A Secure Processing on Payment Reports with Advanced Encryption Standard in Multihop Wireless Networks

Kesavan P[#1], Selvavinayagam G[*2]

[#] *Post Graduate student, Department of IT, SNS college of Technology, coimbatore-641035, India.*
[1]kesavank7pk@gmail.com

[*] *Assistant Professor, Department of IT, SNS college of Technology, coimbatore-641035, India.*
[2]ohmselva@gmail.com

Abstract - **A system is proposed as SPAES, Secure Processing on Payment Reports with Advanced Encryption Standard in Multihop wireless networks. The node submits report to the trusted party after the communication was over and store a reports called Proofs. The report includes the session information. The trusted party verifies the report by consistency of the report and clears the payment of correct reports. The nodes which do not pass or relay others packets is called selfish nodes. For cheating reports proofs are requested to identify and remove cheating node from the network. In the Trust system is all the attacker nodes are removed before beginning the communication and a trust value was assigned to all the nodes. After removing the selfish nodes, communication can be efficiently established again with increased throughput and less amount of processing and communication overhead. System is essential for the effective implementation of a payment scheme because it uses micropayment and the overhead cost should be much less than the payment value. Trust system will improve the security of the system using AES (Advanced Encryption Standard) algorithm and System has low communication overhead, processing overhead. All nodes details are provided by the Trusted Party (TP).**

Index Terms - **Trusted Party (TP), System-level security and protection, Payment schemes, Trusted based system, Selfishness attacks and Processing & Communication Overhead.**

I. INTRODUCTION

A 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. Multihop Wireless Network (MWN): A wireless multihop networks is end to end relay packet transmission. It is similar to Mobile Ad hoc Networks, Nodes.

The traffic originated from a node is usually relayed through other nodes to the destination. Multi-hop relaying can extend the communication range using limited transmit power, improve area spectral efficiency, and enhance the network throughput and capacity. Moreover, these networks can be deployed more readily and at low deployment cost in developing or rural areas. However, due to involving autonomous nodes in packet relay, the routing process suffers from new security challenges that endanger the practical implementation of the MWNs.

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.

In multihop networks such as mobile ad hoc networks selfish or misbehaving nodes can disrupt the whole network and severely degrade network performance. Trust based models are one of the most promising approaches to enforce cooperation and discourage node misbehaviour. Trust value is calculated through direct interactions with the nodes and/or indirect information collected from neighbours. Trust value is evolved on each node through monitoring or observing its direct interactions and a node can trust its direct information more than the indirect information.

II. RELATED WORKS

RACE: Report based payment scheme for multihop wireless networks, 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 [1].

Sprite: A simple cheat proof credit based system for mobile adhoc networks ,here before sending the message to the intermediate node source node signs it and the intermediate node verifies it. Accounting Center 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 [3].

FESCIM: Fair, Efficient, and secure cooperation incentive mechanism for hybrid adhoc networks, in case of 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 non repudiation can be achieved using a hash chain at the source node side [4].

PIS: Practical Incentive Protocol, 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 [5].

III. SYSTEM DESIGN

The network model consists of set of mobile nodes and Trusted Party. The Trusted Party contains Accounting Center and a Certificate Authority (CA). Each node register with the trusted party to share a secret key between them and this key is used for the entire communication. After the session is completed each node sends a report to the Accounting Center. Once the Accounting Center receives the report it verifies reports and clear the payment if the reports are fair else it request evidence to identify the cheating nodes and cheating nodes are placed in to a list called cheater log, that make the system trusted. Trusted Party also maintains a log that contains the details of the entire registered node that make the system attacker free. The advantage is that it provides more effective secure communication with low overhead.

SPAES can be used with any source routing protocol such as Trust based routing protocol, which establishes an end to end connection before transmitting the data. During the connection establishment phase itself it avoids the attacker or unauthorized node. Secure processing on Payment reports is used to AES algorithm. Trust based routing protocol used in this payment reports it more secure communication.

Comparison between SPAES and the
Existing Payment Schemes:
Table 1.Comparsion between existing System

PAPER	**SPAES**	**RECEIPT BASED SCHEME**	**TPD BASED SCHEME**	**CDS**	**RACE**
COMMUNICAT ION OVERHEAD	Low	High	High	Low	Low
STORAGE AREA	Higher then RACE	More	Low	Less	More
PAYMENT CLEARANCE DELAY	Less	Less	Less	Large	Low
SECURITY	Higher security	1)vulnerable to collusion attack 2)Difficult to identify Cheaters	Not handle malicious behaviour of nodes	1) False Detection 2)Long time to identify Cheaters	No mechanism for identifying cheater nodes and attacker nodes

In this payment reports processing establishing route a trust based protocol is used, it means before the route establishment phase it check the selected nodes in the route is valid, Trusted party maintain the trust value by each node, it contain valid credit for communication, valid certificate, whether these nodes are cheater, attacker. If the checking is successful then only the corresponding path is selected otherwise rejected.

