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

Payment Scheme for Identifying Cheating Reports in Multihop Wireless Networks

Ms.T.Thenmozhi, Mr.Arunkumar\

PG Scholar, Karpagam University, Coimbatore, Tamilnadu, India[1]

Assistant Professor, Department of CSE, Karpagam University, Coimbatore, Tamilnadu, India[2]

ABSTRACT: A Report based payment scheme for multihop wireless network enforces the report fairness and node cooperation. The node submits the report for packet transmission to the accounting centre. Report contains evidences for ensuring the correctness of data's. The AC can verify the payment report by investigating the evidences that are containing the signature of the node and clear the accounting report by evicting the cheating report. RACE can easily identify the cheating report by requesting evidences.Fair reports are updated into the credit account. 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 RACE can secure the payment and precisely identify the cheating nodes without false accusations.

KEYWORDS: Accounting centre (AC), Evidences (PROOF), Trusted Party (TP), RACE (Report based payment scheme).

I. 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. 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 and multimedia data transmission. 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. In multihop networks such as mobile ad hoc networks selfish or misbehaving nodes can disrupt the whole network and severely degrade network performance. Reputation, or trust based models are one of the most promising approaches to enforce cooperation and discourage node misbehaviour. Reputation is calculated through direct interactions with the nodes and/or indirect information collected from neighbours. Reputation is evolved on each node through monitoring or observing its direct interactions and a node can trust its direct information more than the indirect information.

1.1 Micropayment scheme

Payment (or incentive) schemes use credits (or micropayment) 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

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

messages to deplete the intermediate nodes' resources. Moreover, since the communication sessions may be held without involving a trusted party (TP) and the nodes may roam among different foreign networks, the payment schemes can charge the nodes efficiently without contacting distant home location registers.

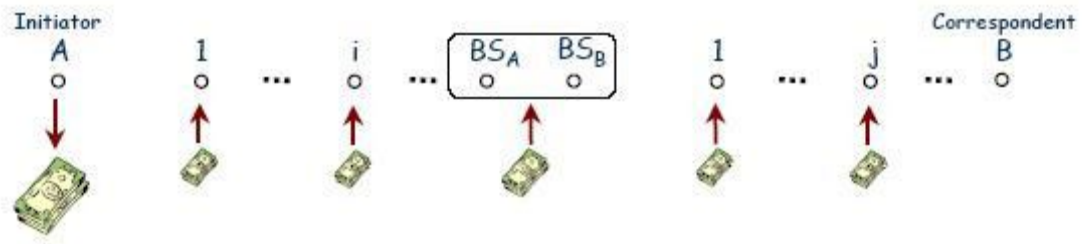

Figure 1-Micropayment Mechanism

1.2 Systematic Micropayment scheme

For every packet, the initiator is charged and all relay nodes are rewarded. Strength : all cheating attempts will be detected.

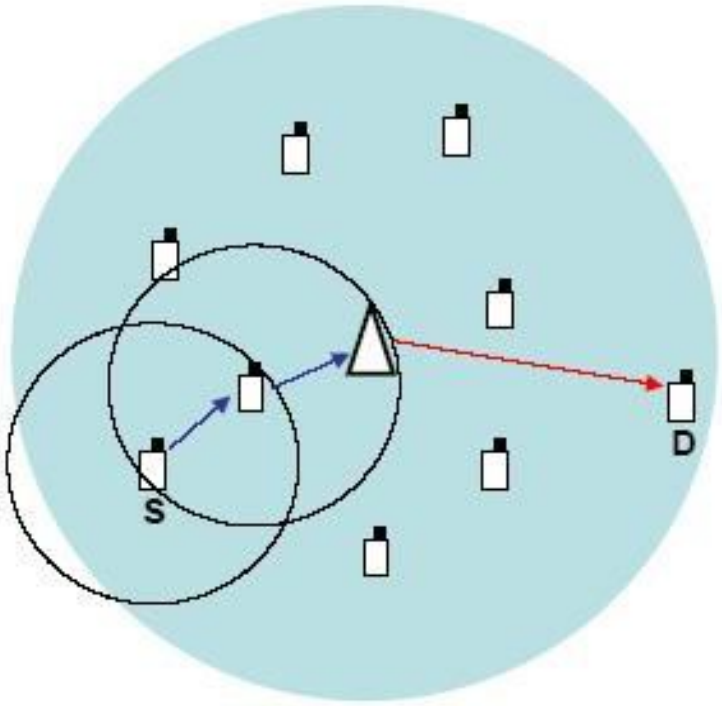

Figure 3.Micropayment path selection

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

II. SYSTEM DESIGN

2.1 Network Model

For military and disaster recovery applications, the network can be considered ephemeral because it is used for a specific purpose and short duration. In this paper, we adopt the network model used in that targets the civilian applications of MWNs, where the network has long life and the nodes have long-term relations with the network. The TP contains the AC and the certificate authority (CA). The AC maintains the nodes' credit accounts and the CA renews and revokes the nodes' certificates. Each node A has to register with the trusted party to receive a symmetric key KA, private/public key pair, and certificate. The symmetric key is used to submit the payment reports and the private/public keys are required to act as source or destination node. We assume that the clocks of the nodes are synchronized. The details of this synchronization process are out of the scope of the paper, but several mechanisms have been proposed to synchronize the nodes'clocks . Once the AC receives the payment reports of a session and verifies them, it clears the payment if the reports are fair; else, it requests the Evidences to identify the cheating nodes. The CA evicts the cheating nodes by denying renewing their certificates.

