Volume 4, Issue 7, July 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Trust based Report Payment Scheme for Multihop Wireless Networks

Anu Susan Chandy
Department of Computer Science and Engg.
Mahatma Gandhi University,
India

Mitha Rachel Jose
Department of Computer Science and Engg.
Mahatma Gandhi University,
India

Abstract— A secure payment scheme, called as the Trust based Report Payment scheme (TRPE) is used in multi hop wireless networks to stimulate node cooperation, regulate packet transmission and enforce fairness. The nodes submit lightweight payment reports (instead of receipts) to the Trusted Authority to update their credit accounts and temporarily store the evidences. The report includes the session information. The Trusted Party verifies the payment by investigating the consistency of the report and clears the fair reports with almost no cryptographic operations or computational overhead. The nodes which do not pass or relay others packets are called selfish nodes. But it makes use of neighbour or cooperative nodes to relay its packets. This degrades the network connectivity and fairness. Such type of nodes also submits reports to the trusted party. But when tested for consistency, it is found to be a cheating node. For such reports, the evidences are requested from the Trusted Party to identify and evict the cheating nodes or selfish nodes. TRPE is the first payment scheme that uses the concept of evidences to secure the payments. It requires cryptographic operations in clearing the payment only in the case of cheating. Also this is the first system that can verify the payment by investigating the consistency of the nodes reports without submitting and processing security tokens and without false accusations. To prevent the multi hop communications from failing due to insufficient credits, the source node can borrow credits from the Trusted Authority. After evicting the selfish nodes, communication can be efficiently established again with increased throughput and less amount of processing and communication overhead. This is done by establishing a route between the source and the destination by sending a route request to the destination and the destination replies with path, a hash element from the hash chain and the signature. All these details are provided by the Trusted Party.

Keywords— Report, Selfish nodes, Payment Scheme, Accounting centre, Cheating nodes, Evidence

I. INTRODUCTION

Multihop wireless networks (MWNs) are those networks in which, the traffic originates from a node and passes through intermediate nodes to the destination. Multihop packet relay can extend the network coverage using limited transmit power, improve area spectral efficiency, and enhance the network throughput and capacity. This helps in improving the network performance and deployment [1] and also enabling new applications such as data sharing [2] and multimedia data transmission [3]. For example, students in a university campus with different wireless devices such as gaming consoles,cell phones, tablets, etc can setup a network to transfer files, play games and communicate.

But the behavior of some nodes degrades the network connectivity significantly, and may cause the MWN strategy to fail [4]. For instance some nodes will not transmit other's packets instead uses other nodes in the MWN to transmit their own packets. This degrades the network connectivity and unfairly overloads the cooperative nodes since network traffic is concentrated through them. Such nodes are termed as selfish nodes. Also some nodes though not selfish, still causes the MWN to fail. For instance some nodes will relay other's packets without fail but usually may leave the network during communication.This causes loss of packets and loss of credits for the source node. Such nodes are termed as unreliable nodes.

Payment schemes can be used in MWN to motivate node cooperation, enforce fairness, discourage Message-Flooding attacks, regulate packet transmission, and efficiently charge for the network services.Relying other's packets helps a node to earn credits; more the packets are transmitted, more the credits they earn. These credits earned can be spend to get their

own packets relayed by others; more the packets sent, more the credits spent. For example, the nodes situated at the network center relay more packets than the other nodes because they are more frequently selected by the routing protocol. Packet transmission is regulated and Message-Flooding attacks are discouraged as the source nodes pay for relaying their packets.

