www.ijiarec.com

ISSN: 2348-2079

MAR-2015

International Journal of Intellectual Advancements and Research in Engineering Computations

CREDENCE BASED RELIABLE ROUTING FOR MULTIHOP WIRELESS NETWORKS

[1]S.Ramnivash M.E, [2]V.M. Arul M.E

ABSTRACT

In a multihop wireless network (MWN), the packets from a source node are relayed through a large number of intermediate nodes before they are delivered to the destination. But such relaying of other's packets will consume valuable resources of these intermediate nodes such as their energy and computing power. That being so, some nodes usually referred to as selfish nodes may not cooperate in relaying other's packets and at the same time they make use of other cooperative nodes to relay their own packets. In such a situation some incentive mechanisms are used to stimulate these selfish nodes to cooperate. For that a protocol is proposed here which not only stimulates the node cooperation and also establishing stable routes. Simulating node cooperation is achieved using incentive credit approach followed by processing the payment receipts to evaluate the node's packet relay probabilities in terms of trust values and thus stable routes are established through the highly trusted nodes.

KEYWORDS – Cooperation incentive scheme, Network-level security, Payment Schemes, and Selfishness attacks.

INTRODUCTION

Multi-hop wireless networks (MWN) appear to be a promising combination of the dynamics of the mobile adhoc networks and the reliability of the infra-structured wireless networks. Each node mobile in the network can set up as and play the role of a base station in that it can transmit to and receive from other nodes in the network. A node can directly communicate to other nodes if they are within line-of-sight. Non-line-of-sight-nodes are called hidden nodes. Communication between a pair of hidden nodes needs to hop over one or more intermediate nodes, in this sense, it is called multihop networks.

Multihop packet relay can extend the network coverage using limited transmit power, improve area spectral efficiency, and enhance the network throughput and capacity. Data Transmission is achieved by Relaying packets through many hops. In multi-hop wireless networks, communication between two end nodes is carried out through a number of intermediate nodes whose function is to relay information from one point to another multi-hop wireless networks can provide data access for large and unconventional spaces. A multihop wireless network is represented as M = (N, L), where N is a set of nodes and L is a set of coordinates on the plane denoting the locations of the nodes. Multi-hop wireless networks utilize multiple wireless nodes to provide coverage to a large area by forwarding and receiving data wirelessly between the nodes. Data can be transmitted at low power over short distances. Several routing protocols are available to choose routing path between nodes. A wireless multi-hop network formed by a set of mobile nodes in a self organizing way without relying on any established

Author for Correspondence:
[1]Assistant Professor, Department of CSE, SVCET, Puliyangudi, India, Email: ramdhina12@gmail.com
[2]Assistant Professor, Department of CSE, SVCET, Puliyangudi, India, Email: arul.banumathy@gmail.com

infrastructure. Due to the absence of infrastructure, all networking functions must be performed by the nodes themselves. For instance, packets sent between two distant nodes are expected to be forwarded by intermediate nodes. This operating of networks renders cooperation among nodes an essential requirement. By cooperation, meant that the nodes perform networking functions for the benefit of other nodes, lack of cooperation may have fatal effects on network performance. In addition, these networks could be larger, have a longer lifetime, and they could be completely self-organizing, meaning that the network would be run solely by the operation of the end-users. In such networks, there is no good reason to assume that the nodes cooperate. Indeed, the contrary is true: In order to save resources (e.g., battery power, memory, and CPU cycles) the nodes tend to be "selfish". Security in multihop wireless networks (MWNs) has received intensive attention recently, whereas the issue of selfish nodes, which may refuse to forward packets for others to save their own resources, is not well addressed yet. This kind of non cooperative action would cause a severe problem that is more likely in wireless compared to their wired counterpart. In such a network its not possible to expect all the nodes to be legitimate and good. In order to avoid this kind of selfishness some incentive mechanisms are adopted where the cooperative nodes in the networks are provided with some points or credits rather than being selfish.

