Received: August 6, 2017

INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Trust Centric Stable Routing For Wireless Mesh Networks

Navamani Thandava Meganathan[1]*

[1] *Department of Computational Intelligence,*
School of Computer Science and Engineering, VIT University, Vellore, Tamilnadu, India
* Corresponding author's Email: navamani.tm@vit.ac.in

Abstract: Wireless Mesh Network (WMN) is an emerging next generation wireless technology with several applications in wireless environment. However, the lack of physical protection and ad-hoc connectivity between the users not only increases its routing overheads but also makes it vulnerable to security attacks such as packet dropping attacks. Hence, it is essential to design a secure, reliable and stable route in WMN to thwart against packet dropping attacks. To address this issue, a protocol named Trust-Centric Stable Routing (TCSR) is proposed for WMNs which incorporates security, reliability enhancement and integration of payment systems. Here, trusted nodes with forwarding reliability are selected for secured and efficient data transmission by introducing reliable reputation based trust computation algorithm. This algorithm well isolates malicious nodes during route discovery and packet transmission. Payment system uses a system of reward and punishment so that nodes which relay others' packets are given credits and those which send the packets are charged. Thus, by integrating these systems, the proposed system has been able to enforce cooperation among nodes to participate in forwarding packets and successfully identify and isolate malicious nodes in the network. The simulation results prove that TCSR provides optimal network performance in terms of throughput and delay and also provides better security against packet dropping attacks.

Keywords: Security, Reliable route, Packet dropping attacks, Trust model, Payment system, Wireless mesh network (WMN).

1. Introduction

Wireless Mesh Networks (WMN) are characterized by a dynamic topology, multi-hop wireless communication infrastructure which is decentralized, reliable and resilient provides a promising paradigm that allows network deployment at an economical cost. Wireless mesh network architecture consists of mesh routers and mesh clients. Mesh routers usually have minimal mobility and multiple network interfaces which can improve performance and aggregate capacity. Mesh routers can be categorized as: Access mesh router, Backbone mesh router and Gateway router. Mesh routers need to have an extra operation capacity to support mesh routing besides normal routing duties. Mesh clients are end-user devices which function not only as hosts but also to route information packets. They can communicate directly with mesh routers to keep users connected such as computers, PDAs and laptops. Mesh clients approach mesh network through access mesh router while mesh backbone is connected to Internet through the gateway routers. Security and reliability issues hinder the success of WMN and finding high performance reliable route is still a challenging issue. The distributed and open nature of the WMN is the major cause for its vulnerability to both active and passive attacks. The existing routing protocols make assumptions that all the nodes participate honestly and all the attacks are from outside. However, some nodes may get compromised by intruders or they may exclude themselves because of their selfish behaviour. Mahmoud, et al. [1] developed a stable and reliable routing protocol named E-STAR in heterogeneous multi hop wireless networks. This protocol combines payment and trust systems with a trust based and energy aware routing protocols. Multi-dimensional trust values are used for

DOI: 10.22266/ijies2017.1231.16

computation of trust and reliability in routing. However, the trust mechanism doesn’t take into account the forwarding reliability of the nodes at network layer. Payment system is used to enforce fairness by stimulating nodes to forward packets and crediting them for successful packet transmission. However, the designed trust metrics are more suited for the nodes which are mobile always. These issues are addressed in the proposed method. Mahmoud, et al. [2] have proposed a mechanism to thwart against rational and irrational packet dropping attacks for multi hop wireless networks by incorporating stimulation and punishment methodologies. This mechanism applies micropayment system to enforce cooperation among the rational packet droppers and reputation system is used to address irrational packet dropping attacks. A new type of monitoring technique which is based on payment receipts is introduced to analyse the frequency of packet dropping within the network. However, the reputation mechanism didn’t take into account about the participants’ past behaviour for determining the routing path and also route stability was not considered. These issues are addressed here. Yu, M et al. [3] proposed a secure routing protocol with quality of service support. It uses both digital signature and encryption instead of using double signatures to protect packets from internal attacks. However it does not solve routing delay and scalability issues. Traditional cryptographic algorithms alone are insufficient to prevent insider attacks as they can’t identify malicious nodes from selfish nodes. The existing secure routing protocols fail to evaluate the link quality by considering the forwarding reliability at the network layer and also not enforcing cooperation among the participating nodes thereby not acquiring high-throughput path. The proposed scheme aims at enhancing the route stability, reliability and also establishing cooperation among the intermediate nodes in wireless mesh networks. A stable route can be established by integrating reputation based trust mechanism and cross-layer based routing metrics. The contributions of our work are the following: 1) Identifying competent nodes and isolating malicious nodes during route establishment by proposing a new novel reliable reputation based trust mechanism. 2) Route discovery based on trust metric and cross layer based link quality metric 3) Enforcing cooperation among the nodes by integrating payment system 4) Designing a trust-centric stable routing protocol for thwarting packet dropping attacks in WMN. The remaining sections are as follows: In Section 2, the related works are reviewed. Section 3 describes the proposed system in detail. Implementation and performance analysis are discussed in section 4. In section 5, conclusion is drawn.

