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, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

# Detection of Cheater Nodes Based On Evidences and Reports in MultiHop Wireless Networks

S.Sowbakiyalakshmi[1], B.Sathishkumar[2]

Department of CSE, Chettinad College of engineering and technology, India[1]

Assistant Professor, Department of CSE, Chettinad College of engineering and technology, India[2]

**ABSTRACT –**A Secure Payment Scheme called as a Report-based payment scheme for multi-hop wireless systems to stimulate node cooperation, regulate package transmission, and enforce fairness. The nodes submit lightweight fee accounts (instead of acknowledgements) to the accounting center (AC) and temporarily being store undeniable security tokens called Evidences. The reports comprise the alleged charges and rewards without security verifications, for example, signatures. The AC can verify the payment by investigating the consistency of the accounts, and clear the fee of the fair accounts with nearly no processing overhead or cryptographic operations. For betraying accounts, the Evidences are requested to recognize and evict the betraying nodes that submit incorrect accounts. Rather than of requesting the Evidences from all the nodes participating in the cheating accounts, RACE can recognize the betraying nodes with requesting few evidences. Furthermore, evidence aggregation technique is utilized to decrease the evidence storage locality. Our analytical and simulation results show that RACE requires much less communication and processing overhead than the existing receipt-based designs with agreeable fee clearance delay and storage locality. Furthermore, RACE can secure the fee and accurately identify the betraying nodes without untrue accusations.

## I.INTRODUCTION

In MultiHop Wireless Networks (MWNs), the traffic began from a node is generally relayed through the other nodes to the place visited for endowing new submissions and enhancing the mesh presentation and deployment. MWNs can be established readily at reduced cost in evolving and country areas. Multi-hop package relay can extend the mesh coverage using restricted transmit power, advance locality spectral effectiveness, and enhance the network throughput and capacity. MWNs can also implement many helpful submissions such as data sharing [1] and multimedia data transmission. For demonstration, users in one locality (residential neighbor-hood, university campus, etc.) having different wireless-enabled device, for example, PDAs, laptops, tablets, cell telephones, etc., can set up a network to communicate, distribute documents, and share information. Although, the assumption that the nodes are willing to spend their scarce resources, such as electric battery energy, CPU circuits, and available mesh bandwidth, to relay others' packets without compensation cannot be held for citizen applications where the nodes are autonomous and aim to maximize their welfare. Self-centered nodes will not relay others' packets and make use of the cooperative nodes to relay their packets, which degrades the mesh connectivity and fairness. The fairness topic arises when the selfish nodes make use of the cooperative nodes to relay their packets without any contribution to them, and therefore the cooperative nodes are wrongly overloaded because the network traffic is intensified through them. The self-centered behavior also degrades the mesh connectivity considerably, which may origin the multi -hop connection to fail.

Fee (or inducement) designs [2] use credits (or micropayment) to motivate the nodes to help in relaying others' packets by making cooperation more beneficial than selfishness. The nodes earn credits for relaying other ones' packets and spend these credits to get their packets relayed by others. In addition to collaboration stimulation, these schemes can enforce fairness, discourage Message-Flooding attacks, regulate packet transmission, and efficiently charge for the network services. Fairness can be enforced by paying the nodes that relay more packets and charging the nodes that drive more packets. For example, the nodes located at the mesh center relay more packets than the other nodes because they are more frequently selected by the routing protocol. Since the source nodes pay for relaying their packets, the fee schemes can furthermore regulate package transmission and disappoint Message-Flooding attacks where the attackers drive false notes to deplete the intermediate nodes' resources. Furthermore, since the communication meetings may be held without engaging a trusted party (TP) and the nodes may roam among distinct foreign systems. The living credit card fee designs are designed for distinct system and risk forms, which are infeasible for MWNs. For demonstration, in borrowing business card payment schemes, each transaction generally has one customer and one merchant, and the merchants' number is reduced and they are renowned before the transaction is held. For the fee schemes in MWNs, there is usually one client (the source node) and multiple merchants (the intermediate nodes). The merchants' number is large because any network node can act as a merchant (or packet relay), and a transaction's value is much less than those in borrowing business card fee designs. The relation between a customer and a merchant is usually short due to the network dynamic topology. Due to these unique characteristics, MWNs require a particularly conceived fee scheme.

