A Payment Scheme with Security, Report Submission and Low Processing Overhead

Merlin Cyriac
PG Scholar
Department of Computer Science and Engineering
K .C.G College of Technology
Chennai, India

Merin Jose
PG Scholar
Department of Computer Science and Engineering
K .C.G College of Technology
Chennai, India

Dr. Frank Vijay .J
Professor and HoD
Department of Information Technology
K .C.G College of Technology
Chennai, India

***Abstract*— In Multihop Wireless Networks (MWNs), the traffic originated from a node is usually relayed through the other nodes to the destination for enhancing the network performance .Thus an efficient payment scheme is inevitable for node cooperation. Payment schemes use credits to motivate the nodes. Thus the nodes cooperate in relaying others' packets by making cooperation. A Report-Based Payment Scheme for multihop wireless networks is proposed for enabling node cooperation, regulating packet transmission, and enforcing fairness. Instead of Receipts the nodes submit lightweight payment reports to the Accounting Center (AC). And the AC temporarily stores security tokens called Evidences. By investigating the consistency of the reports, AC verifies the payment. Thus the cheating nodes are identified and those nodes are evicted. This Payment Scheme does not request all the nodes to submit the evidences, instead it requests only the cheating nodes to submit the evidences. Thus the entire communication and processing overhead is reduced. On detection of cheating nodes, an alternative path for data transmission is identified. Report Based Payment Scheme can also secure the payment.**

***KeyWords*— Selfish Nodes, Cooperative Nodes, Payment Scheme, Cooperation Incentive Schemes.**

1. INTRODUCTION

Multihop wireless network is a wireless network adopting multihop wireless technology without deployment of wired backhaul links. Similar to Mobile Adhoc Networks (MANET), but nodes in MWN is relative 'fixed'. MWN may introduce 'hierarchy' network architecture. Figure 1 shows an example of Multihop Wireless Networs.Multihop wireless networks can be deployed easily and readily at low cost in developing areas. Multihop packet relay can extend the network coverage using limited transmit power. Thus it enhances the network throughput and capacity. MWNs can also implement many useful applications. It includes data sharing and multimedia data transmission. For example, users in one area having different wireless-enabled devices, e.g., tablets, cell phones, PDAs, laptops, etc., can establish a network and it can be used to communicate, distribute files, and share information. The main goal of the project is to propose a Report Based Payment Scheme for Multihop Wireless Networks which have less communication and processing overhead. In Multihop Wireless Networks (MWNs), the traffic originated from a node is relayed through the other nodes to the destination for enhancing the network performance. The network includes both selfish nodes and cooperative nodes. The peculiarity of selfish nodes is that they will not relay others' packets and make use of the cooperative nodes to relay their packets. This degrades the network connectivity and fairness. The issue of fairness arises when the selfish nodes make use of the cooperative nodes to relay their packets, and thus the cooperative nodes are unfairly overloaded because the network traffic is concentrated through them. Thus the need for an efficient payment scheme with low communication and processing overhead arises. The selfish behavior also degrades the network connectivity significantly, which may cause the multi hop communication to fail .Thus the need for an efficient payment scheme arises. The incentive schemes use credits to motivate the nodes to cooperate in relaying others' packets by making cooperation.

