A survey on Report based secure payment scheme for Multihop wireless Networks

S.Maria Sobana

Department of Computer science and Engineering, Fatima Michael College of Engineering and Technology, Madurai

ABSTRACT:

Multi-hop wireless networks use two or more hops to convey information from source to destination. We propose RACE, a report-based payment scheme for multi-hop wireless networks to stimulate node cooperation, regulate packet transmission, and enforce fairness. RACE has four main phases First phase is Communication. Here nodes are involved in communication session and verify the evidence. In Classifier phase is used to classify which one is cheater node and which one is fair node .Identifying cheater phase to check the evidence report and to identifying the cheater node. Finally, Update account phase clear the payment report. The nodes submit lightweight payment report to the accounting center and temporarily store undeniable security tokens called Evidences.

KEYWORDS: *Multi-hop wireless networks, Payment scheme, Communication, Accounting center, Evidences.*

1 INTRODUCTION:

In Multihop wireless networks, communication between two end nodes is carried out through a number of intermediate nodes whose function is to relay information from one point to another [1]. Mesh networks serve as access networks that employ multihop wireless forwarding by non mobile nodes to relay traffic to and from the wired internet. In such [2] environment, hybrid technologies can be used for adhoc and infrastructure wireless links [3]. For example, Military applications multihop wireless networks is useful in establishing communication in the battle field. In emergency operations MWNs are very useful such as rescue, and crowd control.

Fig.1. Multihop wireless networks for internet access

In Fig 1 the base station provides internet access to the network nodes through multihop wireless paths. Multihop wireless networks support the routing mechanism. Routing in MWNs supported by the collaboration of intermediate nodes that retransmit the messages from source to the destination [5]. The protocols are very useful discovering and selecting the path to use for the communication [4].

The payment schemes have the different models for packet transmission [8]. The credit based models are used into the existing system. In proposed report based model is used for secure payment processing. One of the fundamental tasks any adhoc network must perform is routing. Since the network is in general multi-hop, a routing protocol is needed in order to discover and maintain routes between far away nodes, allowing them to communicate along multi-hop paths. Unless carefully designed, routing protocols are performing poorly in presence of selfish nodes behavior. In general, a network node has no interest in forwarding a packet on behalf of another node, since this action would only have the effect of consuming its resources. Thus, if many of the nodes act selfishly, only few multi-hop communication will take place, and the network functionality is compromised.

2 PAYMENT SCHEME:

In the existing receipt based payment scheme processing and communication overhead. The trusted third party may not be involved in the communication, the nodes compose proofs of other packets of the relaying called receipts, and submit them into accounting center (AC) to clear the payment [12]. The receipt size is large they carry security proofs. The AC has large number of cryptographic operations can apply to verify the receipts, which may require impractical computational power and make the practical implementation of these schemes inefficient or complex.

We propose RACE report based payment scheme for MWNs. The nodes submit light weight payment reports to the AC to update the credit accounts and temporarily store undeniable security tokens called evidences. The report contains the alleged charges and rewards of different sessions without security proofs. The AC verifies the payment by investigating the reports of the consistency and clears the payment of fair reports with almost no cryptographic operations or computational overhead. For cheating reports, the requested evidences and evict the cheating nodes that submit incorrect reports. RACE can identify the cheating nodes with submitting and processing few evidences.

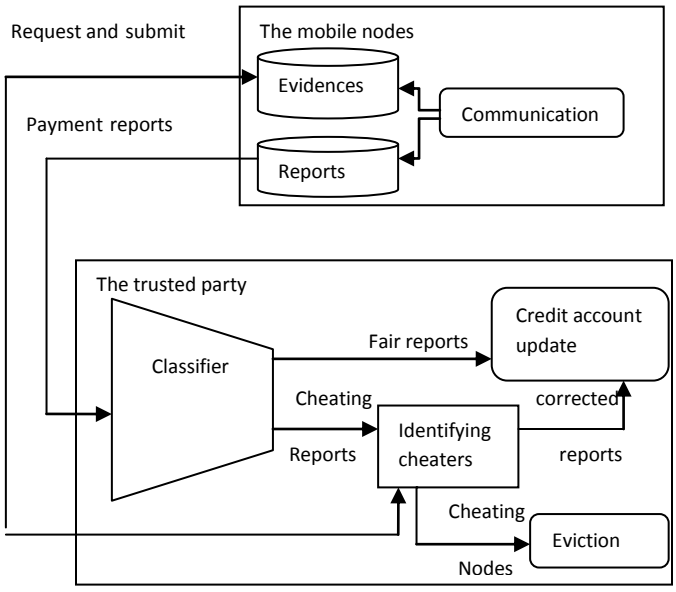

Fig.2.RACE Architecture.

