REPORT BASED PAYMENT SCHEME FOR MULTIHOP WIRELESS NETWORKS

J.Gunasekaran[1], M.Ezhilvendan[2], P.Vijayanand[3], S.Rajasekaran[4], S.Murugesan[5]

M.E-Network Engineering [(1, 2, 4, 5)], Assistant Professor [(3)]
Veltech Multitech Dr.Rangarajan Dr.Sakunthala Engineering College, Chennai, India [(1, 2, 3, 4, 5)]
guna.vnb@gmail.com, vendannetwork@gmail.com, vijayanandparthasarathy@gmail.com, rajasekaran009@gmail.com, murugesan1906@gmail.com

Abstract

We propose RACE, a report-based payment scheme for multihop wireless networks to stimulate node cooperation, regulate packet transmission, and enforce fairness. The nodes submit lightweight payment reports (instead of receipts) to the accounting center (AC) and temporarily store undeniable security tokens called Evidences. The reports contain the alleged charges and rewards without security proofs, e.g., signatures. The AC can verify the payment by investigating the consistency of the reports, and clear the payment of the fair reports with almost no processing overhead or cryptographic operations. For cheating re-ports, the 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, RACE can identify the cheating nodes with requesting few Evidences. Moreover, Evidence aggregation technique is used to re-duce the Evidences' storage area. Our analytical and simulation results demonstrate that RACE requires much less communication and processing overhead than the existing receipt-based schemes with acceptable payment clearance delay and storage area. This is essential for the effective implementation of a payment scheme because it uses micropayment and the overhead cost should be much less than the payment value. Moreover, RACE can secure the payment and precisely identify the cheating nodes without false accusations.

Index Terms: *Cooperation incentive schemes; network-level security and protection; payment schemes; and selfishness attacks.*

----------***----------

1. INTRODUCTION

In multihop wireless networks (MWNs), the traffic originated from a node is usually relayed through the other nodes to the destination for enabling new applications and enhancing the network performance and deployment [1]. MWNs can be deployed readily at low cost in developing and rural areas. Multihop packet relay can extend the network coverage using limited transmit power, improve area spectral efficiency, and enhance the network throughput and capacity. MWNs can also implement many useful applications such as data sharing [2] and multimedia data transmission [3]. For example, users in one area (residential neighborhood, university campus, etc) having different wireless-enabled devices, e.g., PDAs, laptops, tablets, cell phones, etc, can establish a network to communicate, distribute files, and share information. However, the assumption that the nodes are willing to spend their scarce resources, such as battery energy, CPU cycles, and available network bandwidth, to relay others' packets without compensation cannot be held for civilian applications where the nodes are autonomous and aim to maximize their welfare.

Payment (or incentive) schemes [5] use credits (or micro-payment) 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. In addition to cooperation 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 rewarding the nodes that relay more packets and charging the nodes that send more packets. For example, the nodes situated at the network 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 payment schemes can also regulate packet transmission and discourage Message-Flooding attacks where the attackers send bogus messages to deplete the intermediate nodes' resources.

2. REPORT BASED PAYMENT

Moreover, since the communication sessions may be held without involving a trusted party and the nodes may roam among different foreign networks, the payment schemes can charge the nodes efficiently without contacting distant home location registers [6]. The existing credit card payment schemes are designed for different system and threat models, which are infeasible for MWNs. For example, in credit card payment schemes, each transaction usually has one customer