2. Related work

The recent years have seen a surge of research in these networks as these networks are vulnerable to security attacks. This introduced the need to establish secured, reliable and stable routing mechanisms in wireless mesh networks. In [4], the authors have proposed reputation evaluation mechanism to enforce security and to defend against internal attacks in WMNs. Here, the reputation computation incorporates traditional weighted average model to compute the link quality metric which in turn evaluates the direct behaviour of the nodes. However, in general, wireless environment needs cross layer based routing metrics to guarantee the accurate measurement of link quality. Paris, S et al. [5] proposed a novel cross-layer based routing metric, named Expected Forwarding Counter (EFW) to defend against packet dropping attacks. This metric considers link quality of wireless links using Medium Access Control (MAC) layer measurements and also monitors the forwarding behaviour in network layer to select secure reliable routing path in WMN. Two further variants of EFW named Minimum Expected Forwarding Counter (MEFW) and Joint Expected Forwarding Counter (JEFW) are also proposed in the same paper to solve the problem of packet dropping behavior of selfish nodes. Authors proved that MEFW is a robust link quality metric to select secure reliable routing path in WMN. The proposed protocol includes this metric to determine reliable routing path.

Zhong, S et al. [6] developed a cheat-proof credit based system for mobile ad-hoc networks, where for each message; the source node signs the identities of the nodes in the route and the message. The intermediate node that relays the packets will submit the receipts to offline trusted party which will process the receipt and update the credits. The submission of the receipts may flood the network and incurs little amount of overhead also. Li, Y [7] introduced reputation based system for wireless mesh networks using multi-path routing protocol that stimulates each node in different paths to forward packets from others. It detects malicious nodes based on reputation metrics. But, it doesn’t address the issue of false accusations in the identification of malicious nodes. The proposed method addresses this issue by incorporating reliable reputation based trust computation algorithm. Wang, F et al. [8] proposed a reputation-based secure source routing protocol which considers the reputation of a node as its trustworthiness. The best routing path is selected using route reputation. Comparison of the designed protocol with existent systems in dealing with routing attacks has been extensively studied; however, the routing overhead caused due to large number of control messages for each data packet decreases its efficiency.

Khan, S et al. [9] introduced a secure route selection scheme in wireless mesh networks. This scheme is based on two hop passive acknowledgement mechanism which is used to prevent the network from packet dropping attacks. However, this mechanism has not provided complete security solution against all types of packet dropping attacks. You, Z et al. [10] proposed an efficient secure routing protocol for hybrid wireless mesh network. The protocol implements several cross layer parameters to select an optimal route based on security and robust against various multi hop threats in WMNs. Yu, Y et al. [11] have proposed a new dynamic hierarchical reputation evaluation scheme to provide secure solution against intruders for hybrid wireless mesh networks. This scheme is based on virtual cluster structure and behaviour, correlations of the nodes in the network. However this scheme doesn’t address about link reliability to provide high performance routing path. TCSR selects reliable routing path by considering link reliability metrics.

In my previous work [12], Privacy preserved and Secured Reliable Routing protocol for wireless mesh networks is proposed to ensure privacy, security and reliability in WMNs. The privacy and security analysis proved that the proposed protocol is not only resistant to privacy related attacks and also the attacks caused by packet dropping and misdirecting attacks. However, the proposed protocol fails to address cooperation among the nodes completely for better packet forwarding. Here it is addressed. Ferraz, LHG et al. [13] have proposed an efficient distributed access control mechanism to secure and to stimulate cooperation in MANETs by excluding malicious nodes from the network. Simulation results proved that the proposed scheme provides accurate, precise detection and isolation of malicious nodes by combining trust and voting schemes. Wang, B et al. [14] have proposed a Trust based QoS routing algorithm to enhance the security of ad hoc networks by isolating malicious nodes. Trust and Qos metrics are considered for detecting and isolating the misbehaving nodes and higher delay links.

By reviewing the literature, it is analyzed that existing secure routing protocols designed for WMNs failed to provide stable and reliable routing and to establish complete security against malicious nodes. Hence, I have proposed a Trust Centric Stable Routing (TCSR) protocol for WMNs to address the above issues.

3. Trust centric stable routing (TCSR)

3.1 Network model

The system architecture of WMN as shown in Fig. 1 composed of mobile client nodes, static routers and offline Trusted Party (TP) whose public key is known by all the nodes. Each mobile node must first register with the TP, and TP issues a certificate. By having a valid certificate, a node can participate in data transmission. The certificate is valid only for a limited time which has to be renewed periodically. The trusted party processes the receipts to update the credit accounts of the nodes. To implement encryption mechanism, each node is associated with a unique identity and private/public key pair.

3.2 The proposed system

The proposed system describes a Trust-Centric and Stable Routing (TCSR) to thwart against packet dropping attacks in Wireless Mesh Networks. It integrates payment and reputation system with trust and energy aware routing to stimulate nodes to cooperate in forwarding packets of peer nodes. It comprises four modules: Route Establishment, Reliable Reputation based Trust Computation, Data Transmission and Updating Credit Accounts. During route establishment phase, a secure, reliable and stable route is discovered between the source and the destination node.

