ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

Trusted and Attacker Free Credit Based System For Multihop Wireless Networks

Linu Ann Joy[1] Divya T.V[2]

M.Tech in Computer Science and Information Systems, Department of Computer Science and Engineering,

Federal Institute of Science and Technology (FISAT), Angamaly, India[1]

Assistant Professor, Department Of Computer Science and Engineering, Federal Institute of Science and Technology

(FISAT), Angamaly, India[2]

Abstract- A new system is proposed called TACS, trusted and attacker free credit based scheme for wireless networks. It is for stimulate node co-operation, avoid packet drop, and regulate packet transmission. The node submits report to the trusted party after the communication is over and store a temporarily undeniable token called evidences. The trusted party verifies the report and clears the payment of fair report with no processing overhead. For cheating reports evidences are requested to identify and remove cheating node from the system. In the new system all the attacker nodes are removed before beginning the communication and a trust value is assigned to all the nodes. This will improve the security of the system and it has low communication overhead, processing overhead.

Index Terms—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 preexisting 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.

This propose TACS, 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.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

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. This will increase the performance of the system.

After this route established and starts communication in the end of the session submit report to trusted party.TP verify the report and distinguish fair and cheating report. Each node stores a undeniable token called evidence and evidence aggregation is done with the help of onion hashing, It reduces the storage area. Evidences are requested only when cheating action is found.TP request evidence from some of the nodes and find the cheater.

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 nodes 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 network model. Section IV gives the new proposal used to minimize the communication overhead. Section V shows the results. Section VI Shows the conclusion an finally Section VII shows the future work

II RELATED WORKS

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.

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. 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.

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.

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.

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.Inorder 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.

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.

PIS [8], the source node attaches its signature to each transmitted message and the destination node replies with

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

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.

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.

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.

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.

. 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. 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.

PAPER	TACS	RECEIPT BASED SCHEME	TPD BASED SCHEME	CDS	RACE
COMMUNICATION 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

III SYSTEM MODEL

The network model consists of set of mobile nodes and an offline Trusted Party. The TP contains AC and a certificate authority. 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 AC. Once the AC receives the report it verifies them 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. TP 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 secure communication with low overhead.

TACS 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. The nodes can contact the trusted party once during a week, in this time they submit reports, evidences (if requested) and receive the credit then only it can continue using the network. There are mainly four different steps for communication route establishment, classifier, identifying cheater nodes and credit updating phase.

Fig 1 shows the architecture of TACS in this there is a mechanism for finding both attacker and cheater nodes. In 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. It verifies whether all nodes are registered if yes that route is selected otherwise inform the source that there is attacker in the selected path so select other route.

Here for 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, 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.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

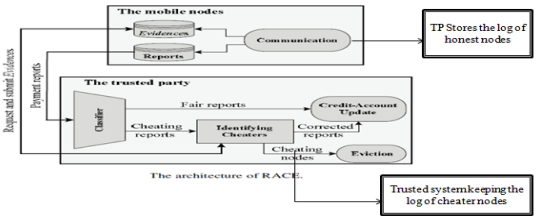

Fig 1: Proposed architecture

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

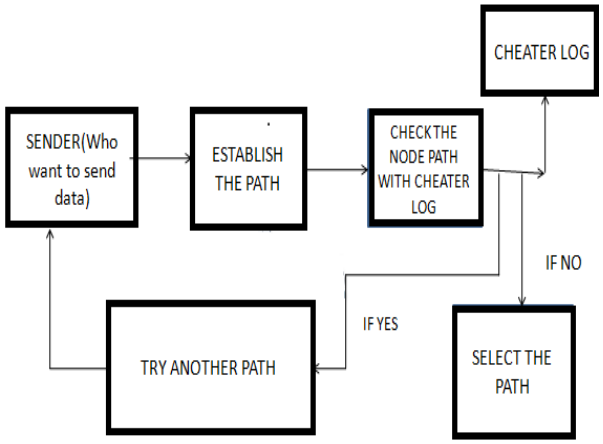

FIG 2: PROPOSED CHEATER SCHEME

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.

In the attacker scheme attacker 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 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 security for communication.