A good fee scheme should be secure, and require reduced overhead. Although, the existing receipt-based fee scheme enforce important processing and communication overhead and implementation complexity. Since a trusted party may not be involved in communication meetings, the nodes compose proofs of relaying others' packets, called acknowledgements, and submit them to an offline accounting center (AC) to clear the fee. The acknowledgements' size is large because they carry security verifications, for e.g, signatures, to secure the payment, which significantly consumes the nodes' assets and the accessible bandwidth in submitting them. The AC has to apply a large number of cryptographic procedures to verify the receipts, which may need impractical computational power and make the practical implementation of these designs complex. Thus, decreasing the communication and the payment processing overhead is absolutely vital for the effective implementation of the fee design and to bypass conceiving a bottleneck at the AC and exhausting the nodes' resources.

In this paper, we suggest RACE, a Report-based payment design for MWNs. The nodes submit lightweight fee reports (instead of acknowledgements) to the AC to update their borrowing accounts, and for the time being store undeniable security tokens called Evidences. The accounts contain the alleged charges and rewards of distinct meetings without security verifications, for example, signatures. The AC verifies the payment by enquiring the consistency of the accounts, and clears the payment of the equitable accounts with nearly no cryptographic procedures or computational overhead. For betraying accounts, the Evidences are requested to identify and evict the betraying nodes that submit incorrect reports, for example, to steal credits or pay less. Instead of requesting the Evidences from all the nodes participating in the betraying accounts, RACE can recognize the betraying nodes with submitting and processing few evidences. Furthermore, evidence aggregation method is used to reduce the storage locality of the Evidences.

In RACE, Evidences are submitted and the AC applies cryptographic operations to verify them only in case of betraying, but the nodes habitually submit security tokens, for example, signatures, and the AC habitually applies cryptographic procedures to verify the fee in the living receipt based designs. RACE can clear the fee almost without applying cryptographic procedures and with submitting lightweight accounts when Evidences are not often requested. Furthermore, betraying nodes are evicted one time they commit one betraying activity and it is neither easy nor cheap to change its identity. Our analytical and replication results illustrate that RACE requires much less communication and processing overhead than the existing receipt-based schemes with acceptable fee clearance hold up and Evidences' storage area, which is necessary to make the functional implementation of the payment design effective. Moreover, RACE can secure the fee and accurately recognize the betraying nodes without untrue accusations or robbing credits.

To the best of our information, RACE is the first fee design that can verify the fee by enquiring the consistency of the nodes' accounts without systematically submitting and processing security tokens and without false accusations. RACE is also the first design that uses the concept of Evidence to protected the payment and needs applying cryptographic procedures in clearing the fee only in case of betraying.

## II. RELATED WORKS

The existing payment schemes can be classified into tamper-proof-device (TPD)-based and receipt-based schemes. In TPD-based payment schemes [3], [4], [5], [6], a TPD is installed in each node to store and manage its credit account and secure its operation. For receipt-based payment schemes [7], [8], [9], [10], [11], [12], [13], [14],[15], [16], an offline central unit called the accounting center stores and manages the nodes' credit accounts. In Nuglets [7], the self-generated and forwarded packets by a node are passed to the TPD to decrease and increase the node's credit account, respectively. In SIP [8], after receiving a data packet, the destination node sends a RECEIPT packet to the source node to issue a REWARD packet to increment the credit accounts of the intermediate nodes. In CASH net [9], the credit account of the source node is charged and a signature is attached to each data packet. The receipt-based payment schemes impose more overhead than the TPD-based schemes because they require submitting receipts to the AC and processing them. However, the TPD-based payment schemes suffer from the following serious issues. First, the assumption that the TPD cannot be tampered with, cannot be guaranteed because the nodes are autonomous and self-interested, and the attackers can communicate freely in an undetectable way if they could compromise the TPDs. Second, the nodes cannot communicate if they do not have sufficient credits during the communication time. In [10], it is shown that the overall credits in the network decline gradually with using TPD-based schemes because the total charges may be more than the total rewards. 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. In Sprite [11], 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. Unlike Sprite that charges only the source node, FESCIM [12] adopts fair charging policy by charging both the source and destination nodes when both of them are interested in the communication. In PIS [13], the source node attaches a signature to each message and the destination node replies with a signed ACK packet. 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. In order to reduce the communication and processing overhead, CDS [14] uses statistical methods to identify the cheating nodes that submit incorrect payment. In [15], 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 [16], each node has to contact the AC in each communication session to get coins to buy packets from the previous node in the route. However, the interactive involvement of the AC in each session is inefficient, causes long delay, and creates a bottleneck. ESIP [17] 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.