Fig 1 shows the architecture of SPAES in this there is a mechanism for finding both attacker and cheater nodes.

This will increase the performance of the system. Fig 1 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 shows how to find the cheater node, when a node want to communicate the first phase is route establishment in this time itself it check whether the selected route contain attacker node, whether nodes present in the cheater log, source is valid, source have a valid certificate and source have enough credit if all these conditions valid then particular route is selected otherwise ignore that route and inform the source to select other route.

In Fig 3 it shows the mechanism to identify attacker nodes in the network. Before the data transmission begins route is established and the nodes in the routes are sends to the trusted party.

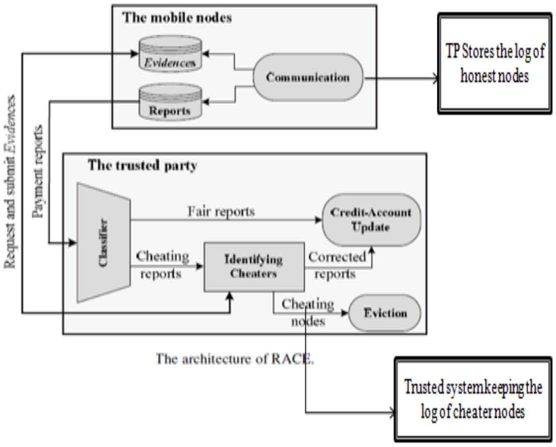

Fig 1: Proposed architecture

Fig 2 describes the comparison of different credit based schemes. Payment reports Comparison is based on storage area, communication overhead, payment clearance delay, security.

In trust based routing protocol 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 is checking 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.

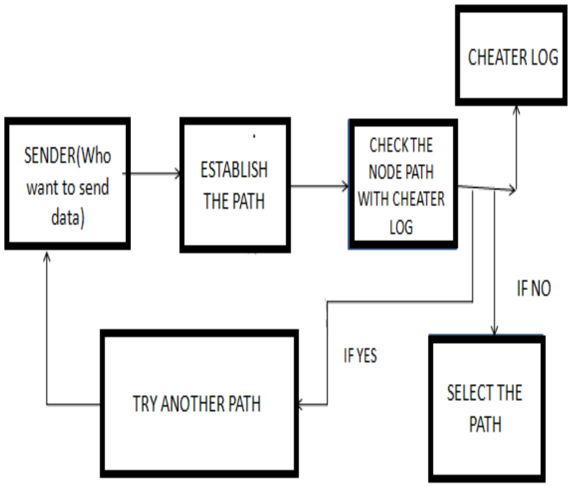

FIG 2: PROPOSED CHEATER LOG

In the attacker scheme attacker is found by, when the communication starts in system the sender who want to send the data first broadcast the message and path is established. Then the trusted party is verify the node list with the node registered with the trusted party. If the node registered then trusted party reports it and the sender select this path for communication. If the nodes are not registered with the trusted party then sender can select another path for communication. This method improves the more security for communication.

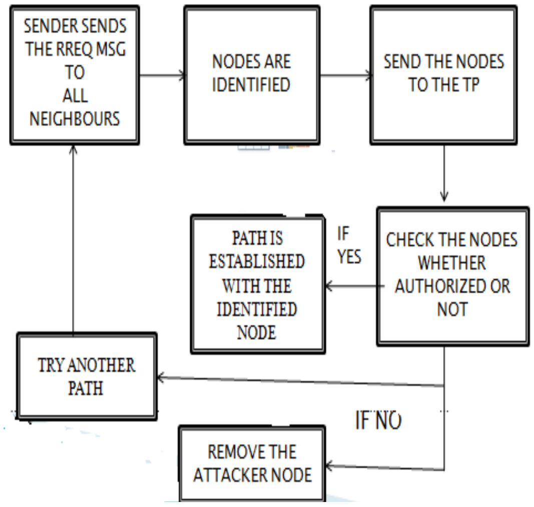
SENDER SENDS THE RREQ MSG TO ALL NEIGHBOURS
NODES ARE IDENTIFIED
SEND THE NODES TO THE TP
PATH IS ESTABLISHED WITH THE IDENTIFIED NODE
IF YES
CHECK THE NODES WHETHER AUTHORIZED OR NOT
TRY ANOTHER PATH
IF NO
REMOVE THE ATTACKER NODE

Fig 3: PROPOSED ATTACKER LOG

IV. PROPOSED SCHEME

SPAES has four main phases. In Communication phase, the nodes are involved in communication sessions and Evidences and payment reports are composed and temporarily stored after the communication is over. During the communication phase itself it evicts attacker nodes from the network. The nodes accumulate the payment reports and submit them in batch to the Trusted Party. For the Classifier phase, the TP classifies the reports into fair and cheating. For the Identifying Cheaters phase, 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, in Credit Account Update phase, the AC clears the payment reports.