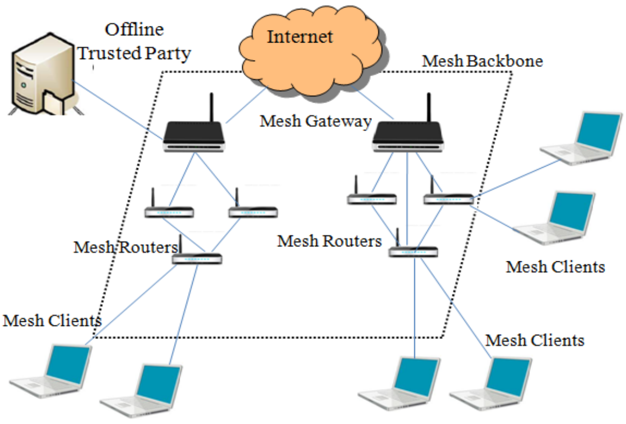

Figure.1 System architecture of WMN

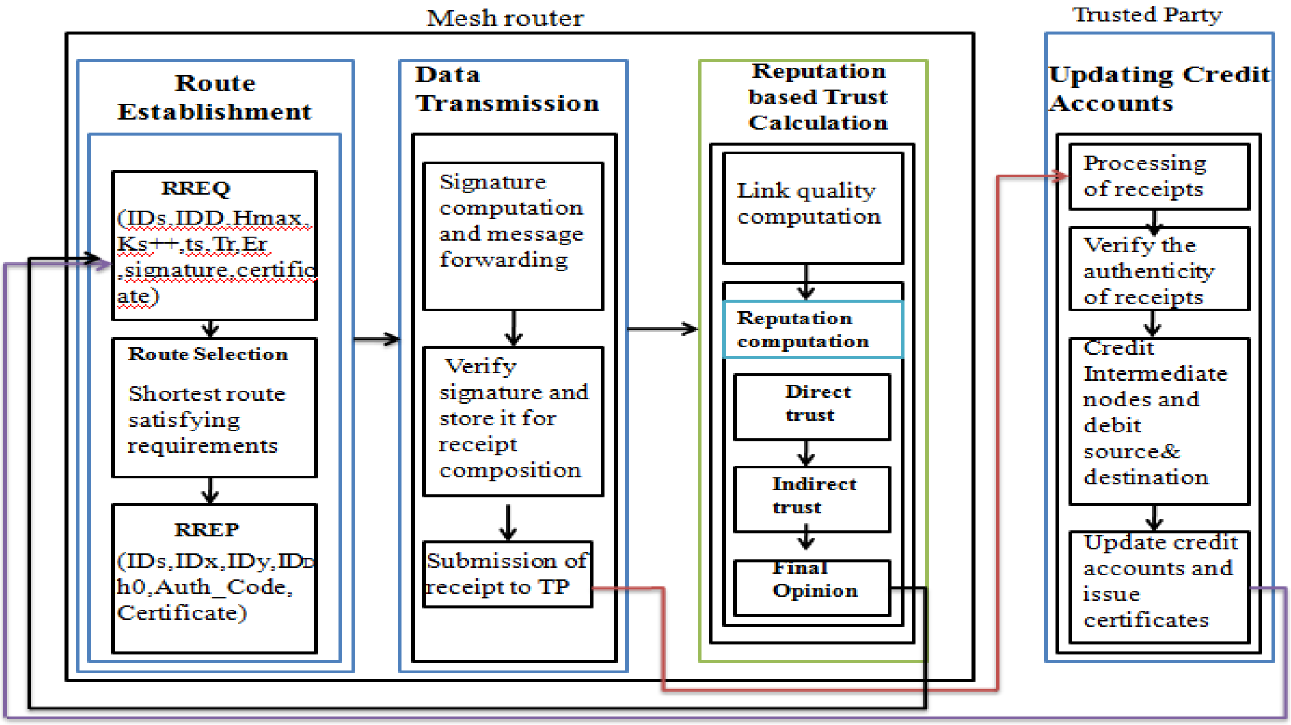
Mesh router
Trusted Party
Route Establishment
RREQ (IDs,IDD,Hmax, Ks++,ts,Tr,Er ,signature,certificate)
Route Selection
Shortest route satisfying requirements
RREP (IDs,IDx,IDy,IDD h0,Auth_Code, Certificate)
Data Transmission
Signature computation and message forwarding
Verify signature and store it for receipt composition
Submission of receipt to TP
Reputation based Trust Calculation
Link quality computation
Reputation computation
Direct trust
Indirect trust
Final Opinion
Updating Credit Accounts
Processing of receipts
Verify the authenticity of receipts
Credit Intermediate nodes and debit source& destination
Update credit accounts and issue certificates

Figure.2 Functional components of the proposed system

Reliability is achieved by ensuring the link quality between the nodes to be above the threshold and also by considering forwarding reliability at network layer. Also, only nodes that have a high reputation value are considered for forwarding packet transmission, thereby preventing malicious nodes from disrupting the network performance. Data transmission phase involves transmitting secured data from the source to the destination node. Every intermediate node that participated in the data forwarding, composes a receipt and sends it to the offline Trusted Party (TP) whenever a connection is available. The TP then processes the receipts and credits the intermediate nodes and debits the source and destination node. It also updates its credit accounts and issues a certificate with the updated credit values to be utilized in the subsequent route discoveries. This system is thus able to discover a secure, reliable and stable route by integrating trust and payment system. The functional components of the proposed system are shown in Fig. 2. It consists of following four phases:

- Route Establishment
- Reliable Reputation based Trust Computation
- Data Transmission
- Updating credit accounts

Route Establishment

To establish a route for data transmission, the source node broadcasts the RREQ control packet embedded with trust and energy requirements. The source node waits for the arrival of the RREP packet. The intermediate nodes that satisfy the requirements broadcast the packet. The destination node chooses the stable and reliable route then it sends the RREP packet through this path.