## III. SYSTEM MODELS

### 3.1 Network Model

The TP comprises the AC and the credentials administration (CA). The AC sustains the nodes' borrowing anecdotes and the CA improves and revokes the nodes' certificates. Each node (A) has to list with the trusted party to obtain a symmetric key KA, Private/public key pair, and certificate. The symmetric key is used to submit the fee accounts and the private/public keys are required to proceed as source or place visited node. Once the AC obtains the fee accounts of a session and verifies them, it clears the payment if the accounts are fair; additional, it demands the Evidences to recognize the cheating nodes. The CA evicts the betraying nodes by rejecting improving their certificates. Source nodes' packets may be relayed some relayed by intermediate nodes to their destinations. The nodes can contact the TP at smallest one time during a period of couple of days. In this attachment, the nodes submit the payment accounts and the Evidences (if requested), and obtain renewed certificates to be able to continue utilizing the network. The nodes also can purchase credits with genuine cash to enable the nodes that will not earn sufficient credits, such as those at the network boundary. This connection can happen by the groundwork stations of cellular systems, Wi-Fi hotspots, or connected systems such as Internet.

### 3.2 ADVERSARY MODEL

The wireless nodes are likely attackers but the TP is completely secure. The wireless nodes are autonomous and self-interested and therefore motivated to misbehave. The TP is run by an operator that is inspired to ensure the mesh correct procedure. The attackers have full control on their nodes and can change their procedure and infer the cryptographic data. The attackers can work individually or collude with each other under the command of one attacker to launch complicated attacks.

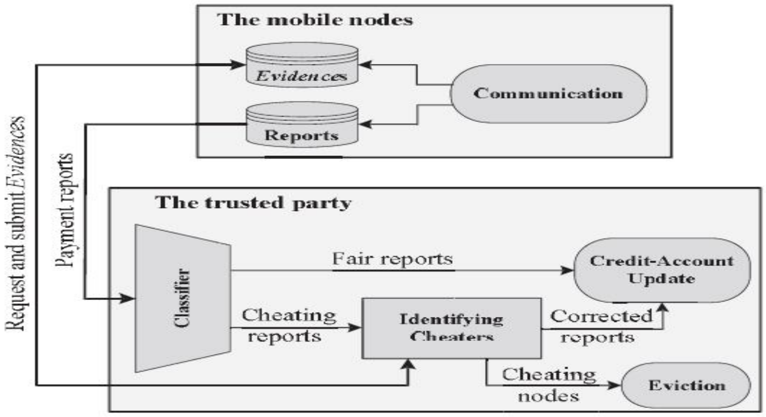


Fig. 2. The architecture of RACE.

## IV THE PROPOSED RACE

As shown in Fig. 2, RACE has four main phases. In communication stage, the nodes are engaged in communication meetings and Evidences and fee accounts are composed and temporarily retained. The nodes accumulate the fee accounts and submit them in batch to the TP. For the Classifier stage, the TP classifies the accounts into fair and betraying. For the Identifying Cheaters stage, the TP request the Evidences from the nodes that are engaged in betraying accounts to identify the cheating nodes. The cheating nodes are evicted and the payment reports are corrected. Eventually, in Credit-Account account phase, the AC clears the fee accounts.

### 4.1 COMMUNICATION

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

### ROUTE ESTABLISHMENT

In alignment to set up an end-to-end route, the source node broadcasts the path demand (RREQ) package containing the identities of the source (IDS) and the place visited (IDD) nodes, time mark (Ts), and Time-To-Live (TTL). TTL is the greatest number of intermediate nodes. After a node obtains the RREQ packet, it appends its identity and broadcasts the package if the number of intermediate nodes is less than TTL. The destination node creates the Route Reply (RREP) package for the nodes broadcasted the first obtained RREQ package, and drives the package back to the source node. The RREP packet comprises the identities of the nodes in the route (e.g., R =IDS, IDA, IDB, IDD) in the route.

