Trust based Secure Reliable Route Discovery in Wireless Mesh Networks

Navmani T M[1*] and Yogesh P[2]
[1] School of Computer Science and Engineering
VIT Vellore, Tamilnadu, Inida
[E-mail: navamani.tm@vit.ac.in]
[2] Department of Information Science and Technology
Anna University, Chennai, Tamilnadu, India
[E-mail: yogesh@annauniv.edu]
*Corresponding author: Navamani T M

Received November 1, 2018; revised January 9, 2019; accepted February 10, 2019; published July 31, 2019

Abstract

Secured and reliable routing is a crucial factor for improving the performance of Wireless Mesh Networks (WMN) since these networks are susceptible to many types of attacks. The existing assumption about the internal nodes in wireless mesh networks is that they cooperate well during the forwarding of packets all the time. However, it is not always true due to the presence of malicious and mistrustful nodes. Hence, it is essential to establish a secure, reliable and stable route between a source node and a destination node in WMN. In this paper, a trust based secure routing algorithm is proposed for enhancing security and reliability of WMN, which contains cross layer and subject logic based reliable reputation scheme with security tag model for providing effective secured routing. This model uses only the trusted nodes with the forwarding reliability of data transmission and it isolates the malicious nodes from the providing path. Moreover, every node in this model is assigned with a security tag that is used for efficient authentication. Thus, by combining authentication, trust and subject logic, the proposed approach is capable of choosing the trusted nodes effectively to participate in forwarding the packets of trustful peer nodes successfully. The simulation results obtained from this work show that the proposed routing protocol provides optimal network performance in terms of security and packet delivery ratio.

Keywords: Wireless Mesh Networks, Trust Model, Reputation, Tag, Link Quality, Security

1. Introduction

Wireless Mesh Networks (WMN) is an emerging wireless technology, which supports a wide range of applications including broadband home networking, community and neighborhood networking, transportation systems, surveillance and security systems, etc. It comprises of Mesh Routers (MR) and Mesh Clients (MC). The backbone of WMN is formed by mesh routers, which are almost static in nature. Mesh clients are mobile wireless devices communicating among themselves over multi-hop paths. WMNs can be categorized into three types. The first type of WMN is a pure form of a mobile ad hoc network in which all the MCs directly communicate with each other without the involvement of Access Points (AP) and gateway. The second type is infrastructure WMN in which the clients access the network or communicate with each other through Mesh Access Points (MAP) or Mesh Routers. The proposed approach is based on infrastructure based WMNs. The third type is Hybrid WMN which is the combination of infrastructure and client meshing. WMNs are typically implemented by using IEEE 802.11 hardware platform. In a WMN, the mesh clients can access the network through mesh routers or directly via other mesh clients. Some mesh routers act as gateway nodes to connect with other external networks and to provide Internet connectivity for other mesh routers [1].

To support end to end communication in WMN, effective routing protocols are required. Routing in WMNs is always a challenging problem since the design of routing protocols should consider the unique characteristics of WMN like power efficiency, mobility, etc., which are much different from other wireless networks. In general, the nodes in the mesh backbone are static and have better power efficiency, whereas the mesh clients are mobile and have power constraints. Moreover, ad hoc networks are infrastructure less, whereas wireless mesh networks are infrastructure based networks. There are several routing protocols designed for ad hoc networks such as Ad hoc On Demand Distance Vector Routing (AODV), Dynamic Source Routing (DSR), Optimized Link State Routing (OLSR), etc.. However, they cannot be used as such in wireless mesh networks since they cannot support the dynamic and static nature of WMN nodes as well as the lack of security, more packet drops, etc. [1] [2]. Several routing protocols designed for capturing the link quality to discover high performance routing paths in wireless mesh networks have been discussed in the literature [3]. Single radio, multi radio and hierarchical routing protocols are reviewed and various link quality based routing metrics are discussed in [4]. However, these routing protocols are designed by having strong assumption that all nodes behave honestly during the forwarding of packets and the network is more reliable. This assumption may not be true always for infrastructure based WMNs, where all the nodes do not cooperate all the times and link reliability is also not guaranteed. Unlike the complex infrastructure of cellular networks like base station and mobile switching center, the WMN infrastructure like mesh router could be relatively easily reached and modified by attackers. Usually they can track the packets in the network and can fetch the information from the packets. This is a kind of external attack in WMNs. Internal attacks in WMNs are caused by the compromised internal nodes, which are participating in the network as legal entities during route discovery and packet transmission phases. Traditional cryptographic schemes and existing authentication schemes are able to detect and prevent the external attacks easily and effectively. However they are unable to deal with the internal attacks and isolate the compromised nodes since they do not anticipate the presence of the internal nodes which are compromised. Internal adversary nodes are dangerous nodes compared to external adversaries,

since the internal nodes possess critical information like keys used in the cryptographic mechanisms and they may reveal such critical security related information to the hackers and intruders. This in turn causes more performance degradation [5]. Hence, apart from cryptographic schemes, it is necessary to devise schemes that can evaluate the reputation or the trust level of the internal nodes of the network to address insider attacks.

By reviewing the existing works, it is known that, there are several security challenges in WMNs and the design of secure, efficient and reliable routing protocols in WMNs is always on demand. Moreover, there is no optimal routing solution that is capable of doing all the three following operations in WMNs: Incorporating Trust model, providing security against adversaries and discovering high performance reliable routing path. Hence, in order to establish secure and reliable routing path with better authentication, the existing routing protocols have to be enhanced further in terms of security and reliability to defend against various Denial of Service (DoS) attacks. Several reputation or trust evaluation methods of internal nodes are found in the literature. However link reliability is an issue to be considered in WMNs since the mesh clients are permitted to move around irrespective of the fact that the backbone network made up of mesh routers is a static one. The mobility of mesh clients results in frequent link failures. Hence, these issues are considered during route discovery in WMNs.

Thus, it is analyzed that, security and reliability issues are the vital problems in the design of WMNs. The clients should have end to end security and reliability assurance. Several secure, reliable routing schemes proposed for WMNs have been discussed in the literature. However, the existing schemes have not addressed the discovering complete, trusted path and also not ensuring the better link reliability to select high performance routing path in infrastructure based WMNs. In [5], the authors have proposed Role based Privacy-Aware Secure Routing Protocol (RPASRP) for wireless mesh networks. A dynamic reputation evaluation scheme with role based multilevel security and hierarchical key management are introduced to determine secure, efficient routing paths for WMN. Also the authors have proved by simulation results that the protocol has provided better security to defend against various internal attacks. In [6], the authors have proposed Privacy-Aware Secure Hybrid Wireless Mesh Protocol (PA-SHWMP) which also combines the same reputation evaluation scheme along with multi level security for privacy information classification and provides better privacy and security against the internal attacks caused by the compromised nodes in WMN. These protocols use a few metrics to deal with the link quality of the network. However, it has been observed that these link quality metrics are not able to ensure the forwarding reliability of the network nodes all the time. Hence, to consider this issue in this research work, a suitable routing metric called Minimum Expected Forwarding Counter (MEFW) [7] has been applied to improve the forwarding reliability of the nodes and thereby to improve the performance of the WMN. A stable and reliable routing protocol named E-STAR for heterogeneous multi hop wireless networks was discussed in [8]. E-STAR combines payment and trust systems with a trust-based and energy-aware routing protocol. Multidimensional trust values are used for computation of trust and reliability in routing. Payment systems are used for rewarding the nodes which are forwarding the packets. However, the protocol incurs more overhead in terms of processing payment receipts and trust metrics evaluation. Yau Yu et al. have designed a secure routing technique for WMNs to protect against social selfish node attacks. Initially, a dynamic reputation evaluation model is incorporated to analyze node reputation and cooperation among the intermediate nodes. The selfish nodes are detected effectively and social relationships among the nodes are well studied. However, this technique fails to handle misleading trust information provided by malicious nodes [9]. Lin et al. have proposed a trustworthy energy aware secure routing protocol for software defined hybrid

wireless mesh networks to defend against security attacks. Trustworthy nodes within the routing path are selected by incorporating subjective logic based dynamic reputation mechanism. Though the protocol provides security protection against blackhole, grayhole and wormhole attacks, it fails to assess the quality of wireless links to ensure reliable forwarding of packet transmission [10]. In all these reputation evaluation mechanisms, the reputation computation incorporates traditional weighted average model to compute the link quality metric which in turn evaluates the direct behavior of the nodes. However, in general, wireless environment needs cross layer based routing metrics to guarantee the accurate measurement of link quality. Hence, in the proposed work, cross layer design in reputation evaluation mechanism is employed to enhance the link reliability and security of WMNs.

