MANET) and the time that the schemes require to converge for a selfish node.

Yanghas.R presented a 'Sprite: A Simple, Cheat-Proof, and Credit Based System for Mobile Ad-Hoc Networks [12] ', Mobile ad hoc networking has been an active research area for several years. In this paper Sprite, a simple, cheat-proof, credit based system for stimulating cooperation among selfish nodes in mobile ad hoc networks. Here the system provides incentive for mobile nodes to cooperate and report the actions honestly thereby AC verifies the signature and guarantees that the payment is correct. It does not require any tamper proof hardware, mainly focuses on node selfishness. When a node receives a message it keeps a receipt for those messages.

Credit Based System automatically generates the sign to be attached as a proof, intermediate node checks for availability and convey to accounting center with the corresponding receipt for claiming a payment report. The design of the system addresses two main issues. First, there is no need of a tamper-proof hardware and the credits are based on the reports of selfish nodes. As an example, a selfish node may withhold its receipt, or collude with other nodes to forge receipts, if such actions can maximize its welfare. This is the security perspective of the system. Second, a node should receive enough credit for forwarding a message for another node, so that it can send its own messages with the received credit,

A main reward is given to the entire intermediate node for performing the works by transmission of received packets. Sprite contains the signature to be signed for the information they are successfully transforming. Such messages make the transaction to be highly reliable. Sprite,

is mainly focused on the credit based system for stimulating cooperation among selfish nodes in mobile ad hoc networks .Certain evaluations of a prototype implementation are proved to show that the overhead of our system is small. Hence the mobile nodes can cooperate and forward each other's message, unless the resource of each node is extremely low.

Some of the difficulties of Sprite are that the received reports to CCS Credit Clearance Service determine the lack in integrity. Mobile nodes can cooperate and forward the messages; unless the resource of each node is extremely low. so there occurs a problem for each of the participatory nodes. Meanwhile certain issues would also be occurred, before receiving the packet they approximately convey that they have received, there occurs a loss in integrity since the node fails to forward the received reports or reports in advance to the CCS.

Shen.X, 'PIS: A Practical Incentive System for Multi-Hop Wireless Networks [5]', here in the multi-hop wireless networks, the mobile nodes usually act as routers to relay other nodes packets for enabling new applications and enhancing the network performance and deployment.PIS can reduce the receipts number by generating a fixed-size receipt per session regardless of the number of messages instead of generating a receipt per message in Sprite. However, micropayment schemes have been originally proposed for web-based applications, so a practical incentive system should consider the differences between web-based and cooperation stimulation applications.

Receipt aggregation technique is used for providing the hash value to be attached instead of signature there occur a lot of communication overhead.

Jakobsson, 'Node Cooperation in Hybrid Ad Hoc Networks [9]', here hoc network is a structure-based network that is extended using multi-hop communications. Indeed, the existence 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 relays. Compared with conventional (single-hop) structure-based networks, this new generation can lead to a better use of the available spectrum and to a reduction of infrastructure costs. However, these benefits would vanish if the mobile nodes did not properly cooperate and forward packets for other nodes.

'MAC layering' is secondhand to reduce the space overhead in the packets and a stream cipher encryption mechanism is enabled to provide 'implicit authentication' of the nodes. Node cooperation would sufficiently encourage the several fundamental operation, namely packet forwarding. Whenever a node are transforming the packets it need to report a particular node ,such a role may lead to any suboptimal routes and makes the base station to be involved in all of the communication session. There occur certain deviations at the calibration of the relevant parameters, and the study of the network to sophisticated attacks. While communicating to the intended node there occur certain violation towards the intermediate nodes, so there occur a lack in integrity and authenticity.

Mahmoud.M and Shen.X,[6]here a selfish nodes do not relay other nodes' packets and make use of the cooperative nodes to relay their packets, which has negative impact on the network fairness and performance. Incentive protocols use credits to stimulate the selfish node cooperation, but the existing protocols usually rely on the heavy-weight public-key operations to secure the payment. SIP transfers messages from the source to the destination nodes with limited number of public key cryptography operations. In this ESIP, a secure cooperation incentive protocol that uses the public-key operations only for the first packet in a series and uses the light-weight hashing .So that the operations in the next packets, would cause certain overhead over the packet and hence it converges with the hashing operations. Hash chains and keyed hash values are used to achieve payment non-repudiation and thwart free riding attacks.