COOPERATION ENFORCEMENT MECHANISMS

In multihop networks such as mobile ad hoc networks selfish or misbehaving nodes can disrupt the whole network and severely degrade network performance. The basic cooperation enforcement approaches are listed as token based, reputation based and credit based mechanism. In token based approach, Nodes without a valid token are isolated in the network, and all of their legitimate neighbors will not interact with them in routing and forwarding services. Upon expiration of the token, each node renews its token via its neighbors. The lifetime of a token is related to the node's behavior. A well behaving node with a good record needs to renew its token less often. In reputation based mechanism presents an extension to the routing protocol in order to detect and isolate misbehaving nodes. The protocol is designed to be able to make cooperation fair. Each node has four components: a monitor, a reputation system, a trust manager, and a path manager. In credit based mechanism, a secure credit-based remuneration protocol is carefully designed to ensure the correct charging and rewarding of the credits on each node for packet sending, receiving, and forwarding. These cooperation enforcement schemes also providing focus on thwarting packet-dropping and selfishness attacks, preserving user privacy, and establishing stable communication routes to minimize the probability of breaking the route, thus boosting the network performance in terms of end to-end packet delay, packet delivery ratio, throughput, etc.

SYSTEM DESIGN

In Multihop wireless networks the selfish nodes which may refuse to forward packets for others to save their own resources. Specifically, a selfish node is an economically rational node whose objective is to maximize its own welfare, which is defined as the benefit of its actions minus the cost of its actions. Since forwarding a message will incur a cost (of energy and other resources) to a node, a selfish node will need incentive in order to forward others' messages. There are two main approaches aiming to address this issue, namely, reactive approaches and preventive approaches. The former is intended to enforce the cooperation by firstly detecting the selfish nodes, avoiding routing through them, and then punishing them by spreading their bad reputations and thus isolating them. As for the latter, most of the proposals are related to provide some kinds of incentives for the selfish nodes to participate in packet forwarding. The possibility to provide incentive is to use credit where a node receives one unit of credit for forwarding a message of another node, and such credits are deducted from the sender. This incentive payment should be fair and secure such that only the legitimate nodes who actually participated in data communication cooperatively would beneficial and those selfish nodes in the network shouldn't gain anything fruitful. Whereas deploying such a Secure Payment Scheme in

multihop wireless networks requires more Communication and Processing Overhead. Further the payment schemes alone are not sufficient for stable routes that require selecting the nodes that behaved well in the past, thus includes the trust based routing protocol proposed in this paper enhance the security level and also improves the faith factor of source and destination on the selected trusted path in the network. The proposed protocol not only stimulates the node cooperation and also establishing stable routes. Simulating node cooperation is achieved using incentive credit approach followed by processing the payment receipts to evaluate the node's packet relay probabilities in terms of trust values and thus stable routes are established through the highly trusted nodes.