Figure 1 Multihop Wireless Networks

A Report-Based Payment Scheme for multihop wireless networks is proposed for enabling node cooperation, regulating packet transmission, and enforcing fairness. Instead of Receipts the nodes submit lightweight payment reports to the Accounting Center (AC). And the AC temporarily stores security tokens called Evidences.The payment is verified by Accounting Center by checking the consistency of the reports. It also clears the payment of the fair reports and no cryptographic operations are involved. Thus the computational overhead is very less. The cheating reports are identified and the Evidences are requested to nodes having cheating reports. Thus the cheating nodes are identified and are evicted. That is the nodes that submit incorrect reports are requested to produce their evidences. Thus the nodes who steal credits or pay less are identified. In other words, the Evidences are used to identify the nodes who disagree about the payment. Report based payment scheme can identify the cheating nodes with submitting and processing very few Evidences. This is made possible by requesting evidences only from those nodes with cheating reports. And also to reduce the storage area of the Evidences, Evidence aggregation technique is used. In Report based Payment Scheme, Accounting Center applies cryptographic operations to verify the evidences submitted only in case of cheating. But in the existing receipt based schemes the nodes always submit security tokens (signatures), and the AC always applies cryptographic operations to verify the payment. Comparing to receipt based payment schemes; RACE can clear the payment without applying cryptographic operations. It only includes submitting lightweight reports and also Evidences are not frequently requested. Receipt based payment scheme have the packet transmission on desired path. Cryptographic operations are systematically applied. Light weight statistical operations are used in credit based existing system. These will enhance the payment processing overhead. Due to the above payment processing overhead Report Based Payment Scheme is Proposed. In multihop wireless networks the main motivation is disconnected networks like vehicular and disaster adhoc networks. Instead of resorting to flooding- based routing techniques, which lead to significant waste of resources and bad performance, a family of routing algorithms are presented that routes a small , fixed number of copies to a carefully selected number of relays, and routes each copy intelligently towards the destination. The Results shows that the proposed schemes are highly scalable. It outperforms all existing practical schemes with respect to both delivery delay and number of transmissions per message delivered. Existing Receipt based payment scheme in multihop wireless networks the nodes submit reports for each nodes. The Accounting Center in Report Based Payment Scheme stores the undeniable security evidences. With almost no processing overhead the fair reports can be cleared . The cheating reports are used to identify which node act as a cheater. Our scheme can used to reduce the overhead of submitting and processing the payment data.

2. RELATED WORKS

Tamper-proof-device (TPD)-based and receipt-based schemes are the two existing payment schemes. In order. to store and manage the credit account and for its secure operation a TPD is installed in each node in TPD-based payment schemes [4], [13], [1], [2].Where as in receipt-based payment schemes [12], [7], [8], [9], [11], [3], [6], [5] an offline central unit is employed. This central unit is called accounting center. It manages the nodes' credit accounts. For relaying packets, the nodes submit proofs called receipts to the AC to update their credit accounts. The forwarded packets by a node are passed to the TPD in Nuglets [4].Thus the node's credit account can be decreased and increased respectively. Packet trade models and Packet purse have been proposed. In the packet purse model, the source node should give the full payment before starting with the data transmission. And the intermediate nodes can acquire the payment for relaying each packet. Where as in packet trade model the case is different. There each intermediate node each intermediate node applies an auction to sell the packets to the next node in the route. The total payment is done by the destination node.

In SIP [13], the destination node sends a RECEIPT packet to the source node each time it receives a data packet. As a result the source node issues the REWARD packet to increment the credit account of the intermediate nodes. In CASHnet [1], along with each data packet a signature is attached and the source node is charged. The destination node is also charged upon receiving each data packet. Then an acknowledgement packet is send back to the source node to increment the intermediate nodes' credit account. More overhead is imposed by receipt-based payment schemes than the TPD-based schemes. Because in receipt-based payment schemes, submitting receipts to the AC and processing them imposes more overhead. In Sprite [12], the identities of the nodes in the route are signed by the source node for each message, and as a proof a signature is send. The signature verification is done by the intermediate nodes and the receipts are composed which contains the identities of the nodes in the route and the source node's signature. Then the receipts are submitted to AC so as to claim the payment. The signature verification is done by AC to make sure whether the payment is correct. Since receipts are generated for each message, the network overhead is increased. Sprite that charges only the source node, where as FESCIM [7] charges both the source and destination nodes when both the parties are interested in communication.