In this article, a Trust based Secured Reliable Routing (TSRR) protocol for infrastructure based Wireless Mesh Networks is proposed to provide a complete reliable routing path and to have maximum security against adversaries. Reliable routing paths in WMNs are discovered by considering trusted nodes and forwarding reliability of network nodes during route discovery. Moreover, the proposed protocol protects the network against packet dropping and misdirecting attacks. For this purpose, a new Cross Layer and Subject Logic based Dynamic Reputation (CLSL-DR) mechanism is introduced in this work at the mesh routers and a novel security tag model is developed in the proposed system. It also provides an optimal path for data transmission by selecting only secured and reliable path during route discovery. Each mesh node (MR/MC) has to register with the Certificate Authority (CA) and then the nodes will receive the tokens from CA after successful verification. This is done as an offline process. Whenever the nodes (MC/MR) want to enter into the network, they have to submit the tokens to the CA for authentication purpose. In response, the nodes will get security tags from the CA after successful verification of tokens. Once the nodes have the security tags, they can communicate during route discovery and data packet communication. During route discovery, along with a RREQ packet identifier, Trust Value (TV) metric, maximum number of hops (maxh), timestamp (ts) and sequence number (snum) are attached in the RREQ packet for forwarding towards the destination.

The major contributions of this paper include 1) Designing a novel secured tag based authentication system 2) Protection against packet dropping and misdirecting attacks by introducing a new Cross Layer and Subject Logic based Dynamic Reputation mechanism (CLSL-DR) 3) Minimizing the control packets overhead by means of Trust Level (TL) metric and 4) Design of a new Trust based Secured Reliable Routing protocol for WMNs for efficient data transmission by selecting a secured reliable path using cross layer information exchange. The experimental results of the proposed approach show that the improved level of authentication over the mesh nodes and also improves the performance of the network substantially even in the presence of malicious users. The rest of the paper is organized as follows: Section 2 discusses the related works of the proposed approach. Section 3 has presented the proposed work in detail. Section 4 describes in detail about security and cost analysis. Section 5 provides the simulation results and analysis of the proposed work. Section 6 gives conclusion and future enhancements.

2. Related Work

Many works have been done by various researchers in the past in this direction. Among them, the routing enhancement in protocols designed for WMN is an active area of research, but unfortunately less attention is given to security aspects of routing protocols. To address security concerns, several secure routing protocols [11] and trust based routing protocols have

been proposed. Secure Ad hoc On demand Distance Vector (SAODV) routing protocol which is a secure variant of Ad hoc On demand Distance Vector (AODV) protocol is designed for ad hoc networks [12]. SAODV uses hash chain and digital signature to secure the mutable field (hop count) and non-mutable field (the rest of the routing message except hop count field) and successfully defends against impersonation attacks, modification of hop count and sequence number attacks. However, it does not provide hop-by-hop authentication and the proposed scheme achieves this. Security-aware Ad hoc Routing (SAR) [13] is another secure routing protocol which was designed based on AODV or DSR protocol. Here, security attributes are used to select a secured route between source and destination nodes. If more than one route fulfills the required security attributes, then the shortest routing path is selected for communication. The protocol just ensures that the nodes participating in the route discovery should have the same trust level required by the source node. Thus, the protocol defends against fabrication, interception and interruption attacks. However, the protocol fails to handle DoS and replay attacks successfully and our work focuses on DoS attacks. Khan et al. have proposed a Cross layer Secure and Resource aware On demand Routing protocol (CSROR) for Hybrid WMN to ensure routing security and fulfill different applications' specific requirements for multimedia delivery and real-time transmissions. An optimal route can be selected on the basis of routing security by considering different cross layer parameters. It is resilient to different packet dropping attacks, but the protocol is not suitable for the network with nodes having high mobility and it is also not providing a solution for packet modification attacks [14]. Paris et al. have proposed a novel cross-layer based routing metric, named Expected Forwarding Counter (EFW) to defend against packet dropping attacks. Two more variations 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. Among these metrics, MEFW is proved as a robust link quality metric to select a secure, reliable routing path in WMN [7]. In the proposed work, this metric is used as a link quality metric to choose reliable routing path as well as to check whether the packet drops are intentional or due to poor link quality. Azhari et al. have proposed a routing metric to improve the lifetime of battery operated wireless mesh networks. They have integrated a bandwidth estimation algorithm along with the routing process to detect and isolate the victim nodes which are not satisfying the requirements and adjust the data traffic accordingly. However, the internal adversaries cannot be detected which have the objective of intentional packet dropping. This issue is addressed in the proposed work [15]. Nanda et al. have designed a secure geo-location oriented routing protocol for wireless mesh networks by applying hybrid encryption and hybrid authentication approaches. By incorporating both symmetric and asymmetric encryption techniques, the authors have proven that there exists good network performance, minimal computation load and also quicker encryption and decryption cycles. Although the protocol applies hybrid encryption model and hybrid authentication approaches, it does not employ any key management strategy and hence cannot address internal threats and attacks successfully [16]. Mahmoud et al. have proposed a low-overhead secure privacy preserved routing protocol in hybrid ad hoc networks in which symmetric-key-cryptography operations and payment system are used to develop secure privacy preserved route discovery and data transmission. However, this protocol cannot be applied for WMNs where there is no centralized server to process the payment receipts [17].

Khan et al. have proposed a secure routing protocol based on Ad hoc On demand Distance Vector (AODV) exclusively for Infrastructure based WMNs. Each node in the network maintains two hop information in the routing table to ensure security. The authors introduced a new routing metric called 'Unreliability value' to determine the shortest secure routing path.

This protocol provides secure packet data transmission in infrastructure based networks, but it is not applicable for hybrid WMNs where more number of mobile nodes exist at the lower end. Moreover, the protocol is more vulnerable to attacks caused by internal adversaries [18]. This research work deals with the internal adversaries effectively apart from the external attackers. Li et al. have proposed Security Enhanced AODV protocol for WMN. In this work, to ensure security, BLOM's key pre distribution scheme is used to generate pairwise transient keys and group transient keys, and defends against route control packet manipulation attacks, tunneling attacks and other attacks. Although the protocol defends against all kinds of routing attacks, it does not address DoS attacks and our scheme has dealt DoS attacks effectively [19]. In [20], the authors have surveyed the threats and vulnerabilities faced by WMNs and also identified a number of security goals.

