INTERNATIONAL JOURNAL OF COMPUTER SCIENCE ENGINEERING RESEARCH AND DEVELOPMENT (IJCSERD)

ISSN 2248 – 9363(Print)
ISSN 2248 – 9371(Online),
Volume 4, Number 2, April- June (2014), pp: 34-40
© PRJ Publication, http://www.prjpublication.com/IJCSERD.asp

IJCSERD

© PRJ PUBLICATION

A SECURE PAYMENT SCHEME IN MULTIHOP WIRELESS NETWORK BY TRUSTED NODE IDENTIFICATION METHOD

[1]Soumya A V, [2]Mrs.Prajna M R

[1]Dept of CS&E VTU, Belgaum KVGCE, SULLIA, DK-574327
[2]Assoc.prof, Dept of CSE VTU, Belgaum KVGCE, SULLIA, DK-574327

ABSTRACT

The papers propose an improvised version of the report based payment scheme by adopting a trust system which will assign trust value for each and every node in the network. In report based payment scheme the nodes submit light weight payment report to the Trusted Third party .By checking the consistency of the report the third party classify the reports to fair report and cheating report. If it is a fair report means there is an immediate payment clearance. Otherwise trusted party will ask evidence from all the nodes and cheater nodes are evicted. To increase the performance the proposed system will assign trust value for all the nodes in the network. The nodes have high trust value if they relay more messages successfully in the past. So that packet transmission will be through highly trusted nodes which will reduce probability of dropping messages. Thus increase packet delivery ratio and through put and hence network performance.

Index Terms: Payment schemes; Trust value; Trust centre; cheater node.

I. INTRODUCTION

In Multihop wireless Network the packets from a node is usually transmitted through the intermediate node to reach to the destination [1]. There will be some selfish nodes that will not relay others packets but they make use of others to relay their messages which will give a negative effect hence, there is performance degradation [2]. Payment scheme will give credit to all the nodes participated in the packet transmission which motivate the nodes [3]. This scheme treats the packet forwarding task as a service which can be charged and valuated. This scheme enforces fairness, node cooperation, regulate packet transmission.

A high-quality payment scheme should be secure and need less communication and processing overhead. MWNs can't be implemented without a secured payment scheme because the nodes are autonomous and aim to maximize their welfare. Since a trusted party may not be involved in communication session, the nodes create proofs of other's packets of the transmitting called receipts, and for getting the payment they will submit receipts to the Accounting Centre (AC).Here the receipt carries security proof so they are large in size. The AC must carry out large number of cryptographic operations to certify the receipts which leads to communication and processing overhead. In report based schemes the nodes submit light payment reports to the trusted third party to update the credits. The reports contain the alleged charges and the rewards of different sessions without security proofs. The trusted third party verifies the consistency of the report and categorizes them into fair or cheating report. Without any cryptographic operations trusted party will clear the payment for fair report. If it is a cheating report then evidences is requested to discover and evict the cheater node.

To increase the performance of report based payment scheme the trust centre will give a trust value for the nodes in the network. Trust values are assigned based on the past performance of the nodes. Thus communication is always routed through the nodes with higher trust values which will reduce the probability of message failure and enhance the delivery ratio and throughput.

The rest of the paper is structured as follows. Section 2 describes related works of this area .Section 3 presents the proposed system. Section 4 discusses the experimental work .Then description of the performance discussion in section 5 and conclusion in section 6.

II. RELATED WORKS

In these days several researches have come up with several payment schemes including tamper-proof-device (TPD)-based [4] 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 operation. In tamper proof-device (TPD) is any payment-based approach require some kind of tamper proofness essential for guaranteeing the security process of the payment.

In Nuglets [4], the forwarded packets by a node are passed to the TPD to decrease and increase the node's credit account. In SIP [5] after getting data packets, the destination node sends a RECEIPT packet to the source to issue a REWARD packet to increment credit count of intermediate node.

In CASHnet [6], the credit account of the source node is charged and a signature is attached to each packet. When the packet is received, the credit account of the destination node is charged, and a digitally signed acknowledgement (ACK) packet is send back to the source.TPD based schemes have lot of limitations. First the assumption that TPD can't be tampered with. But if the attacker can compromise with the TPD then he can communicate with the TPD in an unnoticeable way.

To eliminate the use of TPDs, an offline central bank called the Accounting Center is used to store and administer the nodes credit accounts. Different receipt based schemes [12] are SPRITE, PIS, CDS, FESCIM, ESIP.

In sprite [7] 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, create receipts which contain the identities of the nodes in the path and the source's signature, and submit the receipts to the AC to get the payment. After verification AC give the payments. The problem is the communication overhead

In FESCIM [8] the source and destination is charged, if they are interested in communication. In PIS [9], the source adds a signature to each message and the destination node acknowledges with a signed packet.

