Volume 3, Issue 5, May 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Secure Communication Mechanism for MHC Networks Using Payment Ratio

Kavya Shree B S*
Department of Computer Science & Engineering,
East West Institute of Technology, VTU, India.

Sharada K. A
Department of Computer Science & Engineering,
East West Institute of Technology, VTU, India.

Abstract— Multi-hop cellular networks (MCN) appear to be a promising combination of the dynamics of the mobile adhoc networks and the reliability of the infra-structured wireless networks. In MCN, the mobile nodes usually depend on other packets to improve network performance. However, there are some selfish users who are reluctant to act as packet relays in order to save their own resources. Such non-cooperative behaviour would cause sharp degradation and negative impact on network fairness and performance. In this paper, we propose a fair and secure incentive mechanism to stimulate node cooperation in multihop wireless networks. Fairness is achieved by using credits to reward the cooperative nodes. To implement this charging policy efficiently and securely, light weight hashing operations are used in ACK packets to reduce the number of public-key-cryptography operations. Moreover, reducing the overhead of payment checks is essential for the efficient implementation of the incentive mechanism due to the large number of payment transactions. Instead of generating a check per message, a small-size check can be generated per route, and a check submission scheme is proposed to reduce the number of submitted checks and protect against collusion attacks.

Keywords- Security, Selfish nodes, Payment schemes, Wireless network.

I. INTRODUCTION

Multihop cellular network is a network architecture that incorporates the ad hoc characteristics into the cellular system. The network nodes traffic is usually dependable on some intermediate nodes to reach the destination node. The network nodes form a pool of resources which contains the data storage, battery power, bandwidth, CPU cycles, etc. that can be shared by all of them. The MCN is used for civilian applications where the network has long life and the mobile nodes are supposed to have long-term relations with the network. Multihop packet relay can reduce the dead areas by extending the communication range of the base stations without additional costs. It can also reduce the energy consumption because packets are transmitted over shorter distances, and improve the area spectral efficiency and the network throughput and capacity [1], [2], [3].However, the packet routing process suffers from new security challenges due to involvement of autonomous devices in packet relay that endanger the practical implementation of MCN. Selfish nodes do not forward the packets to other nodes without incentives, but make use of the cooperative nodes to relay their packets, which has a negative impact on the network fairness and performance. A fairness issue arises when selfish nodes take advantage of the cooperative nodes without any contribution to them. The selfish behaviour also significantly degrades the network performance, which may result in failure of the multihop communications [4], [5].The diagram below shows how projecting a laser dot onto a target that is in the field of view of a camera. Reputation-based and incentive mechanisms [6], [7] have been proposed to avoid selfishness attacks. For reputation-based mechanisms [8], [9], [10], the nodes usually monitor the transmissions of their neighbours to make sure that the neighbours relay other nodes' traffic, and thus, selfish nodes can be identified and punished. For incentive mechanisms, packet relay is a service not a commitment. The source and destination nodes pay credits (or virtual currency) to the intermediate nodes for relaying their packets. Credits can stimulate the nodes' cooperation by proving that it is more beneficial for the nodes to cooperate than behaving selfishly.

Reputation-based mechanisms have some disadvantages that discourage implementing them in MCN. First, reputation-based mechanisms do not achieve fairness because the highly contributing nodes are not compensated. For example, although the nodes at the network centre relay more packets than those at the periphery, they are not compensated. Second, the mechanisms suffer from unreliable detection of the selfish nodes and false accusation of the honest nodes. That is because it is difficult to differentiate between a node's unwillingness and incapability to cooperate, e.g., due to low resources, packet collision, and network congestion. Third, monitoring the nodes transmissions by overhearing the channel is not energy efficient for transmitters. Fourth, incentive.

A. Objective of the Study

- Here we propose Fair, Efficient, and Secure Cooperation Incentive Mechanism, to stimulate the node cooperation in MCN.
- The destination node generates a hash chain and signs its root, and acknowledges message reception by releasing a hash value from the hash chain. In this way, the destination node generates a signature per group of messages instead of generating a signature per message.
- Furthermore, instead of generating a check per message or generating a nodal check for each intermediate node,

a small-size check containing the payment data for all the intermediate nodes is generated per route.
- Trusting one node to submit the check is not secure because this node may collude with the source and destination nodes to not submit the check.

B. Scope

In order to efficiently and securely charge the source and destination nodes, the lightweight hashing operations are used in the ACK packets to reduce the number of public-key-cryptography operations.

II. SYSTEM ANALYSIS

A. Existing System

In Existing System nodes were not cooperating with each other in a proper manner and energy consumption was more. Two signatures are usually required per message to securely implement charging policy. Submitting and processing a large number of checks implies significant communication and computation overhead and implementation complexity.