Siddiqui et al. have proposed a secure multipath hybrid routing protocol for wireless mesh networks. The authors have identified the operations to be secured in WMN such as corrupted access points, routing and fairness and also proposed some solutions. However, this multipath approach is more appropriate for mobile ad hoc networks and wireless sensor networks where the nodes have multiple paths and this is not required for WMNs due to the presence of the backbone network [21]. Bansal et al. have introduced a secure routing protocol for hybrid wireless mesh network, which uses cryptographic extensions to provide authenticity and integrity. This protocol provides more routing acquisition delay and control packet overhead because of cryptographic extensions during route discovery. And also, it is more vulnerable to attacks caused by colluding compromised nodes within the network [22]. You et al. have proposed an efficient, secure routing protocol for hybrid wireless mesh network. The protocol is designed based on Cross-layer Secure and Resource-aware On-demand Routing (CSROR) protocol. The protocol implements cross layer based routing metrics as in CSROR and selects an optimal route based on security and robustness against various multi hop threats in WMNs. It incorporates symmetric, asymmetric cryptographic operations to enforce security strength and MAC mechanisms for authentication, which in turn causes additional routing overhead during route discovery and packet transmission phases. Even though it implements hybrid security mechanisms, it fails to provide effective solutions for DoS attacks like selective forwarding attacks, hello flooding attacks, etc.[23].

Konwar et al. have proposed a trust model for WMNs based on multiple criteria decision making. The model is capable of categorizing the nodes as a trustworthy node and an untrustworthy node which is essential for discovering secured routing path in WMNs. In this model, trust values are determined based on entropy theory [24], whereas our proposed trust model is based on subjective logic. Matam et al. have proposed a trust based secure routing protocol for Wireless Mesh Networks to detect and exclude the malicious nodes during route discovery. Here, the protocol uses an approach to let the nodes to determine the trust of their peer nodes based on packet loss as a trust metric. Hence, the criterion for routing path selection is based on the trustworthiness of nodes. However, the protocol fails to provide an effective authentication mechanism to ensure security [25]. Hwang et al. have proposed an efficient, secure routing protocol for WMNs by considering both symmetric and asymmetric links. Also the authors have proposed a neighbor discovery scheme which provides the benefit of increased communication range. The protocol ensures that reliable and trustworthy nodes are participating during the path selection process. However, the protocol fails to utilize effective link quality based routing metrics to ensure reliable links and forwarding reliability of network nodes [26]. In our proposed work, this issue has been considered to provide a better link reliability. Yu et al. have introduced a new secure routing protocol with the quality of service support, called Trustworthiness-based Quality of Service (TQOS) routing, which discovers

secured route by implementing trustworthiness-based QoS routing metrics. Trustworthiness can be established by means of verification done at each node. By using message redundancy and route redundancy, most of the internal attacks are detected. However, the procedures for the implementation of the security mechanisms applied in TQOS are not described in detail [27]. Popalyar et al. have proposed a trust model to discover secure routing path in WMNs based on evidence based subjective logic. Selfish behavior of the intermediate nodes is detected by incorporating watchdog monitoring mechanism at the nodes. During route discovery, untrustworthy nodes are excluded and only trustful nodes are present in the discovered routing path. The comparison of various existing reputation models is also discussed [28]. Tan et al. [29] have proposed a non-biased trust model for WMNs which combines two techniques such as dissimilarity test and Dempster Shafer Theory [30] to compute the trust values of the nodes effectively. Compared to existing trust models, this model handles fabricated trust information efficiently and also protects against badmouthing and ballot-stuffing attacks. Our proposed trust model is also designed based on Shafer theory to compute the trust values.

From the literature review, it is observed that there are various secure routing protocols designed specifically for WMNs based on cryptographic techniques. However, they cannot effectively identify the trusted nodes to participate in the route discovery and packet transmission phases. Reputation mechanisms play a vital role in identifying the trusted nodes as well as detecting and isolating malicious nodes from the routing path. Hence, by integrating efficient reputation mechanisms along with the cryptographic mechanisms, routing protocols become more secure and robust against various types of internal attacks. An important observation which has been made from the survey is that not much work has been done in achieving an integrated route discovery scheme that satisfies both security and reliability requirements and thereby isolates malicious nodes in a better way in the process of routing packets from source to destination. Hence, a Trust based Reliable Route Discovery method is proposed for Infrastructure based WMNs that tries to overcome the limitations of the above mentioned research works.

3. Trust Based Secure Reliable Route Discovery

In this section, Trust based Secure Reliable Route (TSRR) Discovery scheme and their functions for Infrastructure based wireless mesh networks are discussed. The proposed scheme introduces a novel tag based authentication to ensure security and a new Cross Layer and Subject Logic based Dynamic Reputation mechanism (CLSL-DR) mechanism to defend against the internal attacks caused by compromised nodes of WMN.

3.1 System Model

This subsection provides the architectural model and assumptions of WMN and the notations used for describing the security primitives.

3.1.1 Network Model and Assumptions

The WMN architecture is considered at metropolitan-scale and it comprises of three entities: a trusted Certificate Authority (CA), Mesh Routers (MRs) and Mesh Clients (MCs). **Fig. 1** depicts the basic architecture of WMN that includes certificate authority, mesh routers, mesh clients and connectivity with the internet. Each MC is connected with one of the nearest edge mesh routers (MR) available in the mesh backbone. Initially, each new node has to register

with the CA by sending its personal details and in turn, it gets information about key generation mechanisms from CA. These nodes will generate their public and secret keys accordingly and forward their public key ($PK_{M/C}$) to CA. After getting this information, CA will generate a new token ($TOK_{MR/MC}$) with all the required information, sign it and forward it to new MR/MC. This entire process is an offline process, which happens before joining the network. CA will grant network access to network users who are holding valid tokens.

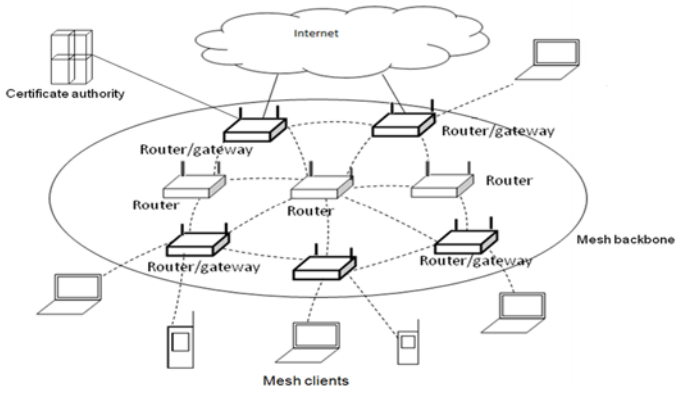

Fig. 1. Wireless Mesh Network Architecture

3.1.2 Notations

The notations which are used for describing security primitives are summarized in **Table 1**.

3.2 The Proposed Scheme TSRR

The proposed scheme consists of three phases, namely Security Tag model, Trust model based on CLSL-DR mechanism and Route Discovery. The functional components of the proposed scheme are shown in **Fig. 2**. Initially, each node has to register with the CA by forwarding the required details. After successful verification, nodes (MR and MC) will receive the tokens ($TOK_{MR/MC}$). By submitting the tokens, mesh routers and mesh clients will receive security tags ($TAG_{MR/MC}$) and the shared secret keys (K_{CAMR}/K_{CAMC}) are exchanged between the Certificate Authority (CA) and the corresponding nodes. According to the proposed scheme, the discovered routing path is secured, reliable and efficient. During route discovery, CLSL-DR mechanism is invoked on the mesh routers to compute cross layer based reputation to isolate the malicious nodes in the routing path. In the route discovery process, the source node forwards a Route Request (RREQ) packet based on the Trust Level (TL) metric to minimize the control packet overhead and the request reaches the destination through the intermediate nodes. This metric is appended in the RREQ packet, and cumulatively added at each node until it reaches the destination. Since the source node broadcasts the route request, the destination receives several route request packets until the time period T through different paths. It selects the most trusted path as the optimal path for efficient data transmission. Then the destination performs a unicast route reply to the source through the discovered route. Finally the packets are transmitted from a source and reach the destination through this path. Following subsections describe the functions of each module in detail.

