ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 2, February 2013

Survey on Routing in Multihop Wireless Networks Using Micropayment Schemes

Presty Kasmir, Sakhi S Anand

***Abstract*— In a multihop wireless network (MWN), the packets from a source node are relayed through a large number of intermediate nodes before they are delivered to the destination. But such relaying of other's packets will consume valuable resources of these intermediate nodes such as their energy and computing power. Hence some nodes, usually referred to as selfish nodes may not cooperate in relaying other's packets and at the same time they make use of other cooperative nodes to relay their own packets. In such a situation we may use some incentive mechanisms based on micropayment to stimulate these selfish nodes to cooperate. There exist a lot of such mechanisms. In this paper we make a survey on a few of them.**

***Index Terms*— Multihop wireless networks, selfish nodes, cooperation stimulation, reputation systems, incentive schemes**

I. INTRODUCTION

A micropayment is an e-commerce transaction involving a very small sum of money in exchange for something made available online, such as an application download, a service or Web-based content. Micropayments are sometimes defined as anything less than 75 cents and can be as low as a fraction of a cent. Micropayments were initially devised as a way of allowing the sale of online content. For these products, the use of payment instruments like on-line credit cards tends to be more expensive than the actual product. For this reason, a micropayment mechanism needs to keep the cost of the individual transaction low. Digital products including music, news, pictures or commodities in online games can be purchased using these micropayments.

Digital products are usually provided through subscription and advertising. In subscription, groups of products are sold as a unit and the access is allowed only for a period of time. Other problems associated with subscription are high administration costs and lack of impulse buying. Due to these reasons consumers are usually hesitant to subscribe. Problems of advertisement are, it is an annoyance for users and only effective for very popular sites. Hence micropayment can be used as an alternative for subscription and advertising. Uses of micropayment include publishing, marketing, software, entertainment and web services. Currently there exist a number of micropayment systems such as Flattr, M-Coin, Payclick, Zong, PayPal etc. Also these micropayment schemes can be used to stimulate mobile nodes to cooperate in relaying other's packets.

Manuscript received Feb 7, 2013.

Presty Kasmir, *Department of Computer Science and Engineering, College of Engineering, Trivandrum.*

Sakhi S Anand*, Department of Computer Science and Engineering, College of Engineering, Trivandrum.*

II. BACKGROUND

A. Basic Concepts

Basic architecture of a micropayment scheme is shown in Fig 1. Basically a micropayment scheme consists of three parties: customers, merchants and a bank. Customer is the one who benefits from the transaction and who pays for it. Merchant is an entity which helps in carrying out the transaction and receives the payment. Bank manages these payment activities. First, a customer has to register with the bank. Then the bank issues a short-term certificate to the customer with which it can compose receipts. Also the customer has to contact the bank periodically to update its certificate. The receipts generated by the customers are send to the merchants for carrying out the transaction. Then merchants contact the bank with these receipts, so that it will clear those receipts by paying merchants and charging the customers.

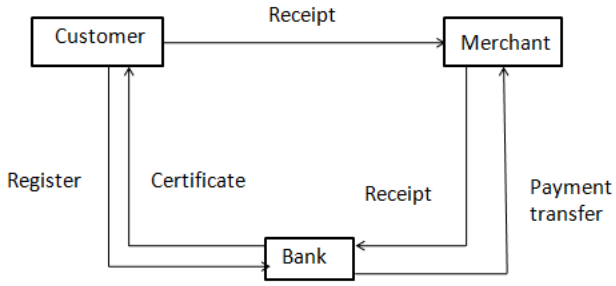

Fig. 1 Micropayment architecture

B. Motivation

In MWNs, the mobile nodes act as routers to relay the source nodes' packets to their destinations. But relaying of packets consumes the intermediate node's valuable resources, such as energy and computing power without any benefits to them. Hence some nodes may selfishly make use of other cooperative nodes to relay their packets but not relay other's packets. Such nodes are called selfish nodes. Sometimes there can be nodes which drop packets intentionally. Hence we need a mechanism to stimulate nodes to relay other's packets and to punish irrational packet droppers who intentionally drops the packets. For that we may use micropayment based systems.

