Trust Based Secure Payment Scheme for Multihop Wireless Networks

T. Boobathy Ramkumar[#1], Dr.T.Kalaikumaran[#2] ,Dr.S.Karthik[#3]

[1#] *PG Scholar, Dept of CSE, SNS College of Technology, India.*
E Mail: boobathy@gmail.com
[2#] *Professor & HoD, Dept of CSE, SNS College of Technology, India.*
E Mail:hodcse@snsct.org
[3#] *Professor & Dean, Dept of CSE, SNS College of Technology, India.*
E Mail: profskarthik@gmail.com

Abstract- **The payment system rewards the nodes that relay others' packets and charges those that send packets. The trust system evaluates the nodes' competence and reliability in relaying packets in terms of multi-dimensional trust values. The trust values are attached to the nodes' public-key certificates to be used in making routing decisions. We develop routing protocols to direct traffic through those highly-trusted nodes having sufficient energy to minimize the probability of breaking the route. By this way, it can stimulate the nodes not only to relay packets, but also to maintain route stability and report correct battery energy capability. This is because any loss of trust will result in loss of future earnings. Moreover, for the efficient implementation of the trust system, the trust values are computed by processing the payment receipts. Analytical results demonstrate that proposed system can secure the payment and trust calculation without false accusations. Simulation results demonstrate that our routing protocols can improve the packet delivery ratio and route stability.**

Keywords **- Packets delivery, routes, trust based system.**

I. INTRODUCTION

Multi-hop or ad hoc, wireless networks use two or more wireless hops to convey information from a source to a destination. There are two distinct applications of multi-hop communication, with common features, but different applications. A wireless network adopting multihop wireless technology without deployment of wired backhaul links.

A Mobile Ad hoc Networks (MANETs) consists of a group of mobile nodes that communicate without requiring a fixed wireless infrastructure. In contrast to conventional cellular systems, there is no master-slave relationship between nodes such as Òbase station to mobile usersÓ in ad hoc networks. Communication between nodes is performed by direct connection or through multiple hop relays. Mobile ad hoc networks have several practical applications including battlefield communication, emergency first response, and public safety systems (M. Mahmoud, X. Shen: 2010). Despite extensive research in networking, many challenges remain in the study of mobile ad hoc networks including development of multiple access protocols that exploit advanced physical layer technologies like MIMO, OFDM, and interference cancellation, analysis of the fundamental limits of mobile ad hoc network capacity, practical characterization of achievable throughputs taking into account network overheads.

Cellular systems conventionally employ single hops between mobile units and the base station. As cellular systems evolve from voice centric to data centric communication, edge-of-cell throughput is becoming a significant concern. This problem is accentuated in systems with higher carrier frequencies (more path loss) and larger bandwidth (larger noise power). A promising solution to the problem of improving coverage and throughput is the use of relays. Several different relay technologies are under intensive investigation including fixed relays (powered infrastructure equipment that is not connected to the network backbone), mobile relays (other users opportunistically agree to relay each others' packets), as well as mobile fixed relays (fixed relays that are mounted on buses or trains and thus moving). There has been extensive research on multi-hop cellular networks the last few years under the guise of relay networks or cooperative diversity. The use of relays, though, impacts almost every aspect of cellular system design and optimization including: scheduling, handoff, adaptive modulation, ARQ, and interference management. These topics are under intense investigation.

Benefits of multi-hop technology like us, Rapid deployment with lower-cost backhaul, Easy to provide coverage in hard-to-wire areas, Under the right circumstances, it may,Extend coverage due to multi-hop forwarding, Enhance throughput due to shorter hops and Extend battery life due to lower power transmission.

To enhance the network performance in multihop wireless networks the traffic originated from a node is usually relayed through the other nodes to the destination for

enabling new applications. Multihop packet relay can extend the network coverage using limited transmit power, improve area spectral efficiency, and enhance the network throughput and capacity.

II.RELATED WORK

The current wireless network installations consists of a number of access points deployed in selected areas, where they are expected to serve a minimum amount of customers to bring revenue to the provider, e.g., at airports or railway stations. With multi-hop cellular networks, also called hybrid networks, the single-hop limit does not exist anymore. The computing devices of the customers participate in the packet forwarding process and a gateway offers the connection to the Internet. This gives the provider a greater coverage area with more customers and reduces the network installation costs.

