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

International Journal of Advanced Research in Computer and Communication Engineering

IJARCCE

nCORETech

LBS College of Engineering, Kasaragod

Vol. 5, Special Issue 1, Feburary 2016

A Secure Payment Scheme in Multihop Wireless Network Using Shortest Reliable Routing

Ms. Jyothi Padmanabhan[1], Ms. Navya E K[2]

M Tech Student, Computer Science & Engineering, Malabar Institute of Technology, Kannur, India[1]

Assistant Professor, Computer Science & Engineering, Malabar Institute of Technology, Kannur, India[2]

Abstract: In multi-hop wireless networks, nodes traffic is usually relayed through other nodes to the destination. Multi-hop relaying can enable new applications and enhance the network performance and deployment. Moreover, in developing or rural areas, multi-hop wireless networks can be deployed more readily and at low cost. A secure payment scheme in MWN using SRR is a report-based payment scheme for multihop wireless networks to stimulate node co-operation, 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 store the evidences. The nodes which do not pass or relay others packets are called selfish nodes. But it makes use of neighbor or co-operative nodes to relay its packets. This degrades the network connectivity and fairness. The nodes submit lightweight payment reports (instead of receipts) to the accounting center (AC). 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. Then these reports are saved in TP. These reports can be used in future communication to select reliable cheater free route.

Keywords: Multihop Wireless Network (MWN), Trusted Party (TP), Accounting Centre (AC), Shortest Reliable Routing (SRR).

I. INTRODUCTION

In multi-hop wireless network (MWN) [1], nodes traffic is usually relayed through other nodes to the destination. Multi-hop relaying can enable new applications and enhance the network performance and deployment. It can Extend the communication range using limited transmit power, and enhance the network throughput and capacity. Moreover in developing or rural area, multi-hop wireless network can be deployed more readily and low cost. Multi-hop wireless network can also implement many useful applications such as data sharing and multimedia transmission. In multi-hop wireless network some intermediate nodes in communication may be selfish. Selfish nodes will not relay other packets and make use of the co-operative nodes to relay their packets, which degrades the network connectivity and fairness. Selfish node is economically rational node whose objective is to maximize its own welfare. The fairness issue arises when the selfish nodes make use of the co-operative nodes to relay their packets without any contribution to them, and thus the co-operative 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 multi-hop communication to fail, so a selfish node will need incentive in order to forward others messages.

One possibility to provide incentive is to use credit scheme which motivate the nodes to co-operate in relaying others packet by making cooperation more beneficial than selfishness. Here we use Report based payment scheme for MWN. In MWN the nodes are assigned a trust value. Based on trust value the routing is performed. Trust value is assigned based on relaying packet successfully. Each node submits 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 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. The evidences are used to resolve disputes when the nodes disagree about the payment. Once the cheater is found it is placed in the cheater list and for future communication TP studies the cheater list and select a shortest reliable cheater free route.

II. LITERATURE SURVEY

The existing payment schemes can be classified into tamper-proof-device (TPD) based and receipt-based schemes. In TPD-based payment schemes, a TPD is installed in each node to store and manage its credit account and secure its

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
IJARCCE
nCORETech
LBS College of Engineering, Kasaragod
Vol. 5, Special Issue 1, Feburary 2016

operation. For receipt-based payment schemes, 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.

A. SPRITE

In Sprite [2], a simple, cheat-proof, credit-based system for mobile ad-hoc networks with selfish nodes. Sprite system also uses credit to provide incentive to selfish nodes. However, one of the novel and distinguishing features is that our system does not need any tamper-proof hardware at any node. When a node receives a message, the node keeps a receipt of the message. Later, when the node has a fast connection to a Credit Clearance Service (CCS), it reports to the CCS the messages that it has received/forwarded by uploading its receipts. The CCS then determines the charge and credit to each node involved in the transmission of a message, depending on the reported receipts of a message.

Sprite consists of the Credit Clearance Service (CCS) and a collection of mobile nodes. The nodes are equipped with network interfaces that allow them to send and receive messages. To identify each node, we assume that each node has a certificate issued by a scalable certificate authority; we assume that the sender knows the full path from the sender to the destination, using a secure ad hoc routing protocol based on DSR.