and one merchant, and the merchants' number is low and they are known before the transaction is held. For the payment schemes in MWNs, there is usually one customer (the source node) and multiple merchants (the intermediate nodes The relation between a customer and a merchant is usually short due to the network dynamic topology, and the nodes are involved in low-value trans-actions very frequently because once a route is broken, a new transaction should be done to re-establish the route. Due to these unique characteristics, MWNs require a specially designed payment scheme. Due to these unique characteristics, MWNs require a specially designed payment scheme. In this paper, we propose RACE, a Report-based pAyment sChemE for MWNs. The nodes submit lightweight payment reports (instead of receipts) to the AC to update their credit accounts, and temporarily store undeniable security tokens called Evidences. The reports contain the alleged charges and rewards of different sessions without security proofs, e.g., signatures. The AC verifies the payment by investigating the consistency of the reports, and clears the payment of the fair reports 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. In other words, the Evidences are used to resolve disputes when the nodes disagree about the payment. Instead of requesting the Evidences from all the nodes participating in the cheating reports, RACE can identify the cheating nodes with submitting and processing few Evidences. Moreover, Evidence aggregation technique is used to reduce the storage area of the Evidences.

In RACE, Evidences are submitted and the AC applies cryptographic operations to verify them only in case of cheating, but the nodes always submit security tokens, e.g., signatures, and the AC always applies cryptographic operations to verify the payment in the existing receipt-based schemes. RACE can clear the payment nearly without applying cryptographic operations and with submitting lightweight reports when Evidences are not frequently requested. Wide-spread cheating actions are not expected in civilian 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.

Our analytical and simulation results demonstrate that RACE requires much less communication and processing overhead than the existing receipt-based schemes with acceptable payment clearance delay and Evidences' storage area, which is necessary to make the practical implementation of the payment scheme effective. Moreover, RACE can secure the payment and precisely identify the cheating nodes without false accusations or stealing credits. To the best of our knowledge, RACE is the first payment scheme that can verify the payment by investigating the consistency of the nodes' reports without systematically submit- ting and processing security tokens and without false accusations. RACE is also the first scheme that uses the concept of Evidence to secure the payment and requires applying cryptographic operations in clearing the payment only in case of cheating. 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 This is because the source node is fully charged after sending a packet but some intermediate nodes may not be rewarded when the route is broken. 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 [12], 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 [11] uses statistical methods to identify the cheating nodes that submit incorrect payment. 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 [10], 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 [12] 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.

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, RACE aims to reduce the overhead of submitting the payment data to the AC and processing them. Although the communication protocol proposed in ESIP can be used with RACE, we use a simple protocol due to space limitation and to focus on our contributions.

A mechanism is proposed in [10] to thwart packet dropping attacks. Payment is used to thwart the rational packet-dropping attacks, and a reputation system is used to identify and evict the irrational packet dropping attackers once their packet- dropping rates exceed a threshold. In [9], Zhu et al. propose a payment scheme, called SMART, for delay tolerant wireless networks (DTNs). SMART uses layered coins and can secure the payment against a wide range of attacks such as Credit-Forgery, Nodular-Tontine, and Submission-Refusal. Lu et al. [2] propose a payment scheme for DTNs which focuses on the fairness issue. From false accusations, missed detections, and delay in identifying attackers, and it can thwart collusion attacks.

A mechanism is proposed in [8] to thwart packet dropping attacks. Payment is used to thwart the rational packet-dropping attacks, and a reputation system is used to identify and evict the irrational packet dropping attackers once their packet-dropping rates exceed a threshold. SMART uses layered coins and can secure the payment against a wide range of attacks such as Credit-Forgery, Nodular-Tontine, and Submission-Refusal. Propose a payment scheme for DTNs which focuses on the fairness issue. The intermediate nodes earn credits for for-warding the delivered messages and gain reputation for forwarding the undelivered messages which gives them preference in forwarding future messages. However, the payment schemes designed for DTNs may not be efficiently applicable to MWNs because DTNs lack fully connected end-to-end routes and tolerate long packet delivery delay.

2.1 Adversary Model

The mobile nodes are probable attackers but the TP is fully secure. The mobile nodes are autonomous and self interested and thus motivated to misbehave. The TP is run by an operator that is motivated to ensure proper operation. As discussed in [24], it is impossible to realize secure payment between two entities without a trusted third party. The attackers have full control on their nodes and can change their operation and infer the cryptographic data. The attackers can work individually or collude with each other under the control of one attacker to launch sophisticated attacks. If a node in the route does not receive a data or ACK packet within a time interval, the session is considered stale. The node A can estimate this interval as nA (cryptographic delay +transmission delay), where nA is the number of nodes between A and the source node for data packets, and the number of nodes between A and the destination node for ACK packets. The cryptographic delay is the maximum computation time required by a node to perform the cryptographic operations, and the transmission delay includes any other delays, such as the propagation, queuing, and channel contention delays.