In PIS [8], each message is attached with a signature by the source node. A signed ACK packet is send as the reply by the destination node. The no of receipts is reduced in PIS by generating fixed size receipts per session. Thus it differs from sprite. To minimize communication and processing overhead, statistical methods are used by CDS [9] to identify the selfish nodes that submit incorrect payment. But due to the nature of the statistical methods the chances of false accusations. And missed detections are also possible. Another issue faced is that it takes long time to identify the cheating nodes. In ESIP [6], a communication protocol is proposed which can be used for a payment scheme. It uses only limited number of public key cryptography operations, identity-based cryptography, and hash function for transfer of messages from source to destination. When compared to PIS,ESIP involves only fewer cryptographic operations. The aim of ESIP is to transfer the data efficiently where as the aim of Report Based Payment Scheme is to minimize the communication and processing overhead of submitting the payment data to the AC. i.e., The proposed scheme reduces both the communication and processing overhead comparing to receipt-based schemes [12], [7], [8], [6] and the payment clearance delay and the storage area are also acceptable.

3. THE PROPOSED SYSTEM

Report Based Payment Scheme has four main phases. In Communication phase, the nodes are involved in communication sessions and Evidences and payment reports are composed and temporarily stored. The payment reports are accumulated by the nodes and are submitted in batch to the Trusted Party. The next phase is Classifier phase. In this phase, the Reports are classified into fair and cheating. The cheating nodes are detected in Identifying cheaters phase. The evidences are requested from the nodes that submit cheating reports. This request is done by the TP. Then the eviction of cheating nodes and correction of payment reports are done. The Final phase is Credit-Account Update phase. In this phase the payment reports are cleared by Authority Centre.

3.1Communication phase:

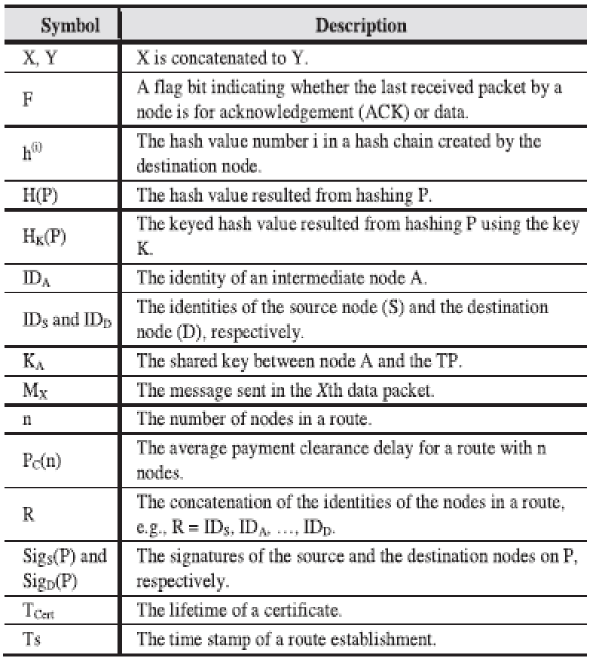
The four processes of Communication phase are route establishment, data transmission, Evidence composition, and payment report composition/submission.

Route establishment: The end-to-end Route is established by broadcasting the Route Request (RREQ) packet. RREQ contains the identities of the destination (IDD) nodes and the source (IDS), time stamp (Ts), and Time-To-Live(TTL). The maximum number of intermediate nodes is indicated by TTL. When a node receives the RREQ packet, it attaches its identity and relays the packet if the number of intermediate nodes is fewer than TTL. The Route Reply (RREP) packet is composed by the destination node. This is composed for the first received RREQ packet and this (RREP) packet is send back to the source node. By iteratively hashing a random value ($h^{(K)}$) K times, a hash chain is created by the destination node. Thus a hash chain root ($h^{(0)}$) is produced, where $h^{(i-1)} =H(h^{(i)})$ and1 <= i <=K. The RREP packet consists of the destination node's certificate, signature ($Sig_D(R,T_S,h^{(0)})$) and the identities of the nodes in the route. This signature is used to authenticate the hash chain and also for linking it to the route. The destination node's signature is verified by the intermediate nodes. The intermediate nodes also relay the RREP packet, and store the signature and $h^{(0)}$ for composing the Evidence.

Data transmission: The data packets are send to the destination node by the source node through the established route and the destination node replies with ACK packets. For example, for the Xth data packet, the source node appends the message M_X and its signature to R, X, Ts, and the hash value of the message ($H(M_X)$). And the packet is send to the first node in the route.

