International Journal of Modern Engineering Research (IJMER)
www.ijmer.com Pp-87-91 ISSN: 2249-6645

Reducing the Communication and Processing Overhead and Ensuring the Security in Multihop Wireless Networks - using RACE Mechanism

P.Visalakshi[1], R. Dineshbabu[2] and K. Vijayalakshmi[3]
[1,2]SRM University, MCA Department, Kattankulathur, Kanchipuram, India
[3]St. Peter's University, Department of Computer Science & Engineering, Avadi, Chennai, India

Abstract: *A secure payment scheme, called as the Report based pAyment sChemE(RACE) is used in multi hop wireless networks to stimulate node cooperation, regulate packet transmission and enforce fairness. The nodes submit lightweight payment reports (instead of receipts) to the Trusted Authority to update their credit accounts and temporarily store the evidences. The report includes the session information. The Trusted Party verifies the payment by investigating the consistency of the report and clears the fair reports with almost no cryptographic operations or computational overhead. The nodes which do not pass or relay others' packets are called selfish nodes. But it makes use of neighbor or cooperative nodes to relay its packets. This degrades the network connectivity and fairness. Such type of nodes also submits reports to the trusted party. But when tested for consistency, it is found to be a cheating node. For such reports, the evidences are requested from the Trusted Party to identify and evict the cheating nodes or selfish nodes. RACE is the first payment scheme that uses the concept of evidences to secure the payments. It requires cryptographic operations in clearing the payment only in the case of cheating. Also this is the first system that can verify the payment by investigating the consistency of the node's reports without submitting and processing security tokens and without false accusations. To prevent the multi hop communications from failing due to insufficient credits, the source node can borrow credits from the Trusted Authority. After evicting the selfish nodes, communication can be efficiently established again with increased throughput and less amount of processing and communication overhead. This is done by establishing a route between the source and the destination by sending a route request to the destination and the destination replies with path, a hash element from the hash chain and the signature. All these details are provided by the Trusted Party.*

Keywords: *TP (Trusted Party) , AC (Accounting Center) , payment schemes, RACE(Report based pAyment sChemE) , RREQ (Route REQuest) , RREP (Route REPly)*

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 Multihop Wireless Networks

My first research direction aims to develop a suite of efficient security mechanisms and protocols for mobile ad-hoc and multihop cellular networks. Specifically, we focus on thwarting packet-dropping and selfishness attacks, preserving user privacy, and establishing stable communication routes to minimize the probability of breaking the route, thus boosting the network performance in terms of endto- end packet delay, packet delivery ratio, throughput, etc.

1.1.1 Efficient and Secure Credit-Based Incentive Mechanism

In mobile ad hoc and multihop cellular networks, the mobile nodes should relay others' packets for enabling new applications and enhancing the networks' deployment and performance. However, selfish nodes do not relay others' packets, because it consumes their resources without benefits and makes use of the cooperative nodes to relay their packets, which has a negative impact on the network fairness and may cause multihop communications to fail.

We develop a secure and efficient credit-based incentive mechanism that uses credits (or micropayment) to charge the nodes that send packets, and to reward those relaying packets. This mechanism can stimulate the selfish nodes to relay packets to earn credits, enforce fairness by rewarding credits to the nodes that relay more packets, and discourage packet-flooding attacks by charging the nodes that send packets. Since a trusted party may not be involved in the communication sessions, the nodes compose digital payment receipts, or undeniable proofs of relaying packets, and submit them to a trusted party to update their credit accounts. However, in order to make practical implementation possible, the payment should be

secured with low overhead because the nodes have limited resources.

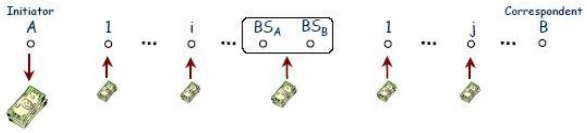

Figure 1 Payment mechanism – Micro payments

1.2 Systematic micro-payments
Principle : for every packet, the initiator is charged and all relay nodes are rewarded.
Strength : all cheating attempts will be detected.
Weakness : Overhead (increase of the communication cost)

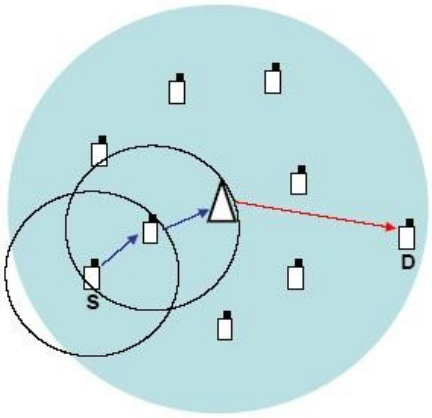

Figure 2 A Micro-Payment Scheme Encouraging

Collaboration in Multi-hop Cellular Networks (Multi-hop
Up-link, Single-hop Down-link)

II. SYSTEM DESIGN

In multihop networks such as mobile ad hoc networks selfish or misbehaving nodes can disrupt the wholenetwork 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.