Route Request

During route establishment, the source node broadcasts the RREQ control packet containing the following attributes: Packet type identifier (RREQ), identities of source and destination node (ID_S and ID_D), maximum number of intermediate nodes (Hmax), timestamp (ts), source nodes' signature and certificate embedded with trust (Tr) and energy (Er) requirements. The link quality is estimated using cross layer metrics to ensure the reliability of the link. The reputation is checked at every node by obtaining a direct and an indirect trust values from the neighbors. These values are used to estimate a final trust value about the nodes which is used to measure the trustworthiness of the nodes. These values are used to estimate a final trust value about the nodes which is used to measure the trustworthiness of the nodes. Only the nodes that satisfy source nodes' requirements can act as relay. The packet's signature is verified by using public key taken from nodes' certificate. Thus ensuring the transmission of packets by authenticated nodes and it also verifies that the trust values are signed by TP. Before forwarding the packets, the intermediate

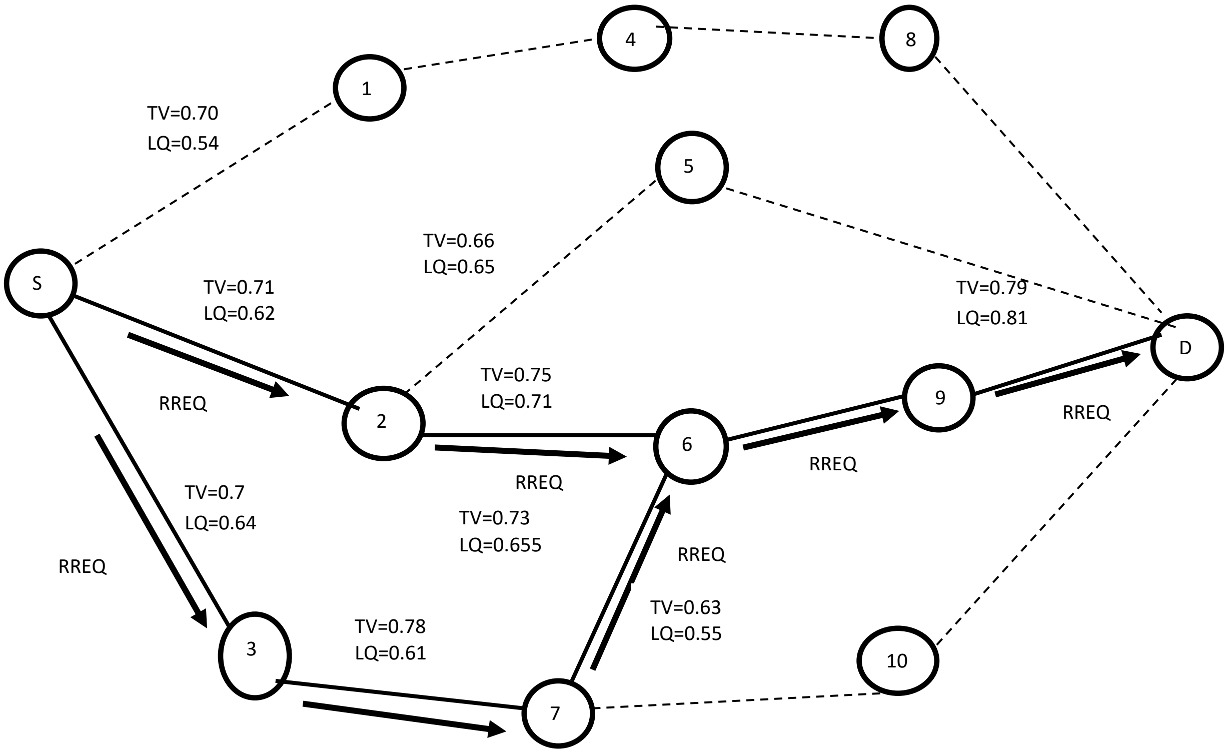

Figure.3 Route discovery process in TCSR

node signs the packet and adds its identities and certificates. Upon receiving multiple yet same request packets from nodes, only the first packet is considered, while others are discarded.

Let us consider a wireless network topology as in Fig. 3 of twelve nodes where source S wants to discover a route to destination D for data transmission. There are four different paths of varying trust and link quality measures. Only the route that satisfies the source node's requirement is chosen for data transmission. Assume that threshold for trust value and link quality is set as 0.70 and 0.6.

S – Source node
TV-Trust value of node
D –Destination node
LQ-Link quality between nodes n- Intermediate nodes (1 to 10)
RREQ-Route Request Packet

TCSR discovers the routes for data transmission only when they are needed. The source node broadcasts the RREQ packet for finding a route to destination node. To select the most reliable path, the quality of wireless links and forwarding behavior of nodes are considered. As the RREQ packet passes through each available route, the link quality and reliability of the nodes are also checked using its trust values. The destination node chooses the route through which the first RREQ packet was received. It is also considered as optimal path as trust-worthiness and link quality are checked while forwarding RREQ itself. Then the RREP packet is unicasted through the chosen route.

In Fig. 3, the available routes from source to destination are:
Route 1 : [S→1→4→8→D]
Route 2 : [S→2→5→D]
Route 3 : [S→2→6→9→D]
Route 4 : [S→3→7→6→9→D]
Route 5 : [S→3→7→10→D]
The steps to discover a secure and reliable route between source (S) and destination (D) are as follows:

Step 1: In route 1 [S→1→4→8→D], the link quality is below the threshold and hence RREQ packet is forwarded through route 2 and route 5.
Step 2: In route 2, the trust value of node 5 is less than the threshold, so the subsequent link in route 2[S→2→5→D] is not chosen for route selection. Therefore RREQ goes through route 3 [S→2→6→9→D] and route 5 [S→3→7→10→D].
Step 3: In route 5, the link quality and trust value from 7 to 10 are below the threshold. Hence route 5 [S→3→7→10→D] is eliminated in route selection.