When a node sends its own messages, the node (or the destination, see later) will lose credit (or virtual money) to the network because other nodes incur a cost to forward the messages. On the other hand, when a node forwards others messages, it should gain credit and therefore be able to send its messages later.

In order to get credit for forwarding others messages, a node needs to report to the CCS which messages it has helped to forward. Thus, although we require that the CCS be trusted in terms of maintaining credit balance, the nodes do not need to trust the CCS in terms of message confidentiality. Since the mobile nodes are selfish, without a proper payment scheme, they may not forward others messages or they may try to cheat the system, if the Cheating can maximize their welfare.

In Sprite, for each message, the source node signs the identities of the nodes in the route and the message, and sends the signature as a proof for sending a message. The intermediate nodes verify the signature, compose receipts containing the identities of the nodes in the route and the source nodes signature, and submit the receipts to the AC to claim the payment. The AC verifies the source nodes signature to make sure that the payment is correct. However, the receipts overwhelm the network because the scheme generates a receipt per message.

B. NUGLETS

A mobile ad hoc network is a wireless multi-hop network formed by a set of mobile nodes in a self-organizing way without relying on any established infrastructure. Due to the absence of infrastructure, all networking functions must be performed by the nodes themselves. For instance, packets sent between two distant nodes are expected to be forwarded by intermediate nodes. Assume that each node belongs to a different authority, its user, which has full control over the node. In particular, the user can tamper with the software and the hardware of the node, and modify its behavior in order to better adapt it to her own goals.

In [3] Butty'an et al. propose nuglets, in nuglets a tamper proof device (TPD) is installed in each device to store its credits and to secure its operation. The self-generated and forwarding packets are passed to the TPD to decrease and increase the credit account, respectively. A node cannot transmit its generated packets if it does not have sufficient credits. Two models, called the packet purse model (PPM) and the packet trade model (PTM) have been proposed. In the PPM, the source node pays for relaying its packets by loading some credits in each packet before sending it. Each forwarding node acquires the amount of credits that covers its forwarding cost. A packet is discarded if it does not have enough credits to be forwarded.

In the PTM, each intermediate node buys a packet and sells it to the following node in the route until the destination node pays the total cost. Using tamper-proof devices can reduce the complexity of the incentive mechanism but the assumption that they cannot be tampered is neither secure nor realistic for networks with autonomous nodes. Tamper-proof devices with high security level may be expensive, and if they are compromised, attackers can attack the mechanism brutally in undetectable way. In a subtle attack, two tamper proof devices can be installed in one device, and a packet is passed through them for double rewarding. Fairness issue arises when a node loses its credits without any benefits. It is difficult to estimate the required amount of loaded credits so the surplus credits are lost in over estimation and all the loaded credits are lost in underestimation. In addition, the source node pays a complete payment for every generated packet even if it does not reach its destination. The PTM suffers from high bandwidth and latency

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
IJARCCE
nCORETech
LBS College of Engineering, Kasaragod
Vol. 5, Special Issue 1, Feburary 2016

overhead because an auction occurs at each node. Dropping the packets with insufficient credits degrades the network throughput. Unbalanced payment may lead to credit inflation if the rewards are greater, or credit depletion if the charges are greater. In credit inflation, the nodes are rich and their stimulation to cooperation becomes less, whereas, in credit depletion, the nodes are poor and they cannot initiate communications.

C. SMART

In [4] Zhu et al. propose a secure multilayer credit-based incentive (SMART) scheme for DTNs afflicted with selfish nodes .SMART uses credits to provide incentives to selfish nodes. One of its novel and distinguishing features is that it allows the credit to be transferred/ distributed by the current intermediate node without the involvement of the sender.