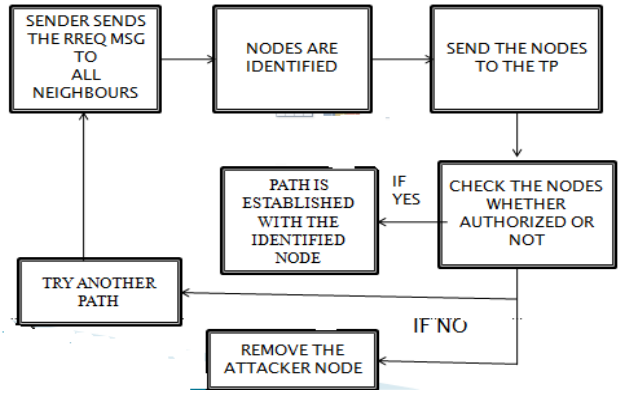

Fig 3: PROPOSED ATTACKER SCHEME

IV PROPOSED SCHEME

TACS 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 TP. 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.

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).

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

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 node's 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 node's signature is an Undeniable proof for transmitting X messages and ensures the message's authenticity and integrity. Before relaying the packet, each intermediate node verifies the signature to ensure the message's 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 session's 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 doesn't got. Third is for example there are 5 nodes in the network they send 7 packets after this they all got acknowledgment and the third node is break then the first node send next packet ,it is received only by first and second node. Others don't receive it. 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. Fig shows the cheating action

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

Case №		S	A	B	C	D
1	X	6	10	10	10	10
	F	1/0	1	1	1	1
2	X	6	10	10	9	9
	F	1/0	0	0	1	1
3	X	5	12	12	12	5
	F	1	1/0	1/0	1/0	1

Fig 4: cheater scheme

There are different ways of cheating action all nodes send same data but during the time of report submission one claims that they send the data more than the other ones or claims that send the data less than the other ones in this case trusted party find there is cheater present in the node so they send a evidence request message to the node that claims that it sends more message then they reply with evidence reply then only trusted party confirms cheater in the session. Trusted party evicts cheater from the system and others credit is updated. Cheater node is send to the cheater log.

Credit-Account Update

In case of fair report the credit is updated by, Consider A wants to send 10 packets to the destination. After the packet reach the destination, it sends an ack. Ack is set based on a flag bit (f).F=0, ack not received=1, ack received After completion of the process all the nodes send a payment report the trusted party. TP verifies the report and check the fair and cheater report.
If fair report then the credit is updated. Request Evidences from nodes that submit report with more payment Credit is updated as, for node A consider F=0(ack not received) Credit=10*2=20-1=19

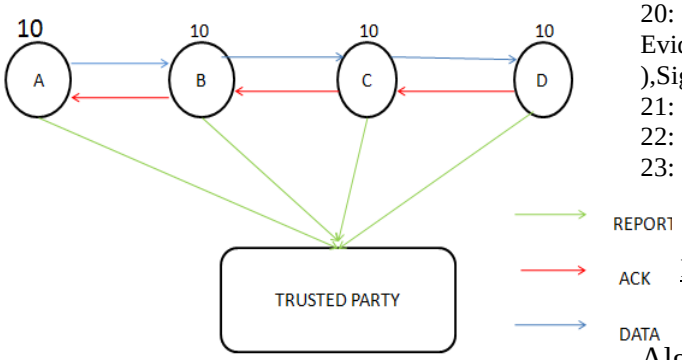

Fig 5: fair report

In the case of cheater report credit is updated by, after sending packets from A-D, they send payment report to the trusted party. Trusted party verify all the reports and noticed that A, C, D claims they send 10 packets and B claim that they send 20 packets. Trusted party noticed that B is a cheater node and to confirm this they request evidence .B send the evidence to the trusted party. If B is a cheater then TP doesn't update credit for that node and update credit for all the other nodes.

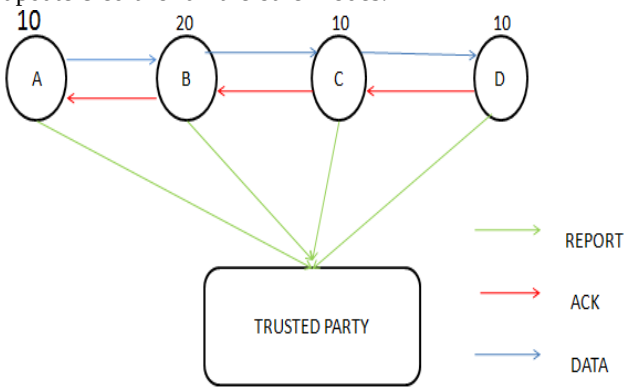

Fig 6 :cheater report

1: ni is the source, intermediate or destination node that is running the algorithm
2: if (ni is the source node) then
3: Store [R, X, Ts, Mx, sigs(R, X, Ts, H (Mx))] in Px;
4: send (Px);
5: else
6: If ((R, X, Ts are correct) and verify (sigs(R, X, Ts, H (Mx))) ==TRUE) then
7: if (ni is an intermediate node) then
8: Relay the packet;
9: Store Sigs(R, X, Ts, H (Mx));
10: end if
11: if (ni is the destination node) then
12: send (h(X));
13: endif
14: else
15: Drop the packet
16: Send error packet to the source node
17: endif
18: endif
19: If (Px is last packet) then
20: Evidence={R,X,Ts,H(Mx),h(0),h(x),H(Sigs(R,X,Ts,H(Mx),SigD(R,Ts,h(0))))};
21: Report={R, Ts, F, X}
22: Store report and evidences
23: endif