But there exists another route 4, through which RREQ packet will pass now. As node 6 has already received this RREQ packet, it discards this request which was received from node 7. Hence, route 4 is also eliminated.

Step 4: In route 3 [S→2→6→9→D], node 9 is a trusted node and the link quality between node 6 and node 9 is Good. Hence, RREQ packet is forwarded by node 6 to node 9.

Step 5: The link quality between node 9 and destination node is appreciable. Thus the RREQ packet reaches destination node and route 3 [S→2→6→9→D] is chosen as the reliable route for communication. The detailed Route Request algorithm is as shown below:

Algorithm: Route Request

```
Input: Set of nodes, Ni (Source/Intermediate or
                              Destination)
Output: Secured, Reliable route
1.  Begin
2.  If (Source node)
        2.1  Check if link quality between the
             nodes is above threshold
        2.2  Invoke Get_Trust (Neighbor n)
        2.3  Forward RREQ= {$ID_D$, $ID_S$, Hmax,
             ts, Tr, Er, {D} Ks+, Cert} from S to
             D to start route discovery
3.  Else if (Intermediate node)
        3.1  If (not_duplicate_request)
               3.1.1 Check if Link quality between
                     the nodes is above threshold
               3.1.2 Invoke Get_Trust (n)
               3.1.3 if (trust>=threshold
               &&energy<=threshold && Hmax>
                 No. of_intermed_nodes)
                   3.1.3.1 Authenticate packet
                           signature
                   3.1.3.2 Add its signature, identity
                           and certificate
                   3.1.3.3 Forward packet
               3.1.4 Else
                   3.1.4.1 Drop RREP packet
        3.2  Else
               3.2.1 Discard request and the
                     Procedure ends
4.  Else if (Destination node)
        4.1  Choose route whose RREQ reached
             first
5.  Else
        5.1  Discard request
6.  End
```

Routine Get_Trust(x)

```
1.  Begin
2.  For (each node x and its neighbor y)
3.  If (Link Quality >Threshold)
        3.1  Compute Direct Trust, Dt= {Fx(y),
             Sx(y), Q(x,y)}
        3.2  Store Dt in the local reputation table
             of x
        3.3  If (Direct trust sufficient to make a
               decision)
        3.4  If (Dt >Threshold)
               3.4.1 Node is trustworthy
        3.5  Else
               3.5.1  Get Indirect trust (It) from
                      neighboring nodes
               3.5.2  n = Number of Indirect trusts
               3.5.3  If ((n==2) &&
                      (Recommendations conflict))
               3.5.4  Choose node with greater
                      Dt by x
        3.6  Else if (n>2)
               3.6.1  R = Set of recommenders
               3.6.2  For each i ϵ R
                   3.6.2.1  Allocate weight wi to
                            indirect trust
                   3.6.2.2 Obtain final trust=
                                         {Dt, It}
4.      End
```

Reliable Reputation based Trust computation

For trust computation, we propose variation of the trust model which is discussed in [3]. Trust values are determined by using a belief metric termed as trusts that expresses a nodes' subjective belief. Each trust is framed by the node itself or the neighbor nodes based on four considerations which decides whether the node is trust-worthy to relay packets. The four tuples are node's trust (t) on other node, node's mistrust (m) on other node, node's indecisiveness (i) about other node and node's readiness (r) to believe other node. Here, reputations on nodes are computed based on link quality. The link quality between the nodes such as x and y is computed using cross-layer based routing metrics as described in [5] and it is shown in Eq.(1).

$$Q(x,y) = \frac{1}{(1-p_f).(1-p_r)} \cdot \frac{1}{(1-max\,\{p_{df}, p_{rf}\})} \quad (1)$$

Where *(1- p_f)* and *(1- p_r)* are link qualities in forward and reverse direction respectively. It is possible to discover high performance, reliable routing paths to provide better throughput and packet delivery ratio since this metric is able to decide the quality of the links.

The reliable reputation computation is done through the computation of Direct (D_t) and Indirect trust (I_t) metrics. A direct trust is maintained by a node on every other node. If node x wants to transmit a packet to node y, the node x computes direct trust on y as shown in Eq. (2) which is stored in its local reputation table.

$$\left.\begin{aligned} {t_{xy}}^{dt} &= F_x(y)/\big(S_x(y) * Q(x,y)\big) \\ {m_{xy}}^{dt} &= N_x(y)/(S_x(y) * Q(x,y)) \\ {i_{xy}}^{dt} &= 1.0 - {t_{xy}}^{dt} - {m_{xy}}^{dt} \end{aligned}\right\} \qquad (2)$$

Where $F_x(y)$ represents the number of packets node y has successfully forwarded, $S_x(y)$ represents the total number of packets node x had transmitted to node y for forwarding, $N_x(y)$ represents the number of packets node y has not forwarded and $Q(x,y)$ represents the link quality between node x and node y. The tuples given are node's trust (t) on other node, node's mistrust (m) on other node and node's indecisiveness (i) about other node. When the direct trust is not enough to make conclusion, then it computes indirect trust by passing recommendation query to the common neighbouring nodes R. These nodes will forward their direct trust with the node y to node x. By having these values, Indirect trust is computed which is shown in Eq. (3).

$$\left.\begin{aligned} {t_{xy}}^{it} &= \textstyle\sum_{k\in R} w_k \,.\, {t_{ky}}^{dt} \\ {m_{xy}}^{it} &= \textstyle\sum_{k\in R} w_k \,.\, {m_{ky}}^{dt} \\ {i_{xy}}^{it} &= \textstyle\sum_{k\in R} w_k \,.\, {i_{ky}}^{dt} \\ {r_{xy}}^{it} &= \textstyle\sum_{k\in R} w_k \,.\, {r_{ky}}^{dt} \end{aligned}\right\} \qquad (3)$$