In specific, SMART is based on the notion of a layered coin that provides virtual electronic credits to charge for and reward the provision of data forwarding in DTNs. Such a coin is composed of multiple layers, each of which is generated by the source/destination or an intermediate node. The first layer, which is also named the base layer, is generated by the source to indicate the payment rate (credit value), remuneration conditions, the class-of-service (CoS) requirement and other reward policies. During the subsequent bundle propagation process, each intermediate node will generate a new layer based on the previous layers by appending a no forgeable digital signature. This new layer is also called the endorsed layer, which implies that the forwarding node agrees to provide forwarding service under the predefined CoS requirement and will be rewarded according to the reward policy in the future. With endorsed layers, it is easy to track the propagation path and determine each intermediate node by checking the signature of each endorsed layer. In the rewarding and charging phase, if the provided forwarding service satisfies remuneration conditions defined in the predefined reward policy, each forwarding node along one or multiple path(s) will share the credit defined in this coin depending on different data-forwarding algorithms (single-copy/multicopying forwarding) and the actual forwarding results (bundle delivered along one or multiple paths).

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.

D. ESIP

In [5] Mahmoud et al. propose secure cooperation incentive protocol that uses the public-key operations only for the first packet in a series and uses the light-weight hashing operations in the next packets.

In this paper, we propose an Efficient and Secure co-operation Incentive Protocol (ESIP) that uses public-key operations only for the first packet in a series, and then the efficient hashing operations are used in the next packets. Security analysis and performance evaluation demonstrate that the proposed protocol is secure and the overhead is incomparable to the signature-based incentive protocols because the hashing operations dominate the nodes operations.

In ESIP, the source and the destination nodes generate hash chains by iteratively hashing random values to obtain final hash values called the hash chains roots. The two communicating nodes authenticate their hash chains
by digitally signing the roots and sending the signatures to the intermediate nodes in the route reply and the first data packets. From the second data packet, only the efficient hashing operations are required. Payment no repudiation
can be achieved by releasing the pre-image of the last sent hash value because the hash function is one-way, i.e., only the user can generate the hash chain.

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. ESIP requires fewer public key cryptography operations but with larger receipts size.

E. FESCIM

In [6] FESCIM, a fair, efficient, and secure cooperation incentive mechanism is proposed to stimulate the nodes to cooperate in hybrid ad hoc network. Our mechanism can enforce fairness by rewarding or charging credits to balance between the nodes contributions and benefits. In order to reduce the number of the submitted receipts, each receipt contains complete payment data to all the session nodes.

Therefore, instead of transmitting all the receipts by all the nodes, they can be transmitted by some. A payment aggregation technique is proposed to generate a receipt for multiple packets instead of generating a receipt per packet. A hash chain is applied to integrate the incentive mechanism in the routing protocol. FESCIM adopts fair charging policy by charging both the source and destination nodes when both of them are interested in the communication.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
IJARCCE
nCORETech
LBS College of Engineering, Kasaragod
Vol. 5, Special Issue 1, Feburary 2016

III. PROPOSED SYSTEM

So we can propose a trusted secure routing. Shortest Reliable Route (SRR) is used to find the route Figure shows the secure route establishment.

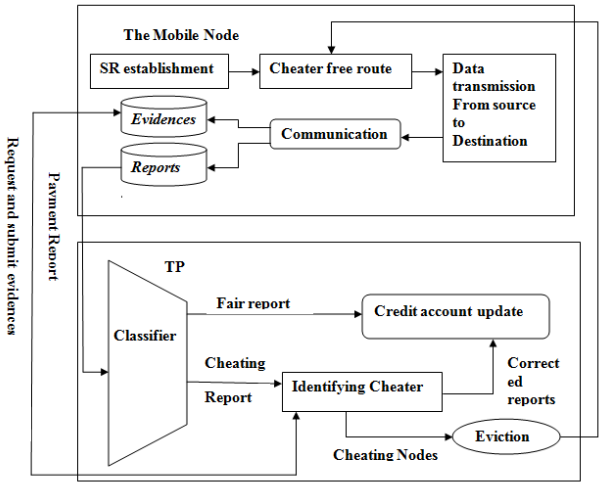

Fig. 1. Architecture of secure routing.

As illustrated in Figure, the considered MWN has an offline TP and mobile nodes. The TP contains the AC and the certificate authority (CA). The AC maintains the nodes credit accounts and the CA renews and revokes the nodes certificates. Each node A has to register with the trusted party to receive a symmetric keyKA, private/public key pair, and certificate. The symmetric key is used to submit the payment reports and the private/public keys are required to act as source or destination node. Once the AC receives the payment reports of a session and verifies them, it clears the payment if the reports are fair; else, it requests the Evidences to identify the cheating nodes. The CA evicts the cheating nodes by denying renewing their certificates. The nodes can contact the TP at least once during a period of few days. In this connection, the nodes submit the payment reports and the Evidences (if requested), and receive renewed certificates to be able to continue using the network.