CDS [10] uses statistical methods to find the cheater nodes. Due to the nature of statistical method some sincere node may incorrectly accused as cheater. Some cheaters may not be recognized.

ESIP [11] suggests communication protocol that can be used for a payment scheme. ESIP transmits messages from the source to destination node with limited number of public key cryptography operation by integrating public key cryptography, identity based cryptography and hash function. Comparing to PIS, ESIP needs less public key cryptography operations but larger receipt size.

In proposed paper to avoid the communication and processing overhead of the existing schemes introducing report based payment scheme and using a trust system to improve the performance.

III. PROPOSED SYSTEM

In the proposed system the considered Multihop Wireless Network has an offline Trusted party(TP), responsible for maintaining the nodes credit account.TP is also responsible for cancel and update the certificate for nodes.ie, TP has Accounting Centre, Certificate Authority and Trust centre. Trust centre is responsible for maintaining the trust value of the node according to the no of relayed and dropped messages. Each node has to register with TP to get symmetric key, public key/private key and certificate. Only registered nodes can communicate each other. After the communication session the TP will verify the payment report submitted by the nodes and clear the payments if the report is consistent. This scheme can be used with any dynamic source routing protocol which set up end to end route before sending the data.

As shown in fig.1 the payment scheme has 5 main phases. The first phase is communication phase. In this Route is established through highly trusted nodes and data is transmitted. Second is classifier which classifies the report into fair or cheating. From the cheating report the trusted party will discover the cheaters by asking evidences from the suspicious nodes. .This is fourth phase called Identifying cheaters. Then the trusted party evicts the cheaters from the network. The next is credit account update .In this phase the correct credit is assigned to all the nodes by trusted party. After the packet transmission the trust centre assigns the trust value for the nodes, participated in the packet transmission.

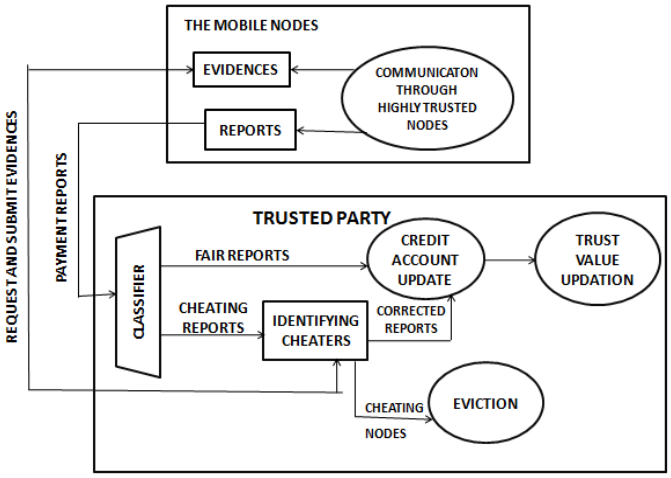

Fig.1 Architecture of proposed scheme

A. Communication

The communication phase includes 4 processes: Route establishment, Data transmission, Evidence composition, payment composition/submission. The source node broadcasts the route request which contains the source identity, Destination identity, Time stamp and Time To live. Time To live means maximum number of intermediate nodes. The route is established by considering the nodes that have high trust values. The node that relay more messages in the past have high trust values. So during route establishment instead of considering shortest path they will consider the route with nodes having high trust values as in figure.2. So that chance of message dropping is less. The nodes that relay more messages have high trust value. After route establishment data is transmitted and destination node replies with acknowledgement. Then the intermediate node composes the evidences for data transmission. All the nodes participated in data transmission compose payment report and submitted to the trusted party.

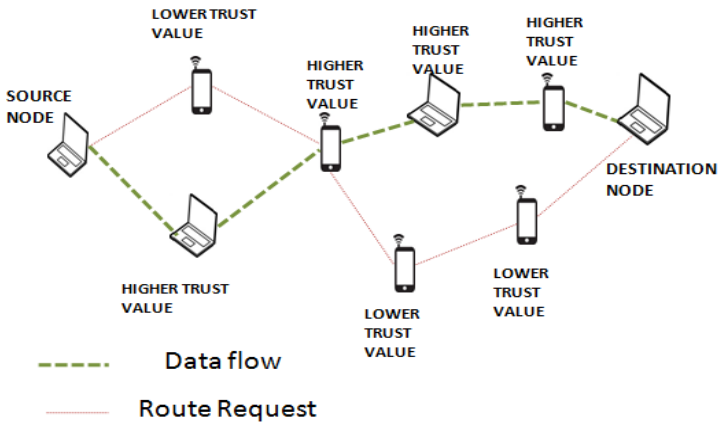

Figure 2. Data transmission through high trusted nodes

B. Classifier

When Accounting Centre obtains the session's payment report it verifies them by checking the consistency of the report and categorize them into fair or cheating. In the case of fair report all the nodes will be submitting the correct payment report so all will be asking for equal credits but for cheating report at least one node will submit incorrect payment report. Fair report can be for complete and broken sessions. For fair report the trusted party will do payment clearance immediately. The evidence is legal if the calculated proof is similar to the evidences.