We can identify two types of uncooperative nodes: faulty/malicious nodes and selfish nodes. By saying faulty/malicious nodes, we refer to the broad class of nodes that are either faulty and therefore cannot follow a protocol, or are intentionally malicious and try to attack the system. The problems of faulty/malicious nodes need to be addressed from many layers, for example, using spread-spectrum encoding to avoid interference over the communication channel (S. P. Santhoshkumar *et al*; 2013), using a reputation system to identify the faulty/malicious nodes and subsequently avoid or penalize such nodes; and applying the techniques from fault tolerant computing to perform computation correctly even in the presence of faulty/malicious nodes.

In particular, these signature schemes require performing modular exponentiation with a large modulus as part of the signing process, and this in turn requires many modular multiplications. Furthermore, these costly operations can start only once the message to be signed becomes known. Consequently, these signature schemes will become much more attractive if only a few (say, two or three) modular multiplications need to be performed once the message becomes known, while the more costly operations can be pre processed. This leads to the notion of an on-line/off-line signature scheme.

A Report-based payment scheme for MWNs. 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 verifies the payment by investigating the consistency of the reports, and clears the payment of the fair reports with almost no cryptographic operations or computational overhead. For cheating reports, the Evidences are requested to identify and evict the cheating nodes that submit incorrect reports, e.g., to steal credit or pay less (D.Prabakar *et.al*: 2012). In other words, the Evidences are used to resolve disputes when the nodes disagree about the payment. Instead of requesting the Evidences from all the nodes participating in the cheating reports, RACE can identify the cheating nodes with submitting and processing few Evidences. Moreover, the Evidence aggregation technique is used to reduce the storage area of the Evidences.

The proposed system develops a trust system based on processing the payment reports to maintain a trust value for each node. The nodes that relay messages more successfully will have higher trust values, such as the low-mobility and the large-hardware-resources nodes. The payment system uses credits (or micropayment) to charge the nodes that send packets and reward those relaying packets. Since a trusted party may not be involved in the communication sessions, an offline trusted party (TP) is required to manage the nodes' credit accounts. The nodes compose proofs of relaying packets, called receipts, and submit them to TP. The payment system can stimulate the selfish nodes to relay others' packets to earn credits. It can also enforce fairness by rewarding the nodes that relay more packets such as those at the network center.

However, the payment system is not sufficient to ensure route stability. It can stimulate the rational nodes to not break routes to earn credits, but the routes can be broken due to other reasons. Examples for these reasons include low resources, node failure, and malicious attacks. Based on these trust values, we will propose a trust-based routing protocol to route messages through the highly trusted nodes (which performed packet relay more successfully in the past) to minimize the probability of dropping the messages, and thus improve the network performance in terms of throughput and packet delivery ratio. Advantages of Proposed System are Low-mobility and the large-hardware-resources nodes and Compare with Existing system, the proposed system is secure.

III. PROPOSED SYSTEM

The main goal is to enable the nodes to indirectly build trust relationships using exclusively monitored information. Trust values are used to decide which nodes to select/avoid in routing. Since a trust value depicts the probability that the node conducts an action, route reliability can be computed using its nodes' trust values to give probabilistic information about the route stability and lifetime. This information is very useful for establishing stable routes and selecting proper routes that can satisfy the source nodes' requirements. Once a node's trust values fall behind those of the majority of the nodes, the node will almost not participate in routing without the need for determining good thresholds. To evaluate the nodes' trust values accurately because it can monitor/evaluate the nodes' behavior over different times and sessions.

3.1 Network module

A network is simulated, with minimum of 30 nodes moving in a defined area. Each node moves randomly in this area, with a speed selected in a range [0, vmax] with no pause time. We create a number of nodes using ns2.

3.2 Adversary module

The mobile nodes are probable attackers but the TP is fully secure. The mobile nodes are autonomous and self-interested and thus motivated to misbehave. The TP is run by an operator that is motivated to ensure the network proper operation. It is impossible to realize secure payment between two entities without a trusted third party. The attackers have full control on their nodes and can change their operation and infer the cryptographic data. The attackers can work individually or collude with each other under the control of one attacker to launch sophisticated attacks.

3.3 Communication Establishment

In Communication phase, the nodes are involved in communication sessions and Evidences and payment reports are composed and temporarily stored. The nodes accumulate the payment reports and submit them in batch to the TP illustrated in figure 1. 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.