### DATA TRANSMISSION

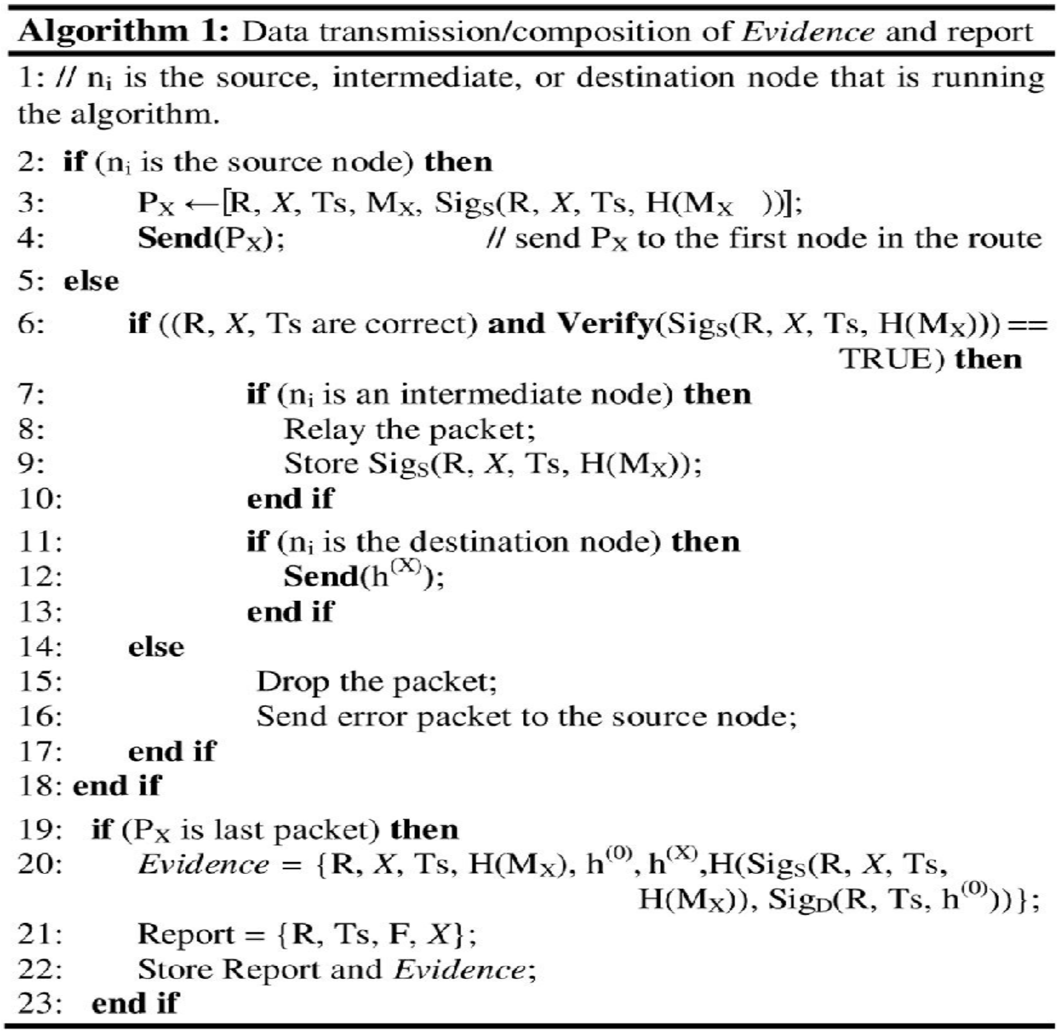
The source node drives data packets to the place visited node through the established path and the place visited node answers with ACK packets. For the Xth data packet, the source node appends the note $M_x$ and its signature to R, X, Ts, and the hash value of the message ($H(M_x)$) and sends the package to the first node in the route. The source node's signature is an undeniable proof for transmitting X messages and ensures the message's authenticity and integrity.