Fig 7:Data transmission and Evidence Composition

Algorithm 2: Submission/Clearance of report and evidences

1: ni -> TP: Submit (Report [ti-1, ti]);
2: TP -> ni: Evidences Request (Ses_IDS [ti-2, ti-1]);
3: ni -> TP: Submit (Req_Evs [ti-2, ti-1]);
4: TP: Identify_cheaters ();
5: TP: Clear the payment of the report;

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

6: if (ni is honest) then
7: TP ->ni: A renewed certificate;
8: endif

Fig 8:Evidence and Report submission

Fig 7 shows the data transmission algorithm how the data is transmitted from one node to another Fig 8 shows how report and evidence is submitted after the communication ends. Fig 9 shows the algorithm for finding fair nodes in the network.

```
If(X==X && F==F) {
                    Having same X value and F, credit granted
                  }
else if(X==X && F==0) {
                    Having the same X but the ACK not received, Requesting for
evidence
                    }
 } else if ((X-1) ==X && F==1){
                    Having the packet count is one less than the fair count but
previous ACK is received, Requesting for evidence
                    }
else if ((X+1)==X && F==0){
                    Having the packet count is one less than the fair count but
previous ACK is received, Requesting for evidence
                    }
```

FIG 9: ALGORITHM FOR FINDING FAIR REPORT

V RESULTS

The Figure10 shows the payment clearance delay how much fast the trusted party process the payment report. It is tested based on varying the payment process time of trusted party. Then the result is when tp=20 sec then payment processing is fast. When tp=40 then processing time is larger than first one.

The Figure11 shows the scenario of payment delay and request delay. Request delay is the time required for all nodes to send the report submission packet to trusted party. Payment 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. so payment, request delay is small.

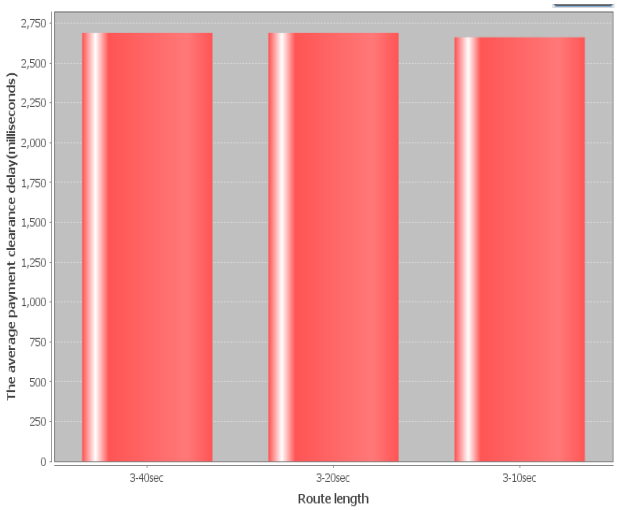

Fig 10: Payment clearance delay

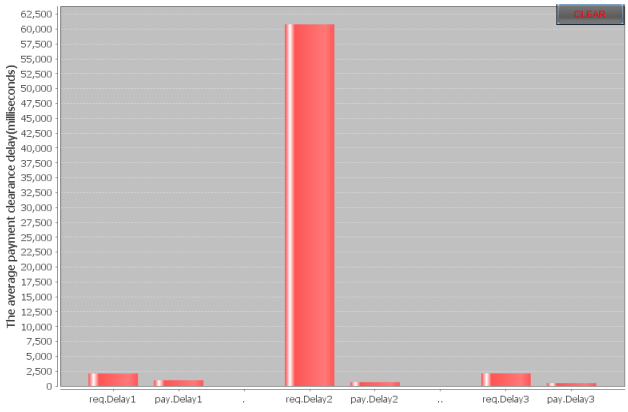

Fig 11: Scenariao

VI CONCLUSION

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.

VII FUTURE WORKS

In this paper the evidence aggregation is done based on onion hashing 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 AES,DES etc.It will increase the security and also performance will increase

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

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