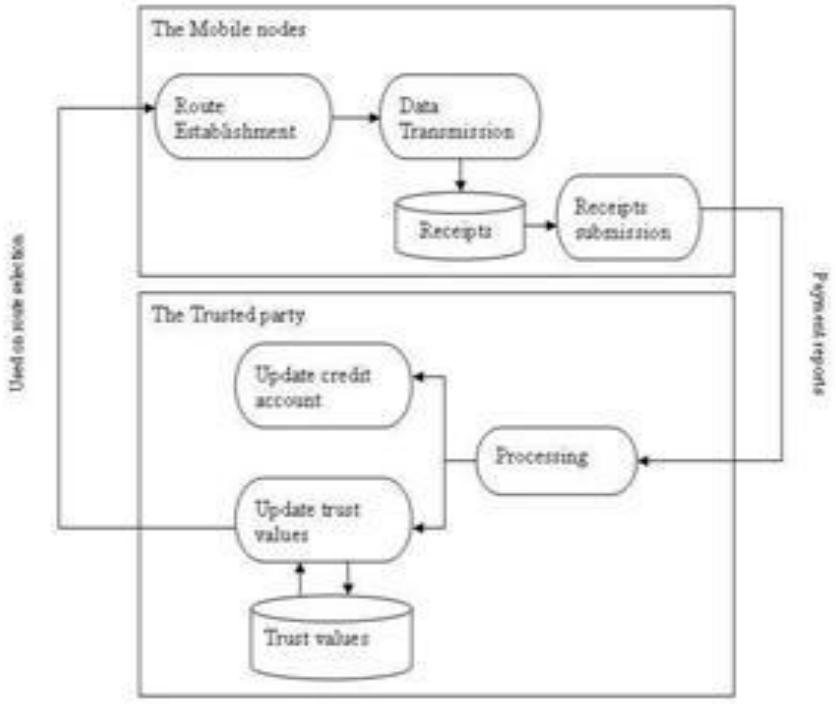


Fig: The Proposed System

IMPLEMENTATION

The proposed approach has four main phases as shown in the diagram includes data transmission phase where the nodes are involved in communication sessions and payment reports were composed and stored. The nodes accumulate the payment reports and submit them in batch to the Trusted Party. By processing reports the credit account update phase that receives fair and corrected payment reports and update the nodes credit accounts. The payment reports are cleared using the charging and rewarding policy and get the payment correctly. In trust value updation the node's trust value is updated based on its recent behavior. Finally in route establishment phase the routes were established through highly trusted nodes.

COMMUNICATION

The Communication phase has three processes,

- Route establishment
- Data transmission
- Report submission

Every node that is created has to be registered with a Trusted Party in order to communicate effectively and to get the payment correctly. Upon registration, the trusted party will give a public and private key pair, a symmetric key and a certificate. In order to establish the communication, 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 RREP packet contains the identities of the nodes in the route. The signature authenticates the hash chain and links it to the route. The intermediate nodes verify the destination nodes signature, relay the RREP packet, and store the signature and H(Mx).

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 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. Each node stores only the last signature for composing the evidence, which is enough to prove transmitting X messages. The data transmission process ends when the source node transmits its last message, or if the route is broken.

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 DATA contains the identities of the nodes in the route (R), the number of received messages (X), the session establishment time stamp, the hash value of the last message (H(Mx)), and the last received hash value ($h^{(V)}$). 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

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. A node sends a Report Submission Packet (RSP) to the TP at time ti to submit the reports of the sessions held since the last contact at t_{i-1}. The packet contains the reports of the sessions held in $[t_{i-1},ti]$ (Reports$[t_{i-1},t_i]$), time stamp, and a keyed hash value ($H_{KA}()$) to ensure the packet's integrity and authenticity, where KA is the long term symmetric key shared between a node and the TP. Thus, the TP can make sure that the packet has not been manipulated and the reports are indeed sent by the intended node, which is important to secure the payment and hold the nodes accountable for any misbehavior.

CREDIT ACCOUNT UPDATE

The Credit-Account Update phase receives fair and corrected payment reports to update the nodes credit accounts. The payment reports are cleared using the charging and rewarding policy. The Credit-Account Update phase receives fair and corrected payment reports to update the nodes credit accounts. The payment reports are cleared using the charging and rewarding policy and get the payment correctly. Upon registration the trusted party will give a public and private key pair, a symmetric key and a certificate. The public and private key pair is used in communication are required to act as source or destination node. The symmetric key is used to submit the payment reports. 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), i.e., at least one report is submitted after TCert of the session occurrence. It is worth to note that the maximum time duration for a node's two consecutive contacts with the TP is TCert to renew its certificate to be able to use the network. The worst case timing of the submission and clearance of the reports with considering that the reports are submitted every TCert. At t_1, the nodes submit the payment reports of the sessions held in $[t_0; t_1]$ and the fair reports of these sessions are cleared. Thus, the maximum payment clearance delay of fair reports is TCert for the sessions held shortly after t_0, but the average payment clearance delay is TCert/2 for the sessions held in $[t_0,t_1]$ assuming that the sessions are held according to uniform random distribution.