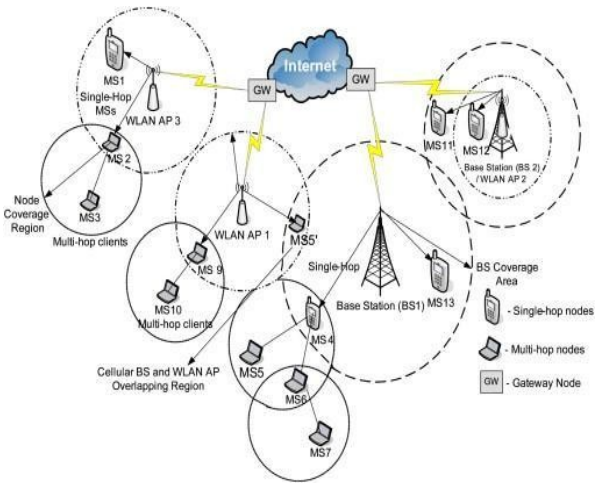

Figure 3 A logical Multihop wireless network architecture

This system consists of *: Multi-hop network establishment, Registration, path finding and communication, RACE mechanism.*

2.1 Multi-hop network establishment

In this first module, we have to establish the multi-hop wireless network. These nodes are used to communicate with each other directly or through the neighbor nodes. If one node send the message 'Hello' means, first of all this message is received by the neighboring node. There after it will check whether the destination is neighbor or not. If destination is found the message is send or else it is forwarded to the next intermediate node.

2.2 Registration, path finding and communication

In this module every node that is created has to be registered with a Trusted Party in order to communicate effectively and to Evidence is valid if the computed PROOF is similar to the Evidence's PROOF. 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.

The Trusted Party will keep Account details of every node. After that for the communication process the source will send a Route request to the destination. Packet containing the identities of the source (IDS) and the destination (IDD) nodes, time stamp (Ts), and Time-To-Live(TTL) or the maximum number of intermediate nodes. After a node receives the RREQ packet, it appends its identity and broadcasts the packet. The destination will reply with a Route reply that means the route reply contains the path. The destination node generates a hash chain by iteratively hashing a random value (h (K)) K times to produce the hash chain root (h(0)). The RREP packet contains the identities of the nodes in the route (e.g., R = IDS, IDA, IDB, IDD in the route h (0), and the destination node's certificate and signature (SigD(R, Ts, h(0))). This signature authenticates the hash chain and links it to the route. The intermediate nodes verify the destination node's signature, relay the RREP packet, and store the signature and h (0) for composing the Evidence through that path we send the data.

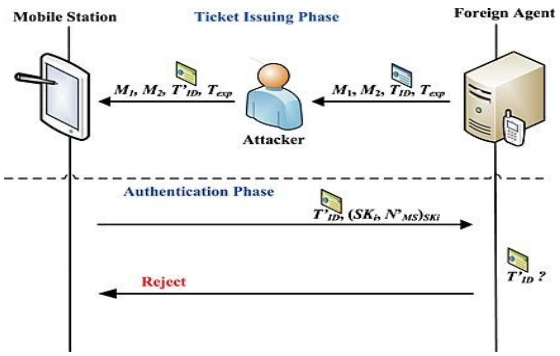

Figure 4 Ticket issuing and Authentication

2.3 RACE mechanism.

In the data communication process every node will temporarily store the reports and evidences. After a session every node will submits the reports to the trusted party. Reports include the session IDs,A flag bit representing the last packet sent is whether Data or Acknowledgment and X (the number of packets that is transmitted).Report=R,F,X. The Classifier part in the trusted party will check the reports and find the suspected reports. Then the trusted party will ask the suspected node to submit the evidence through a Evidence request.The Evidence = {R, X, Ts, H (MX), h (0), h(X), H (SigS(R, X, Ts,H(MX)), SigD(R, Ts, h(0)))}; Upon getting the request the node will submit the Evidence that it is temporarily stored. The Identifying cheaters part of the trusted party will then verify the Evidence and if the node found to be culprit then that node will be evicted from the network by the trusted party. And according to the payment scheme the nodes will get the payment for the data they are passed. The amount is deducted from the source nodes account and credited in intermediate nodes that are in the path. Evidences are undeniable, unforgettable and un- modifiable. The source node cannot deny initiating a session and the amount of payment because its signature is included in the Evidence. Moreover, it is also impossible to modify the source nodes' signatures, compute the private keys from the public ones, and compute the hash value of the signatures without computing the signatures. Instead of Tokens, here we using the Evidence mechanism and also the storage area of the evidences is low and without false accusations. Hence we can reduce the communication and processing overhead.