## EVIDENCE COMPOSITION

Evidence is characterized as information that is utilized to establish proof about the incident of a happening or activity, the time of incident, the parties engaged in the event, and the conclusion of the event. The purpose of evidence is to resolve a argument about the allowance of the fee resulted from data transmission.

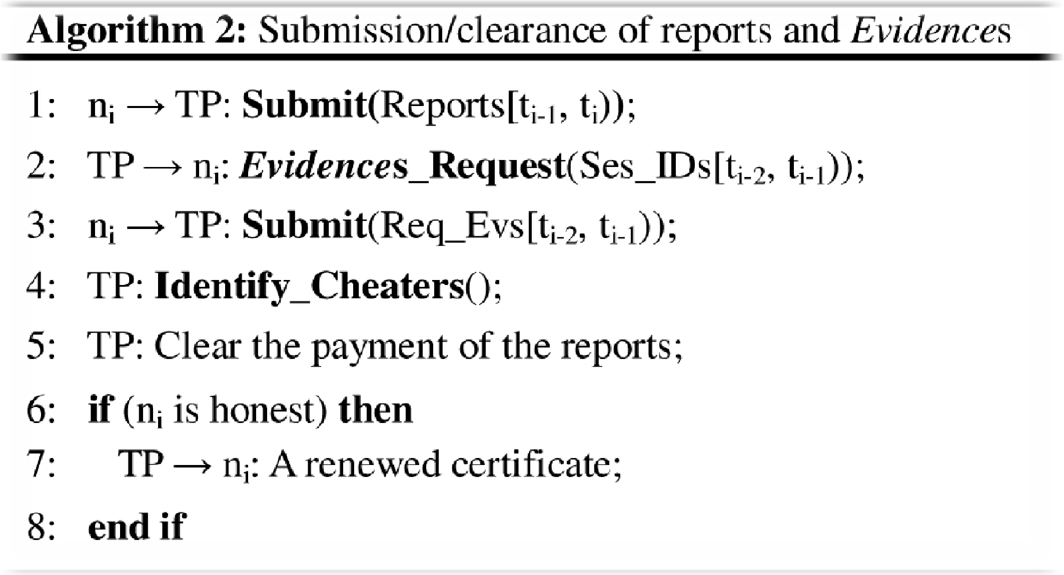
## PAYMENT REPORT COMPOSITION/ SUBMISSION

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.



**Algorithm 1:** Data transmission/composition of *Evidence* and report

```
// $n_i$ is the source, intermediate, or destination node that is running the algorithm.
if ($n_i$ is the source node) then
        $P_X \leftarrow [R, X, Ts, M_X, Sig_S(R, X, Ts, H(M_X))]$;
        Send($P_X$);                // send $P_X$ to the first node in the route
else
        if ((R, X, Ts are correct) and Verify($Sig_S(R, X, Ts, H(M_X))$) == TRUE) then
                if ($n_i$ is an intermediate node) then
                        Relay the packet;
                        Store $Sig_S(R, X, Ts, H(M_X))$;
                end if
                if ($n_i$ is the destination node) then
                        Send($h^{(X)}$);
                end if
        else
                Drop the packet;
                Send error packet to the source node;
        end if
end if
if ($P_X$ is last packet) then
        Evidence = $\{R, X, Ts, H(M_X), h^{(0)}, h^{(X)}, H(Sig_S(R, X, Ts, H(M_X)), Sig_D(R, Ts, h^{(0)}))\}$;
        Report = $\{R, Ts, F, X\}$;
        Store Report and Evidence;
end if
```



**Algorithm 2:** Submission/clearance of reports and *Evidences*

```
$n_i$ → TP: **Submit**(Reports[$t_{i-1}$, $t_i$]);
TP → $n_i$: ***Evidences*_Request**(Ses_IDs[$t_{i-2}$, $t_{i-1}$]);
$n_i$ → TP: **Submit**(Req_Evs[$t_{i-2}$, $t_{i-1}$]);
TP: **Identify_Cheaters**();
TP: Clear the payment of the reports;
**if** ($n_i$ is honest) **then**
    TP → $n_i$: A renewed certificate;
**end if**
```

