A Survey on Credit Based Scheme for Multihop Wireless Network

Linu Ann Joy[1] Divya T.V[2]
[1]M.Tech [2]Assistant Professor
[1,2]Department of Computer Science and Engineering
[1,2]Federal Institute of Science and Technology (FISAT), Angamaly, India

Abstract--Wireless Network (WSN) is an evolving technology that has various applications both for mass public and military. The performance of wireless networks depends on the cooperation of all active nodes. However, supporting a wireless network is a cost-intensive activity for a mobile node. For a single mobile node perspective, the detection of routes as well as forwarding packets consumes local CPU time, memory and bandwidth. Sometimes the mobile nodes denying the packet of other nodes, while at the same time use their services to deliver its own data. This behaviour of an independent mobile node is commonly known as misbehaving or selfishness. There are different schemes used for minimizing malicious behaviour of mobile nodes. Here provide different payment based schemes that provide co-operation among nodes in the network.

Keywords: Cooperation incentive schemes, network-level security and protection, payment schemes, trusted based system and selfishness attacks

I. INTRODUCTION

A computer network is a telecommunications network that connects a collection of computers to allow communication and data exchange between systems, software applications, and users. The computers that are involved in the network that originate, route and terminate the data are called nodes. The interconnection of computers is accomplished with a combination of cable or wireless media and networking hardware. Multihop Wireless Network (MWN): A wireless network adopting Multihop wireless technology without deployment of wired backhaul links. It is similar to Mobile Ad hoc Networks (MANET), Nodes in the MWN is relative 'fixed'.

Mobile ad-hoc network is one of the most promising fields for research and development of wireless network. As the popularity of mobile device and wireless networks significantly increased over the past years, wireless ad-hoc networks has now become one of the most vibrant and active field of communication and networks. A wireless network is a decentralized type of wireless network. The network is ad hoc because it does not rely on a pre-existing infrastructure, such as routers in wired networks or access points in managed wireless networks. Instead, each node participates in routing by forwarding data for other nodes, so the determination of which nodes forward data is made dynamically on the basis of network connectivity.

For example users in a college campus having different wireless devices such as cell phones, laptops etc. in order to share information and distribute files they can establish a communication. The assumption is that each node willing to share its resources such as clock cycles, bandwidth etc. There are selfish nodes they doesn't relay others packet and uses cooperative nodes to relay their own packets, this causes performance degradation and failing of multihop networks. To avoid this a payment scheme is introduced such that when a node relays forwarded packet they get a credit and that credit can be used for forwarding self-generated packet also.

Wireless networks have many applications in various fields including military, environmental, health and industry and all these applications require secure communications. Wireless networks are more vulnerable to attacks than wired ones because of the broadcast nature of transmission medium. The security in wireless network is extremely important. Many securities had been designed for wired and wireless networks but they can't be used in wireless sensor networks because of the limited energy, memory and computation capability. Here for avoiding the selfish behaviour of nodes different credit based schemes are used. The works in a way that when a node relay the packet of other node they get a credit. This credit can be used for them to relay their own packet also.

The remainder of this article is organized as follows: Section II describes the Survey related to credit based scheme Section III gives the comparison of various schemes. Section IV gives the new proposal used to minimize the communication overhead. Finally Section V summarises the technologies used.

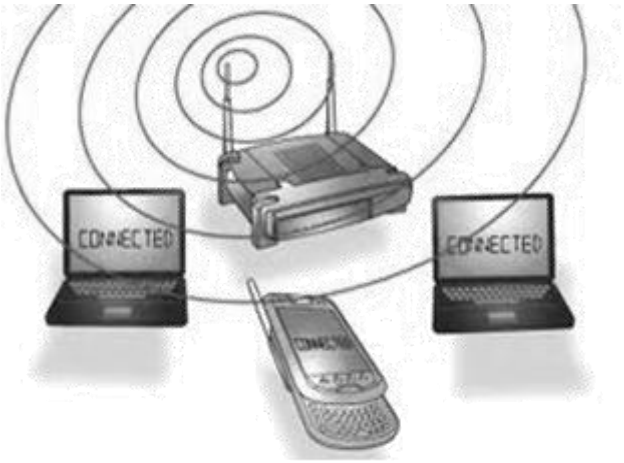

Fig. 1:

II. SURVEY

The existing payment schemes can be classified into Tamper-proof-device (TPD)-based, 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 operation. For receipt-based payment schemes an offline central unit called the accounting centre (AC) 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. CREDIT BASED SCHEMES

The following section deals with various credit based schemes

1) RACE

RACE: Report based payment scheme for Multihop wireless networks [1], there are mobile nodes and an accounting centre (AC).After the end of the communication session each nodes sends a payment report to the AC.AC verifies it and determine the fair report and cheating report. Here onion hashing algorithm is used for evidence aggregation .For identifying cheating report evidence is requested from some of the nodes not all. The disadvantage is it has no method for identifying cheaters during the route establishment phase itself and also finding attackers or unauthorized nodes. More overhead is caused when evidence is requested.

2) TPD BASED SCHEME

Stimulating co-operation in self-organizing mobile Adhoc networks [2], here its own and forwarded packets by a node are passed to the TPD that decrease and increase the node's credit account. Here a Packet purse models have been proposed. Packet purse model, here before sending a packet the source node credit is fully charged, and each intermediate node acquires the payment for relaying the packet. For each packet, the source node increases its paid credits with the same number of the intermediate nodes to pay a credit for each node regardless whether the packet reaches the destination or not. Several security measures have been taken to thwart false accusation, stealing credits attacks. Here no mechanism is proposed.

3) CASHNet

Cooperation and accounting in multi hop cellular networks [3], In CASHNet, source node is charged with a certain credit and a signature is attached to each data packet.

Upon receiving the packet, the credit account of the destination node is also charged, and a signed acknowledgement (ACK) packet is sent back to the source node to increase the credit accounts of the intermediate nodes. The advantage is we allow selfish nodes, but encourage them to participate in packet forwarding via rewards. We allow initiator as well as receiver based payment. The disadvantage is not actively handle malicious behaviour of nodes.

4) SPRITE

Sprite: A simple cheat proof credit based system for mobile adhoc networks [4],here before sending the message to the intermediate node source node signs it and the intermediate node verifies it.AC verifies the signature and assure that the payment is correct. It does not require any tamper proof hardware, mainly focuses on node selfishness. Node receives a message; it keeps a receipt of the message. It uses Credit to provide incentive to selfish nodes. There is a credit clearance system that determines the credit of each node that relay message more successfully. Depending upon the receipts submitted, CCS determines charge and credit to each node. Disadvantage is that it charges only the source node, it generate receipt per message that causes overhead.

The major issues to be addressed

1. Security Aspect
   Each node is autonomous and the charge and credit is based on receipts submitted by each node.
2. Incentive Aspects
   Node should receive enough credit for forwarding a message so it can send its own message with the received credit

5) FESCIM

FESCIM: Fair, Efficient, and secure cooperation incentive mechanism for hybrid adhoc networks [5], in case of [4] that charges only the source node, but in this source and destination node is charges, both of them are interested in communication. IN order to securely charge the nodes a light weight hashing operation is used in the ACK. The advantage is that one small size check is generated per session. It reduces the no of public key cryptographic operation. The payment nonrepudiation can be achieved using a hash chain at the source node side.

6) DSC

DSC: Cooperation Incentive Mechanism for Multi-Hop Cellular Networks [6], in this a micropayment mechanism is used for the stimulation of node cooperation. This does not require a TPD installed on all the nodes and an online interactive authority. Charges both the source and destination nodes efficiently. Instead of generating signatures from the source and destination nodes to protect the payment, the destination node uses the efficient hash chain. Here the payment is aggregated and reduce the number of receipts generated.

7) ESIP

In ESIP [7], the source and destination nodes generate signatures only for one packet and the efficient hashing operations are used in the next packets to achieve payment non-repudiation and protect against free riding attacks. SIP 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. One of the disadvantage is it has largest receipt size.