The system has four main phases. Communication phase in which the nodes establish routes and transmit data packets. Evidence composition phase in which proof about the packet transmission is created. Payment report composition and submission phase in which reports are submitted to the AC. Classifier phase in which, the TP classifies the reports into fair and cheating. Cheater identification phase in which the TP requests the Evidences from the nodes that are involved in cheating reports to identify the cheating nodes. The cheating nodes are evicted and the payment reports are corrected. Finally, Credit account update phase, the AC clears the payment
reports.

Communication Phase: The Communication phase has four processes: route establishment, data transmission, Evidence composition, and payment report composition/ submission.

SRR establishment: The source node embeds its requirements in the Route REQuest (RREQ) packet, and the nodes that satisfy these requirements broadcast the RREQ packet. The RREQ packet contains the identities of source, destination, maximum number of intermediate nodes, trust, source nodes signature and certificate. Source nodes trust requirements are verified at each intermediate node. If the intermediate node has low trust values, then it is verified at each subsequent intermediate node till it reaches at the highly trusted nodes. Each intermediate node ensures that it can satisfy the source nodes trust/energy requirements. It also verifies the packet signature using the public key extracted from the nodes certificate for generating the receipt. A receipt is a packet which contains all the information about the behavior and status of those nodes that processes the data. The receipt is used by Trust Party (TP) to calculate the trust values of the nodes. These verifications are necessary to ensure that the packet is sent and relayed by genuine nodes and satisfy the trust requirements signed by TP. The intermediate node signs the packets signature forming a chain of signed nodes that broadcast the packet. This signature authenticates the intermediate node and proves that the node is the certificate holder and thus the attached trust values belong to the node. The destination node composes the RREP packet for the route traversed by the first received RREQ packet, and sends it to the source node. This route is the shortest one that satisfies the source nodes requirement. The source node requirements cannot be achieved if it does not receive the RREP packet within a time period. The source can initiate a second RREQ packet with more flexible

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
IJARCCE
nCORETech
LBS College of Engineering, Kasaragod
Vol. 5, Special Issue 1, Feburary 2016

requirements. The destination node verifies the hash message and certificate of intermediate nodes to make sure that it satisfies with trust requirements. The destination node responses with RREP packet through the best route among all possible routes.

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 (H (M(X))) and send the packet to the first node in the route. Before relaying the packet, each intermediate node verifies the signature to ensure the messages authenticity and integrity, and verifies R and X to secure the payment. After receiving the Xth data packet, destination node sends back an ACK packet containing the pre image of the last sent hash value (or hX) to acknowledge receiving the message MX. An intermediate node cannot drop the Xth data packet and claim delivering it because the hash function is one way, i.e., it is computationally infeasible to compute hX from h (X-1).

Evidence composition: Evidence is defined as information that is used to establish proof about the occurrence of an event or action, the time of occurrence, the parties involved in the event, and the outcome of the event. The purpose of Evidence is to resolve a dispute about the amount of the payment resulted from data transmission. Evidence contains two main parts called DATA and PROOF. The DATA part describes the payment, i.e., who pays whom and how much, and contains the necessary data to regenerate the nodes signatures. The PROOF is an undeniable security token that can prove the correctness of the DATA and protect against payment manipulation, forgery, and repudiation. The PROOF is composed by hashing the destination nodes signature and the last signature received from the source node, instead of attaching the signatures to reduce the Evidence size. Evidences have the following main features:

- Evidences are un-modifiable: If X messages are delivered, the intermediate nodes can compose Evidences for fewer than X messages, but not for more. The intermediate nodes cannot compose Evidences for more than X because it is computationally infeasible to compute
- 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 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.

Payment report composition or submission: A payment report contains the session identifier, a flag bit, and the number of messages. The session identifier is the concatenation of the identities of the nodes in the session and the time stamp. The flag bit is zero if the last received packet is data and one if it is ACK.