III. IMPLEMENTATION

3.1Proposed Race

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.

RACE can be used with any source routing protocol, such as DSR , which establishes end-to-end routes before transmitting data. Source nodes' packets may be relayed several hops by intermediate nodes to their destinations. The nodes can contact the TP at least once during a period of few days.

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 receiptbased schemes. RACE can clear the payment nearly without applying cryptographic operations and with submitting lightweight reports when Evidences are not frequently requested. 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.

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

3.2 Race Architecture

RACE 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 nodes accumulate the payment reports and submit them in batch to the TP. For the Classifier phase, the TP classifies the reports into fair and cheating. For the Identifying Cheaters phase, the TP requests the Evidences from the nodes that are involved in cheating reports to identify the cheating nodes. The cheating nodes are evicted and the payment reports are corrected. Finally, in Credit-Account Update phase, the AC clears the payment reports.

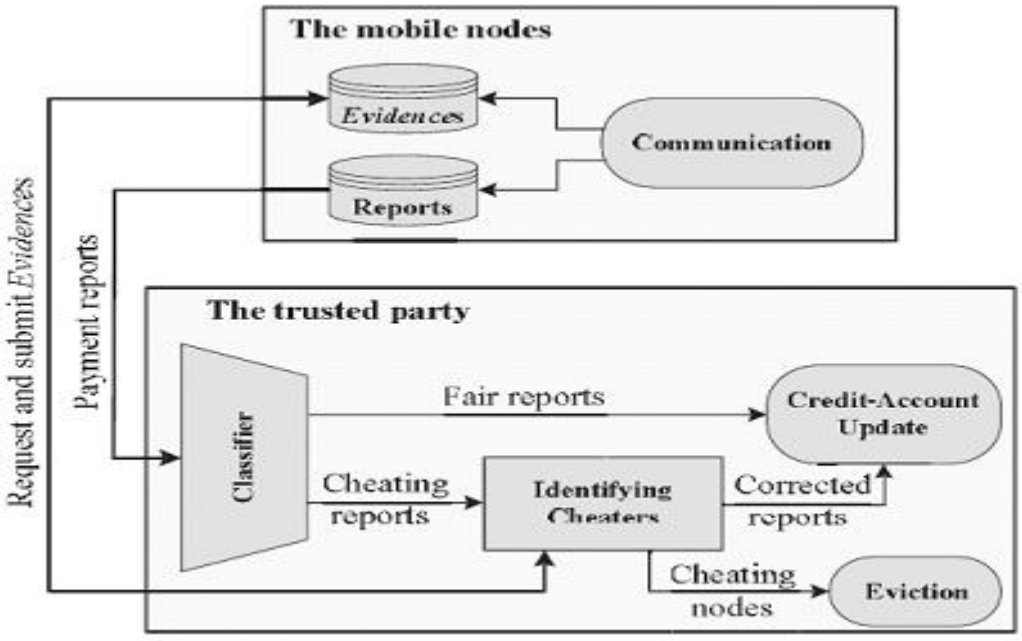

Figure 3.RACE Structure

3.2.1 communication

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

Route establishment: In order to establish an end-to-end route, the source node broadcasts the Route Request (RREQ) packet containing the identities of the source (IDS) and the destination (IDD) nodes, time stamp (Ts), and Time-To-Live (TTL). TTL is the maximum number of intermediate nodes. After a node receives the RREQ packet, it appends its identity and broadcasts the packet if the number of intermediate nodes is fewer than TTL. The destination node composes the Route Reply (RREP) packet for the nodes broadcasted the first received RREQ packet, and sends the packet back to the source node.

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

Data transmission: The source node sends data packets to the destination node through the established route and the destination node replies with ACK packets. For the Xth data packet, the source node appends the message MX and its signature to R, X, Ts, and the hash value of the message (H(M(X)) and sends the packet to the first node in the route.

Evidence composition: Evidence is defined as information that is used to establish proof about the occurrence of an event or action, the time of occurrence, the parties involved in the event, and the outcome of the event. The purpose of an Evidence is to resolve a dispute about the amount of the payment resulted from data transmission. Fig. 4 gives the general format of an Evidence. The figure shows that an 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. 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(X) the hash value of the last message (H(M(X)), The PROOF is an undeniable security token that can prove the correctness of the DATA .