A good payment scheme should be secure, and require low overhead. MWNs require a specially designed payment scheme due to unique characteristics such as there is usually one customer (the source node) and multiple merchants (the intermediate nodes),short relation between customer and merchants due to the network dynamic topology, and also the nodes are involved in low-value transactions very frequently (because once a route is broken, a new transaction should be done to reestablish the route). Currently receipt-based payment schemes are used, where the nodes compose proofs of relaying others packets, called receipts, and submit them to an offline accounting center (AC) to clear the payment. But this scheme impose significant processing and communication overhead and requires complex implementation. In-order to secure the payment the receipts contain security proofs, e.g., signatures, which significantly consumes the nodes resources and the available bandwidth in submitting them. The AC has to apply a large number of cryptographic operations to verify the receipts, which may require impractical computational power and make the practical implementation of these schemes complex or inefficient.Thus, reducing the communication and the payment processing overhead is essential for the effective implementation of the payment scheme and to avoid creating a bottleneck at the AC and exhausting the nodes resources. In this paper, we propose a system which can reuse a preestablished route, can dynamically avoid cheating and unreliable nodes, and also uses a report based payment scheme for MWNs. Before requesting a new route from source node to destination, system can check whether such a route was preestablished and used successfully. While establishing a new route from source node to destination the system can detect and avoid selfish nodes and unreliable nodes (except in
worst case scenarios). The nodes submit lightweight payment reports (instead of receipts) to the AC to update their credit accounts, and temporarily store undeniable security tokens called Evidences. The reports contain the alleged charges and rewards of different sessions without security proofs, e.g., signatures. The AC checks the constitency of reports and for the fair reports payment is cleared without any cryptographic operations or computational overhead. Evidences are requested by the AC from those nodes which submit unfair (cheating) reports and denies payment if the evidences are invalid. Evidence aggregation technique is used to reduce the storage area of the Evidences.

A. Current Implementations

In Sprite [11] payment scheme method, receipt is generated by the intermediate nodes for each message, and submitted to the AC. At source node, for each message, it 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, compose receipts containing the identities of the nodes in the route and the source nodes signature, and submit the receipts to the AC to claim the payment. The AC verifies the source nodes signature to make sure that the payment is correct. Ac charges only the source node for the packet transmission. In FESCIM (Fair, Efficient, and Secure Cooperation Incentive Mechanism) [12] payment scheme method a fair and efficient incentive mechanism is proposed to stimulate the node cooperation. This applies a fair charging policy by charging the source and destination nodes when both of them benefit from the communication. To implement this charging policy efficiently, hashing operations are used in the ACK packets to reduce the number of public-key-cryptography operations. Moreover, reducing the overhead of the payment checks is essential for the efficient implementation of the incentive mechanism due to the large number of payment transactions. Instead of generating a check per message, a small-size check can be generated per route, and a check submission scheme is proposed to reduce the number of submitted checks and protect against collusion attacks.

In PIS (Practical Incentive System) [13] payment scheme, the source node attaches a signature to each message and the destination node replies with a signed ACK packet. 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. Incentive systems implement micropayment in the network to stimulate the selfish nodes to cooperate. However, micropayment schemes have originally been proposed for Web-based applications; therefore, a practical incentive system should consider the differences between Web-based applications and cooperation stimulation. In this paper, first, these differences are investigated, and a payment model is developed for the efficient implementation of micropayment in MWNs. Second, based on the developed payment model, an incentive system is proposed to stimulate the nodes cooperation in MWNs. Third, a reactive receipt submission mechanism is proposed to reduce the number of submitted receipts and protect against collusion attacks.

In CDS (Connected Dominating Set) [14] Payment scheme, statistical methods are used to identify the cheating nodes that submit incorrect payment. However, due to the nature of the statistical methods, the colluding nodes may manage to steal credits, and some honest nodes may be falsely accused of cheating which is called false accusations. Moreover, some cheating nodes may not be identified which is called missed detections, and it may take long time to identify the cheating nodes. Connected dominating set has a wide range of applications in multihop wireless networks. The Minimum CDS problem has been studied extensively in multihop wireless networks with uniform communication ranges. However, in practice, the nodes may have different communication ranges either because of the heterogeneity of the nodes, or due to interference mitigation, or due to a chosen range assignment for energy conservation.