Evidence composition: Evidence is composed in this phase. In order to establish a proof about the occurrence of an event, evidence's are used. It can also be used as an information about the time of occurrence, the parties involved and the outcome of the event

Table 1 Description of Used Symbols



Symbol	Description
X, Y	X is concatenated to Y.
F	A flag bit indicating whether the last received packet by a node is for acknowledgement (ACK) or data.
$h^{(i)}$	The hash value number i in a hash chain created by the destination node.
H(P)	The hash value resulted from hashing P.
$H_K(P)$	The keyed hash value resulted from hashing P using the key K.
ID_A	The identity of an intermediate node A.
ID_S and ID_D	The identities of the source node (S) and the destination node (D), respectively.
K_A	The shared key between node A and the TP.
M_X	The message sent in the Xth data packet.
n	The number of nodes in a route.
$P_C(n)$	The average payment clearance delay for a route with n nodes.
R	The concatenation of the identities of the nodes in a route, e.g., $R = ID_S, ID_A, \ldots, ID_D$.
$Sig_S(P)$ and $Sig_D(P)$	The signatures of the source and the destination nodes on P, respectively.
T_{Cert}	The lifetime of a certificate.
Ts	The time stamp of a route establishment.

But the real purpose of Evidence is to resolve a dispute about the amount of the payment resulted from data transmission. Evidence contains two main parts called DATA and PROOF. The DATA part describes the payment, i.e., who pays whom and how much, and contains the necessary data to regenerate the nodes' signatures. the DATA contains the identities of the nodes in the route (R), the number of received messages (X), the session establishment time stamp, the root of the destination node's hash chain $h^{(0)}$,the hash value of the last message ($H(M_X)$), and the last received hash value ($h^{(V)}$). V = X -1 when the last received packet is the Xth data packet because the route is broken before receiving the Xth ACK packet that carries $h^{(X)}$, but V = X when the last received packet is the Xth ACK packet. The DATA does not have $h^{(1)}$ when the route is broken after receiving the first data packet because the ACK that has $h^{(1)}$ is not received. The PROOF is an undeniable security token that can prove the correctness of the DATA and protect against payment manipulation, forgery, and repudiation .The PROOF is composed by hashing the destination node's signature and the last signature received from the source node, instead of attaching the signatures to reduce the Evidence size.

Algorithm: Report and evidence Verification, Cheating node detection, Alternate Path finding.

```
// $n_i$ is the source, intermediate, or destination node

for each node $n_i$
verify report();
Report={R,$T_{S,}$,F,X};
if Reports==Cheating
          Request Evidence();
```

```
        Evidence={$R,X,T_{S,}H(M_X),h^{(0)},h^{(x)},H((Sigs(R,X,T_{S,}H(M_X))),SigD(R,T_s,h^{(0)}))$}
        Verify Evidence();
        If evidence==false;
        Evict node();
End if
        for each $n_i$ evicted
        //NNlist is the neighboring node list
        NNlist=NNlist-$n_i$;
        Altpath();
End if
```

Payment report composition/submission: A payment report contains the session identifier, a flag bit (F), and the number of messages (X). The session identifier constitutes the the identities of the nodes in the session and the time stamp. The flag bit is used to identify whether the last received packet is data or acknowledgment. It is indicated as zero when it is data and one if it is ACK.

3.2 Classifier:

AC verifies the payment reports by checking the consistency of the reports. After verifying the reports are classified into fair or cheating. If the nodes submit correct payment reports it comes under fair reports. If at least one node does not submit the reports it can be classified under Cheating Reports. This is done in order to steal credits or pay less. Fair reports can be for complete or broken sessions. For a complete session, all the nodes in the session report the same number of messages and F of one. If a session is broken during relaying the Xth data packet, the reports of the nodes from S to the last node that received the packet report X and F of zero, but the other nodes report X - 1 and F of one. If a session is broken during relaying the Xth ACK packet, the nodes in the session report 5 messages, and the nodes from D to the last node that received the ACK report F of one, but the other nodes report F of zero. The reports are classified as cheating if they do not satisfy one of the above mentioned rules.