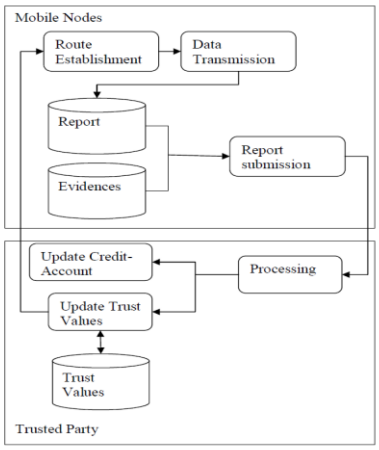

Fig 1: Packet Transmission Phase

Finally, in Credit-Account Update phase, the AC clears the payment reports. The Communication phase has four processes: route establishment, data transmission, Evidence composition, and payment report composition/submission.

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 MX and its signature to R, X, Ts, and the hash value of the message (H(MX)) and sends the packet to the first node in the route. The security tokens of the Xth data and ACK packets. The source node's signature is an undeniable proof for transmitting X messages and ensures the message's authenticity and integrity.

Signing the hash of the message instead of the message can reduce the Evidence size because the smaller-size H(MX) is attached to the Evidence instead of MX. 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 as shown in figure 2. Each node stores only the last signature for composing the Evidence, which is enough to prove transmitting X messages, e.g., after receiving the Xth data packet, the nodes should store SigS(R, X, Ts, H(MX)) and remove SigS(R, X-1, Ts, H(MX-1), and so on. The data transmission process ends when the source node transmits its last message, or if the route is broken, e.g., due to node mobility or channel impairment.

```
1. // n_i is the source, intermediate, or destination node that is running the algorithm
2. if(n_i is the source node) then
3. P_X← [ R,X, M_X, Sigs( R,X, T_s, H(M_X ))];
4. Send(P_X);            // send P_X to the first node in the route
5. else
6. if(R,X, T_s are correct) and verify (Sigs( R,X, T_s, H(M_X ))) == TRUE) then
7.if( n_i is an intermediate node) then
8. Relay the packet;
9. Store Sigs( R,X, T_s, H(M_X ));
10. endif
11. if(n_i 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(P_X is last packet) then
20. Evidence = {R, X, T_s, H(M_X), h^((0)), h^((x)), H,0))}
21. Report = { R, T_s, F,X);
22. Store Report and Evidence;
23. endif
```

Fig 2: Data transmission/composition of evidence and report

3.4 Evidence and Payment 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. The figure shows that 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 DATA contains the identities of the nodes in the route (R), the number of received messages (X), the session establishment time stamp, the root of the destination node's hash chain h(0), the hash value of the last message (H(MX)), and the last received hash value (h(V)). V ¼ X _ 1 when the last received packet is the Xth data packet because the route is broken before receiving the Xth ACK packet that carries h(X), but V= X when the last received packet is the Xth ACK packet.

The DATA does not have h(1) when the route is broken after receiving the first data packet because the ACK that has h(1) is not received. The PROOF is an undeniable security token that can prove the correctness of the DATA and protect against payment manipulation, forgery, and repudiation. The PROOF is composed by hashing the destination node's signature and the last signature received from the source node, instead of attaching the signatures to reduce the Evidence size.

3.5 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. For the first report, A is the source node and claims sending 12 messages, but it did not receive the ACK of the last message because F is zero. For the second report, A is the destination node and claims receiving 17 messages. For the third report, A is an intermediate node and claims receiving 15 messages, but it did not receive the ACK of the last message.

3.6 Trust based system

We propose a trust system that maintains multi-dimensional trust values for each node to evaluate the node's behavior from different perspectives. Multi-dimensional trust values can better predict the node's future behavior, and thus help make smarter routing decisions. In our trust system, the nodes that frequently drop packets, break routes, or are not active in relaying packets have low trust values. Moreover, for the efficient implementation of the trust system, TP computes the trust values by processing the payment receipts. A node's trust values are attached to its public- key certificate to be used in making routing decisions.

Trust values are used to decide which nodes to select/avoid in routing. Since a trust value depicts the probability that the node conducts an action, route reliability can be computed using its nodes' trust values to give probabilistic information about the route stability and lifetime. This information is very useful for establishing stable routes and selecting proper routes that can satisfy the source nodes' requirements.

3.7 Performance Evaluation

The number of nodes having high trust values, medium trust value and low trust values and their trust values are uniformly distributed. Compare the existing and proposed system with following parameters packet delivery ratio and throughput. The graph of Packet Delivery Ratio is shown in following Fig.1, We can infer, as the number of nodes increases, the packet delivery ratio also increases because there are more route choices for the packet transmission. Among the two response mechanisms, we also notice the packets delivery ratio of the payment scheme and trust based payment scheme. The proposed system result is better than the existing system. We observe that trust based payment scheme has a PDR (Figure 1) of about 95% for dense networks. As the node density decreases, this rate gradually goes down to about 80% in figure 3. In contrast, payment scheme PDR ranges between 90% and 75% for dense networks and quickly drops to around 60% for networks.