8) PIS

PIS [8], the source node attaches its signature to each transmitted message and the destination node replies with a signed ACK. In the Communication phase, 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. PIS can reduce the receipts' number by generating a fixed-size receipt per session regardless of the number of messages instead of generating a receipt per message in Sprite. The reactive receipt submission mechanism has been proposed to reduce the number of submitted receipts and protect against collusion attacks. The disadvantage is less storage area and processing overhead is high

9) CDS

Stimulating cooperation in multi-hop wireless networks using cheating detection system [9], here using a cheating detection system (CDS) which uses statistical methods to secure the payment. The basic idea is that, the network nodes independently and periodically submit their activity reports containing the financial data resulted from sessions

they participated in. The cheating detection system investigates the trustworthiness of the reports and identifies the cheating nodes. It is easy to identify cheating actions. Instead of generating a receipt per packet one activity report that contains payment information for a large number of packets is issued. It reduces the consumed storage space. The disadvantage is some cheating nodes may not be identified which is called missed detections. It may take long time to identify the cheating nodes.

10) IDENTITY BASED SCHEME

Identity-based secure collaboration in wireless ad hoc networks [10], in this each node has to contact the AC in each communication session to get coins to buy packets from the previous node in the route. Here the packets' buyers contact the AC to get deposited coins and the packets' sellers submit the coins to the AC to claim their payment. Peer (e.g., a user carrying a battery-powered laptop computer with wireless LAN interfaces) joins a group of other peers. Peers have to be assured that they indeed exchange information with intended peers, even when they no longer communicate with each other directly. Peers have to be assured that the confidentiality, integrity, and authenticity of information exchange are not compromised. The disadvantage is the interactive involvement of the AC in each session is inefficient, causes long delay, and creates a bottleneck.

11) SIP

A secure incentive protocol for mobile ad hoc networks [11], the basic idea is, each node imprints a non-forged "stamp" on each packet forwarded as the proof of forwarding. Based on which packet relays are remunerated, while packet sources and destinations are charged with appropriate credits. In SIP, after receiving a data packet the destination node sends a RECEIPT packet to the source node. To issue a REWARD packet to increment the credit accounts of the intermediate nodes. It is immune to a wide range of attacks and is of low communication overhead and can withstand a wide range of cheating actions by using hash functions intelligently. The disadvantage is node selfishness it can avoid by combine SIP with reputation based approaches to provide a unified solution against node selfishness.

III. COMPARISON OF DIFFERENT CREDIT BASED SCHEMES

Credit based schemes in earlier networks are assessed based on some evaluation metrics overhead, security.

A. Overhead

The amount of processing time used by system software, such as the operating system, TP or database manager. In communications, the additional codes transmitted for control and error checking, which take more time to process. The different overhead in the networks are storage overhead, payment clearance delay.

B. Security

Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to

Data in a network, which is controlled by the network administrator

Serve as passive routers without knowing the secrets that they help to forward. This can lower the key disclosure probability.

IV. PROPOSED SYSTEM

The existing schemes suffer from many drawbacks. In order to avoid all these shortcomings a new method was proposed a trusted and attacker free credit based system for multihop wireless networks in order to provide node cooperation, efficient data transmission, low storage overhead and high performance. To provide efficient data transmission first of all establish a route containing honest and cheat proof nodes, for this we introduce a trust and attacker free system. In this during the route establishment we find certain nodes and compare it with the nodes present in the trusted party and nodes present in the cheater log.

When a new node wants to enter in to the communication first of all it will contact the trusted party, and TP share a secret key with the node. Then only the node is considered as genuine. However an attacker or an unauthorized node is found by comparing the node in the route with the node present in the TP. If an attacker is found the we can try another path or attacker node is evicted from the system. When a node behaves like cheater node during the communication put that node in to cheater log by doing this we can easily identify cheaters.

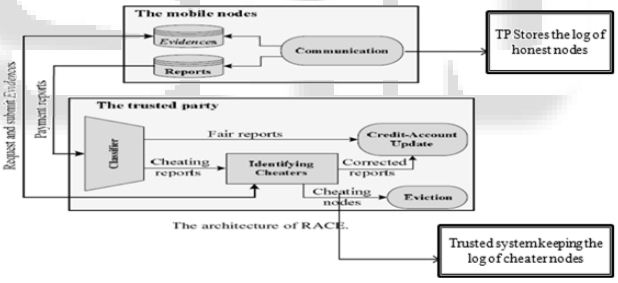

Fig. 2 Proposed Architecture

This will increase the performance of the system. Fig 2 describes the proposed architecture that includes the identification of attacker nodes and also identification of cheater nodes. This provides the system more secure and less communication overhead. Fig 2 describes the comparison of different credit based schemes. Comparison is based on storage area, communication overhead, payment clearance delay, security.