B. Proposed System

In Proposed System, the light weight hashing operations are used to reduce the number of public-key-cryptography operations. Instead of generating a check per message or generating a nodal check for each intermediate node, a small-size check containing the payment data for all the intermediate nodes is generated per route.

C. System Specification

Hardware Requirement (Minimum Requirement)

Processor	: Pentium 4
RAM	: 256 MB
Hard Disk	: 40 GB

Software Requirement

Technology	: JAVA
Tools	: JDK 1.6, Net beans (IDE)
Database	: MySQL Server

D. System Modules

- Digital Signature Generator Module.
- Route Establishment Module.
- Asymmetric Encryption and Decryption Module.

E. System Architecture

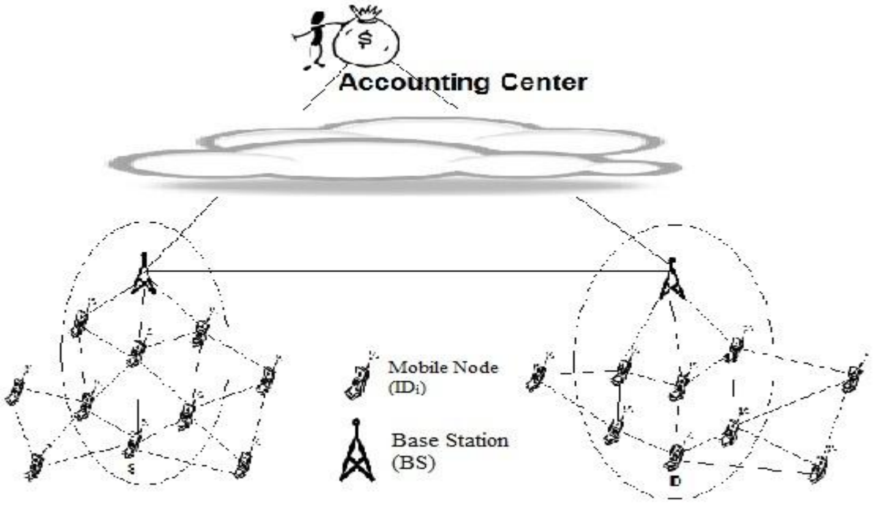

Fig. 1 System Architecture

III. MODULE DESCRIPTION

A. Digital Signature Generator Module

In digital signature generator module, we are using RSA key generator to generate a messages to communicate for source and destination nodes.

B. Route Establishment Module

In route establishment module we use UDP Sockets to establish end to end communication between source and destination nodes.

C. Asymmetric Encryption and Decryption Module

In asymmetric encryption and decryption module we are using Data Encryption Standard (DES) to encrypt and decrypt the data.

IV. SYSTEM IMPLEMENTATION

FESCIM can be implemented on the top of any routing protocol, such as DSR [11] and AODV [12], to establish an end-to-end communication session provided that the full identities of the nodes in the route are known to the source and destination nodes. It is important to include these identities in the source and the destination node's signatures to compose valid checks.

A. Basic Theory

The basic theory behind the project is the following;

All communications are unicast and the nodes can communicate in one of two modes: pure ad hoc or hybrid. For pure ad hoc mode, the source and destination nodes communicate without involving base stations. The source node's messages may be relayed in several hops by the intermediate nodes to the destination node. For hybrid mode, at least one base station is involved in the communication. The source node transmits its messages to the source base station (BSS), if necessary in multiple hops. If the destination node resides in a different cell, the messages are forwarded to the destination base station (BSD) that transmits the messages to the destination node possibly in multiple hops. The nodes can contact the AC at least once every few days. This connection can occur via the base stations or the wired networks such as the Internet. During this connection, the nodes submit checks, renew their certificates, and convert credits to real money and/or purchase credits with real money.

B. Implementation Algorithm

Hybrid Mode:

1. Network Establishment:

- Initialize, BSS, BSD, AC, Intermediate node of source packet, destination packet.
- Provide connectivity between BSS→BSD, BSS→AC, BSD→AC using internet and intermediate node of source packet→BSS through multiple hops, intermediate node of destination packet→BSD through multiple hops.

2. Network Connectivity

- Any one of the intermediate node start receiving the source packet messages and starts sending packet to its nearer BSS.
- If the destination node resides in a different cell, the messages are forwarded to destination base station (BSD).
- The BSS and BSD communicate with each other and finally send information to the accounting centre.