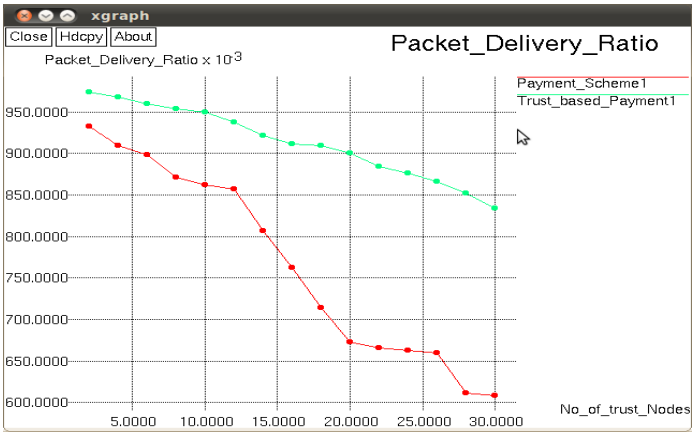

Fig 3: Packet Delivery Ratio graph

IV. CONCLUSIONS

We have proposed trust based payment scheme that uses payment/trust systems with trust-based routing protocol to establish stable/reliable routes in HMWNs. It stimulates the nodes not only to relay others' packets but also to maintain the route stability.

It also punishes the nodes that report incorrect energy capability by decreasing their chance to be selected by the routing protocol. We have proposed routing protocols and evaluated them in terms of overhead and route stability. Our protocols can make informed routing decisions by considering multiple factors, including the route length, the route reliability based on the nodes' past behaviour, and the route lifetime based on the nodes' energy capability. It establishes routes that can meet source nodes' trust requirements. It is useful in establishing routes that avoid the low-trust nodes, e.g., malicious nodes, with low overhead. The analytical results have demonstrated that based payment scheme can secure the payment and trust calculation without false accusations. Moreover, the simulation results have demonstrated that based payment scheme can improve the packet delivery ratio due to establishing stable routes.

ACKNOWLEDGMENT

Our Sincere thanks to our most respective Professor and Dean - Department of Computer science and Engineering , Dr.S.Karthik, Our beloved professor and Head of the Department Dr.T.KalaiKumaran and the people who are mainly motivated to prepare and publish this article in your esteemed journal. Last but not Least, We highly thanks to Prof.R.M.Bhavatharani Madam, Associate Professor/Department of CSE suggest to concluding about this work.

REFERENCES

[1] G. Shen, J. Liu, D. Wang, J. Wang, and S. Jin, 2011"Multi-Hop Relay for Next-Generation Wireless Access Networks," *Bell Labs Techn*ical J., vol. 12, no. 5, pp. 175-193.

[2] G. Marias, P. Georgiadis, D. Flitzanis, and K. Mandalas,2011 "Cooperation Enforcement Schemes for MANETs: A Survey," *Wiley's J. Wireless Comm. and Mobile Computing*, vol. 6, no. 3, pp. 319-332.

[3] B. Wu, J. Chen, J. Wu, and M. Cardei, 2010"A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks," *Wireless Network Security, Springer Network Theory and Applications*, vol. 17, pp 103-135.

[4] Y. Zhang, W. Lou, and Y. Fang, 2012"A Secure Incentive Protocol for Mobile Ad Hoc Networks," ACM 15) 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.

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

[6] M. Mahmoud and X. Shen, 2011"Stimulating Cooperation in Multihop Wireless Networks Using Cheating Detection System," Proc. *IEEE INFOCOM* '11.

[7] M. Mahmoud and X. Shen, 2011"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.

[8] S. P. Santhoshkumar , Mr. D. Prabakar, Dr. S. Karthik,2013," Frequent Data Updating Using Random Checkpointing Arrangement in Decentralized Mobile Grid Computing" ,*IJAIR*, Vol 2 issue 11,pp 425-431.

[9] D.Prabakar,Dr.M.Marrikkannan, Dr.S.Karthik,2012," A relative study of Various Routing Protocols in Wireless Sensor Networks", *IRACST* ISSN: 2250-3501Vol.2, No6.