Evidence even if the route is broken or the other nodes in the route collude to manipulate the payment. This is because it can verify the Evidences to avoid being fooled by the attackers. Reducing the storage area of the Evidences is important be-cause they should be stored until the AC clears the payment. Onion hashing technique can be used to aggregate Evidences. The underlying idea is that instead of storing one PROOF per session, one compact PROOF can be computed to prove the credibility of the payment of a group of sessions. The compact Evidence contains the concatenation of the DATAs of the individual Evidences and one compact PROOF that is computed by onion hashing the PROOFs of the individual Evidences. Let PROOF (i) refer to the PROOF of the Evidence number i, the compact PROOF is computed as follows:

H(…..,
H(H(PROOF(1), PROOF(2)), PROOF(3)),
… , PROOF(n))

PROOF (1) and PROOF (2) are concatenated and hashed, and then PROOF (3) is added to the compact PROOF by adding one hashing layer and so on. The compact PROOF has the same size of the PROOF of individual Evidence, but it can prove the credibility of the payment of multiple sessions. The onion hashing technique enables the nodes to aggregate recent Evidence with the old compact Evidence, i.e., Evidences are always stored in an aggregated form to reduce their storage area. The technique is called onion hashing because each aggregation operation requires adding one hashing layer.

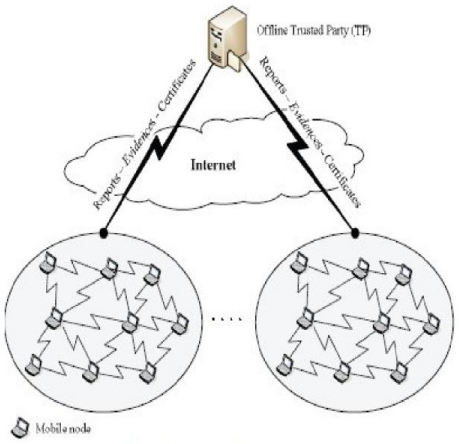

Fig. 1: The architecture of the considered network.

However, the Evidence aggregation process is irreversible because the hash function is unidirectional, i.e., the compact Evidence cannot be decomposed to individual Evidences. Thus, if the TP requests Evidence that is aggregated in the com-pact Evidence, the node has to submit the compact Evidence and the TP has to verify all the PROOFs of the sessions of the compact Evidence, instead of verifying only the PROOF of the requested Evidence. Therefore, aggregating more Evidences can further reduce their storage area, but with more communication and processing overhead if Evidence is requested. This is acceptable because Evidences are requested only in case of cheating and RACE requests the Evidences from few nodes instead of all the nodes in the cheating reports. The aggregation level can be

flexible and dependent on the available memory space.

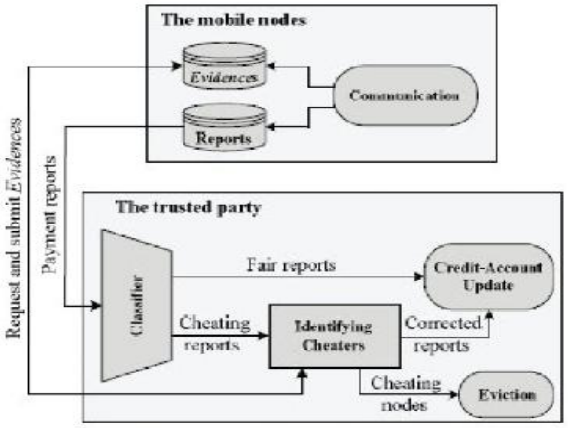

Fig. 2: The architecture of RACE.