Table 1. Notations

Notation	Meaning
MC	Mesh Client
MR	Mesh Router
CA	Certificate Authority
K_{CAMR}	Shared Secret key between CA and MR
K_{CAMC}	Shared Secret key between CA and MC
K_{CA}	Private key of CA
TAG_{MR}	MR's Tag
TAG_{MC}	MC's Tag
$TOK_{MR/MC}$	Token of MR/MC
$PK_{M/C}$	Public Key of MR/Client
$( )K_{MC}$	Message digitally signed by MC's Private Key
$[ ]K_{MCMC}$	Encrypted data with shared key between two MCs

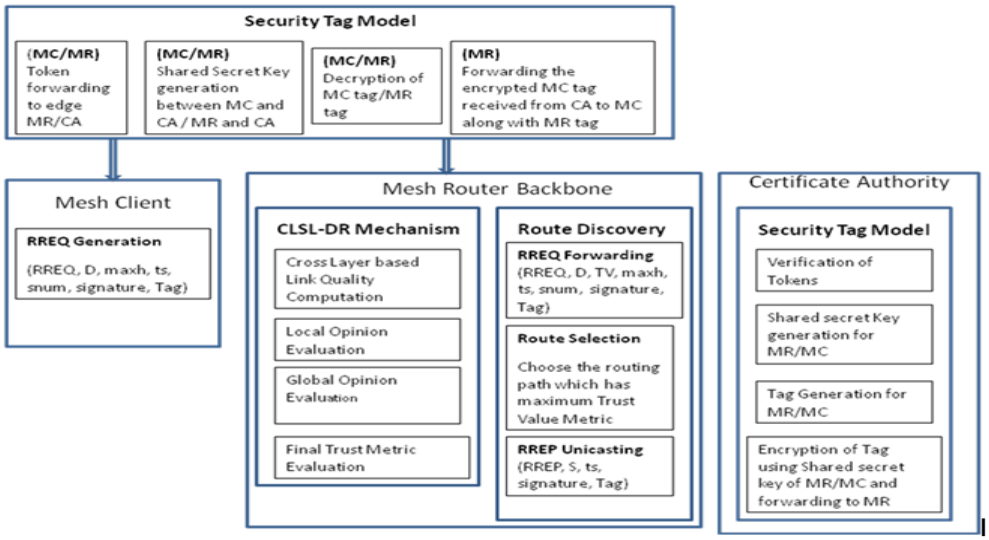

Fig. 2. Functional Components of the Proposed Scheme

3.2.1 Security Tag Model

The proposed approach uses two types of security tags such as Mesh Router Tag (TAG_{MR}) and Mesh Client Tag (TAG_{MC}) issued by a Certificate Authority to the enrolled entities for providing authentication during communication. This subsection focusses on the issuance of MR-Tag and MC-Tag. Initially, each node (MR/MC) receives a unique token from the CA, by submitting its public key. The token format is shown below.

$$CA \rightarrow MR: TOK_{MR/MC} = (T_{num}, PK_{CA}, PK_{MR/MC}, T_{Is}, T_{Ex})K_{CA}$$

The token of either MR or MC ($TOK_{MR/MC}$) contains the unique token number, Public key of the CA, Public key of MR/MC, Issue time (T_{Is}) and Expiration time (T_{Ex}). The token is digitally signed by CA and will be issued to MR/MC. This is an offline process which is to be completed before joining into the network. Here, elliptic curve cryptographic algorithms have been implemented for key exchange, signature, encryption and decryption.

3.2.1.1 Issuance of MR Tag and Key Exchange

Whenever a new MR wants to join existing WMN, it needs to submit its token to CA and then the CA will issue a new tag to it after successful verification of its token as shown in **Fig. 2**. The steps followed during joining process are as follows:

1. New MR → CA: TOK_{MR}
2. CA → New MR: $[TAG_{MR}]\ K_{CAMR}$

In step 1, new MR submits its token to CA. Once the CA verifies the token, it generates shared secret key for new MR on the basis of public key of MR and its secret key by using Elliptic Curve Diffie Hellman Key Exchange (ECDH) protocol. CA will generate a new tag for new MR as in the following format:

$$TAG_{MR} = (ID_{MR}, IP_{MR}, PK_{MR}, T_{Is}, T_{Ex})K_{CA}$$

The Tag for MR contains the unique ID of the MR, IP address of MR, the public key of MR, Issue time and Expiration time which is signed by the CA with its private key. After signing, CA encrypts the tag with the shared secret key and then forwards this encrypted tag to the new MR as shown in step 2. Now, MR generates a shared secret key on the basis of the CA's public key and its secret key (as CA generated). Then it decrypts the tag using the generated key.

3.2.1.2 Issuance of MC Tag and Key Exchange

Whenever a new MC wants to join existing WMN, it has to submit its token to nearby MR. MR forwards this information along with its tag to CA. CA will issue a tag to new MC, after successful verification of its token as shown in **Fig. 2**. The steps involved in this process are as below:

1. New MC → MR: TOK_{MC}
2. MR → CA: $[TOK_{MC}]K_{CAMR}$, TAG_{MR}
3. CA → MR: $[TAG_{MC}]K_{CAMC}$
   Where $TAG_{MC} = (ID_{MC}, IP_{MC}, PK_{MC}, T_{Is}, T_{Ex})\ K_{CA}$
4. MR → New MC: $[TAG_{MC}]K_{CAMC}$, TAG_{MR}

In step 1, new MC will submit its token to nearby MR. Then, MR will forward MC's token for verification to CA after encrypting it with the shared secret key between CA and MR (K_{CAMR}) along with its tag as shown in step 2. Now CA authenticates the MR by the submitted TAG_{MR} and then it decrypts the remaining encrypted message. After verifying the token TOK_{MC}, CA will generate a shared secret key for new MC by using ECDH protocol. Then it will send a tag for new MC, encrypting it by shared secret key between CA and new MC through the corresponding MR as shown in step 3. The tag for MC contains mesh client ID, IP address of MC, the public key of MC, Issue time and Expiration time. In step 4, MR will forward this encrypted tag to new MC along with its tag for authentication. After MC receives the encrypted tag, it generates a shared secret key (as CA generated) using its secret and public key of CA and will decrypt that tag. MR and MC will use their tags during the route discovery process and data packet forwarding for better authentication. Thus, before route discovery, every node has an authenticated tag issued by the CA.

3.2.2 Trust Model based on CLSL-DR mechanism

Here, a new cross layer and subject logic based reputation mechanism is proposed which is an improved version of the scheme presented in [5] [6] is used to measure the trust values of the nodes. In this mechanism, cross layer based metric and uncertainty metric are incorporated in association with subject logic into the reputation computation algorithm to detect and isolate the malicious nodes and thereby finding reliable routing paths. The metric considers network layer observations of forwarding behavior, in combination with MAC layer measurements of wireless link quality to select more reliable and higher performance path. According to subject logic, a trust metric is represented as an opinion to express subjective beliefs. Each opinion is defined by four parameters and it is specified as Om:n = (Tm:n, Dm:n, Um:n, Rm:n), where Tm:n represents node m's trust on node n, Dm:n represents node m's distrust on node n, Um:n represents node m's uncertainty on node n and Rm:n is the base rate of m's trust on node n. These parameters should satisfy the following conditions:

$$\begin{Bmatrix} T_{m:n} + D_{m:n} + U_{m:n} = 1.0 \\ T_{m:n}, D_{m:n}, U_{m:n}, R_{m:n} \in [0.0, 1.0] \end{Bmatrix} \quad (1)$$