TRUST VALUE UPDATE

The notion of trust used in this paper is defined as the degree of belief, the expectation, or the probability that a node will act in a certain way in the future based on the nodes past behavior. Trust values are calculated from the past behavior to predict the expected future behavior. A node can protect its trust values by not involving itself in routes with a neighbor that frequently breaks routes or has low trust values. 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. The TP considers that a node relayed a message if there is a successor in the route reports receiving the message, i.e., the possession of SigS(R, TS, C, H(MC)) by node entails that all the nodes before it in the route indeed relayed *C* messages. The rationale here is that the nodes that drop the packets more frequently will be accused more and thus suffers from more trust degradation.

T(A)= No. of relayed messages in the last ω sessions / No. of received messages in the last ω sessions (1)

T(A) refers to the trust value of node A, which is represented with a number in the range [0, +1] signifying a continuous range from complete distrust (0) to complete trust (+1), T(A) is the number of relayed messages to the number of received messages by A in the last ω sessions. If A drops a large ratio of the packets, e.g., due to malicious action or high mobility, T (A) will be very low.

$$T(WXYZ) = T(W) \times T(X) \times T(Y) \times T(Z) \quad (2)$$

Route reliability can be computed using the nodes' trust values to get probabilistic information about the route stability, which can be used in route selection. Eq. 2 gives the probability that a packet can be transferred through a route with nodes W, X, Y, and Z. Comparing the reliabilities of routes 1 and 2 in Table 1, the low-trust node, such as X in route 2, has very little chance to be involved in a session because it significantly degrades the route reliability. Although the nodes' trust values of route 3 are the same as those of route 1, route 3 has higher reliability, which demonstrates that the shortest routes are preferable. The probability that a packet is transferred through route 4 is close to zero because the nodes have very low trust values, which demonstrates the importance of choosing good nodes.

Table 1: Numerical example for trust calculation

Route No.	T(W)	T(X)	T(Y)	T(Z)	T(WXYZ)
1	0.8	0.8	0.8	0.8	0.4096
2	0.8	0.2	0.8	0.8	0.1024
3	0.8	0.8	0.8	---	0.512
4	0.2	0.2	0.2	0.2	0.0016

ROUTE ESTABLISHMENT

In this section, the route selection is achieved by selecting the best route in the BAR (Best Available Route) protocol.

RREQ DELIVERY

To establish a route to the destination node D, the source node S broadcasts the Route Request Packet (RREQ) that contains the identities of the source (IDS) and the destination (IDD) nodes, time stamp (TS), the Time-To-Live (TTL) or the maximum number of intermediate nodes, and the trust requirements. If a node breaks the route before relaying Cm messages, the node's trust value is decreased. The route reliability is bounded by the minimum trust value raised to the TTL-th power. A node broadcasts the packet after attaching its identity if it can meet the source node's requirements and TS is within a proper range. To reduce the number of RREQ broadcastings, when an intermediate node receives a RREQ, it introduces a Wait Period to collect subsequent packets, if any, traveling through different routes and then selects some then it selects the most reliable route among them.