III. IMPLEMENTATION

Multihop wireless networks (MWNs), or the next-generation wireless networks, can significantly improve network performance and deployment and help implement many novel applications and services. However, when compared to wired and single-hop wireless networks, MWNs are highly vulnerable to serious security threats because packets may be relayed through integrated networks and autonomous devices. My research has been focusing on developing security protocols for securing MWNs. Specifically, we are interested in securing route establishment and data transmission processes, establishing stable routes, and preserving users' anonymity and location privacy.

Therefore the attempt is to reduce the communication and processing overhead and ensuring the security in Multihop Wireless Networks using the RACE Mechanism.
The RACE Mechanism consists of four main phases:
Communication phase, Classifier phase, Identifying Cheaters phase, Credit Account phase.

3.1 Communication phase

The Communication phase has four processes: route establishment, data transmission, evidence composition, payment report composition/submission. Route establishment is done 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. The destination node creates a hash chain by iteratively hashing a random value K times to produce the hash chain root. The optimal value of K depends on many factors such as the number of messages the source node needs to send, and the average number of messages sent through a route before it is broken, i.e., due to node mobility. Estimating a good value for K can save the destination node's resources because once a route is broken, the unused hash values in the hash chain should not be used for another route to secure the payment. The nodes can estimate the value of K and periodically tune it. The RREP packet contains the identities of the nodes in the route. The signature authenticates the hash chain and links it to the route. The intermediate nodes verify the destination node's signature, relay the RREP packet, and store the signature and H(Mx) for composing the Evidence.

Evidences have the following main features:

- Evidences are unmodifiable.
- If the source and destination nodes collude, they can create Evidences for any number of messages because they can compute the necessary security tokens.
- Evidences are unforgeable: If the source and destination nodes collude, they can create Evidence for sessions that did not happen, but the intermediate nodes cannot, because forging the source and destination nodes' signatures is infeasible.
- Evidences are undeniable: This is necessary to enable the TP to verify them to secure the payment. A source node cannot deny initiating a session or the amount of payment because it signs the number of transmitted messages and the signature is included in the Evidence.
- An honest intermediate node can always compose valid 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 because 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.

3.2 Classifier 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.

3.3 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.

3.4 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 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.

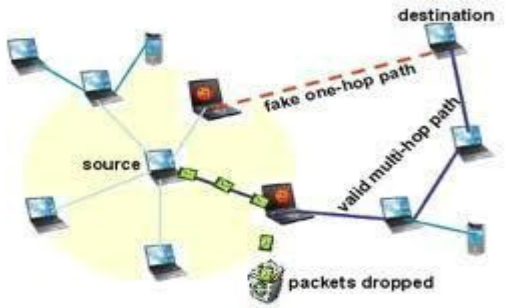

Figure 5 Identifying the fake path.

References

[1] Mahmoud And Shen: A Secure Payment Scheme With Low Communication And Processing Overhead For Multihop wireless networks., IEEE Transactions On Parallel And Distributed Systems, Vol. 24,No. 2, pp. 209-224, February 2013.

[2] G. Shen, J. Liu, D. Wang, J. Wang, and S. Jin, "Multi-Hop Relay for Next-Generation Wireless Access Networks," Bell Labs Technical J., vol. 13, no. 4, pp. 175-193, 2009.

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

[4] H. Gharavi, "Multichannel Mobile Ad Hoc Links for Multimedia Communications," Proc. IEEE, vol. 96, no. 1, pp. 77-96, Jan. 2008.

[5] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. MobiCom '00, pp. 255-265, Aug. 2000.

[6] 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.

[7] Y. Zhang and Y. Fang, "A Secure Authentication and Billing Architecture for Wireless Mesh Networks," ACM Wireless Networks, vol. 13, no. 5, pp. 663-678, Oct. 2007.

[8] 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.

[9] 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.

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

[11] 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.

[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] 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.

[14] 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.

[15] M. Mahmoud and X. Shen, "Stimulating Cooperation in Multihop Wireless Networks Using Cheating Detection System," Proc. IEEE INFOCOM '10, Mar. 2010.

[16] 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.

[17] 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.

[18] 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.