IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 2, Issue 2, Apr-May, 2014
ISSN: 2320 – 8791 (Impact Factor: 1.479)
www.ijreat.org

RACE for Multihop Wireless Networks

Suganya.S[1], Janani.S[2]

[1]PG Scholar, Department of Computer Science and Engineering, SreeSastha Institute of Engineering and Technology

[2]Assistant Professor, Department of Computer Science and Engineering, SreeSastha Institute of Engineering and Technology

Abstract

In this project is to develop an efficient secure payment system with reduced communication and processing overhead in multihop wireless networks (MWN) using mechanism called RACE. In RACE to increase the efficiency of the system by reducing the communication overhead and processing overhead that is incurred in the existing system and also to reduce the storage area required by the communication process and also to secure the payment. In the data sending process every node will temporarily store the evidences and report and submit the reports of a session to the trusted authority. Classifier classifies each report and verifies them to fair or unfair reports, after checking the unfair reports the trusted party requested evidence to the particular node the identifying cheater module find a node weather it is a cheater node or not. Cheater nodes are evicted from the network and the good nodes get their account updated. then 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.

Keywords: *Report, Evidence, Classifier, Communication overhead , Processing overhead, Trusted Authority, False accusation.*

I.Introduction

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.In multihop wireless networks (MWNs), the traffic isoriginated from a node is usually relayed through the other nodes to the destination for enabling newapplications and enhancing the network performanceand deployment (1). MWNs can be deployed readily at low cost in developing and rural areas.

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 end-to- end packet delay, packet delivery ratio, throughput, etc.

In RACE to increase the efficiency of the system by reducing the communication overhead and processing overhead that is incurred in the existing system and also to reduce the storage area required by the communication process and also to secure the that payment of the data communication in a Multihop Wireless Network. In this system every node has to be register first with the trusted Authority to get the public and private key, a certificate, and a symmetric key. Then a route is established between the source and the destination by sending a route request to the destination and the destination reply with path, a hash element from the hash chain and the signature generated by the destination, the signature and the hash value. The intermediate nodes store those values for the calculation of evidences.

In the data sending process every node will temporarily store the evidences and reports and submit the reports of a session to the trusted authority.The nodes submit lightweight payment report (instead of receipts) to the Trusted Authority to update their credit accounts and temporarily store the evidences. Trusted party includes many parts such as a classifier, An Identifying cheater module, an account update, and an eviction part.

Classifier verifies each report and classifies them to fair or unfair reports after checking the unfair reports the trusted party request evidences to the particular node the identifying cheater module find a node whether it is a cheater node or not. Cheater nodes are evicted from the network and the good nodes get their account updated. Payment schemes [5] 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 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 neighbour. 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.

In RACE, the AC can process the payment reports to know the number of relayed/dropped messages by each node then 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 ,then will develop 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.

II. Related Work

In existing system the payment scheme they are using is a receipt based payment scheme for securing the payment and the data. Since the receipt submission has to be done gradually, the communication and processing overhead will be there. The existing payment systems are designed for different system and threat models, which makes using them in MWNs infeasible.For receipt-based payment schemes [1], [2], [3], [4], [5], [6], [7], [8],[9], an offline central unit called the accounting center stores and manages the nodes' credit accounts. The nodes usually submit undeniable proofs for relaying packets called receipts, to the AC to update their credit accounts.

ESIP [2] 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 nonrepudiation 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.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.

In [14], 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. [15] propose a payment scheme for DTNs which focuses on the fairness issue. The intermediate nodes earn credits for forwarding 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.

Moreover, RACE requires much less communication and processing overhead comparing to receipt-based schemes [1], [2], [3], [7], yet with more and acceptable storage area and payment clearance delay.

III System Design

3.1Multi-hop Network Establishment:

In RACE to establish the multi-hop wireless network. These nodes are used to communicating 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 neighbor node. There after it will check whether the destination is neighbor or not. If destination is found the message is send or forward to the next intermediate node.

3.2Registration, 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 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.

3.3 The 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. *Evidence*s 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. Thenwe 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.