In ESIP [15] Payment Scheme, communication protocol that can be used for a payment scheme is proposed. ESIP 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. Public key cryptography and hash function are used to ensure message integrity and payment nonrepudia-tion to secure the payment. Identity-based cryptography is used to efficiently compute a shared symmetric key between the source node and each node in the route. Using these keys, the source node computes and sends a keyed hash value for each intermediate node to verify the message integrity.

II. PROPOSED SYSTEM

The proposed system has six main phases. Communication phase in which the nodes establish routes and transmit data packets. Evidence composition phase in which proof about the packet transmission is created. Payment report composition and submission phase in which reports are submitted to the AC. Report Classifier phase in which, the TP classifies the reports into fair and cheating. Cheater identification phase in whch 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 accounting phase, the AC clears the payment reports.

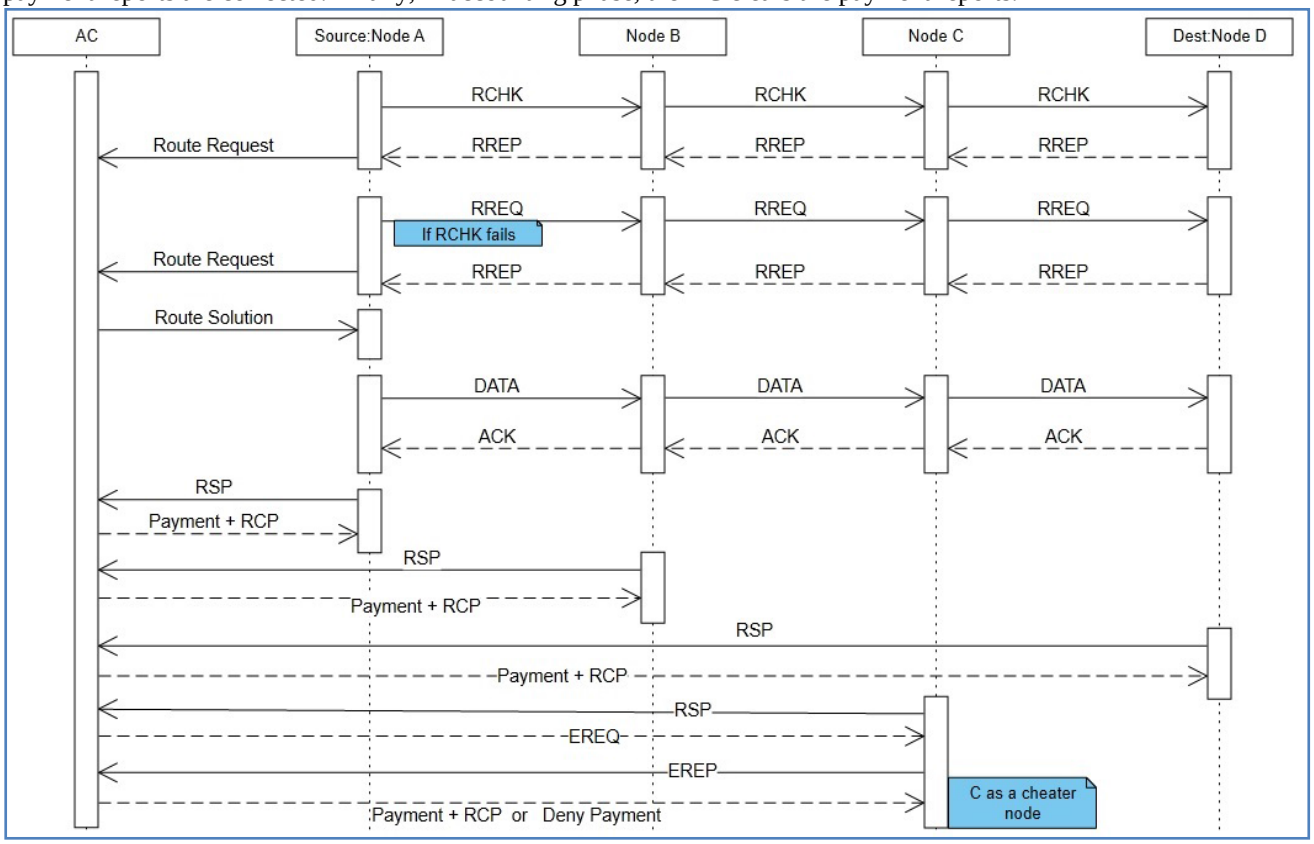

Fig. 1: Proposed system flow

A. Communication

The Communication phase consists of route establishment and data transmission.

1) Route Establishment: This process finds out the optimal route from the source node to destination evicting the cheating nodes and the unreliable nodes. First a check is made *if a route was pre-established packets transmitted, between these nodes successfully.*

If a pre-established route exists, the source node broadcasts the Route Check (RCHK) packet to the first node in the path, with the following information - [Source node id (ID_s), Destination node id (ID_d), Intermediate nodes id, Time stamp (T_s), Maximum number of intermediate nodes; Time-To-Live (TTL)]. Once the RCHK packet is received by a node, it checks the next node in list and broadcasts the packet if the number of intermediate nodes is fewer than TTL. If the destination node receives the RCHK packet, it composes the Route Reply (RREP) packet and sends to the source node. If the packet doesnt reach the destination in time, the nodes will timeout and starts searching for a new route. RREP has following information [R = Source node id (ID_S) + Destination node id (ID_d) + Intermediate nodes id, Hash chain root ($h^{(0)}$), Destination node's certificate, Destination node's signature ($Sig_D(R,Ts,h^{(0)})$)].