C. Identifying Cheaters

The Trusted party processes the cheating report to identify the cheaters. The objective is to avoid the attackers from stealing credits. The Trusted party asks evidence from the node which requests more payment. In this way, the AC can precisely identify the cheating nodes with requesting few Evidences .To verify the evidences the Trusted party creates the proof by generating the nodes signature and hashing them. After identifying the cheaters the cheater node is evicted from the network.

D. Credit Account Update

The Credit-Account Update phase obtains fair and corrected payment reports to update the credit of the nodes.The payment clearance is done by charging and rewarding policy. For the payment clearance the trusted party needs reports from all the nodes in the communication session. When registration the trusted party will give a Public and Private Key pair, a symmetric key and a certificate. The public and private key pair is used in communication are required to act as source or destination node. The symmetric key is used to submit the payment reports.

E. Trust Value Update

The Trust centre assigns the trust value to the nodes that relayed the packets success fully in the communication session. This trust value of the node is considered during the next route establishment phase. Stationary nodes and nodes with large resources to spare will have higher trust value .Nodes at the boundary are more likely to have lower trust value.

IV. EXPERIMENTAL WORK

All the nodes must be registered with the trusted third party, in order to issue certificate for the nodes. In order to transmit the packets from source to destination the source node produces route request which contains source node identity, destination identity, Time stamp and TTL. Then the source node broadcast the request to all the intermediate nodes. The intermediate node forwards this route request to the next intermediate node until it reaches the destination. The destination node send route selection request to the trusted party to get a path which has a high trust value. Once the path is established by the destination node the source node transmit the packets to the destination node through the established route.

After transmitting the packets the nodes can request for the payment .So all the nodes submit the payment report together to the trusted third party. The trusted third party verifies it. If it is consistent means the report will be fair. But the attacker or cheater they will always request for more payment without relaying the packet .So the trusted party can easily find out the cheater by checking the consistency. The trusted party can ask for the evidence and if it is

not valid then trusted party can assign a cheating count to the node. So during the next route establishment the nodes having high cheating count is rarely considered.

V. PERFORMANCE DISCUSSION

The performance of proposed scheme is more in terms of throughput and packet delivery ratio. Since this method assigns a trust value for the nodes according to the number of messages relayed in the past and the packet transmission is through the high trust valued nodes, the probability of dropping of messages will reduce. Since the payment clearance in report based scheme is with almost no cryptographic operations, the processing overhead is less and less payment delay is less. Since all the nodes submit the report together the report based payment scheme reduces the communication overhead.

VI. CONCLUSION

The proposed system improves the performance of the network and provides a secure payment scheme. In this there is a trust system which will assign trust value to each node that relayed the packets more successfully in the past. The report based payment scheme eliminates the communication and processing overhead of other payment schemes and the inclusion of trust centre significantly improves the performance of the network since the data transmission is routed through highly trusted nodes whenever possible.

REFERENCES

[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] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. MobiCom '00, pp. 255-265, Aug. 2000.

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

[4] 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.

[5] 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, Oct. 2007.

[6] A. Weyland, "Cooperation and Accounting in Multi-Hop Cellular etworks," PhD thesis, Univ. of Bern, Nov. 2005.

[7] S. Zhong, J. Chen, and R. Yang, "Sprite: A Simple, Cheat-Proof, Credit based System for Mobile Ad-Hoc Networks," Proc. IEEE INFOCOM '03, vol. 3, pp. 1987-1997, Mar./Apr. 2003.

[8] M. Mahmoud and X. Shen, "FESCIM: Fair, Efficient, and Secure ooperation Incentive Mechanism for Hybrid Ad Hoc Networks,"IEEE Trans. Mobile Computing, vol. 11, no. 5, pp. 753-766, May 2012.

[9] M. Mahmoud and X. Shen, "PIS: A Practical Incentive System for Multi-Hop Wireless Networks," IEEE Trans. Vehicular Technology,vol. 59, no. 8, pp. 4012-4025, Oct. 2010.

[10] M. Mahmoud and X. Shen, "Stimulating Cooperation in Multihop Wireless Networks Using Cheating Detection System," Proc.IEEE INFOCOM '10, Mar. 2010.

[11] Networks," IEEE Trans. Mobile Computing, vol. 10, no. 7, pp. 997-1010, July 2011

[12] N. Salem, L. Buttyan, J. Hubaux, and M. Jakobsson, "Node Cooperation in Hybrid Ad Hoc Networks," IEEE Trans. Mobile Computing, vol. 5, no. 4, pp. 365-376, Apr. 2006.

[13] 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