The RACE has four phases. In communication phase the nodes are involved in the communication session. The classifier phase to classify the reports into fair and cheating. For identifying cheaters phase to identify the cheating node. Finally Credit-account update phases clear the payment reports.

3 PAYMENT SCHEME TECHNIQUE

Payment scheme have the following issues.

A ROBUSTNESS

It must be able to recover and reconfigure [11] quickly.

B EFFICIENCY

It should make a minimum number of transmissions to deliver a packet.

C CONTROL OVERHEAD

It demands [10] minimal control overhead.

D SCALABILITY

It should be able to scale for the large [14] network.

E SECURITY

To provide the secure [9] payment scheme for multi-hop wireless networks.

4 COMPARISONS OF PAYMENT SCHEME TECHNIQUES

Different types of payment scheme techniques have been developed for multi-hop wireless networks.

J. Pan et al. [6] propose secure identity-based ad hoc protocol for mobile devices to construct a group key for a setup of a secure communication network in an efficient way and propose a collision-free method for computing such keys. Unlike group key management protocols, we use identity-based keys that do not require certificates which simply key management. In contrast to other interactive protocols, we only need one broadcast to setup the group key member removal is also highly efficient. In the next generation of wireless communication systems, there

will be a need for the rapid deployment of independent mobile users. Significant example include establishing survivable, efficient, dynamic communication for emergency operations, disaster relief efforts and military networks.

C. Chou et al. [2] propose an efficient anonymous protocol, called MANET anonymous peer-to-peer communication protocol (MAPCP), for p2p applications over mobile ad-hoc networks (MANETs). It requires no hop-by-hop encryption/decryption along anonymous paths and power consumption than those MANET anonymous routing protocols. Since MAPCP builds multiple paths to multiple peers within a single query phase without using an extra route discovery process, it is more efficient in p2p applications. Through analysis and extensive simulations, we demonstrate that MAPCP always maintains a higher degree of anonymity than a MANET anonymous single path routing protocol in a hostile environment.

G. Marias et al. propose [5] cryptographic and hashing schemes. These schemes although effective, produce significant processing and communication overheads and consume energy, and they do not take into account the idiosyncrasies of a MANET. More recently, cooperation enforcement have been proposed for trust establishment in MANET. These schemes classified as reputation based and credit based, are considered suitable for ad hoc networks, where key or certificate distribution centers are absent or present, and for networks that consist of devices with limited processing, battery, and memory resources. Cooperation enforcement methods do not provide strong authentication of entities.

N. Salem et al. [7] propose a charging and rewarding scheme to encourage the most fundamental operation, namely packet forwarding. We use “MAC layering” to reduce the space overhead in the packets and a stream cipher encryption mechanism to provide “implicit authentication” of the node involved in the communication. We analyze the robustness of our protocols against rational and malicious attacks. We show that using our solution collaboration is rational for selfish nodes. We also show that our protocols and detect malicious attacks. The resulting hybrid ad hoc network also called multi-hop cellular network, offers several benefits. First of all, the coverage of network is increased while the number of antennas is kept relatively small. Reducing the number of antennas is beneficial for the operator because it represents a cost reduction and also because of the “NIMBY” (not in my back yard) attitude that makes site acquisition and approval both tedious and difficult. Second the energy consumption of the nodes can be reduced because the signal has to cover a small distance. And finally, as the radiated energy is reduced, the interference with other nodes diminishes as well.

H. Zhu et al. [8] propose SMART system. Delay tolerant networks (DTNs) provide a promising solution to support wide-ranging applications in the regions where end to end network connectivity is not available. In DTNs, the intermediate nodes on a communication paths are expected to store, carry, and forward the in-transit messages in opportunistic way, which is called opportunistic data forwarding. Such a forward method depends on the hypothesis that each individual node is ready to forward packets for others. This assumption, however, might easily be violated due to the existence of selfish or even malicious nodes, which may be unwilling to waste their precious wireless resources to serve as bundle relays. To address this problem, we propose a secure multi layer credit based incentive scheme to stimulate bundle forwarding cooperation among DTN nodes. The proposed scheme can be implemented in a fully distributed manner to thwart various attacks without relying on any tamperproof hardware. In addition, we introduce several efficiency optimization techniques to improve the overall efficiency by exploiting the unique characteristics of DTNs. Extensive simulations demonstrate the efficiency of the proposed scheme.