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. 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.

3.2.2Classifier phase
The Trusted Party 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 reports, e.g., to steal credits or pay less. Fair reports can be for complete or broken sessions.

3.2.3 Identifying Cheaters phase
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. 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. To verify an Evidence, the TP composes the PROOF by generating the nodes‟ signatures and hashing them.

3.2.4 Credit Account phase
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 and get the payment correctly. Upon registration the trusted party will give A Public & 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.

IV. CONCLUSION

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 (without 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

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

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.

V. FUTURE ENHANCEMENT

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.

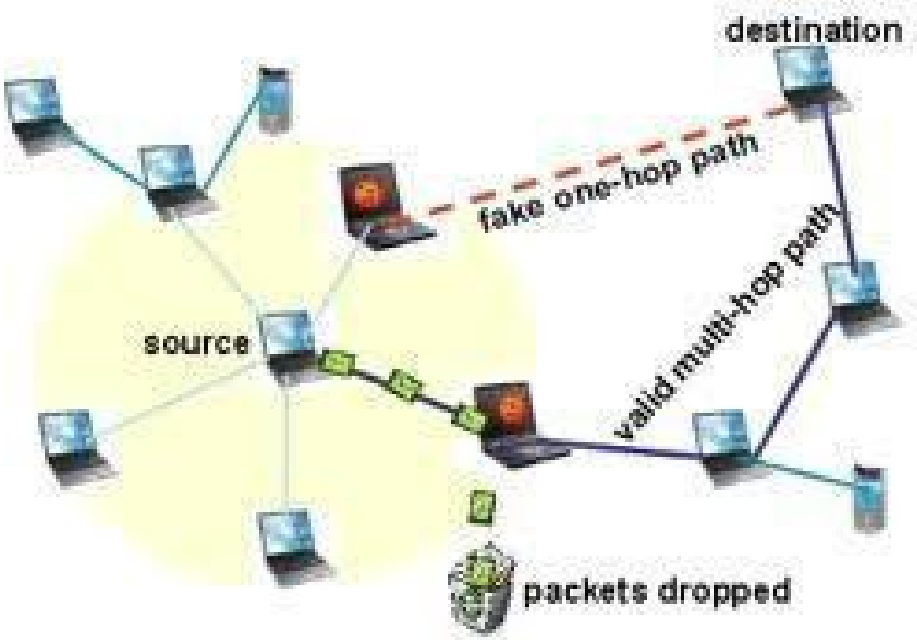

Figure 4.Identifying fake path

REFERENCES

1. Buttyan, L. and Hubaux, J.(2004) 'Stimulating Cooperation in Self- Organizing Mobile Ad Hoc Networks', Mobile Networks and Applications, Oct vol. 8, no. 5, pp. 579-592.
2. Gharavi, H.(2008) 'Multichannel Mobile Ad Hoc Links for Multimedia Communications' Proc. IEEE, vol. 96, no. 1, pp. 77-96.
3. Marti, S. T. Giuli, T. K. Lai, K. and M. Baker, M. (2000).'Mitigating Routing Misbehavior in Mobile Ad Hoc Networks'Proc. MobiCom '00,Aug pp. 255-265.

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

4. Marias, G. Georgiadis, P. Flitzanis, D. and Mandalas, K.(2006). 'Cooperation Enforcement Schemes for MANETs: A Survey'
5. Mahmoud, M. and Shen, X. "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.
6. Mahmoud, M.and Shen,X. "PIS: A Practical Incentive System for Multi-Hop Wireless Networks," IEEE Trans. Vehicular Technology, vol. 59, no. 8, pp. 4012-4025, Oct. 2010.
7. Shen, G. Liu, J.. Wang, J. Wang, and S. Jin,(2009)Multi-Hop Relay for Next- Generation Wireless Access Networks," Bell Labs Technical J.. 13, no. 4, pp. 175-193, 2009.
8. 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 Comm., Jan .vol. 25, no. 1, pp. 192-203.
9. Wiley's J. Wireless Comm. and Mobile Computing, vol. 6, no. 3,pp. 319-332, 2006.
10. Zhang, Y. and Fang, Y.(2007) 'A Secure Authentication and Billing Architecture for Wireless Mesh Networks' ACM Wireless Networks, Oct vol. 13, no. 5, pp. 663-678
11. Zhang, Y. W. Lou, W. and Y. Fang, Y. (2007), 'A Secure Incentive Protocol for Mobile Ad Hoc Networks' ACM Wireless Networks, Oct. vol. 13, no. 5,pp. 569- 582, Oct. 2007.
12. Weyland, A. (2005) 'Cooperation and Accounting in Multi-Hop Cellular Networks' PhD thesis, Nov, Univ. of Bern.