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

```
1: // n_i is the source, intermediate, or destination node that is running the algorithm.
2: if (n_i is the source node) then
3:     P_X ← R, X, Ts, Mx, Sigs(R, X, Ts, H(Mx));
4:     Send(P_X);                    // send P_X to the first node in the route
5: else
6:     if ((R, X, Ts are correct) and Verify(Sigs(R, X, Ts, H(Mx)) == TRUE )) then
7:         if (n_i is an intermediate node) then
8:             Relay the packet;
9:             Store Sigs(R, X, Ts, H(M_X));
10:        end if
11:        if (n_i is the destination node) then
12:            Send(h^(X));
13:        end if
14:    else
15:        Drop the packet;
16:        Send error packet to the source node;
17:    end if
18: end if
19: if (P_X is last packet) then
20:    Evidence = {R, X, Ts, H(M_X), h^(0), h^(X), H(Sigs(R, X, Ts, H(Mx)), Sign(R, Ts, h^(0)))};
21:    Report = {R, Ts, F, X};
22:    Store Report and Evidence;
23: end if
```

payment report composition/submission: A payment re-port 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. it gives numerical examples for the payment reports of node A. For the first report, A is the source node and claims sending 12 messages, but it did not receive the ACK of the last message because F is zero.

For the second report, A is the destination node and claims receiving 17 messages. For the third report, A is an intermediate node and claims receiving 15 messages, but it did not receive the ACK of the last message. The submission of reports and Evidences are illustrated in Algorithm

$$f(T_i) = \frac{\lambda \cdot e^{-\lambda \cdot t}}{1 - e^{-\lambda \cdot T_{Cert}}} \quad (1)$$

$$P(T_i \le t) = \frac{1 - e^{-\lambda \cdot t}}{1 - e^{-\lambda \cdot T_{Cert}}} \quad (2)$$

$$P(T_i \le t) = \frac{t}{T_{Cert}} \quad (3)$$

$$P(T(n) \le t) = \prod_{i=1}^{i=n} P(T_i \le t) \quad (4)$$

$$f(T(n)) = e^{-\lambda \cdot t} \cdot \lambda \cdot n \cdot \frac{(1 - e^{-\lambda \cdot t})^{n-1}}{(1 - e^{-\lambda \cdot T_{Cert}})^n} \quad (5)$$

$$f(T(n)) = \frac{n}{T_{Cert}} \cdot \left(\frac{t}{T_{Cert}}\right)^{n-1} \quad (6)$$

$$E(T(n)) = \int_0^{T_{Cert}} t \cdot f(T(n))\, dt \quad (7)$$

$$P_C(n) = \frac{E(T(n))}{2} \quad (8)$$

$$E(T_i) = \frac{1}{\lambda} \cdot \left[\frac{1 - (\lambda \cdot T_{Cert} + 1) \cdot e^{-\lambda \cdot T_{Cert}}}{1 - e^{-\lambda \cdot T_{Cert}}}\right] \quad (9)$$

Algorithm 2: Submission/clearance of reports and Evidences

1: n_i Í TP: **Submit(**Reports[t_{i-1}, t_i]**)**;

2: TP Ín_i: ***Evidence*s_Request**(Ses_IDs[t_{i-2}, t_{i-1}]);

3: n_i Í TP: **Submit**(Req_Evs[t_{i-2}, t_{i-1}]);

4: TP: **Identify_Cheaters**();

5: TP: Clear the payment of the reports;

6: **if** (n_i is honest) **then**

7: TP Ín_i: A renewed certificate;

8: **endif**

3. CLASSIFIER

After receiving a session's payment reports, the AC verifies them by investigating the consistency of the reports, and classifies them into fair or cheating. For fair reports, the nodes submit correct payment reports, but for cheating reports, at least one node does not submit the reports or submits incorrect re-ports, e.g., 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 X 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 achieve one of the aforementioned rules. It gives numerical examples for fair reports. Case 1 is reports for complete session and Cases 2 to 4 are reports for broken sessions. For Case 1, all the nodes report the same number of messages and F of one. For Case 2, the session was broken during relaying the ACK packet number 11 and B is the last node that received the packet. For Case 3, the session was broken during relaying the data packet number 8 and node A is the last node that received the packet. For Case 4, the session was broken during relaying the first data packet, and node B is the last node that received the packet, and therefore nodes C and D did not submit the payment report of session.