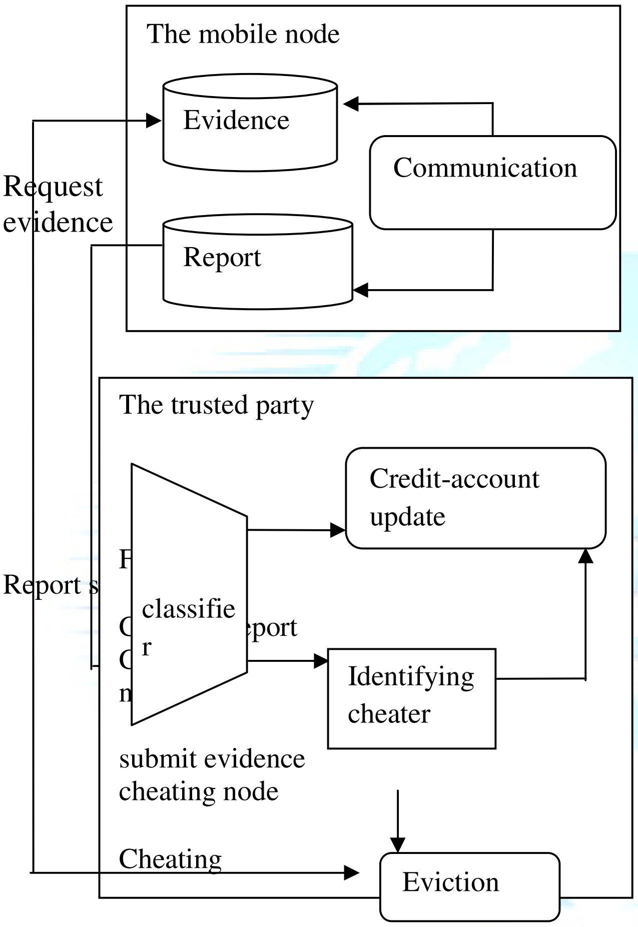

Fig. 1. The architecture of RACE.

IV. Implementation

My research has been focusing on developing security protocols for securing MWNs. Specifically, we interested in securing route establishment and data transmission processes, establishing stable routes, and preserving users anonymity and location privacy. Therefore the attempt is reduce the communication and processing overhead and ensuring the security in Multihop Wireless Networks using the RACE Mechanism. The RACE Mechanism consists four main phases: Communication phase, Classifier phase, Identifying Cheaters phase, Credit Account phase.

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 nodes 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 nodes 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.

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.

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.

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.

V. Conclusion

In the system we are using RACE (Report based payment Scheme) to secure the payment and also to reduce the communication and processing overhead.The nodes submit lightweight payment report (instead of receipts) to the Trusted Authority to update their credit accounts and temporarily store the evidences.The nodes submit the reports that include the session information to the trusted party.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.For cheating reports the evidences are requested to identify and evict the cheating nodes that submit incorrect details about the sessions.Race is the first payment scheme that uses the concept of evidences to secure the payment and requires cryptographic operations in clearing the payment only in the case of cheating and also this is the first system that can verify the payment by investigating the consistency of the nodes reports without submitting and processing security tokens and without false accusations.

VI. Future Work

In RACE, the AC can process the payment reports to know the number of relayed/dropped messages by each node. 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] M Mohamed and X. Shen, "A Secure Payment Scheme with Low Communication and Processing Overhead for Multihop Wireless Networks,"IEEE Trans on Parallel and Distributed System,vol.24, no.2, Feb 2013.

[2] 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.

[3] 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.

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

[5] 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.

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

[7] 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.

[8] 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.

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

[10] 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.

[11] H. Zhu, X. Lin, R. Lu, Y. Fan, and X. Shen, "SMART: A Secure Multilayer Credit Based Incentive Scheme for Delay-Tolerant Networks," IEEE Trans. Vehicular Technology, vol. 58, no. 8, pp. 4628-4639, Oct. 2009.

[12] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. MobiCom , pp. 255-265, Aug. 2000.

[13] 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.

[14] R. Lu, X. Lin, H. Zhu, X. Shen, and B.R. Preiss, "Pi: A PracticalIncentive Protocol for Delay Tolerant Networks," IEEE Trans.Wireless Comm., vol. 9, no. 4, pp. 1483-1493, Apr. 2010.

[15] H. Zhu, X. Lin, R. Lu, Y. Fan, and X. Shen,"SMART: A Secure Multilayer Credit BasedIncentive Scheme for Delay-Tolerant Networks,"IEEE Trans. Vehicular Technology, vol. 58