By assuming the opinion as a decision, the final trust metric is computed as,

$$F(O_{m:n}) = T_{m:n} + R_{m:n}\, U_{m:n} \quad (2)$$

3.2.2.1 Reputation Computation

Let m and n are the two neighboring nodes. The final opinion of node m to n $O_{m:n}^{final}$ is computed by having both local observation (Local Opinion) and global observation (Global Opinion).

$$O_{m:n}^{final} = \left\{ O_{m:n}^{loc}, O_{m:n}^{glo} \right\}$$

Local Opinion:

The local opinion of node m to node n $O_{m:n}^{loc} = T_{m:n}^{loc}, D_{m:n}^{loc}, U_{m:n}^{loc}, R_{m:n}^{loc}$ is computed and it is stored in m's local reputation table with respective node's id and the values are computed as follows:

$$\begin{Bmatrix} T_{m:n}^{loc} = ST_{m\to n}/(NT_{m\to n} * LQ_{m\to n}) \\ D_{m:n}^{loc} = NF_{m\to n}/(NT_{m\to n} * LQ_{m\to n}) \\ I_{m:n}^{loc} = 1.0 - T_{m:n}^{loc} - D_{m:n}^{loc} \end{Bmatrix} \quad (3)$$

Where $ST_{m\to n}$ represents the number of packets received from m and n has successfully forwarded, $NF_{m\to n}$ represents the number of packets received from m and n has not forwarded, and $NT_{m\to n}$ is the total number of packet transmissions received from m. $LQ_{m\to n}$ denotes the link quality metric from m to n, which is computed as in equation (4).

To measure link quality in WMNs, a novel cross-layer based reliable routing metric named Minimum Expected Forwarding Counter (MEFW) [7] is used to isolate the malicious or selfish nodes during route discovery. MEFW considers the worst dropping behavior of the

nodes and it is more robust against packet dropping attacks. Compared to the traditional mechanisms for estimating the link quality in WMNs, MEFW metric simplifies the network representation and selects the most reliable and highest performance routing path by considering routing layer observations of forwarding behavior as well as MAC-layer measurements of wireless link quality.

$$LQ_{m\to n} = MEFW_{m\to n} = MEFW_{n\to m} = \frac{1}{(1-P_{mn})(1-P_{nm})} \cdot \frac{1}{(1-\max(P_{d,mn},\ P_{d,nm}))} \tag{4}$$

Where P_{mn} and P_{nm} denote the packet loss probability of the wireless link (m, n) in forward and reverse directions respectively. $P_{d,mn}$ and $P_{d,nm}$ represent the dropping probabilities in m to n direction and n to m direction respectively at the network layer of node n. It is possible to discover high reliability paths that are able to provide better packet delivery ratio with the help of this metric since this metric is able to decide the quality of the links. At any time, a new node joins the network, the default trust opinion for the new node set by the other nodes as (0.0, 0.0, 1.0, R). These local opinions are updated in the local reputation table periodically from time to time.

Global Opinion:

These are useful when the local opinions are not enough to judge a node. If a node m wants to collect global opinions on node n from their common neighbor nodes, it just passes the reputation query to them. When node m receives global opinions on node n from two recommenders, and if their opinions conflict with each other, then m has to decide which recommender node is more trustworthy and get the opinion from that node and discards the opinion from the other node. For more than two recommenders, let R is assumed as the set of recommenders, and for each recommender i ϵ R, a unique weight is assigned and it is computed according to equation (5).

$$\left\{\begin{array}{l} w_i = F(O_{m:i}) / \sum_{k\in R} F(O_{m:k}) \\ F(O_{m:i}) = T_{m:i} + R_{m:i} U_{m:i} \end{array}\right\} \tag{5}$$

Now, the global opinion $O^{glo}_{m:n} = (T^{glo}_{m:n}, D^{glo}_{m:n}, U^{glo}_{m:n}, R^{glo}_{m:n})$ is computed according to equation (6).

$$\left\{\begin{array}{l} T^{glo}_{m:n} = \sum_{k\in R} w_k\, T^{loc}_{k:n} \\ D^{glo}_{m:n} = \sum_{k\in R} w_k\, D^{loc}_{k:n} \\ U^{glo}_{m:n} = \sum_{k\in R} w_k\, U^{loc}_{k:n} \\ R^{glo}_{m:n} = \sum_{k\in R} w_k\, I^{loc}_{K:n} \end{array}\right\} \tag{6}$$

Final Opinion:

After obtaining the local opinion and the global opinion, a final opinion $F^{final}_{m:n} = (T^{final}_{m:n}, D^{final}_{m:n}, U^{final}_{m:n}, R^{final}_{m:n})$ is computed as shown in equation (7).

$$\begin{cases} T_{m:n}^{final} = \left(T_{m:n}^{dir} \cdot U_{m:n}^{glo} + T_{m:n}^{glo}.U_{m:n}^{dir}\right) / \left(U_{m:n}^{dir} + U_{m:n}^{glo} - U_{m:n}^{glo}.U_{m:n}^{dir}\right) \\ D_{m:n}^{final} = \left(D_{m:n}^{dir} \cdot U_{m:n}^{glo} + D_{m:n}^{glo}.U_{m:n}^{dir}\right) / \left(U_{m:n}^{dir} + U_{m:n}^{glo} - U_{m:n}^{glo}.U_{m:n}^{dir}\right) \\ U_{m:n}^{final} = \left(U_{m:n}^{dir}.U_{m:n}^{glo}\right) / \left(U_{m:n}^{dir} + U_{m:n}^{glo} - U_{m:n}^{glo}.U_{m:n}^{dir}\right) \\ R_{m:n}^{final} = \left(R_{m:n}^{dir} \cdot U_{m:n}^{glo} + R_{m:n}^{glo}.U_{m:n}^{dir}\right) / \left(U_{m:n}^{dir} + U_{m:n}^{glo} - U_{m:n}^{glo}.U_{m:n}^{dir}\right) \end{cases} \quad (7)$$

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 computed by using a moving average model as shown in equation (8).

$$F_{t1} = \alpha F_{t0} + (1-\alpha) F_{t1} \quad (8)$$

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

3.2.3 Route Discovery

Here, the route discovery procedure of the proposed protocol based on the security tag model and the computed trust level between the neighbor nodes is discussed. It is assumed that source node S wants to find a route to destination node D. The route discovery process is carried out by Route Request (RREQ) and Route Reply (RREP) packets. The generation of RREQ and RREP packets is discussed as follows. Route discovery parameters such as timestamp (ts) which specifies the time required to complete the route discovery, maximum number of intermediate hops required (maxh) and sequence number (snum) to uniquely identify the RREQ message are appended within the RREQ message to reduce the route discovery time. Before broadcasting RREQ, source S applies CLSL-DR mechanism to compute the reputation values of its neighbors according to the following steps.

1. Source S checks its local reputation table to retrieve local opinion $O_{S:Ij}^{loc}$ of a neighbor node Ij and computes the final trust metric F ($O_{S:Ij}^{loc}$).
2. If F ($O_{S:Ij}^{loc}$) ≥ θ, then Ij is considered as trustworthy node; else if F ($O_{S:Ij}^{loc}$) < θ then S tries to collect the global opinions from the common neighbor nodes with Ij, where θ is the threshold parameter which lies between [0.0, 1.0].
3. To retrieve the global opinion, S forwards the Rep_query message to the common neighbor nodes and waits for the time period T.
4. If any neighbor node has an uncertainty opinion on node Ij is less than 1, and then it forwards its local opinion on Ij to S.
5. When the time period T is ended, S collects all the global opinions from common neighbor nodes and assigns a unique weight to them.
6. Then S computes $O_{s:Ij}^{glo}$ and evaluates the final trust metric F ($O_{S:Ij}^{glo}$). If F ($O_{S:Ij}^{glo}$) ≥ θ then Ij is considered as trustworthy node; otherwise Ij is considered as malicious node and this state is recorded in the trust table.