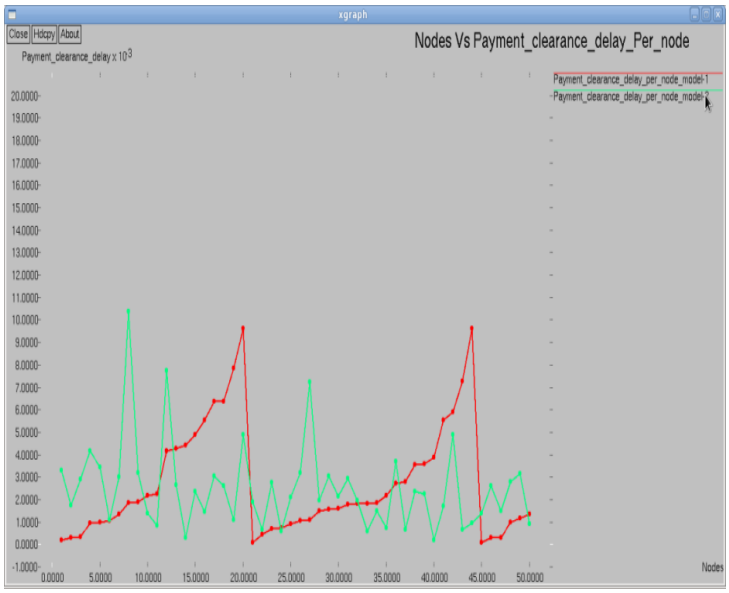
ROUTE SELECTION

After receiving the first RREQ packet, the destination node waits for τD time window and keeps receiving other RREQ packets if there are, and then selects the best available route by the destination node which excludes the routes with very low reliability.

RREP DELIVERY

The RREP packet contains R, h0, and the destination node's signature SigD (R, TS, h0, Cm) and certificate. This signature authenticates the hash chain and links it to the session, and proves the destination node's approval to pay for the session, which is impotent to secure the payment. Each intermediate node signs the RREP packet's signature to authenticate itself and relays the packet after attaching its certificate. It also verifies the RREP packet's signatures to authenticate the nodes between itself and the destination node, and saves h0 for the receipt composition. The source node receives the RREP packet containing the nodes' authentication code.. This authentication process is important to make sure that the nodes are indeed participated in the session, and thus hold them accountable for the packet drop. The source node verifies the Auth_Code and the nodes' certificates to make sure that the nodes meet its trust requirements. If a node lies in its residual energy, the route will be broken at this node and thus its trust value degrades. In the first data packet, the source node attaches the Auth_Code to enable the nodes to authenticate the previous nodes in the route. This signature verification process is necessary to make sure that the Auth_Code is correct and thus to ensure the receipt integrity to protect the payment.

Fig: Nodes Vs Payment Clearance Delay



Acceptable payment clearance delay is necessary to make the practical implementation of the payment scheme effective. The maximum payment clearance delay 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.

CONCLUSION AND FUTURE WORK

Thus the payment/trust system uses trust-based routing protocol to establish stable/reliable routes in MWN, stimulates the nodes not only to relay other's packets but also to maintain the route stability. By processing the payment reports a trust value is maintained for each node. Nodes which relay messages more successfully will have higher trust values. Based on these trust values, a trust-based routing protocol proposed to route messages through the highly trusted nodes. By thus the probability of packet droppings get reduced results improved network performance in throughput and packet delivery ratio.

REFERENCES

[1]. Buttyan.L and Hubaux.J, "Stimulating Cooperation in Self- Organizing Mobile Ad Hoc Networks," Mobile Networks and Applications, vol. 8, no. 5, pp. 579-592, Oct 2004.

[2]. Mahmoud.M and Shen.X, (2010) "PIS: A Practical Incentive System for Multi-Hop Wireless Networks," IEEE Trans. Vehicular Technology,vol. 59, no. 8.

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

[4]. Mahmoud.M and Shen.X, (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, July 2011

[5]. Mahmoud.M and Shen.X, (2012) "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.

[6]. Mahmoud.M and Shen.X, (2013) "A Secure Payment Scheme with Low Communication and Processing Overhead for Multihop Wireless Networks," IEEE Transactions on Parallel and Distributed Systems, Vol. 24, No. 2, February 2013

[7]. Weyland.A, (2007) "Cooperation and Accounting in Multi-Hop Cellular Networks," PhD thesis, Univ. Of Bern

[8]. Wu.B, Chen.J, Wu.J, and Cardei.M, (2007) "A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks," Wireless Network Security, Springer Network Theory and Applications, vol. 17, pp 103- 135.

[9]. Zhang.Y, Lou.W, and Fang.Y, (2007) "A Secure Incentive Protocol for Mobile Ad Hoc Networks," *ACM Wireless Networks*, vol. 13, no. 5, pp. 569-582.

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