Main issue is that it lack in space and there occur a degradation of network performance by involving themselves in communication sessions and in dropping the packets intentionally. In ESIP, since the receipt format reveals the node at which the route was broken, there occurs a lack in the irrational packet droppers is a major drawback. The AC cannot inspect the submitted receipts to build a reputation system to identify the irrational packet droppers. Lead the attackers to identify in short span of time to reduce their harm, and to avoid falsely identifying honest nodes as irrational packet droppers.

Preiss[2],a class of networks characterized by lack of guaranteed connectivity, typically low frequency of encounters between DTN nodes and long propagation delays within the network.

Mahmoud.M and Shen.X [7] presented an incentive mechanism to stimulate cooperation in multi-hop wireless networks. And also mobile nodes usually act as routers to relay packets generated from other nodes. However, selfish nodes do not cooperate but make use of the honest ones to relay their packet, which has negative effect on fairness, security and performance of the network. Instead of generating a receipt per packet (or few packets), one activity report is generated containing a payment for the particular transmission. The basic idea is that, the network nodes independently and periodically submit their activity reports containing the financial data. Here, the network nodes independently and periodically submit their activity reports containing the financial data resulted from sessions they participated in.

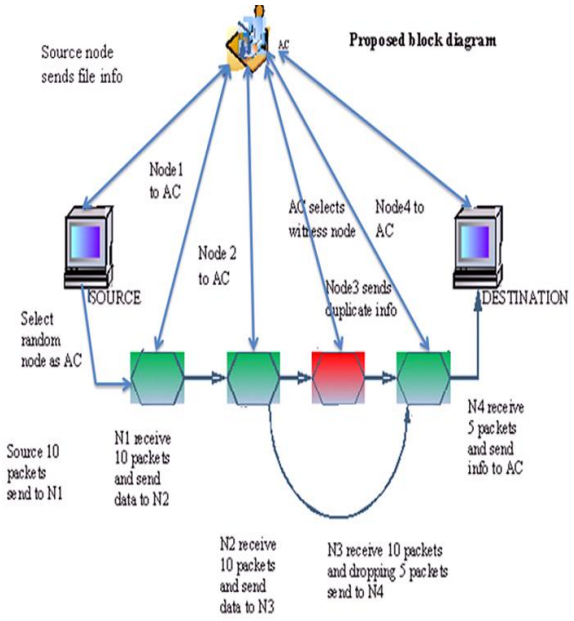
Better fairness is achieved for stimulating the node cooperation in multi-hops wireless networks by a usage of novel incentive mechanism. In the cooperative nodes several statistical methods is used to secure the payment by using credits to reward. Overhead is reduced by using the cheating detection system and also have a great extent towards the fairness by the usage of credit values, security and performance. In order to reduce the communication and processing overhead, CDS uses statistical methods to identify the cheating nodes that submit incorrect payment. However, due to the nature of the statistical methods, the colluding nodes may manage to steal credits, and some honest nodes may be falsely accused of cheating which is called false accusations. Moreover, some cheating nodes

may not be identified which is called missed detections, and it may take long time to identify the cheating nodes

Mark.J[8] offered a session to be generated where every node has to contact the AC in each communication session for the favor of coins to buy the packets from the previous node in the route. Here the packet buyers contact the AC to get deposit their coins and the packets sellers submit the coins to the AC to claim their payment.

III. PROPOSED SYSTEM

In the proposed system, the nodes submit a lightweight to the AC to for making an alternative route to be chosen and also it update their credit accounts, and temporarily stores the undeniable security tokens called Evidences, where the network contains an assumed charges of different sessions without any security proofs like