3.3 Identifying Cheaters:

In the Identifying Cheaters' phase, the Trusted Party processes the cheating reports. After processing the cheating nodes are identified and the financial data are corrected. Our objective of securing the payment is preventing the attackers from stealing credits or paying less, i.e., the attackers should not benefit from their misbehaviors. We should also guarantee that each node will earn the correct payment even if the other nodes in the route collude to steal credits. 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 for identifying the cheating node(s). In this way, the AC can precisely 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 valid if the computed PROOF is similar to the Evidence's Proof. The identified cheating nodes are then evicted from the network.

3.4 Credit-Account Update:

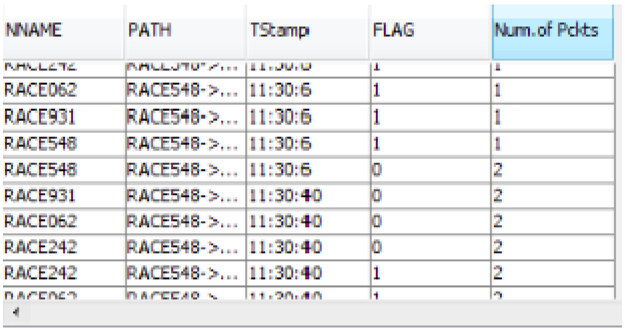
The Credit-Account Update phase receives fair and corrected payment reports to update the node's credit accounts. The payment reports are cleared using the charging and rewarding policy. In receipt-based payment schemes, a receipt can be cleared once it is submitted because it carries undeniable security proof, but the AC in RACE has to wait until receiving the reports of all nodes in a route to verify the payment. The maximum payment clearance delay (or the worst case timing) occurs for the sessions that are held shortly after at least one node contacts the AC and the node submits the report after the certificate lifetime (TCert), i.e., at least one report is submitted after TCert of the session occurrence.

3.5 Alternate Path Finding:

This phase is done after the cheating nodes are detected and evicted. Upon eviction of a particular node, the path for the particular data transmission is broken. After eviction of the cheating nodes, an alternate path has to be identified. This is done by using Path Finding technique. After eviction of the cheating node, the source node which tries to send the data to the destination node sends the route request to all the neighboring nodes. Prior to this step, the neighboring node list is updated. Each node contains a neighboring node list which consists of all of its neighboring nodes. Once a node is evicted from the network, all the nodes containing that evicted node in the neighboring list must update the list. After updating the Neighboring list the source node sends the RREQ (Route Request) to the neighboring nodes. RREQ contains the identities of the destination (IDD) nodes and the source (IDS), time stamp (Ts), and Time-To-Live(TTL). The maximum number of intermediate nodes is indicated by TTL. When a node receives the RREQ packet, it attaches its identity and relays the packet if the number of intermediate nodes is fewer than TTL. The Route Reply (RREP) packet is composed by the destination node. This is composed for the first received RREQ packet and this (RREP) packet is send back to the source node. The RREP packet consists of the destination node's certificate, signature ($Sig_D(R,T_S,h^{(0)})$) and the identities of the nodes in the route. This signature is used to authenticate the hash chain and also for linking it to the route.

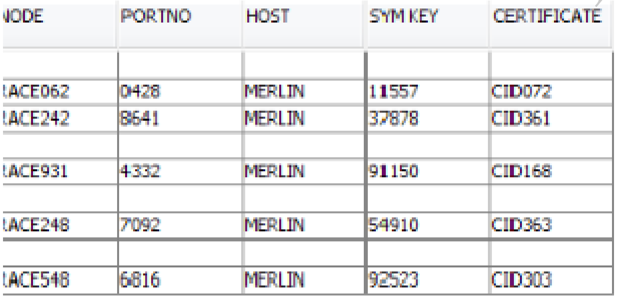
4. RESULT AND ANALYSIS:

A Report-Based Payment Scheme for multihop wireless networks is proposed for enabling node cooperation, regulating packet transmission, and enforcing fairness. The nodes submit lightweight payment reports (instead of receipts) to the accounting center (AC) and temporarily store security tokens called Evidences. The reports contain the alleged charges and rewards without security proofs. First the multihop wireless network is established and the nearest nodes are identified. Whenever a node is created, each node registers with the authority centre. The authority centre provides each node with a private and public key pair. The node registration details are shown in figure 3.It also provides a symmetric key for secure report submission. For the secure data transmission, RSA algorithm is used. HMAC algorithm is used to ensure both authenticity and integrity. Comparing to Receipt based Payment scheme, Report based Payment Scheme have got less communication and processing overhead. The composition of report is shown in figure 2. The Trusted Party classifies the reports into fair and cheating reports. The nodes that submit the cheating reports are requested for their evidence. Thus the evidence of all nodes are not checked. Instead evidence are requested from nodes who submit cheating reports. Thus the overall overhead is reduced. Once the cheating nodes are identified by checking the evidence, those nodes are evicted.



NNAME	PATH	TStamp	FLAG	Num.of Pckts
RACE242	RACE548->...	11:30:6	1	1
RACE062	RACE548->...	11:30:6	1	1
RACE931	RACE548->...	11:30:6	1	1
RACE548	RACE548->...	11:30:6	1	1
RACE548	RACE548->...	11:30:6	0	2
RACE931	RACE548->...	11:30:40	0	2
RACE062	RACE548->...	11:30:40	0	2
RACE242	RACE548->...	11:30:40	0	2
RACE242	RACE548->...	11:30:40	1	2
RACE062	RACE548->...	11:30:40	1	2

Figure 2 Light Weight Report Composition



ODE	PORTNO	HOST	SYM KEY	CERTIFICATE
ACE062	0428	MERLIN	11557	CID072
ACE242	8641	MERLIN	37878	CID361
ACE931	4332	MERLIN	91150	CID168
ACE248	7092	MERLIN	54910	CID363
ACE548	6816	MERLIN	92523	CID303

Figure 3 Node Registration Details

5. CONCLUSION AND FUTURE WORK

In this paper, a Report-Based Payment Scheme for MWNs is proposed. In this Payment Scheme lightweight payment reports are submitted by each node. The nodes temporarily store Reports and evidences. The reports are light weight since it does not contain proofs. It contains only alleged charges and rewards. Report Based Payment Scheme does not involve much processing overhead. The reports are cleared without any cryptographic operations and thus less overhead. Only in case of cheating reports the Evidences are submitted and are processed. This processing is done to detect the cheating nodes. Since Reports are used instead of Receipts, the communication and processing overhead is reduced. Report-Based Payment Scheme secures the payment. It can identify the cheating nodes easily and precisely without any missed detections and false accusations. The Authority Centre process the payment reports and thus the number of dropped messages are known. On detection of cheating nodes, an alternative path for data transmission is identified. As a future work a trust based system which includes a trust value for each node can be developed. In such a system, higher trust values will be will be assigned to nodes that transmit messages more successfully. A trust based routing protocol can be proposed to transmit the messages through the highly trusted nodes. The highly trusted nodes are identified by examining the previous performance of the nodes. This helps to improve the network performance in terms of packet delivery ratio and throughput. It also reduces the probability of dropping messages. But the trust system should be secure against all collusive and singular attacks.

REFERENCE

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

[2] 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

[3] 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. 853-865, 2007.

[4] 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.

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

[6] 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.

[7] 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.

[8] 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.

[9] M. Mahmoud and X. Shen, “Stimulating Cooperation in Multihop Wireless Networks Using Cheating Detection System,” Proc.IEEE INFOCOM ’10, Mar. 2010.

[10] Mohamed M.E.A. Mahmoud and Xuemin (Sherman) Shen, Fellow, IEEE” A Secure Payment Scheme with Low Communication and Processing Overhead for Multihop Wireless Networks” ieee transactions on parallel and distributed systems, vol. 24, pp 209-213,february 2013

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

[12] 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.

[13] 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.