Survey on Secure Payment Method in Wireless Sensory Networks Using Low Cost Paying Methods and Hashing Methods

Hemanthkumar K.
M.Tech Student
Department of CSE
East West Institute of Technology
Bangalore, India

Sharada K. A.
Assistant Professor
Department of CSE
East West Institute of Technology
Bangalore, India

Abstract—. We propose RESM, a report-based payment scheme for multi-hop wireless networks to stimulate cooperation, packet transmission can be regulated and fairness can enforce. The nodes submit the lightweight payment reports to the accounting centre (AC) and store the temporary payment reports disputed security tokens called Evidences. The reports contain alleged charges and achievement without any proof of the security, e.g: signatures. The payment can verify from the AC by investigating the consistency of the reports, and the payment of the fair reports can be clear with almost no processing overhead or cryptographic operations. For cheating reports, the Evidences are identify from the regulated and detect the cheating nodes that submit incorrect reports. Instead of the requesting evidences from all the nodes in the cheating reports, RESM can identify the cheating nodes with requesting of the few Evidences. Our simulation and analytical results demonstrate that RESM requires much less communication and processing overhead than the existing receipt-based payment scheme with acceptable clearance storage area and delay. Moreover, RESM payment can secure and accurately identify the cheating nodes.

Index Terms— Cooperation incentive schemes; network- level security and protection; payment schemes; and selfishness attacks.

I. INTRODUCTION

In Multi-hop wireless networks(MWN) defined by Mobile ad-hoc network(MANET),Vehicular ad-hoc network(VANET),Multi-hop cellular network(MCN) and Wireless mess network(MWN).In MWNs can be deployed more readily at less developing cost in rural areas. A node's traffic is usually relayed through the destination of the other nodes. The number of existing protocols assumes that multi-hop wireless network nodes are willing to relay other nodes' packets. Wireless networks are self-organized systems without relaying an any pre existing packets. In recent evaluations have that ad-hoc networks not only flexible and robust, but also can have good performance in terms of throughput, delay and power efficiency. For example, users in one area (In apartment, college campus) having different wireless devices eg; cell phones, laptops, tablet etc can establish a network to communicate share information and distribute files. Selfish nodes will not relay other's packets and use of make the relay of their packets in the cooperative nodes, which self respect of the fairness and the network connectivity. Selfish nodes of the unreliable detection and false accusation of the honest nodes because it is difficult to differentiate between a node's unwillingness and incapability to cooperate eg; due to network congestion.

The payment schemes use credit-based models the packet forwarding task is treated as a service which can be charged and valuated. A fair charging policy is to support the cost sharing between the source and destination nodes when both of the benefited from the communication. The basic payment model contains three parts: the customer, the communicating nodes, the merchant and the packet relaying nodes and the accounting centre or bank. We can argue that a more fair payment approach is to change both packet sources and destinations. In addition to the stimulation of cooperation, these schemes enforce fairness, regulate the packet transmission, efficiency charge for the network services and discourage the message-flooding attacks. Fairness can be something by rewarding the nodes that relay more packets and charging the nodes that send more packets.

A good payment scheme should be scheme should be secure and require less overhead. The existing receipt based payment schemes processing and communication overhead. Since a trusted party may not be involved in session of the communication, the nodes compose proofs of other's packets of the relaying called receipts, and submit them to the accounting centre (AC) to clear the payment. The receipt's size is large they carry security proofs eg: Signature to secure the payment which significantly consumes the nodes resources and submitting the available bandwidth. 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.

In this paper, we purpose RESM a Report based payment Scheme for MWNs. The nodes submit light weight payment reports (instead of receipts) to the AC to update the credit accounts and temporarily store undeniable security tokens called evidences. The reports contain the alleged charges and the rewards of different sessions without security proofs eg: Signature. 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 are to identify and evict the cheating nodes that submit incorrect reports eg: pay less. RESM can identify the cheating nodes with submitting and processing few evidences. Evidence aggregation technique is used to reduce the storage area of the evidences.

II. RELATED WORKS

The existing payment schemes can be distinguished into receipt-based schemes and tamper proof-device (TPD).In tamper proof-device (TPD) is any payment-based approach demands some sort of tamper proofness indispensable for guaranteeing the security process of the payment. In TPD based incentives mechanisms, a TPD are installed in each node manage its credit account and its secure operation. The packet purse and the packet trade models have been defined. In the packet price model, only the source node pays by loading some credits in each packet before sending it. Each intermediate node acquires the amount of credits that cover the relaying cost packet's. In SIP after data packets a receiving, the destination node sends a RECEIPT packet to the source node to issue a REWARD packet to increment the intermediate nodes of the credit accounts. In CASHnet: the source nodes of the credit account are charged and a signature is each packet to attach. Upon packet can receiving, the destination node of the credit account is also charged, and a digitally signed acknowledgement (ACK) packet is sent back to the source node to intermediate nodes of the increase the credit accounts.