Multi-hop network establishment in this first module, we have to establish the multi-hop wireless network. These nodes are used to communicate with each other directly or through the neighbor nodes. If one node send the message "Hello" means, first of this entire message is received by the neighboring node. Thereafter it will check whether the destination is neighbor or not. If destination is found the message is send or else it is forwarded to the next intermediate node. Accounting center is the second module that finds the path that is created has to be registered with a Trusted Party in order to communicate effectively and for every valid Evidence if the computed PROOF is similar to the Evidence's PROOF. Forwarding node phase receives a fair and corrected payment reports to update the nodes credit accounts and also it forwards the received packets. In the existing RACE paper here a cheating action will be only tracked rather in the proposed it switches the cheating to reach the destination trust based scheme makes an alternative route to be chosen for the successful transactions of packets towards the destination. The payment reports are cleared using the charging and rewarding policy and get the signatures, etc. The AC verifies the payment by exploring the reliability of the reports, and clears the payment with almost no cryptographic operations or computational overhead. For cheating reports, the Evidences are requested to identify and evict the cheating nodes that submit incorrect reports, e.g., to steal credits or pay less.

To detect such variation, a small part of each contact record is dispersed to some selected nodes which can collect appropriate contact records and detect the misbehaving nodes with certain probability. The Evidences are used to resolve disputes when the nodes disagree about the payment. With submitting and processing few Evidences. RACE can clear the payment nearly without applying cryptographic operations and with submitting lightweight reports when Evidences are not frequently requested.

payment correctly. Upon registration the trusted party will give a public and 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.

//n_i is the source, intermediate or destination nodethat 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

$H(M_X)))$;===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 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;

Some of the parts of the proposed system are data center, accounting center, Forwarding Node, Packet Dropping and Deducting, Evidence Node and Credit Allocation

Data Center

This module is mainly designed to data transfer between the server and the receiver. The Message transfer to the destination or intermediate nodes. This module is the initiate module for the data transfer between the nodes in network communication. Whenever the packets are transferring absolute intimation is registered in the data center.

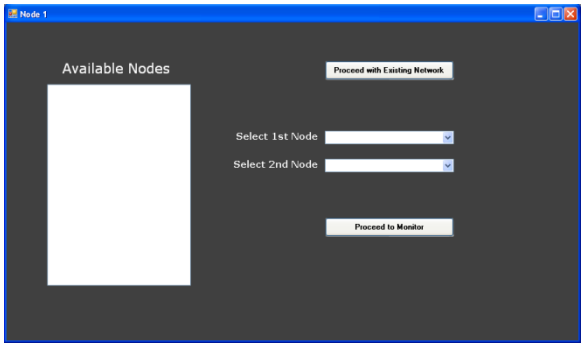
Accounting Center

In this module, a node is required to keep a few signed contact records of its previous contacts, based on which the next contacted node can detect if the node has dropped any packet. The AC has to apply a large number of cryptographic operations to verify the receipts, which may require impractical computational power and make the practical implementation of these schemes complex or inefficient. Moreover, since a transaction (relaying packets) value may be very low, the scheme uses micropayment, and thus a transaction's overhead in terms of submitting and clearing the receipts should be much less than its value.

Therefore, reducing the communication and the payment processing overhead is essential for the effective implementation of the payment scheme and to avoid creating a bottleneck at the AC and exhausting the nodes' resources. In this module receive the payment reports and AC can verify the payment by investigating the consistency of the reports.

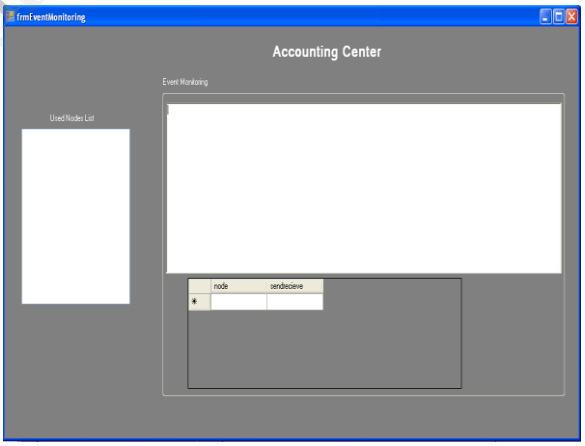
Forwarding Node

In the forwarding modules, the data is transmitted between the server and the receiver. Before the data forwarding the routing is constructed to perform the forwarding mechanism. Once the data is forward then the acknowledgement will be sent to the accounting center about the successful data transmission information.