Classifier Phase: After receiving a sessions payment reports, the AC 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 to steal credits or pay less. Fair reports can be for complete or broken sessions. For a complete session, all the nodes in the session report the same number of messages and F of one. If a session is broken during relaying the Xth data packet, the reports of the nodes from S to the last node that received the packet report X and F of zero, but the other nodes reportX - 1and F of one. If a session is broken during relaying the Xth ACK packet, the nodes in the session report X messages, and the nodes from D to the last node that received the ACK report F of one, but the other nodes report F of zero. The reports are classified as cheating if they do not achieve one of the aforementioned rules.

Identifying Cheater: 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 then attackers from stealing credits or paying less, the attackers should not benefit from their misbehaviors. Guarantee should be there, 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 for identifying the cheating node. In this way, the AC can precisely

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
IJARCCE
nCORETech
LBS College of Engineering, Kasaragod
Vol. 5, Special Issue 1, Feburary 2016

identify the cheating nodes with requesting few Evidences. To verify Evidence, the TP composes the PROOF by generating the nodes signatures and hashing them. The Evidence is valid if the computed PROOF is similar to Evidences PROOF.

Credit Account Update: The Credit Account Update phase receives fair and corrected payment reports to update the nodes credit accounts. In receipt-based payment schemes, a receipt can be cleared once it is submitted because it carries undeniable security proof, but the AC in RACE has to wait until receiving the reports of all nodes in a route to verify the payment. The maximum payment clearance delay occurs for the sessions that are held shortly after at least one node contacts the AC and the node submits the report after the certificate lifetime, at least one report is submitted after TCert of the session occurrence. It is worth to note that the maximum time duration for a nodes two consecutive contacts with the TP is TCert to renew its certificate to be able to use the network.

IV. CONCLUSION

In multi-hop wireless network (MWN), nodes traffic is usually relayed through other nodes to the destination. In multi-hop wireless network some intermediate nodes in communication may be selfish. Credit scheme which motivate the nodes to co-operate in relaying others packet by making cooperation more beneficial than selfishness. The nodes submit lightweight payment reports (instead of receipts) to the accounting center (AC). 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. Then these reports are saved in TP. These reports can be used in future communication to select reliable cheater free route.

ACKNOWLEDGMENT

The authors are grateful to the anonymous referees for their valuable comments and suggestions to improve the presentation of this paper.

REFERENCES

[1]. Secure Payment Scheme with Low Communication and Processing Overhead for Multihop Wireless Networks Mohamed M.E.A. Mahmoud and Xuemin (Sherman) Shen, Fellow, IEEE.
[2]. S. Zhong, J. Chen, and R. Yang, Sprite: A Simple, Cheat-Proof, Credit Based System for Mobile Ad-Hoc Networks , Proc. of Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM03), Vol. 3, pp. 1987-1997, San Francisco, CA, March 30-April 3,2003.
[3]. 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.
[4]. N. Salem, L. Buttyan, J. Hubaux, and M. Jakobsson, Node Cooperation in Hybrid Ad Hoc Networks, IEEETrans. Mobile Computing, vol. 5, no.4, pp. 365-376, Apr. 2006.
[5]. M. Mahmoud and X. Shen, ESIP: Secure Incentive Protocol with Limited Use of Public-Key Cryptography for Multi-HopWireless Networks, IEEE Trans. Mobile Computing, vol. 10, no. 7, pp. 997- 1010, July 2011.
[6]. M. Mahmoud and X. Shen, FESCIM: Fair, E_cient, and Secure Cooperation Incentive Mechanism for Hybrid Ad Hoc Networks, IEEE Trans.Mobile Computing, vol. 11, no. 5, pp. 753-766, May 2012.

BIOGRAPHY

Jyothi Padmanabhan born at Kannur, Kerala, India. She received the B.Tech degree (2012) in Computer Science and Engineering from CUSAT University, Kerala, India. She is now pursuing her M.Tech degree in Computer Science and Engineering from Malabar Institute of Technology, Kannur, Kerala, India. The author's area of interest and research work involve Information Security and Network Security.