In Receipt based payment schemes have been defined to enforce and stimulate node cooperation respectively. In receipt based payment scheme, each network node usually monitors the transmissions of its neighbors to make sure that the neighbors forward other's traffic, and thus selfish nodes can be punished. However the TPD based payment schemes suffer from the following serious problems. First the assumption that the TPD can be tampered is neither secure nor MCNs for practical. That is because the nodes are self-interested and attackers can communication freely in an undetectable way if they could compromise the TPDs.

In Sprite, the source node signs the full paths identify and each transmitted message from append its signature. The intermediate and destination nodes compose receipts and submit them claim the payment to the AC. In express, the source node generates a hash chain for every relaying node ID_k by iteratively hashing random value (V_s) times to hash value Vo obtained. Each time the node IDk relays a message, the source node releases the previous image of the last sent hash value. The source intermediate node and destination nodes compose receipts and submit them to the AC. However the nodes have to store and generate a large number of hash chains because only node in the network may act as an intermediate node to mobility of the node. In Express and Sprite, only the source node pays no matter how the destination node benefits from the communication moreover an intermediate node is rewarded for every successfully relayed packet even if it does not reach the destination, so all the session nodes submit the receipts because a node's packet forwarding is considered successful its next node on the path reports a valid receipt. We call this receipt submission scheme All submitters because all the intermediate nodes submit all the receipts. In Express and Sprite, significant communication and computational overhead is implied due to generating and submitting a large number of receipts because receipts generated per message and all the nodes in a full path submit all the receipts.

In an incentive mechanism has been defined for ad hoc network that is used as access network to connect the nodes to the Internet. The source node signs the identifies of the nodes in the full path and appends this signature to the message, and the destination node signs a receipt and sends it to the last intermediate node to submit the AC. Since only the last intermediate node submits the receipts, we call this receipt submission scheme Fixed submitter. However the defined system does not handle collusion attacks. For example, the communicating nodes can communicate freely and the relaying nodes are not rewarded when the last intermediate node colludes with the payers so as to not submit the receipts.

III. SYSTEM MODEL

1. NETWORK MODEL

The network model includes mobile nodes, a set of base stations and the trusted party (TP).The base stations are connected with each other and with the trusted party is responsible for the security and financial issues in the network. As illustrated in fig1, the considered MWN has mobile nodes and a trusted party. The trusted party (TP) contains the accounting centre (AC) and the certificate authority (CA).The AC contains nodes the CA renews and revokes the nodes and credit accounts. Each node X has to register with trusted party to receive a symmetric key K_x, public/private key pair, and certificate. The symmetric key is used to submit the payment reports and the public/private keys are required to act as source or destination node. The details of the synchronization process are out of the scope of the paper, but number of mechanisms has been defined to synchronize the nodes' clocks. Once the accounting centre (AC) receives the payment reports of a session and verifies them, it clears the payment if the reports are failing; otherwise, it requests the evidences to identify the cheating nodes. The certificate authority (CA) evicts the cheating nodes by denying renewing their certificates.

RESM can be used with any source routing protocol, such as Dynamic source routing (DSR),which establishes end to end routes before transmitting the data. Source nodes' packets may be relayed number of hops by intermediate nodes to destinations. The nodes can contact the trusted party(TP) at least once during a period of few days. In this connection the nodes submit the payment reports and the evidences and received renewed certificates to be able to continue using the network. This connection can occur via the base stations of cellular networks, wired network such as Internet, Wi Fi Hot spots.

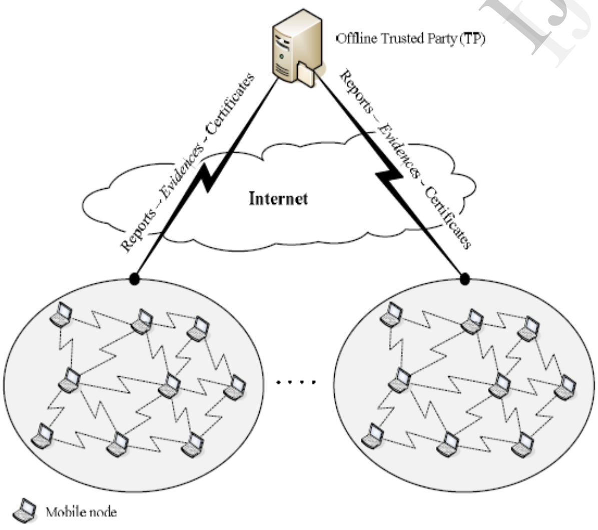
Offline Trusted Party (TP)
Reports – Evidences – Certificates
Internet
Reports – Evidences – Certificates
. . . .
Mobile node

Fig. 1: The architecture of the considered network.