Packet Dropping and Deducting

To address the problem, a new concept is proposed in a distributed scheme to detect packet dropping in distributed networks where it determines, how to detect packet dropping and how to limit the traffic flowing to the misbehaving nodes. For that a new scheme is proposed detect the packet dropping in a distributed manner. In this scheme, a node is required to keep previous signed contact records such as the buffered packets and the packets sent or received, and report them to the next contact node which can detect if the node has dropped packets based on the reported records.



Evidence Node

Evidences are requested to identify and evict the cheating nodes that submit incorrect reports. Instead of requesting the Evidences from all the nodes participating in the cheating reports, to detect misreporting, the contacted node also randomly selects a certain number of evidence nodes for the reported records and sends a summary of each reported record to them when it contacts them. The evidence node that collects two inconsistent contact records can detect the misreporting node To detect misreporting, for each contact record that a normal node generates with (or receives from) other nodes, the normal node selects evidence nodes and transmits the record summary to them. The summary only includes a part of the record necessary for detecting the inconsistency caused by misreporting

Credit Allocation

Payment schemes use credits to motivate the nodes to cooperate in relaying others' packets by making cooperation more beneficial than selfishness. The nodes earn credits for relaying others' packets and spend these credits to get their packets relayed by others. These schemes can enforce fairness, discourage Message-Flooding attacks, regulate packet transmission, and efficiently charge for the network services. Here credit points will be allocated to the every node after every transaction. Based on the node transmission and evidence of transaction the credit point will be updated. Hence the time and cost can be efficiently managed.

IV. CONCLUSION AND FUTURE ENHANCEMENT

A general wireless network are based on the hop by transmission, through a multihop has been proposed. In order to fairly charge the source and destination nodes, the multihop wireless network chose an effective route for the successful transmission. As a trust based payment scheme is taken for motivating node collaboration and for regulation of packet broadcast. Every node submits a light weight payment reports to the Accounting Center (AC) and stores an evidence report. For every successful packet transmission, when an occurrence of false action are known, an alternative path are chosen for moving the packets to the respective destination node and also provide a trust value to be fixed for every node. A node containing a better route path is chosen for performing an effective packet transmission and also consistency depends on the transmission of packets to the end nodes. As on a future work an efficient algorithm for making this payment scheme under a real time using a hash chain is need to be proposed, by the involvement of DES/AES at the source node for verifying the integrity of the intermediate nodes.

REFERENCES

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

[2] Lu.R, Lin.X, Zhu.Z, Shen.X, and Preiss.B.R (2010) 'Pi: A Practical Incentive Protocol for Delay Tolerant Networks', IEEE Transaction Wireless Communication., vol. 9, no. 4, pp. 1483-1493.

[3] Mahmoud.M and Shen.X (2012) 'FESCIM: Fair, Efficient, and Secure Cooperation Incentive Mechanism for Hybrid Ad Hoc Networks', IEEE Trans. Mobile Computing, vol. 11, 753-766.

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

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

[6] Mahmoud.M and Shen.X (2011) 'ESIP: Secure Incentive Protocol with Limited Use of Public-Key Cryptography for Multi-Hop Wireless Networks', IEEE Trans. Mobile Computing, vol. 10, 997-1010,

[7] Mahmoud.Mand Shen.X (2010) 'Stimulating Cooperation in Multihop Wireless Networks Using Cheating Detection System', Proc. IEEE INFOCOM '10.

[8] Pan.J, Cai.L, Shen.X, and Mark.J (2007) 'Identity-Based Secure Collaboration in Wireless Ad Hoc Networks', Computer Networks ,vol. 51, no. 3, pp. 853-865.

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

[10] Weyland.A (2005) 'Cooperation and Accounting in Multi-Hop Cellular Networks', PhD thesis, Univ. of Bern.

[11] Zhu.H, Lin.X, Lu.R, Fan.Y, and Shen.X (2009) 'SMART: A Secure Multilayer Credit Based Incentive Scheme for Delay Tolerant Networks', IEEE Trans. Vehicular Technology, vol. 58,4628-4639.

[12] Zhong.S, Chen.J, and Yang.R (2003) 'Sprite: A Simple, Cheat-Proof, Credit Based System for Mobile Ad-Hoc Networks', Proc. IEEE INFOCOM '03, vol. 3, pp.

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