### 4.2 CLASSIFIER

After obtaining a session's fee accounts, the AC verifies them by enquiring the consistency of the accounts, and classifies them into fair or cheating. For fair accounts, the nodes submit correct payment accounts, but for cheating reports, at smallest one node does not submit the accounts or submits incorrect accounts, for example, to rob credits or pay less. Fair accounts can be for entire or broken meetings. For a entire meeting, all the nodes in the session report the same number of messages and F of one. If a meeting is broken throughout relaying the Xth facts and figures package, the reports of the nodes from S to the last node that obtained the package report X and F of none, but the other nodes report X 1 and F of one. If a session is broken during relaying the Xth ACK package, the nodes in the meeting report X notes, and the nodes from D to the last node that obtained the ACK report F of one, but the other nodes report F of none. The accounts are classified as cheating if they do not achieve one of the aforementioned directions.

### 4.3 IDENTIFIER CHEATER

As shown in Fig. 2, in the recognizing Cheaters' phase, the TP methods the betraying accounts to identify the betraying nodes and correct the financial facts and figures. Our objective of protecting the fee is stopping the attackers (singular of collusive) from Robbing credits or paying less, i.e., the attackers should not benefit from their misbehaviors. We should also assurance that each node will profit from the correct payment even if the other nodes in the route collude to rob credits. The AC request the evidence only from the node that submits report with more fee rather than of all the nodes in the route because it should have the essential and undeniable verifications (signatures and hash string of links components)for identifying the betraying node(s). In this way, the AC can precisely identify the cheating nodes with requesting few Evidences. To verify an Evidence, the TP creates the verification by developing the nodes' signatures and hashing them. The evidence is valid if the computed PROOF is similar to the Evidence's PROOF.

### 4.4 CREDIT-ACCOUNT UPDATE

As shown in Fig. 2, the Credit-Account update stage receives fair and corrected fee accounts to revise the nodes' credit accounts. In receipt-based payment designs, a receipt can be cleared one time it is submitted because it carries undeniable security proof, but the AC in RACE has to wait until obtaining the reports of all nodes in a route to verify the payment. The greatest payment clearance hold up (or the poorest case timing) happens for the sessions that are held soon after at least one node associates 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 meeting occurrence. It is worth to note that the greatest time length for a node's two consecutive associates with the TP is TCert to renew its certificate to be able to use the network.

## V. CONCLUSION

In this paper, the proposed RACE, a report-based payment scheme for MWNs. The nodes submit lightweight fee accounts encompassing the alleged allegations and pays (without proofs), and temporarily shop undeniable security tokens called Evidences. The fair accounts can be cleared with nearly no cryptographic procedures or processing overhead, and Evidences are submitted and processed only in case of cheating accounts in alignment to recognize the cheating nodes. Our analytical and replication results demonstrate that RACE can considerably reduce the connection and processing overhead matching to the living receipt-based fee schemes with acceptable fee clearance delay and Evidences' storage area, which is necessary for the productive implementation of the design. Moreover, RACE can secure the fee, and identify the cheating nodes accurately and rapidly without false accusations or missed detections. In RACE, the AC can process the payment reports to understand the number of relayed/dropped notes by each node. In our future work, we will evolve a trust scheme founded on processing the fee accounts to maintain a trust worth for each node. The nodes that relay messages more effectively will have higher trust values, such as the low-mobility and the large-hardware-resources nodes. Based on these trusted standards, we will suggest a trust-based routing protocol to route messages through the highly trusted nodes (which presented package relay more effectively in the past) to minimize the likelihood of dropping the notes, and therefore advance the network performance in periods of throughput and package delivery ratio. Although, the trust scheme should be protected against singular and collusive attacks, and the routing protocol should make smart decisions considering node assortment with reduced overhead.

## REFERENCES

[1] C.Chou, D.wei, C.Kuo, and K.Naik, "An Efficient Anonymous Communication Protocols for Peer-to-Peer Applications Over Mobile Ad-Hoc Networks,"IEEE vol.25,no.1,pp.192-203,Jan.2007

[2] 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.

[3] 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.

[4] 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.

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

[6] 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.

[7] 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.

[8] 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.

[9] 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.