According to the above steps, S evaluates the Trust Value (TV) metric of its neighbor nodes. S forwards the RREQ message along with the computed trust metric only to its neighbors whose

trust metric is greater than θ. If the trust metric of the neighbor node does not meet the threshold, then it won't forward RREQ towards that node. This process is repeated until the RREQ reaches the destination MR. Every RREQ message is digitally signed by the source and only destination can send back reply message after verification of the signature. The intermediate nodes verify only the signature and on successful verification, create or update reverse route to the source, computing trust metric of the neighbor nodes, forwarding the request to the neighbor nodes based on trust metric after attaching its tag. Before forwarding the RREQ message at each mesh router, the computed trust metric is cumulatively added to the stored trust value in the request message.

For the verification process, intermediate nodes and the destination can get the public key of the source from its tag attached with that RREQ message. Finally, with every RREQ and RREP messages, tag of the source (in case of RREQ) and tag of the destination (in case of RREP) are attached. The route discovery process is implemented through the following steps:

Step 1:	S → *:	(RREQ, TV, ts, maxh, snum, D)K_S, TAG_S
Step 2:	I1→ *:	(RREQ, TV, ts, maxh, snum, D)K_S, TAG_S, TAG_{I1}
Step 3:	I2→*:	(RREQ, TV, ts, maxh, snum, D)K_S, TAG_S, TAG_{I2}
Step 4:	D→ I2:	(RREP, S, ts)K_D, TAG_D
Step 5:	I2→I1:	(RREP, S, ts)K_D, TAG_D, TAG_{I2}
Step 6:	I1→S:	(RREP, S, ts)K_D, TAG_D, TAG_{I1}

To discuss the working of the trust based secure, reliable routing protocol, it is assumed that S is the source and D is the destination. I1 and I2 are intermediate nodes. TAG_S is the tag that belongs to S; TAG_{I1} belongs to I1 and so on. Therefore, Source S generates signed RREQ message (RREQ) which includes TV metric of the neighbor node which is selected as the forwarding node, timestamp (ts), maximum number of hops (maxh) required for route discovery and Destination D's IP address, attaches its tag and forward it to the selected neighbors based on the trust metric as discussed above for route discovery as shown in Step 1.

Intermediate node (I1) first verifies the tag attached with RREQ and then verifies the actual signed RREQ message with the help of the public key of the sender from its tag. On successful verification, it creates or updates reverse route to the source, checking whether ts and maxh requirements are satisfied, computes trust metrics of the neighbor nodes as source node S does and forward only to the selected neighbors by cumulatively adding the trust metric with the value stored in the received RREQ message by attaching its tag (Step 2). Another intermediate node (I2) receives this request and first verifies the tag of intermediate node (in this case I1) and on successful verification, does the computing of trust metric, checking the requirements, removes the tag of the previous intermediate node and then creates or updates reverse route to the last node and attaches its tag with it and rebroadcasts the RREQ packet to the selected neighbors until it reaches the destination MR (Step 3). On receipt of the RREQ packet by the destination MR, it will verify the tag of the last node and then verifies the signed RREQ message. Destination MR will receive several RREQ messages through multiple paths from S. To select the secured, reliable path, it waits for time period T. Once T is over, it compares the TV metric available in the received RREQ messages. The RREQ message which has the highest TV metric is chosen as the secured reliable path and RREP message is unicasted only to the selected path in the reverse direction. Now, D generates and digitally signs the RREP message, which includes the IP address of source, time stamp, tag and forwards to the destination MR and then to the next hop of the chosen optimal reverse path towards the source (Step 4). Every intermediate node verifies the received RREP message, updates its routing table

and then it forwards the message to the source. (Step 5, Step 6). After receiving a RREP, and the tag of the destination, source S will generate the shared secret key by using its secret key and public key of the destination. Thus, the optimal secured path is found and both source and destination have the shared secret key that is used for further communication. The algorithm for route discovery of the proposed protocol is shown below.

Algorithm: Route Discovery

Input: Set of nodes, Ni (Source/Intermediate or Destination)
Output: Secured, reliable route

- Begin
- If (Source node)
  Invoke Get_Trust (Neighbor n)
  Forward Route Request(RREQ) as (RREQ, TV, ts, maxh, snum, D)K_S, TAG_S
  from Source node (S) to Destination node (D) to start route discovery
- Else if (Intermediate node)
- If (not_duplicate_request)
  Invoke Get_Trust (n)
  - If (trust>=threshold && maxh>No. of_intermed_nodes && ts<=TS_threshold)
    Authenticate packet signature and the attached tag
    Cumulatively add the computed trust metric with the stored metric in the RREQ packet
    Attach its own tag by replacing the previous intermediate node's tag
    Forward RREQ packet to the selected neighbor node
  - Else
    Drop RREQ packet
- Else
  Discard request and the procedure ends
- Else if (Destination node)
  Wait for Time period T
  Compare TV metric available in the received RREQ messages over multiple paths once T is over
  Choose the path with the highest TV metric in the RREQ packet
  Generate Route Reply (RREP) message as (RREP, S, ts)K_D, TAG_D
  Find secured, reliable routing path and D unicasts the RREP packet towards the selected path to S
- Else
  Discard request
- End

Routine Get_Trust (n)

- Begin
- For (each node m and its neighbor n)
  Compute Final Trust Metric by receiving Local Opinion and Global Opinion
  Compute Local Opinion (O^{loc})
  Store O^{loc} in the local reputation table of x
- If (O^{loc} >Threshold)
  Node is considered as trustworthy

- Else
  Get Global Opinion (O^{glo}) from neighboring nodes
  N= Number of Global Opinions
- If ((N==2) && (Global opinions conflict))
  Choose node n with higher O^{loc} with m
- Else if (N>2)
  R = Set of recommenders
  For each i ϵ R
  Allocate unique weight w_i to each global opinion (O^{glo})
  Obtain final trust = {O^{loc}, O^{glo} }
- End

4. Security and Cost Analysis

It is observed that most of the external and internal attacks against the routing protocols can be prevented with encryption and authentication mechanisms. In the proposed scheme, in addition to the security tag model for efficient authentication, a new Cross Layer and Subject Logic based Dynamic Reputation mechanism (CLSL-DR) is introduced to provide strong security against Denial of Service (DoS) attacks like packet dropping and misdirecting attacks, route disrupting attacks etc. Many network layer attacks are discussed in [11] [31]. Compared to the existing routing mechanisms, the proposed protocol provides better security against the following DoS attacks.

- Sybil Attacks
- Sinkhole Attacks
- Hello Flood Attacks

Sybil Attacks: A Sybil attack is a kind of routing layer attack where a malicious node can create multiple identities in the network, each appearing as a valid node. The legitimate nodes will assume these identities as distinct valid nodes and include these nodes in the discovery of routing paths. When the packets are forwarded through these routing paths, the malicious node processes all these packets by using the multiple identities. Now, the malicious node can launch any type of attack. In this proposed protocol, tag based authentication is implemented for each node and CA issues a tag for each new node after verifying the token. The tag contains the new node's id, public key, IP address and timestamp information. And also, by implementing CLSL-DR mechanism at each node, trusted nodes can be selected and these types of malicious nodes can well be identified and isolated during route discovery. Hence, Sybil attacks can be prevented.

Sinkhole Attacks: A black hole attack (or sinkhole attack) is another kind of denial of service attack in WMNs. In this attack, the attacker node always replies positively to a RREQ, even though it may not have a valid route to the destination. Hence, all the data traffic within the vicinity of the malicious node will be directed towards the malicious node, which in turn drops all the packets. In this proposed protocol, malicious nodes can be detected easily by getting the local opinion and global opinion from the neighboring nodes. By having the history of forwarding capability of the nodes, these malicious can well be detected and only the destination node can send the RREP message after selecting the optimal path and other intermediate nodes cannot. Along with RREP, the destination node has to send its own tag for authentication purpose and the RREP message is digitally signed by the shared secret key between source and destination. Hence the attack can be prevented.