The four tuples are node's trust (t) on other node, node's mistrust (m) on other node, node's indecisiveness (i) about other node and node's readiness (r) to believe other node. When a node receives two contradicting trust values, then the trust values of the two neighbor nodes T and T' are compared and the node with higher trust value is taken using dominance relation. When a node receives more than two contradicting trust values, then for each recommender i∈R, a suitable weight wi is computed using node's trust on its neighbor. A Final Trust (F_t) value about the node's trustworthiness is made by bringing the direct and indirect trust values together as shown in Eq. (4).

$$\left.\begin{aligned} {t_{xy}}^{ft} &= ({t_{xy}}^{dt}.{i_{xy}}^{it} + {t_{xy}}^{it}.{i_{xy}}^{dt})/({i_{xy}}^{dt} \\ &\qquad +{i_{xy}}^{it} - {i_{xy}}^{dt}.{i_{xy}}^{it}) \\ {m_{xy}}^{ft} &= ({m_{xy}}^{dt}.{i_{xy}}^{it} + {m_{xy}}^{it}.{i_{xy}}^{dt})/ \\ &\qquad ({i_{xy}}^{dt} + -{i_{xy}}^{dt}.{i_{xy}}^{it}) \\ {i_{xy}}^{ft} &= ({i_{xy}}^{dt}.{i_{xy}}^{it})/({i_{xy}}^{dt} + {i_{xy}}^{it} \\ &\qquad -{i_{xy}}^{dt}.{i_{xy}}^{it}) \\ {r_{xy}}^{ft} &= ({r_{xy}}^{dt}.{i_{xy}}^{it} + {r_{xy}}^{it}.{i_{xy}}^{dt})/ \\ &\qquad ({i_{xy}}^{dt} + {i_{xy}}^{it} - {i_{xy}}^{dt}.{i_{xy}}^{it}) \end{aligned}\right\} \qquad (4)$$

Since all the trust parameters will change over time, the trust relationship between any two nodes will also change dynamically. Whenever a new observation comes in, each node updates its trust table and the final trust is calculated by using a moving average model as shown in Eq. (5).

$$F_{t1} = \alpha\, F_{t0} + (1-\alpha) F_{t1} \qquad (5)$$

Where α (0<α<1) is the weighting factor which is used as normalizing factor between previous measurement and current measurement. The route discovery process uses this trust metric for selecting the secure reliable routing path from source to destination.

Route Selection

The destination node selects the route through which the first RREQ packet is arrived by satisfying the source nodes' requirements. It unicasts the Route Reply (RREP) packet through this chosen route. Another route request is initiated with flexible requirements, if timestamp (ts) exceeds the threshold.

Route Reply

The RREP packet is composed of packet type identifier (RREP), identities of the nodes in the selected route (R), certificate signed by the destination node, authentication code (Auth_code). The signature of the destination node authenticates the hash chain and its linkage to the session. It also verifies that the node had participated in the packet forwarding. Verification of Auth_code allows checking for receipt integrity and once the destination node is reached, data transmission begins. The algorithm for route reply is as shown below:

Algorithm: Route Reply

```
1.   Begin
2.   If (Destination node)
         2.1  Generate one way hash chain and
```

```
            signing
        2.2 Links signature to the session
        2.3 Unicasts RREP={$(ID_S,ID_x,ID_y,ID_D)$,
            h0,Auth_Code,Cert} from D to S.
3.  Else if   (Intermediate node)
        3.1   Verify Auth_Code
        3.2   Add certificate
        3.3   Store requirements for receipt
              composition
        3.4   Relay packet
4.  Else if   (Source node)
        4.1   Deliver the data packet
5.  Else
        5.1   Discard Request
6.  End
```

Thus the route establishment phase finds the shortest and reliable route from the source to the destination node.

Data transmission

Data Transmission module deals with the transmitting the data packets from the source to the destination through the selected secure, reliable route. To ensure security, the message is hashed and the source node authenticates the data packet by signing it with its private key. The source node S computes the signature as $\xi s\ (i) = \{H\ (H\ (mi), ts, R, i\}\ Ks+$

Where,

$\xi s(i)$ is the signature of the ith data packet
R is the concatenation of the identities of all the nodes in the route
H (mi) is the message mi hashed
K_S+ represents the signature with the private key of S
ts denotes the timestamp of the request

S sends the packet <R, ts, i, mi, ξs(i)> to the first node in the route (R). The source node's signature helps to ensure the authenticity and integrity of the message. The nodes in the route verify and store the signature and hash of the message that formulates the receipt. The receipt consists of R, ts, i, H(mi), h0, hi, Cm and cryptographic token which contains the hash value of the source nodes' signature and Auth_code. Since the hash of the message is embedded in the receipt instead of the message itself, the size of the receipt is reduced. This proof is submitted by the intermediate nodes when connection to the Trusted Party (TP) is established. TP processes these receipts so that these relay nodes can claim their payment. The destination node generates a one-way hash chain iteratively by hashing a random value hs S times to obtain the root of the chain, h0. When the packet reaches the destination node, acknowledgment is sent to the source node by the destination node.

Updating Credit Accounts

When the TP receives the receipt, a unique identifier (R,ts) is used to find out if the receipt has already been processed. The credibility of the receipt is verified by computing node's signature and hash value. The validity of the receipt is checked by comparing the hash value and cryptographic token of the receipt. After verification of the destination node's hash chain, the TP clears the receipt by charging source and destination node while debiting the intermediate nodes' credit accounts.