If a pre-established route doesn't exist or not valid anymore, the source node broadcasts the Route Request (RREQ) packet containing with following information[Source node id(IDs), Destination node id(ID_d), Time stamp (Ts), Maximum number of intermediate nodes; Time-To-Live (TTL)]. Once the RREQ packet is received, a node appends its identity and broadcasts the packet if the number of intermediate nodes is fewer than TTL. For the first received RREQ packet, destination node composes the Route Reply (RREP) packet and sends to the source node. RREP packet has the following information [R = Source node id (ID_s) + Destination node id (ID_d) + Intermediate nodes id, Hash chain root ($h^{(0)}$), Destination node's certificate, Destination node's signature ($Sig_D(R,Ts,h^{(0)})$)].

The intermediate nodes verify the destination nodes signature, relay the RREP packet, and store the signature and ($h^{(0)}$) for composing the Evidence. Once the RREP packet reaches the Source node, it verifies the path for cheater or unreliable nodes. If any such node exists in the path, Source node will resend RREQ for new route.

2) Data Transmission: In this stage data packets are send from the source node to the destination node via the established route and destination node acknowledges the communication using ACK packets.

Consider the packet transmission for X^{th} packet. Source node sends the packet to first node in the route. Packet contains following information [Message (M_X), Sig_X (R,X,Ts, $H(M_X)$); $H(M_X)$ is hash value of message]. The source node's signature is an undeniable proof for transmitting X messages and ensures the messages authenticity and integrity. Smaller sized H (M_X) is attached to the Evidence instead of M_X and thus reduces Evidence size.

Once an intermediate node receives the packet, before relaying it, 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 to compose the Evidence, which is enough to prove transmitting X messages. For instance after receiving the Xth data packet, the nodes store Sigs(R, X,Ts,$H(M_x)$ and remove Sig_S(R,X-1,Ts,$H(M_{(x-1)})$.