Attacker Log and Cheater Log Creation:

Attacker scheme attacker is found by, when the communication starts in system the sender who want to send the data first broadcast the message and path is established. Then the trusted party is verifying the node list with the node registered with the trusted party. If the node registered then trusted party reports it and the sender select this path for communication. If the nodes are not registered with the trusted party then sender can select another path for communication. In this paper using AES algorithm for Encryption for reports and more secure transmission in the networks.

Communication:

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

Route establishment:

In order to establish an end-to-end route, the source node broadcasts the Route Request (RREQ) packet containing the identities of the source (IDS) and the destination (IDD) nodes, time stamp (Ts), and Time-To-Live (TTL). TTL is the maximum number of intermediate nodes. After a node receives the RREQ packet, it appends its identity and broadcasts the packet if the number of intermediate nodes is fewer than TTL. The destination node composes the Route Reply (RREP) packet for the nodes broadcasted the first received RREQ packet, and sends the packet back to the source node. The destination node creates a hash chain by iteratively hashing a random value K times to produce the hash chain root (h0). During the route establishment phase first of all the route is established and the destination node send the selected route to the trusted party. Trusted party check whether there is attacker, cheater in the selected route if no then that route is selected otherwise route is rejected and inform the source to select the other route. The RREP packet contains the identities of the nodes in the route the destination nodes certificate and signature .This signature authenticates the hash chain and links it to the route.

Trust based routing protocol:

TRP is used for establishing route in the other routing protocol route is established without checking any condition so sometimes the route contain the attacker, cheater it degrades the performance of the system. To avoid this trust based routing protocol is introduced. In this after the router established the destination node send the selected route to the trusted party. Trusted party check whether the nodes in the selected route have valid certificate, enough credit, not present in cheater log, not present in the attacker log. If all conditions are valid then only that route is selected otherwise that particular route is rejected and informs the source to select other route.

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 and its signature to R, X, Ts, and the hash value of the message and sends the packet to the first node in the route. The source nodes signature is an Undeniable proof for transmitting X messages and ensures the messages authenticity and integrity. 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. Each node stores only the last signature for composing the Evidence, which is enough to prove transmitting X messages.

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.

Payment report composition/submission:

A payment report contains the session identifier, a flag bit (F), and the number of messages (X). 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:

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, e.g., 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. There are four cases for nodes belongs to fair report, first case is all the nodes send the correct packet and they all receive the acknowledgement. Second is for example there are 5 nodes in the network they send 11 packets and all intermediate node receive this and during the acknowledgment transfer phase the acknowledgment is lost ie 3 of them got the acknowledgment and 2 of them does not got. Fourth is there are 5 nodes in the network when first nodes send the packet three intermediate node receive it and before receiving other two nodes fail these are the conditions for fair report.

Identifying Cheaters:

In the Identifying Cheaters‟ phase, the TP processes the cheating reports to identify the cheating nodes and correct the financial data. The objective of securing the payment is preventing the attackers from stealing credits or paying less, i.e., the attackers should not benefit from their misbehaviours. It also guarantees 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 (signatures and hash chain elements) for identifying the cheating nodes.

V. RESULTS

It is more secure trusted system and very effective to identify the cheating nodes and unauthorized nodes. Using AES algorithm for more secure in the network. Request delay is the time required for all nodes to send the payment report submission packet to trusted party. Payment report clearance delay is the time required for the trusted party to give credit to all nodes. During the time of evidence request and submission time this payment clearance delay and request delay is large. In the case of fair report, then all nodes submit the report to the trusted party very fast.

VI. FUTURE WORKS

In this paper the evidence aggregation is done based on AES,DES algorithm it has some disadvantage that is sometimes attacker can hack the detail so we can replace this hashing techniques with any other encryption algorithm. It will increase the security and also performance will increase.

VII. CONCLUSION

This System is based on credit based scheme for Secure processing on payment report with Advanced Encryption Standard in 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.

ACKNOWLEDGMENT

This work was partly undertaken and submitted as a study for the Multihop wireless networks lesson of the Computer Science postgraduate studies, Department of Information Technology, SNS College of Technology, Coimbatore. We thank Asst.Professor G. Selvavinayagam for their advice.

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

[8]. 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.

[9]. 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.

[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.

[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.