3.1 Identifying Cheaters

As shown in Fig. 2, in the Identifying Cheaters' phase, the TP processes the cheating reports to identify the cheating nodes and correct the financial data. Our objective of securing the payment is preventing the attackers (singular of collusive) 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 (signatures and hash chain elements) for identifying the cheating node(s). In this way, the AC can precisely identify the cheating nodes with requesting few Evidences. Numerical examples will be given in Section 5 to clarify how cheating nodes can be identified without false accusations. To verify an 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 However, the nodes submit the reports at different times be-cause the connection to the TP may not be available on a regular basis, and thus the duration between each two submissions may not be the same and may be less than or equal to TCert. Hence, the maximum payment clearance delay may be less than TCert. Ti is a continuous random variable that denotes the time duration between two submissions for a node, where $T_i \in$

3.2 Credit-Account Update

As shown in Fig. 2, the Credit-Account Update phase receives fair and corrected payment reports to update the nodes' credit accounts. The payment reports are cleared using the charging and rewarding policy discussed in Section 3. 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 re- ports of all nodes in a route to verify the payment. The maxi- mum 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. It is worth to note that the maximum time duration for a node's two consecutive contacts with the TP is TCert to renew its certificate to be able to use the net- work held in [t0, t1). The figure also shows that the maximum time for storing an Evidence is 2¯TCert, e.g., for the reports of sessions held shortly after t0. At t2, the nodes delete the Evidences of the sessions held in [t0, t1) because the AC must have cleared their reports

4. PAYMENT PROCESSING OVERHEAD

Tables 9 and 10 give the processing overhead for clearing the payment of ten-minute data transmission at different node speed in terms of the number of cryptographic operations, the total energy cost, and the processing time, assuming that the AC is a laptop with an Intel processor at 1.2GHZ and 1GB RAM. The tables indicate that RACE does not need any cryptographic operations for clearing the payment in case of fair reports. The tables also give the overhead of verifying an Evidence with X messages. The simulation results indicate that the payment clearance overhead of RACE is much less than the existing receipt-based payment schemes. It can also be seen that more overhead is required at high node mobility because more receipts are generated due to breaking the routes more frequently, which shows that receipt-based payment schemes may not be efficiently applicable in case of high node mobility, but the nodes' speed has no effect on the payment clearance overhead in RACE if the reports are fair.

The low payment processing overhead can reduce the complexity and provide flexibility to the practical implementation of the AC. Moreover, since the payment schemes use micro- payment, the overhead cost should be much less than the payment for the effective implementation of these schemes. The communication and processing overhead of the receipts will be very large with taking into account the following facts: (1) the simulation results given in Tables 8, 9, and 10 are only for ten- minute data transmission; (2) the nodes may contact the TP once every few days because this connection may not be avail- able on a regular basis and to

reduce the communication over- head; and (3) once a route is broken, a new route is established with a new receipt, and thus multiple receipts may be generated per session.

RACE can significantly reduce the overhead of submitting the payment reports and clear the payment with almost no cryptographic operations or processing overhead when cheating actions are infrequent. Widespread cheating is not expected in civilian applications because the common users do not have the technical knowledge to tamper with their devices and the manufacturing companies (which are limited) cannot sacrifice their reputation and face liability for making tampered devices. Moreover, a cheating node is evicted once it commits one cheating action, and changing identity is not easy or cheap, e.g., the TP can impose fees for issuing new certificates.