Once the X^{th} data packet is received, destination node sends back an ACK packet containing the pre-image of the last sent hash value (or $h^{(0)}$) to acknowledge receiving the message M_X. Each intermediate node verifies the hash value by making sure that h(x-1) is obtained from hashing h(x). Nodes store only the last released hash value for composing the Evidence. The data transmission process ends when the source node transmits its last message, or if the route is broken; for instance due to node mobility or channel impairment.

If a node posses h^X, it proves the node has delivered X messages and possession of Sig_S(R,X,Ts,H(M(x)) proves node has delivered X-1 messages + received one. The source node signs the number of transmitted messages (X) while The number of delivered messages can be computed from the number of hashing operations to map h(x) to h(0).An intermediate node cannot drop the Xth data packet and claim delivering it because the hash function is one way. In this method, hash chains are used to reduce the number of public key cryptography operations, i.e., instead of generating a signature per ACK packet to secure the payment, one signature is generated by the destination node per K ACK packets. If a node in the route does not receive a data or ACK packet within a time interval, the session is considered stale.

3) Evidence Composition: In this stage a node composes evidences using the evidence aggregation process. Evidence is 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 an Evidence is to resolve a dispute about the amount of the payment resulted from data transmission.

Evidences can't be modified; if X messages are delivered, the intermediate nodes can compose Evidences for fewer than X messages, but not for more. Evidences can't be forged; if the source and destination nodes collude, they can create Evidence for sessions that did not happen, but the intermediate nodes cannot, because forging the source and destination nodes signatures is infeasible. Evidences are undeniable; this is necessary to enable the TP to verify them to secure the payment. A source node cannot deny initiating a session or the amount of payment because it signs the number of transmitted messages and the signature is included in the Evidence. An honest intermediate node can always compose valid Evidence even if the route is broken or the other nodes in the route collude to manipulate the payment. This is because it can verify the Evidences to avoid being fooled by the attackers. An evidence contains two parts called DATA and PROOF.

DATA describes the payment, i.e., who pays whom and how much, and contains enough data to regenerate the node's signatures [(R,X,Ts, $H(M_x)$,h(0),[h(v)])]; R = nodes in the route, X= the number of received messages, Ts = session establishment time stamp, $H(M_x)$ =root of the destination nodes hash chain, h(0) = hash value of the last message, h(v) = last received hash value.

The PROOF is an undeniable security token that can prove the correctness of the DATA and protect against payment manipulation, forgery, and repudiation. Has the following information [H(Sig(R,X,Ts,$H(M_x)$),Sig(R,Ts,$h^{(0)}$))]; Sig(R,X,Ts,$H(M_x)$) = destination nodes signature, Sig(R,Ts,$h^{(0)}$) = last signature received from the source node.

An aggregated evidence is created by concatenating DATAs of the individual Evidences and computing one compact PROOF of the individual evidences instead of one PROOF per session. This helps in reducing the evidence storage area. If the TP requests an Evidence that is aggregated in the compact Evidence, the node has to submit the compact Evidence and the TP has to verify all the PROOFs of the sessions of the compact Evidence, instead of verifying only the PROOF of the requested Evidence. Onion hashing is used for computing a compact PROOF and is computed as below H(. . . .,H(H(PROOF(1), PROOF(2)), PROOF(3)),. . . , PROOF(n)).

4) Payment report composition/submission: In this stage a node composes and submits a payment report to the AC. AC verifies the payment report and if it finds any mismatch, requests for evidence from the respective node. Once the evidence is received, AC verifies it and may clear or deny the payment. A payment report (R_P) is composed with the following details [session identifier which is concatenation of identities of nodes in session and timestamp, a flag bit (F); 0 if last recieved packet is data, 1 if ACK, number of messages (X)].

A Node sends the Report Submission Packet (RCP) to AC with following details. Consider the report submission by node z, the RCP will have following details [Node Id, T_S, R_P,H_{Kz}(T_S, R_P) ; Kz is the long term symmetric key shared between node z and the AC].