Wireless networks may use credits (or micropayment) to motivate the rational packet droppers to relay packets. The nodes earn credits for relaying others' packets and spend them

to relay their own packets, i.e., these mechanisms make relaying packets more beneficial for the nodes than dropping them. It is impossible to know whether a packet is dropped for malicious or nonmalicious reasons, e.g., due to faulty nodes and bad channel condition; therefore, it is necessary to measure the nodes' frequency of dropping packets, and the nodes that consistently drop the packets are considered attackers because they pose a severe threat to the proper operation of the network.

III. RELATED WORKS

A simple micropayment system namely Payword was proposed by Shamir and Rivest [1] in 1996. It is a credit-based scheme, based on chains of hash values. This protocol involves a customer, vendor and broker, where a customer has to generate a new payword chain for each vendor from which it makes purchase. The customer uses the certificate provided by the bank to make payword chains or hash chains which are analogous to the receipts in Fig. 1. These hash chains are produced using hash functions. Hash functions are faster than signature generation and verification, so they improve Payword's performance. Payword does not provide anonymity. Another micropayment scheme, MicroMint [1] was designed to provide reasonable security at very low cost.

MVPayword [2] is an extension of Payword. This protocol allows the customer to make purchases from different vendors using only one hash chain. But, the payment process is not anonymous. AMVPayword [3] is an extension of MVPayword and it provides anonymity for customers.

[4]-[8] present micropayment schemes to stimulate selfish nodes in MWNs. In [4], first, a payment model is developed for the efficient implementation of micropayment in MWNs. The payment model contains three basic parties: 1) the customer or the communicating nodes 2) the merchant or the intermediate nodes and 3) the bank or the accounting centre (AC). The operations among these parties are as shown in Fig.1. Since both the sender and the receiver benefits from the communication, in this payment model both the sender and the receiver pay for the packet-relaying. Second, an incentive system is proposed based on the developed payment model, to stimulate the nodes' cooperation in MWNs.

The incentive system proposed by [4] consists of three phases: 1) Communication 2) Receipt Submission and 3) Payment Redemption and Colluder Identification. In the Communication phase, the network nodes are involved in communication sessions, and the communicating nodes issue payment receipts to the intermediate nodes. In the Receipt Submission phase, the nodes submit the receipts to the AC to claim their payments. In the Payment Redemption and Colluder Identification phase, the AC clears the receipts and identifies the colluding nodes that do not submit the receipts. Finally, a reactive receipt submission mechanism is proposed to reduce the number of submitted receipts and protect against collusion attacks. One receipt contains the payment data for all the intermediate nodes. Also different receipts can be aggregated to a smaller size aggregated receipt.

Cooperation stimulation mechanisms such as [4] can stimulate the rational packet droppers to relay other's packets. But there are some nodes which drop other's packets intentionally. These cooperation stimulation mechanisms cannot identify such irrational packet droppers. Mohamed Elsalih Mahmoud et.al. [5] proposed a sophisticated mechanism that can prohibit both the rational and irrational packet dropping attacks by adopting stimulation and punishment strategies called TRIPO. TRIPO achieves this by using a micropayment scheme to stimulate the rational packet droppers and a reputation system (RS) to identify and exclude the irrational packet droppers. It proposed a novel monitoring technique to measure the nodes' frequency of dropping packets based on processing the payment receipts instead of using the medium overhearing technique.

In [6], three micropayment based systems are proposed namely ORPay, CoinPay and PlusPay. ORPay is used to implement micropayment in Tor networks. Tor network is a network involving onion routing. Tor routers will be rewarded with micropayments for correct traffic relaying – these can then be aggregated and deposited into accounts provided through a "banking" service run by Tor's directory. The accounts' balance can then be used as actual cash in webclick-like incentive schemes, in QoS enforcement (e.g., by prioritization of traffic) or in reputation-based mechanisms.

A protocol called TETO (Trust-based and Energy-aware routing and incenTive prOtocol) presented in [7] stimulates the intermediate node's cooperation using credits or micropayments. It also processes the payment receipts to check whether the packets are relayed correctly and based on this processing it assigns trust values to the intermediate nodes. Stable routes are then established through the nodes having high trust values.

Mohamed Elsalih Mahmoud et.al. [8] proposed a secure data-forwarding scheme called SATS for delay-tolerant wireless networks. Some malicious nodes may launch black-hole attacks by dropping messages intentionally to degrade the message delivery rate. SATS prevents the selfishness and black-hole attacks by paying credits to the intermediate nodes for relaying other's packets correctly. The payment model of SATS pays per message which causes large communication overheads. Only the source node is charged and the intermediate nodes are rewarded only if the message is delivered to the destination.