HELLO Flood Attacks: By using the shared keys between a node and CA, HELLO flood attacks are prevented because every node is authenticated by the CA using the tags.

The additional cost involved in processing the routing packets due to the use of the security mechanisms and computation of trust metrics at each node is analyzed. However, in the proposed protocol, broadcasting of control packets is minimized during route discovery based on the Trust Value (TV) metric computation. Hence, the control packet overhead is minimized and the secured, reliable routing path is chosen in less time. For node to node communication, shared secret key is generated one time only, and the same key is used for future communication. The cost required for computation of the keys is also less because symmetric key based encryption scheme is used.

5. Implementation Results and Analysis

The proposed protocol is implemented using the NS-2 simulator. Here, a WMN of 50 nodes, which are based on IEEE 802.11 with data rates ranges from 1 to 5 Mbps is considered. Nodes can move into an area of 1000m X 1000m. Data traffic is produced at Constant Bit Rate (CBR) with a radio range of 100m. Random way point mobility model is used to generate node mobility with packet size of 512 bytes. Source and destination nodes are selected randomly. The various simulation parameter settings are shown in **Table 2**. The proposed protocol TSRR is compared with the similar trust based secure routing protocol such as Role based Privacy Aware Secure Routing Protocol (RPASRP) and other secure routing protocols such as Secure Ad hoc On demand Distance Vector (SAODV) routing protocol, Security-aware Ad hoc Routing (SAR) protocol and Security Enhanced AODV (SEAODV) routing protocol for performance and security analysis in both the normal and the malicious conditions.

Table 2. Simulation Parameters and Values

Parameters	**Values**
Number of Nodes	50
Topology Dimensions	1000m X1000 m
MAC	802.11n
Data Rate	1-5 Mbps
Radio Range	100m
Maximum node speed	1-30m/s
Node pause times	0-5 s
Simulation Time	500s
Mobility Model	Random waypoint
Traffic pattern	CBR/UDP

5.1 Performance Analysis

Here, the scenario of 50 normal nodes with varying node speeds has been taken. The parameters such as Packet Delivery Ratio (PDR), Throughput, End-to-End Delay and Routing Overhead are considered for performance analysis. The PDR for the proposed protocol, RPASRP, SAODV, SAR and SEAODV is shown in **Fig. 3**. For all the node speeds, the proposed protocol TSRR maintains the PDR above 85%. RPASRP also provides similar performance as the proposed protocol since trusted nodes are chosen for route discovery and packet transmission. However, TSRR shows slight improvement in performance than RPASRP by choosing secure, reliable routing paths. Reliable routing paths are guaranteed by

integrating a robust link quality routing metric (MEFW) along with the reputation model. In addition to the reputation evaluation mechanism, the proposed protocol implements a novel security tag model for providing better authentication which in turn improves the packet delivery ratio. It is also observed that SAR and SEAODV protocols more or less show the same performance of PDR for all the node speeds. In the case of SAR protocol, level of trust is used as a security metric to discover the secured route between the source and destination nodes. The nodes which have required security constraints will present in the route and hence only trusted nodes will forward the packets. Also, SEAODV protocol establishes a secured route by ensuring hop by hop authentication and hence only authenticated nodes will participate in the route discovery. Compared to all other protocols, SAODV provides the slightest deviation in performance in PDR since the malicious nodes are not effectively isolated during route discovery and packet transmission phases. Thus, the proposed protocol TSRR gives better performance in delivering packets than the other protocols by establishing a secured reliable routing path with the better link quality.

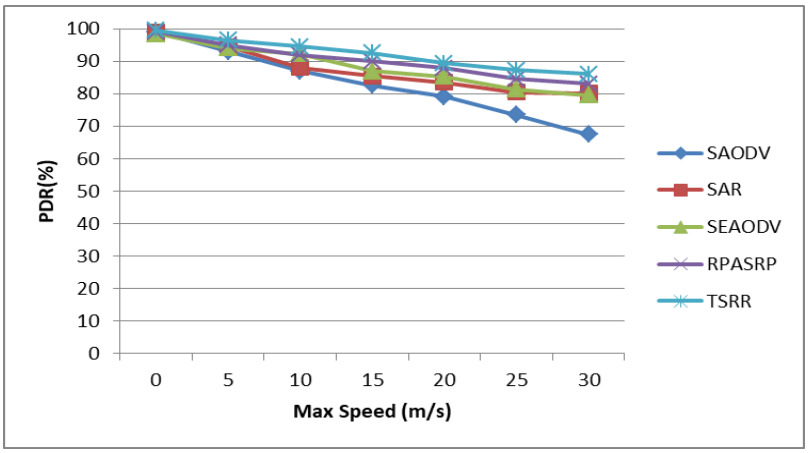

Fig. 3. Packet Delivery Ratio with varying node speeds

Fig. 4 shows the throughput of a network of 50 nodes with varying traffic load. TSRR protocol shows higher throughput performance compared to the other protocols. TSRR protocol chooses only the trusted nodes for forwarding the packets, discovers high performance, reliable routing path by considering forwarding reliability of network nodes and also ensures the security for delivering the packets. Hence it has increased performance in throughput comparing with the other protocols. Initially, when the traffic load is less, RPASRP and the proposed protocol TSRR provide the same performance in throughput and even when the traffic load increases, the difference between the performances of these two protocols is low only. Since the malicious nodes are well isolated during route discovery and packet forwarding, proposed protocol and RPASRP show better performance in throughput. For the considered scenario, the other three protocols such as SAR, SEAODV and SAODV show similar performance in throughput for the increased payload.

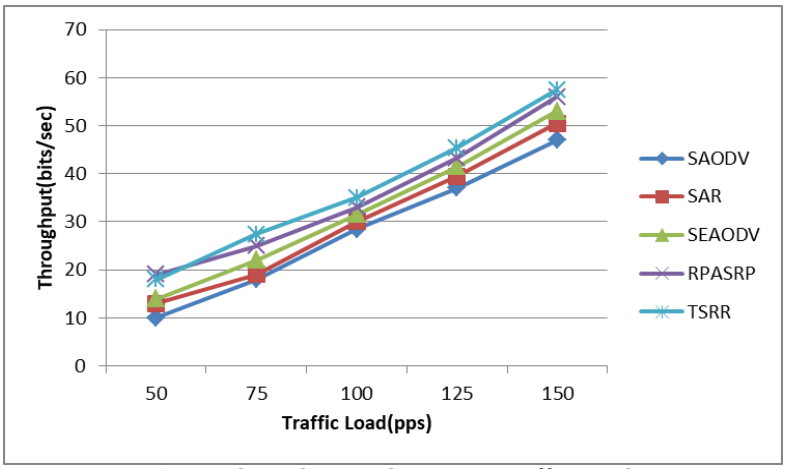

Fig. 4. Throughput with varying Traffic Load

Fig. 5 shows the average end to end delay for a network of 50 nodes with varying speeds. Here, less end to end delay is observed in the case of TSRR protocol. Although it has implemented cryptographic mechanisms and trust metrics computation at each node, broadcasting of control packets during route discovery is minimized by considering the Trust Value (TV) metric of the neighboring nodes. Hence, the routing path is chosen with less delay and the packets will reach the destination with less time compared to the other protocols. However, RPASRP shows slight increase in end-to-end delay performance for the increase in traffic load. This is due to the time taken for trust computation and for other cryptographic computations at each node during route discovery. Increase in traffic load leads to severe congestion in the network and also packets dropped or lost frequently. Hence, it shows less performance in end-to-end delay. Since the proposed protocol TSRR applies a mechanism to minimize the control packet transmission during route discovery, the delay performance is better compared to RPASRP. In the case of the other three secure routing protocols, the cryptographic computations done at each node makes the route discovery process and packet transmission process longer. Initially, for the node speeds, up to 10m/s, SAR and SEAODV protocols show similar performance. When the node speed increases, they show more deviation in the delay values.