If the AC needs evidence, it sends an Evidences Request Packet (EREQ) to the node with following details [Node Id, T_S, H_{Kz} (Ts,Ses_{ID}), Ses_{ID}; Ses_{ID} is the identifier of the reports for which evidences are required]. Once an EREQ is received, node replies with Evidences Reply Packet (EREP) to the AC with following details [Node Id, T_S, H_{Kz} (T_s,Req_{EVS}), Req_{EVS}; Req_{EVS} is the requested evidences, which were composed earlier]. If AC finds the node to be honest, AC sends a renewed certificate for the node with same identity and public/private keys but with updated lifetime. A Renewed Certificate Packet (RCP) is send for this, with following details [Node Id, T_S, Certificate, H_{Kz} (Ts,Certificate)]

B. Report Classifier

In this stage, once the AC receives the payment reports, verifies them by investigating the consistency of the reports, and classifies them into fair or cheating. A set of pre-defined rules validate if the reports are 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. Fair reports can be for complete or broken sessions.

For a complete session, all nodes in the session reports same number of messages (X) and flag Bit (F) = 1. If a session is broken while relaying the Xth DATA packet and node Z is last node that received the DATA packet, all nodes from Source to Z reports number of messages = X and flag Bit (F) = 0 but all other nodes report number of messages = X-1 and flag Bit (F) = 1. If a session is broken while relaying the Xth ACK packet and node C is last node that received the ACK packet, all nodes from Destination to C reports number of messages = X and flag Bit (F) = 1 but all other nodes report number of messages = X and flag Bit (F) = 0.

C. Identifying Cheaters

In this phase, the AC processes the cheating reports to identify the cheating nodes and correct the financial data. Instead of requesting Evidence from all nodes, the AC requests evidence only from the node that submits report with more payment. The requested node should have the necessary and undeniable proofs (signatures and hash chain elements). Thus AC can precisely identify the cheating nodes with requesting few Evidences. Once AC receives the Evidence, it composes the PROOF by generating the nodes signatures and hashing them. The Evidence is valid if the computed PROOF is similar to the Evidences PROOF. If valid, the report is corrected and send for account update. If node is found to be cheater, it will be marked so as to be evicted from future communications.

D. Accounting Update

In this phase, the fair and corrected payment reports are used to update the nodes credit accounts. The AC has to wait until receiving the reports of all nodes in a route to verify the payment. The payment reports are cleared using the charging and rewarding policy -"source nodes are charged for every transmitted message even if it does not reach the destination nodes, but the intermediate nodes are rewarded only for the delivered message". The maximum payment clearance delay (or the worst case timing) occurs for the sessions that are held shortly after at least one node contacts the AC and the node submits the report after the certificate lifetime (TCert).The nodes submit the reports at different times because the connection to the AC may not be available on a regular basis, and thus the duration between each two submissions may not be the same and may be less than or equal to TCert. Hence, the maximum payment clearance delay may be less than TCert.