The above techniques to address the following issues

1. Security Aspects- each node is autonomous and the charge and credit [13] is based on receipts submitted by each node.
2. Incentive Aspects- node should [12] receive enough credit for forwarding a message.

Table 1. Comparison of various payment scheme techniques

Author	Title	Merits	Demerits
J. Pan, L. Cai, X. Shen, and J. Mark	Identity-based secure collaboration in wireless ad hoc networks	Easy to perform the route discovery, packet forwarding, and media access mechanism.	1. It is applicable only desired peer networks. 2. In this system has more selfish networks.
C. Chou, D. Wei, C. Kuo, and K. Naik	An Efficient Anonymous Communication Protocol for peer to peer Applications over mobile ad hoc networks	To establish multiple anonymous path between communication peers.	1. It does not identify cheater node. 2. Performance delay.
G. Marias, P. Georgiadis, D. Flitzaais, and K. Mandalas	Cooperation enforcement schemes for MANETs: A survey	These schemes, although effective, produce significant processing and consume energy.	1. Malicious node may reject the incoming packets. 2. Shortest routes are rejected.
N. Salem, L. Buttyan, J. Hubaux, and M. Jakobsson	Node cooperation in hybrid ad hoc networks	To encourage the most fundamental operation, namely packet forwarding. It detect the malicious attacks.	1. In this system may occur more attacks. 2. It does not have any scheme for preventing attacks.
H. Zhu, X. Lin, R. Lu, Y. Fan, and X. Shen	SMART: A secure multilayer credit-based incentive scheme for delay-tolerant networks	To improve the overall efficiency by exploiting the unique characteristics of delay-tolerant networks.	1. Selfish or malicious nodes easily violet the process. 2. End to end connectivity is not available.

5 PAYMENTS PROCESSING OVERHEAD

The low payment processing overhead can reduce the complexity and provide flexibility to the practical implementation of the accounting center. Since the payment schemes use micro-payment, the overhead cost should be much less than the payment for the effective implementation of these schemes. 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. Moreover, cheating node is evicted once its commits one cheating action, and changing identity is not easy or cheap, e.g., the TP can impose fees for issuing the new certificates.

6 CONCLUSION

We have proposed a report based payment scheme for multi-hop wireless networks. 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. RACE can significantly reduce the communication and processing overhead comparing to the existing receipt based schemes with acceptable payment clearance delay and evidences storage area.

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 J., vol.13, no.4, pp.175-193, 2009.
[2] C. Chou, D. Wei, C. Kuo, and K. Naik, "An Efficient Anonymous Communication Protocol for Peer-Peer Applications Over Mobile Ad-Hoc Networks,'' IEEE J. selected areas in comm., vol. 25, no. 1, pp. 192-203, Jan. 2007.
[3] H. Gharavi, "Multichannel Mobile Ad Hoc Links for Multimedia Communications'' proc. IEEE, vol. 96, no. 1, pp. 77-96, Jan. 2008.
[4] S. Marti, T. Giuli, K. Lai, and M. Basker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks,'' proc. Mobicom '00, pp. 255-265, Aug. 2000.
[5] 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.
[6] J. Pan, L. Cai, X. Shen, and J. Mark, "Identity- Based Secure Collaborationin Wireless Ad Hoc Networks,'' Computer Networks, vol. 51 no. 3 pp. 853-865, 2007.

[7] N. Salem, L. Buttyan, J. Hubaux, and M. Jakobsson, "Node Cooperationin Hybrid Ad Hoc Networks,'' IEEE Trans. Mobile Computing, vol. 5, no. 4, pp. 365-376,Apr. 2006.
[8] 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.
[9] Y. Zhang and Y. Fang, "A Secure Authentication and Billing Architecture for Wireless Mess Networks," ACM Wireless Networks, vol. 13, no. 5, pp.663-678, Oct. 2007.
[10] A. Weyland, "Cooperation and Accounting in Multi-Hop Cellular Networks," PhD thesis, Univ. of Bem, 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] H. Pagnia and F. Gartner, "On the Impossibility of Fair Exchange without a Trusted Third Party," Technical Report TUD-BS-1999-02, Darmstadt Univ. of Technology, Mar. 1999.
[13] 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.
[14] Y. Zhang, W. Lou, and Y. Fang, "A Secure Incentive Protocol for Mobile Ad Hoc Networks, "ACM Wireless Networks, vol. 13, vol. 13, no. 5, pp. 569-582, Oct. 2007.