IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 11, November 2015

A Secure Payment Scheme with Low Communication and Processing Overhead For Multihop Wireless Networks

Muhammad Puzhakkalaveettil[1], Ms. B. Mathumathi[2]

M.Phil, Computer Science, Sree Narayana Guru College, Coimbatore[1]

Assistant Professor, Sree Narayana Guru College, Coimbatore[2]

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 reports, 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 reduce 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.

Keywords: Multihop wireless networks (MWN), Report-based pAyment sChemE (RACE), Mobile ad-hoc network (MANET), Wireless sensor network (WSN), Dynamic Source Routing(DSR), Rivest Shamir Adleman (RSA), Common Language Runtime(CLR), Common Type System(CTS).

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. 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 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. Selfish nodes will not relay others' packets and make use of the cooperative nodes to relay their packets, which degrades the network connectivity and fairness. The fairness issue arises when the selfish nodes make use of the cooperative nodes to relay their packets without any contribution to them, and thus the cooperative nodes are unfairly overloaded because the network traffic is concentrated through them.

The selfish behavior also degrades the network connectivity significantly, which may cause the multihop communication to fail. The existing credit card payment schemes are designed for different system and threat models, which are infeasible for MWNs. A good payment scheme should be secure, and require low overhead. However, the existing receipt-based payment schemes impose significant processing and communication overhead and implementation complexity. Since a trusted party may not be involved in communication sessions, the nodes compose proofs of relaying others' packets, called receipts, and submit them to an offline accounting center (AC) to clear the payment. 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.

DOI 10.17148/IJARCCE.2015.41109

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.

2. PROPOSED SYSTEM

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.

2.1Advantages

1. Evidences are un modifiable
2. Evidences are un forgeable
3. Evidences are undeniable
4. If the source and destination nodes collude, they can create Evidences for any number of messages.

3. MODULES

The following are the modules going to implemented in this project work

- Network Model
- Adversary Model
- Route establishment
- Data transmission
- Trust based routing protocol

3.1Network Model

For military and disaster recovery applications, the network can be considered ephemeral because it is used for a specific purpose and short duration. 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.

3.2 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 the network proper operation. As discussed in, 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.

3.3 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.

3.4 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 (HðMXÞ) and sends the packet to the first node in the route.

3.5 Trust based routing protocol

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. Here we are using SHA1 algorithm for cryptography enhancement. 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.

4. SYSTEM DESIGN AND IMPLEMENTATION

4.1 Hardware requirements

Processor	:	Pentium dual core
Hard Disk	:	80 GB
Monitor	:	17'' Colour Monitor
Mouse	:	Scroll Mouse
RAM	:	1 GB
Keyboard	:	104 keys Standard

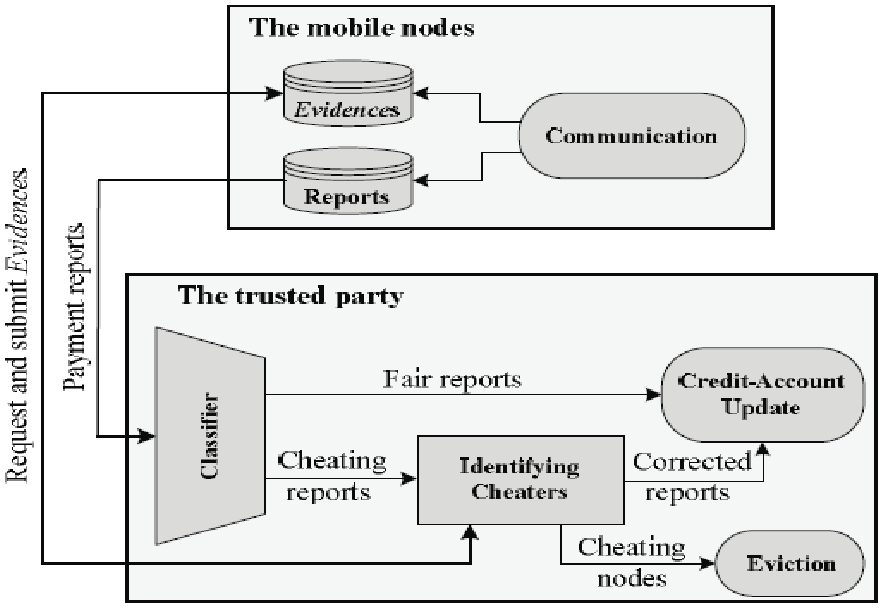
4.2 Software requirements

Operating System: Windows 7

Front End : Microsoft Visual studio 2008
Coding Language: C#.NET
Back End : SQL Server 2000

4.3 System design
System design is the process of planning a new system to complement or altogether replace the old system. The purpose of the design phase is the first step in moving from the problem domain to the solution domain. The design of the system is the critical aspect that affects the quality of the software. System design is also called top-level design.

Input design is one of the most important phases of the system design. Input design is the process where the input received in the system are planned and designed, so as to get necessary information from the user, eliminating the information that is not required.



The architecture of RACE.

Public-key cryptography is widely used to secure the wireless networks. Using public-key cryptography in RACE is necessary to secure the payment because it enables the nodes to compose valid Evidences and enables the TP to identify the cheating nodes. Public-key cryptography technology and hardware implementation have been improved, and the signing and verifying operations can be performed by mobile nodes with acceptable overhead. In digital signatures can be computed efficiently in two steps. The offline step is independent of the message and performed before the message to be signed is available; and a lightweight online step is performed once the message to be signed becomes available. In FPGA implementation of the RSA cryptosystem can efficiently perform the signing and verifying operations in several milliseconds. Moreover, the proposed communication protocol in that transfers messages from the source to the destination nodes with limited number of public-key cryptography operations can be used with RACE, but the focus of this paper is on reducing the communication and the payment processing overhead.

4.4 System implementation
Implementation is the stage of the project when the theoretical design is turned out into a working system. If the implementation stage is not properly planned and controlled, it can cause error. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective. The first stage of implementation includes many activities. Coding is the first activity. The software developers take the design documents and development tools such as editors, compilers, and debuggers and then start writing software. This is usually the longest phase in the product life cycle. The implementation phase is less creative than system design. The final report to the implementation phase includes procedural flowcharts, record layouts, report layouts, and a workable plan for implementing the candidate system design into an operational one. Conversion is one aspect of implementation. This stage involves careful planning, investigation of the existing system and it’s constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

The following are the steps involved in the implementation plan

i. Test the system by opening sample videos.
ii. Detection and correction of errors while using this system.
iii. Checking with the existing system.
iv. Installment of required hardware and software for implementing this system.

At the implementation stage the emphasis must be on

DOI 10.17148/IJARCCE.2015.41109

training in new skills to give staff confidence they can use the system. Once staff has been trained, the system can be tested. After the implementation phase is completed and the user staff is adjusted to the changes created by the candidate system, evaluation and maintenance is to bring the new system to standards. The system will be implemented shortly.

5. FINDINGS AND DISCUSSION

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 submitting 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.

6. CONCLUSION AND FUTURE ENHANCEMENT

6.1 CONCLUSION

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.

6.2 FUTURE ENHANCEMENTS

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 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-to-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. Baker, "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] 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.

[7] 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.

[8] 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.

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

[10] 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.

DOI 10.17148/IJARCCE.2015.41109