III. PERFORMANCE EVALUATION

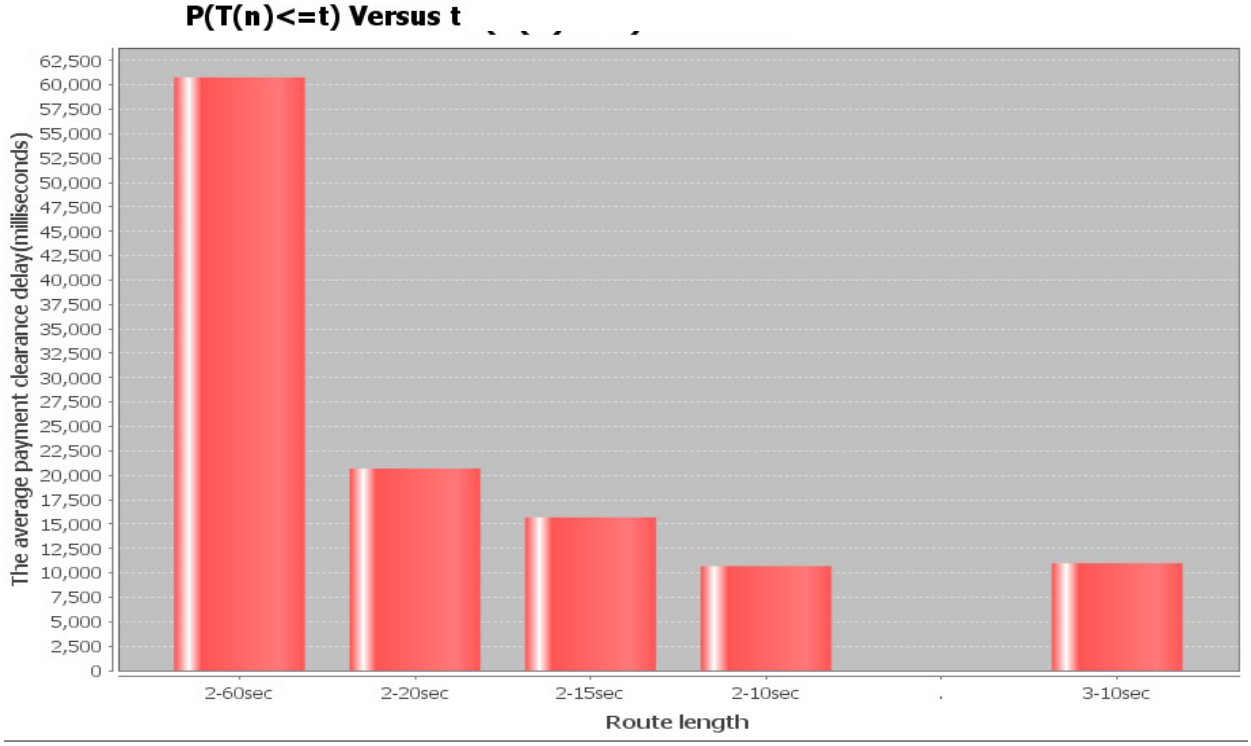

Fig. 2: Payment delay plotting: Route length vs Time

The above plotting shows the average delay in payment respective to the route length between source and the node. Compared to the receipt based system, report based payment scheme submit lightweight reports. The cryptographic operations to be performed is very less in this scheme. And also cheating nodes are evicted so that the source is not losing any extra credits.

The below plotting shows the average delay in processing the submitted report vs the time required to issue the payment.