4. Implementation and analysis

The proposed model is simulated using Network Simulator (NS) with its version 2.35. Table 1 represents the parameters used in the simulated environment. The proposed model is carried out with the simulation time of about 150s. The proposed routing protocol is tested by varying the number of malicious nodes at various levels. Taking the above characteristics into consideration, the performance evaluation of the routing protocol is analyzed. We analyze the performance of the proposed protocol under malicious environment by comparing with the existing routing protocol E-STAR [1] which was designed as a stable reliable routing protocol for heterogeneous multi hop wireless networks.

Table 1. Simulation Parameters

Parameters	Values
Simulation time	150s
Routing protocol	TCSR, E-STAR
Wireless nodes	25
Length of queue	50
MAC protocol	802.11
Packet size	512 bytes
Packet rate	2 packets/sec
Simulated Area	500m X 500m
Antenna	Omni Directional

The following performance metrics are considered for analysis.

- Throughput
- Packet Delivery Ratio
- Route Acquisition Delay
- End-to-end delay

Fig. 4 shows the Packet Delivery Ratio (PDR) analysis with respect to the number of malicious nodes present. This is the ratio of total number of packets successfully received by the destination nodes to the number of packets sent by the source nodes throughout the simulation. In addition to cryptographic mechanisms, TCSR implements cross layer based reliable reputation mechanism to isolate the malicious nodes and also enforces cooperation among the nodes by integrating payment system in the proposed scheme. Hence, by discovering secure, stable and reliable route, TCSR protocol provides better performance in PDR compared to E-STAR, since the packets are forwarded only by the trusted intermediate nodes with better link quality.

Fig. 5 shows the throughput analysis of both the protocols under malicious environment. Compared to E-STAR, our proposed protocol shows better throughput performance by selecting the secured reliable trustworthy path. Reliable path can be ensured in the proposed protocol by incorporating cross layer based routing metrics for link quality computation during reputation computation done at each node. TCSR selects the trustworthy path at the destination node by considering the forwarding reliability of the intermediate nodes at network layer also.

Route Acquisition Delay (RAD) time analysis of the proposed protocol with E-STAR by varying the number of malicious nodes is shown in Fig. 6. It is the time interval between forwarding Route Request (RREQ) message from source to a destination and getting the Route Reply (RREP) at the source node. Both the protocols take more or less the same time for selecting the routing path, since they select the trust worthy path with more computations made at each node. However, the proposed protocol TCSR gives slight increase in RAD time for variation of malicious nodes compared to E-STAR. It is acceptable because secured, stable and reliable route is chosen with minimum packet loss by well isolating malicious nodes.

Fig. 7 shows the end-to-end delay comparison analysis with respect to the number of malicious nodes. It is the time taken for a packet to reach a destination from a source. When an intruder attacks the network, it tries to manipulate the data packet to ensure that the integrity is either lost or the packet is not transmitted. This leads to increase in delay when packets reach at the destination. The delay increases for both the routing protocols as the number of malicious nodes increases. Delay values for both the protocols are more with increase in malicious activity. However, the proposed routing protocol takes more delay time compared to E-STAR for increase in the malicious nodes. This clearly shows that to get high performance secured, reliable route in the network, increase in delay is tolerable for efficient packet transmission.