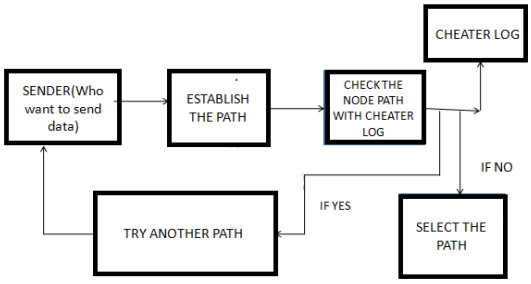

Fig. 3: Proposed Cheater Scheme

In this method cheater is found by, when the communication starts the sender who want to send the data first broadcast the message and path is established. Then the trusted party check the node list with the node present in the cheater log. If the node present in the cheater log then trusted party reports it and the sender select another path for communication. If the nodes are not present in the cheater log the sender can proceed with the path initially selected. This method improves the security for communication.

V. CONCLUSION

The survey on this paper is based on credit based scheme for trusted and attacker free credit systems for wireless networks. Because of the nature of limited resources on wireless nodes, many researchers have conducted different techniques to propose different types of payment schemes. All the schemes have some advantages as well as some disadvantages. Here describe different payment scheme to enforce node co-operation and avoid selfish nodes in the network. A good credit based scheme should be secure and require less overhead. It also secures the data transmission in the network.

PAPER	APPROACH	COMMUNICATION OVERHEAD	STORAGE AREA	PAYMENT CLEARANCE DELAY	SECURITY
RACE	Payment Based Scheme	Low communication overhead	More storage area	Low payment clearance delay	1)No mechanism for identifying cheater nodes and attacker nodes
CDS	Credit Based Scheme	Low communication overhead	Less storage area	Large payment clearance delay	1)False Detection 2)Long time to identify Cheaters
CASHnet	TPD Based Scheme	HIGH	LOW	LOW	1) Not handle malicious behavior of nodes.
SPRITE	Receipt Based scheme	High communication overhead	More storage area than CDS	Low payment clearance delay	1)vulnerable to collusion attack 2)Difficult to identify Cheaters
FESCIM	Receipt Based scheme	High communication overhead	More storage area than CDS	Low payment clearance delay	1)vulnerable to collusion attack 2)Difficult to identify Cheaters
DSC	Payment Based Scheme	1)No TPD is installed in each node.	More storage area	Micropayment scheme to provide node cooperation	1)Difficult to identify cheaters 2)False detection
ESIP	Receipt Based scheme	High communication overhead	More storage area than RACE	Low payment clearance delay	1)Large receipt size 2)High security than Race
PIS	Receipt Based scheme	Low communication overhead	More storage area than RACE	Long payment clearance delay than RACE	1) High security than Race 2)Processing overhead is high

Fig. 4: Comparison of various schemes

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 adhoc 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, p4012-4025, 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

[8] Networks (Elsevier), vol. 51, no. 3, pp. 853-865, 2007.

[9] 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.

[10] M. Mahmoud and X. Shen, "ESIP: Secure Incentive Protocol with Limited Use of Public-Key Cryptography for Multi-Hop Wireless Networks," IEEE Trans. Mobile Computing, vol. 10, no. 7, pp. 997-1010, July 2011.

[11] 10.J. Pan, L. Cai, X. Shen, and J. Mark, "Identity-Based Secure Collaboration in Wireless Ad Hoc Networks," Computer Networks,vol. 51, no. 3, pp. 853-865, 2007.

[12] 11 Y. Zhang, W. Lou, and Y. Fang, "A secure incentive protocol for mobile adhoc networks", ACM Wireless Networks, vol. 13, no. 5,pp. 569-582, October, 2007