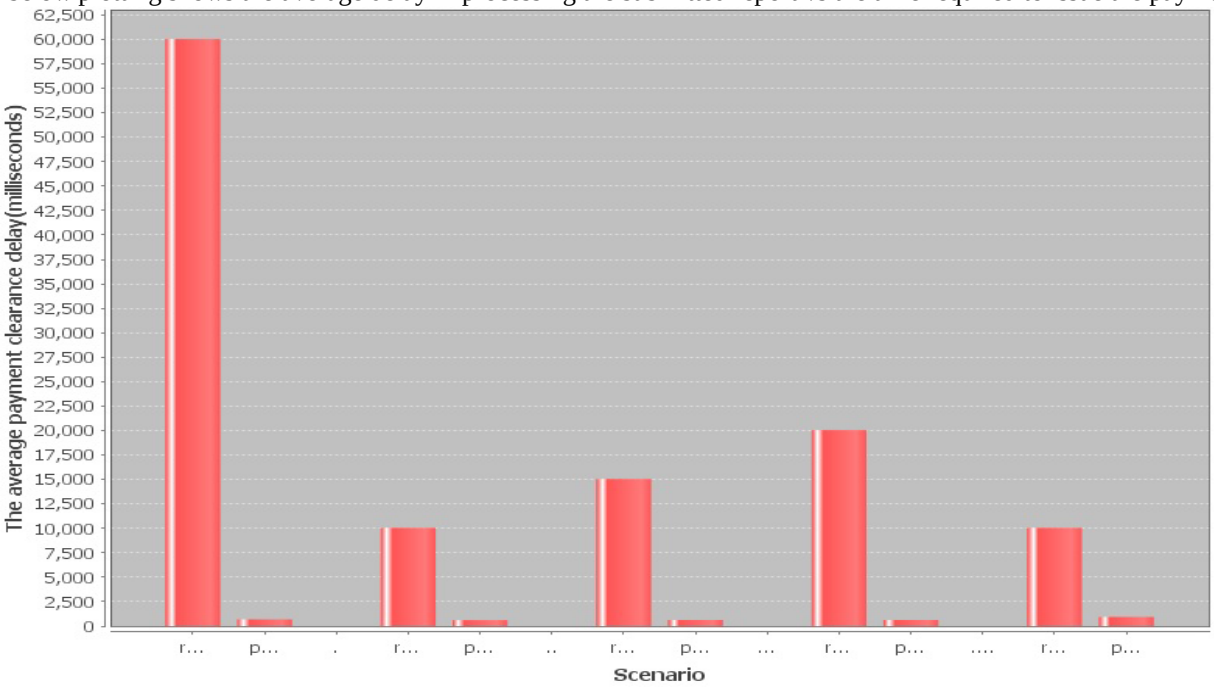

Fig. 3: Processing delay plotting: Report submission vs Actual payment

IV. CONCLUSION

In this Scheme a trust value is assigned to each of the mobile nodes. Routing is performed based on the trust value. Trust value is assigned based on relaying packet successfully. Each node then submits a light weight report to the accounting center. The classifier checks for the consistency of the report and classifies it into fair and cheating report. The payment of the fair reports is cleared. For the cheating report the Evidence is requested. The cheating nodes are identified by performing cryptographic operations and evict those nodes from the payment and cheating count is maintained to modify the trust value. The payment is cleared for the fair nodes. The trust payment model enhances the fairness and connectivity during the communication. The numbers of submission of the inconsistent reports are very less. This reduces the processing overhead and clearance delay than the existing model.

V. FUTURE SCOPE

In the proposed system, during packet transmission if the connectivity is lost - source node looses credit and intermediate nodes which ever transmitted the packet receives credit but destination won't receive the packet. It is a winning situation for intermediate nodes but worst case scenario for source and destination nodes. In the future work, an intelligent routing and transmission algorithm can be introduced. Once the connectivity is lost, system will try to find out alternate route to destination and if one exists, the missed packet will be resend by the intermediate node instead of Source node. Thus the packet is delivered successfully to the destination and since intermediate node is resending the packet, Source node will not loose the credit again. If no alternate route is found, payments are processed as of now.

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] C. Chou, D. Wei, C. Kuo, and K. Naik, An Efficient Anonymous Communication Protocol for Peer-to- Peer Applications Over Mobile Ad-Hoc Networks, IEEE J. Selected Areas in Comm., vol. 25, no. 1, pp. 192-203, Jan. 2007.

[3] H. Gharavi, Multichannel Mobile Ad Hoc Links for Multimedia Communications, Proc. IEEE, vol. 96, no. 1, pp. 77-96, Jan. 2008.

[4] 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.

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

[6] Y. Zhang and Y. Fang, A Secure Authentication and Billing Architecture for Wireless Mesh Networks, ACM Wireless Networks, vol. 13, no. 5, pp. 663- 678, Oct. 2007.

[7] 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.

[8] 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.

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

[10] A. Weyland, T. Staub, and T. Braun, Comparison of Motivation- Based Cooperation Mechanisms for Hybrid Wireless Networks, J. Computer Comm., vol. 29, pp. 2661-2670, 2006.

[11] 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.

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

[13] 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.

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

[15] 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.