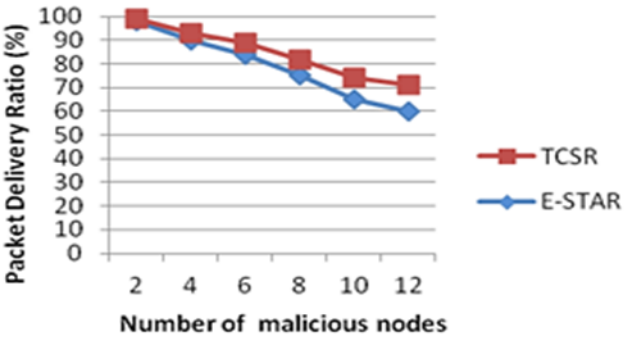

Figure. 4 No. of malicious nodes vs. PDR

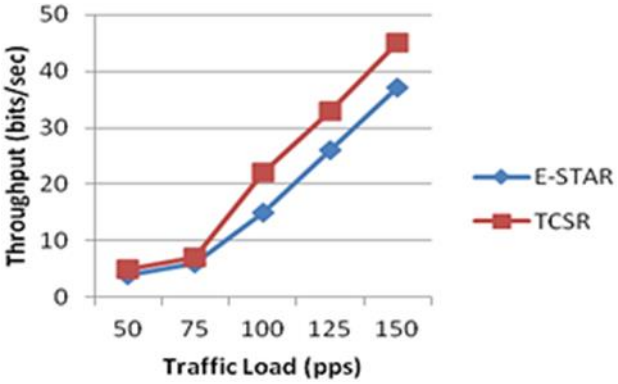

Figure.5 Throughput Analysis: 20% malicious Nodes

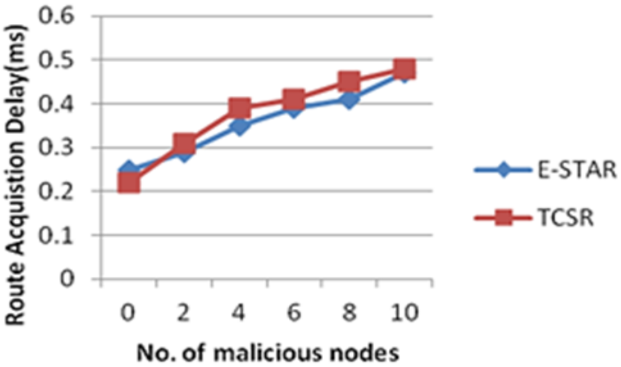

Figure.6 No. of malicious nodes vs. Route Acquisition Delay

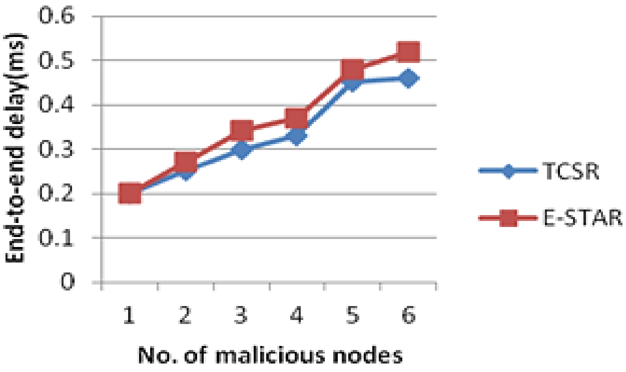

Figure.7 Number of malicious nodes vs. End to End delay

5. Conclusion

In this paper, the design and implementation of Trust-Centric Stable Routing (TCSR) for thwarting packet dropping attacks in Wireless Mesh networks is discussed. The proposed routing scheme has been able to enforce cooperation among the peer nodes in WMN to participate in forwarding of packets based on the integration of payment systems. TCSR successfully identifies and isolates malicious nodes in the network by introducing reliable reputation based trust computation mechanism and also considers better link quality with forwarding reliability at the network layer. The simulation results after the implementation of the proposed algorithm prove that TCSR shows better performance in terms of Packet Delivery Ratio and Throughput parameters and takes slight increase in delay time in terms of Route Acquisition Delay and End-to-end delay compared to E-STAR. TCSR selects high performance reliable routing path for packet transmission with more computations made at each node. Hence, the proposed protocol TCSR is trust centric, reliable and also provides better security against packet dropping attacks. In future work, it is planned to design mechanisms for minimizing the delay time taken by the proposed protocol and also planning to enhance the reputation mechanism by considering trust parameters at different levels and to address various types of Denial of Service (DoS) attacks.

References

[1] M.M. Mahmoud, X. Lin, and X.S. Shen, “Secure and reliable routing protocols for heterogeneous multihop wireless networks”, *IEEE transactions on parallel and distributed systems*, Vol.26, No.4, pp.1140-53, 2015.

[2] M.E. Mahmoud and X. Shen, “An integrated stimulation and punishment mechanism for thwarting packet dropping attack in multihop wireless networks”, *IEEE Transactions on Vehicular Technology*, Vol. 60, No. 8, pp.3947-3962, 2011.

[3] M. Yu and K.K. Leung, “A Trustworthiness-based QoS routing protocol for wireless ad hoc networks”, *IEEE Transactions on Wireless Communications*, Vol. 4, No.8, pp.1888-1898, 2009.

[4] H. Lin, J. Hu, J. Ma, L. Xu, and A. Nagar, “A role based privacy-aware secure routing protocol for wireless mesh networks”, *Wireless Personal Communications*, Vol. 75, No.3, pp.1611-1633, 2014.

[5] S. Paris, C. Nita-Rotaru, F. Martignon, and A. Capone, “Cross-layer metrics for reliable routing in wireless mesh networks”, *IEEE/ACM Transactions on Networking*, Vol. 21, No.3, pp.1003-1016, 2013.

[6] S. Zhong, J. Chen, and Y.R. Yang, “Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks”, In: *Proc. of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications, IEEE Societies*, Vol. 3, pp. 1987-1997, 2003.

[7] Y. Li, “A reputation system for wireless mesh network using multi-path routing protocol”, In: *Proc. of the Performance Computing and Communications Conference, IEEE 30th International*, pp.1-6, 2011.

[8] F. Wang, F. Wang, B. Huang, and L.T. Yang, “COSR: a reputation-based secure route protocol in MANET”, *EURASIP Journal on Wireless Communications and Networking*, p.7, 2010.

[9] S. Khan, N.A. Alrajeh, and K.K. Loo, “Secure route selection in wireless mesh networks”, *Computer Networks*, Vol. 56, No.2, pp.491-503, 2012.

[10] Z. You and Y. Wang, “An efficient and secure routing protocol for a hybrid wireless mesh network”, *Journal of Computational Information Systems*, Vol. 8, No. 21, pp.8693-8705, 2012.

[11] Y. Yu, Y. Peng, Y. Yu, and T. Rao, “A new dynamic hierarchical reputation evaluation scheme for hybrid wireless mesh networks”, *Computers & Electrical Engineering*, Vol. 40, No.2, pp.663-672, 2014.

[12] T.M. Navamani and P. Yogesh, “Privacy Preserved and Secure Reliable Routing Protocol for Wireless Mesh Networks”, *The Scientific World Journal*, Vol. 2015, pp.1-12, 2015.

[13] L.H.G. Ferraz, P.B. Velloso, and O.C.M. Duarte, “An accurate and precise malicious node exclusion mechanism for ad hoc

networks", *Ad hoc networks*, No. 19, pp.142-155, 2014.

[14] B. Wang, X. Chen, and W. Chang, "A light-weight trust-based QoS routing algorithm for ad hoc networks", *Pervasive and Mobile Computing*, *13*, pp.164-180, 2014.