Figure 1: Architecture

IV. PAYMENT MODEL

A fair charging policy is support cost sharing between the source and destination nodes. The source nodes are charged for every transmitted message even if it does not reach destination nodes, but the intermediate nodes are rewarded only for the delivered messages. Some schemes, consider that the relaying of reward a packet is proportional to the relaying the packet of the increased energy, this rewarding policy can be integrated with RESM, we used fixed rewarding rate, eg: λ credits per unit sized packet to simplify focus on our contributions and description. Table 1 gives the used notations in this paper.

Symbol	Description
X, Y	X is concatenated to Y.
F	A flag bit indicating whether the last received packet by a node is for acknowledgement (ACK) or data.
$h^{(i)}$	The hash value number i in a hash chain generated by the destination node.
H(P)	The hash value resulted from hashing P.
$H_K(P)$	The keyed hash value resulted from hashing P using the key K.
ID_A	The identity of an intermediate node A.
ID_S and ID_D	The identities of the source node (S) and the destination node (D), respectively.
K_A	The shared key between node A and the TP.
M_X	The message sent in the *X*th data packet.
n	The number of nodes in a route.
$P_C(n)$	The average payment clearance delay for a route with n nodes.
R	The concatenation of the identities of the nodes in a route, e.g., R = ID_S, ID_A, …, ID_D.
$Sig_S(P)$ and $Sig_D(P)$	The signatures of the source and the destination nodes on P, respectively.
T_{Cert}	The lifetime of a certificate.
Ts	The time stamp of a route establishment.

Table 1: The Useful symbols

ACKNOWLEDGMENT

Special thanks to East West Institute of Technology for helping us in our work and supporting the research. Visveshvaraya Technological research centre are also helping us in this work.

CONCLUSION

The survey on this paper, we have seen a report-based payment scheme for multi-hop wireless networks (MWNs).The nodes submit lightweight payment reports including the rewards and alleged charges, and temporarily stored undeniable security tokens called Evidences. In order to the fairly and efficiently charge the source and destination nodes, the lightweight hashing operations are used to reduce the number of public-key cryptography operations and Evidences are submitted and process only in the case of identify the cheating nodes from the cheating reports in order. Our analytical and simulation results demonstrate that RESM can significantly reduce the communication processing overhead comparing to the existing receipt-based payment schemes with acceptable payment clearance delay and Evidences' storage area,in which process necessary for the effective implementation of the scheme. Moreover, RESM can secure the payment, and identify the cheating nodes rapidly and processing without missed detections.

REFERENCES

.

1. Mohamed M. E. A. Mahmoud and Xuemin (Sherman) Shen, ”A Secure Payment Scheme with Low Communication and Processing Overhead for Multihop Wireless Networks” 2012
2. 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, October, 2007
3. S. Zhong, J. Chen, and R. Yang, “Sprite: A simple, cheat-proof, credit based system for mobile ad-hoc networks”, Proc. of IEEE INFOCOM’03, vol. 3, pp. 1987-1997, San Francisco, CA, USA, March 30-April 3, 2003.
4. M. Mahmoud and X. Shen, “FESCIM: Fair, efficient, and secure cooperation incentive mechanism for hybrid ad hoc networks”, IEEE Transactions on Mobile Computing (IEEE TMC)
5. M. Mahmoud, and X. Shen, "PIS: A practical incentive system for multi-hop wireless networks", IEEE Transactions on Vehicular Technology (IEEE TVT), vol. 59, no. 8, pp. 4012-4025, 2010.
6. M. Mahmoud and X. Shen, "Stimulating cooperation in multi-hop wireless networks using cheating detection system", Proc. IEEE INFOCOM'10, San Diego, California, USA, March 14-19, 2010.
7. J. Pan, L. Cai, X. Shen, and J. Mark, “Identity-based secure collaboration in wireless ad hoc networks”, Computer Networks (Elsevier), vol. 51, no. 3, pp. 853-865, 2007.