3. Packet Communication

- In order to establish end to end communication, the source node broadcasts the (RREQ) containing the identities of the source (IDs) and the destination(IDs)nodes, the route establishment time stamp(Ts) and the payment splitting ratio(Pr).
- The source node is charged the ratio of Pr of the total payment and the destination node is charged the ratio of 1-Pr.
- The destination sends back the RREP to establish the route.
- The source node initiates a new route discovery phase if the route is broken.
- The RREP packet contains the session identifier (Si), the destination node's certificate and the route of the first hash chain and the destination node signature.
- Si contains the ID of the nodes in the route, Ts and Pr.
- Si=IDs, ID1, ID2, BSs, ID3, ID4, IDd, Ts, Pr.
- The destination node's signature authenticates the node and proves its approval to pay for the session.
- The signature also proves that the hash chain has indeed been created by the destination node and links it to the route.
- Upon receiving the RREP packet, each intermediate node relays the packet if the signature is correctly verified, and the source node starts data transmission.

Pure ad hoc Mode:

In pure ad hoc mode, the source and destination nodes communicate without involving base stations. The source node's messages may be relayed in several hops by the intermediate nodes to the destination node.

Limitations

FESCIM can thwart selfishness attacks, but it cannot identify the irrational nodes that involve themselves in sessions with the intention of dropping the data packets to launch Denial of-Service attacks.

V. CONCLUSION

In this paper, we have proposed a fair, efficient, and secure cooperation incentive mechanism for MCN. In order to fairly and efficiently charge the source and destination nodes, the lightweight hashing operations are used to reduce the number of public-key-cryptography operations. Moreover, to reduce the overhead of the payment checks, one small-size check is generated per session instead of generating a check per message In this paper, instead of generating two signatures per packet (one from the source and the other from the destination), we have replaced the destination node's signature with hashing operations to reduce the number of public-key-cryptography operations nearly by half. The source node attaches a signature in each data packet to ensure the payment nonrepudiation and to verify the message integrity at each intermediate node to thwart Free- Riding attacks.

VI. FUTURE WORK

In our future work, we will focus on reducing the number of public-key-cryptography operations due to the source node's signatures. Although the payment nonrepudiation can be achieved using a hash chain at the source node side, we will study how to efficiently verify the message integrity at each intermediate node. In addition, similar to the existing incentive mechanisms, FESCIM can thwart selfishness attacks, but it cannot identify the irrational nodes that involve themselves in sessions with the intention of dropping the data packets to launch Denial of- Service attacks. In our future work, we will study how the AC can process the checks to identify the irrational nodes.

Bibliography

[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] R. Schoenen, R. Halfmann, and B. Walke, "MAC Performance of a 3GPP-LTE Multihop Cellular Network," Proc. IEEE Int'l Conf. Comm. (ICC), pp. 4819-4824, May 2008.

[3] 3rd Generation Partnership Project, Technical Specification Group Radio Access Network, "Opportunity Driven Multiple Access," 3G Technical Report 25.924, Version 1.0.0, Dec. 1999.

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

[5] P. Michiardi and R. Molva, "Simulation-Based Analysis of Security Exposures in Mobile Ad Hoc Networks," Proc. European Wireless Conf., Feb. 2002.

[6] J. Hu, "Cooperation in Mobile Ad Hoc Networks," Technical Report TR-050111, Computer Science Dept., Florida State Univ., Jan. 2005.

[7] G. Marias, P. Georgiadis, D. Flitzanis, and K. Mandalas, "Cooperation Enforcement Schemes for MANETs: A Survey,"J. Wireless Comm. and Mobile Computing, vol. 6, no. 3, pp. 319-332, 2006.

[8] C. Song and Q. Zhang, "OMH-Suppressing Selfish Behaviour in Ad Hoc Networks with One More Hop," Mobile Networks and Applications, vol. 14, no. 2, pp. 178-187, Feb. 2009.

[9] D. Djenouri and N. Badache, "On Eliminating Packet Droppers in MANET: A Modular Solution," Ad Hoc Networks, vol. 7, no. 6, pp. 1243-1258, Aug. 2009.

[10] G. Bella, G. Costantino, and S. Riccobene, "Evaluating the Device Reputation Through Full Observation in MANETs," J. Information Assurance and Security, vol. 4, no. 5, pp. 458-465, Mar. 2009.

[11] D. Johnson and D. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks," Mobile Computing, pp. 153-181, chapter 5, Kluwer Academic, 1996.

[12] C. Perkins and E. Royer, "Ad-Hoc on-Demand Distance Vector Routing," Proc. IEEE Workshop Mobile Computing Systems and Applications, pp. 90-100, Feb. 1999.

[13] FESCIM: Fair, Efficient, and Secure Cooperation Incentive Mechanism for Multihop Cellular Networks. Mohamed M.E.A.Mahmoud and Xuemin (Sherman) Shen.