CONCLUSION AND FUTURE WORK

In this paper, we have proposed RACE, a report-based payment scheme for MWNs. The nodes submit lightweight payment reports containing the alleged charges and rewards (with-out proofs), and temporarily store undeniable security tokens called Evidences. The fair reports can be cleared with almost no cryptographic operations or processing overhead, and Evidences are submitted and processed only in case of cheating reports in order to identify the cheating nodes. Our analytical and simulation results demonstrate that RACE can significantly reduce the communication and processing overhead comparing to the existing receipt-based payment schemes with acceptable payment clearance delay and Evidences' storage area, which is necessary for the effective implementation of the scheme. Moreover, RACE can secure the payment, and identify the cheating nodes precisely and rapidly without false accusations or missed detections.

In RACE, the AC can process the payment reports to know the number of relayed/dropped messages by each node. In our future work, we will develop a trust system based on processing the payment reports to maintain a trust value for each node. The nodes that relay messages more successfully will have higher trust values, such as the low-mobility and the large-hardware-resources nodes. Based on these trust values, we will propose a trust-based routing protocol to route messages through the highly trusted nodes (which performed packet relay more successfully in the past) to minimize the probability of dropping the messages ,and thus improve the network performance in terms of throughput and packet delivery ratio. However, the trust system should be secure against singular and collusive attacks, and the routing protocol should make smart decisions regarding node selection with low overhead.

REFERENCES

[1] G. Shen, J. Liu, D. Wang, J. Wang, and S. Jin, "Multi-hop relay for next-generation wireless access networks", Bell Labs Technical Journal, vol. 13, no. 4, pp. 175-193, 2009.

[2] C. Chou, D. Wei, C. Kuo, and K.Naik,"Anefficientanonymouscommunication protocol for peer-to-peer applications over mobile ad-hoc networks", IEEE Journal on selected areas in communications, vol. 25, no. 1, January 2007.

[3] H. Gharavi, "Multichannel mobile ad hoc links for multimedia communications", Proc. of the IEEE, vol. 96, no. 1, pp. 77-96, January 2008.S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks", Proc. of ACM Mobile Computing and Networking (MobiCom'00), pp. 255–265.

[4]. Boston, Massa- chusetts, USA, August 6-11, 2000.

[5]G. Marias, P. Georgiadis, D. Flitzanis, and K. Mandalas, "Cooperation enforcement schemes for MANETs: A survey", Wiley's Journal of Wireless Communications and Mobile Computing, vol. 6, issue 3, pp. 319–332, 2006.

[6] R. Lu, X. Lin, H. Zhu, X. Shen, and B. R. Preiss, "Pi: A practical incentive protocol for delay tolerant networks", IEEE Transactions on Wireless Communications (IEEE TWC), vol. 9, no. 4, pp. 1483-1493, 2010.

[7] B. Wehbi, A. Laouiti, and A. Cavalli, "Efficient time synchronization mechanism for wireless multi hop networks", Proc. of IEEE Personal, Indoor and Mobile Radio Communications (PIMRC),2008

[8] D. Johnson and D. Maltz, "Dynamic source routing in ad hoc wire- less networks", Mobile Computing, Chapter 5, Kluwer Academic Publishers, pp. 153-181, 1996.

[9]. A. Weyland, "Cooperation and accounting in multi-hop cellular networks", Ph.D. thesis, University of Bern, November 2005.

[10]. A. Weyland, T. Staub, and T. Braun, "Comparison of motivation- based cooperation mechanisms for hybrid wireless networks", Journal of Computer Communications, vol. 29, pp. 2661–2670, 2006.

[11] M. Mahmoud and X. Shen, "FESCIM: Fair, efficient, and secure cooperation incentive mechanism for hybrid ad hoc networks", IEEE Transactions on Mobile Computing (IEEE TMC), to appear.

[12] M. Mahmoud, and X. Shen, "PIS: A practical incentive system for multi-hop wireless networks", IEEE Transactions on Vehicular Technology (IEEE TVT), vol. 59, no. 8, pp. 4012-4025, 2010.