IV. CHALLENGES

Micropayment based wireless routing systems suffer from several challenges as given below.

A. Number of Receipts

When we consider the routing in a MWN, the number of transactions is large and multiple merchants or intermediate nodes are involved in a transaction. Hence, generating a receipt per packet or per merchant increases the number of receipts significantly and it will cause high processing cost. Also, processing a large number of receipts may not be feasible. Another problem is that, the nodes have low resources; therefore the overhead of storing and submitting a large number of receipts may stimulate the nodes to behave selfishly.

The receipt size can be reduced by attaching the hash of the

nodes' signatures instead of the signatures [4]-[5]. One way to reduce the number of receipts is to generate one fixed-size receipt per session regardless of the number of transmitted packets [4]. In [5], the nodes store the receipts and submit them in batch to the AC for redemption.

B. *Certificate Updating Frequency*

Customers have to periodically make contact with the bank for updating their certificate. But the choice of this period is an issue. If the period is too small, it will result in high communication overheads. But if it is too large, it will affect some nodes which have relayed a considerable number of packets recently. In that case, actually the credit of those nodes should be high, but it will be updated only after that particular time period, which will adversely affect its capacity to transmit its own packets. The network nodes can contact the AC at least once during a time interval, which can be in the range of a few days [4]-[5], [7]-[8].

C. *Credit Inflation and Credit Depletion*

Credit inflation and depletion occurs when some of the nodes earn a large amount of money while others remaining poor. For credit inflation, the nodes are rich and thus are unmotivated to cooperate, whereas for credit depletion, the nodes are poor and incapable of initiating communication. Thus the network comes to a halting state. One solution for this problem is proposed in [4], in which the AC can convert credits to real money and sell these credits for real money. This motivates the rich nodes to cooperate, thus improves credit distribution, and protects the network from credit decline. But this solution may not be effective in most wireless networks.

V. CONCLUSION

In this paper we surveyed on some micropayment based incentive schemes to stimulate selfish nodes to relay other's packets. Even though they can achieve their goal, they face certain challenges as given in section IV. Credit inflation and credit depletion are two severe challenges faced by the schemes ([4]-[8]). In our future work, we will present an effective mechanism to overcome these difficulties.

REFERENCES

[1] R. L. Rivest and A. Shamir, "Payword and micromint: Two simple micropayment schemes," in Proc. Int.Workshop on Security Protocols, London, U.K., 1997, pp. 69–87.

[2] A. Esmaeeli and M. Shajari, "MVPayword: Secure and Efficient Payword-Based Micropayment Scheme", *Second International Conference on the Web Technologies (ICADIWT)*, 2009.

[3] Mona Hosseinkhani, Ebrahim Tarameshloo and Mehdi Shajari, "AMVPayword: Secure and Efficient Anonymous Payword-Based Micropayment Scheme", *International Conference on Computational Intelligence and Security*, 2010.

[4] Mohamed Elsalih Mahmoud and Xuemin Shen, "PIS: A Practical Incentive System for Multihop Wireless Networks", IEEE Transactions on Vehicular Technology, Vol.59, No.8, October 2010.

[5] Mohamed Elsalih Mahmoud and Xuemin Shen, "An Integrated Stimulation and Punishment Mechanism for Thwarting Packet Dropping Attack in Multihop Wireless Networks", IEEE Transactions on Vehicular Technology, Vol.60, No.8, October 2011.

[6] Bogdan Carbunar, Yao Chen, and Radu Sion, "Tipping Pennies? Privately Practical Anonymous Micropayments", IEEE Transactions on Information Forensics and Security, Vol. 7, No. 5, October 2012.

[7] Mohamed Elsalih Mahmoud and Xuemin Shen, "Trust-Based and Energy-Aware Incentive Routing Protocol for Multi-hop Wireless Networks", in *Proc. IEEE ICC*, 2011.

[8] Mohamed Elsalih Mahmoud, Mrinmoy Barua and Xuemin Shen, "SATS: Secure Data-Forwarding Scheme for Delay-Tolerant Wireless Networks", in *Proc. IEEE Globecom* , 2011