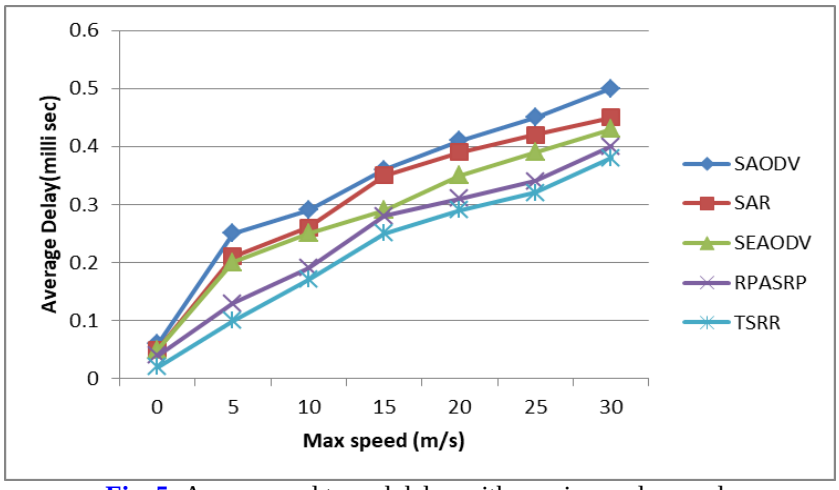

Fig. 5. Average end to end delay with varying node speeds

Fig. 6 shows the comparative analysis of routing overhead for the TSRR protocol, RPASRP and other secured routing protocols. Routing overhead is defined as the average number of control messages sent in one second. TSRR protocol reduces the routing overhead by minimizing the broadcasting of control packets during route discovery. However, the computation of Trust Value metric and security mechanisms applied at each node increases the routing overhead. Compared to the other secured routing protocols, the proposed protocol reduces routing overhead since it goes for a restricted broadcasting of control packets. It is also observed from the **Fig. 6** that, for a number of hops up to 6, RPASRP, SAR and SEAODV show similar performance in terms of routing overhead. The computation involved in cryptography and routing metrics calculation at each node will increase the routing overhead as the number of hops increases. SAODV gives more routing overhead since it has used additional fields in the routing packet and for the computation required at each node.

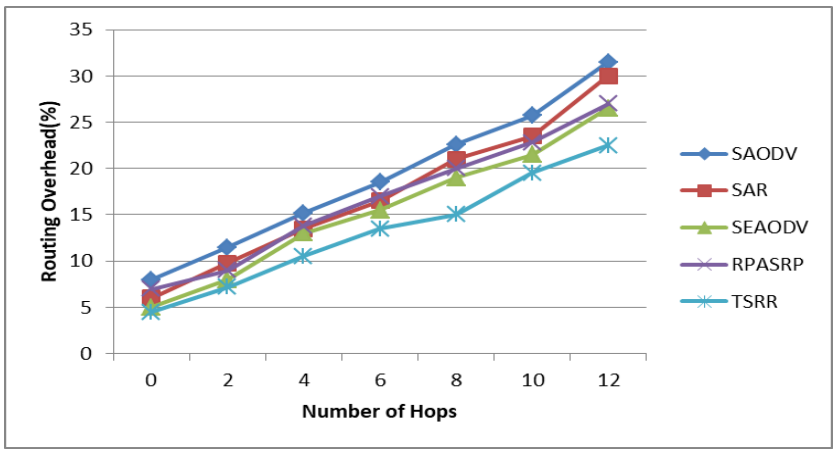

Fig. 6. Routing Overhead with Number of hops

5.2 Security Analysis

To analyze the security of the proposed protocol TSRR against the attacker nodes, the network scenario of 50 nodes has been taken in which 20% of the nodes are malicious nodes. The above discussed parameters are again considered for the security analysis. The packet delivery ratio comparison of the proposed protocol TSRR, RPASRP, SAODV, SAR and SEAODV with varying node speeds in the presence of malicious nodes is shown in **Fig. 7**. The PDR of the TSRR protocol provides better performance compared to the other protocols. It is due to the fact that it is capable of isolating the malicious nodes by selecting trusted nodes for forwarding of packets and also authenticating the nodes before the packets are forwarded through the routing path. Initially, RPASRP and TSRR protocols provide similar performance in the PDR and then the slightest deviation in performance is achieved. Eventhough RPASRP and TSRR implement similar reputation evaluation mechanism, TSRR protocol differs by selecting reliable trust based route by implementing Cross layer based dynamic reputation evaluation mechanism. Next to the proposed and RPASRP protocols, SEAODV shows better performance in terms of PDR since the routing path is selected with strong security requirements and only authenticated nodes are participating in the packet transmission phase. Compared to SAODV, SAR protocol has shown better performance since in SAR protocol, ‘Level of Trust’ is used as a routing metric and hence only the trusted nodes, which satisfy the

required security constraints will participate in the route discovery as well as packet transmission.

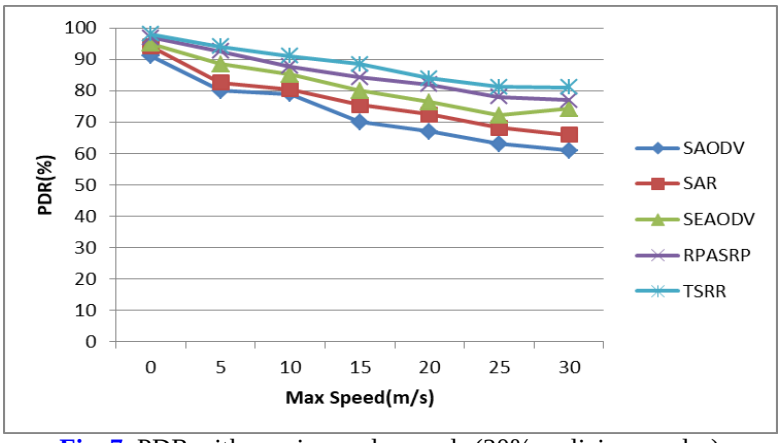

Fig. 7. PDR with varying node speeds (20% malicious nodes)

The throughput of the proposed scheme TSRR, RPASRP, SAODV, SAR and SEAODV with varying traffic load in the presence of 20% of malicious nodes in a network is given in **Fig. 8**. TSRR has relatively higher throughput performance compared to the other protocols. Even though the malicious nodes are present in the network, TSRR protocol well isolates the malicious nodes and routes the packets after proper authentication of the nodes in the routing path. Hence, almost 90% of the traffic reaches the destination. RPASRP shows a slight deviation in throughput performance compared to TSRR protocol because reliable links for packet transmission may not be present all the time. However, in the proposed routing scheme, reliable links and forwarding reliability of network nodes are chosen for packet transmission in addition to finding the trusted nodes by incorporating a novel robust link quality metric for determining reliable links for packet transmission. Also, a novel secure tag model is introduced to provide better authentication along with the CLSL-DR mechanism to ensure secure and reliable packet transmission. In case of the other secured routing protocols, SEAODV provides better throughput with increase in traffic load since hop by hop authentication done at each node and also secured data traffic is ensured by the discovered routing path. From **Fig. 8**, it is also observed that, SAR and SAODV have more or less similar performance of the traffic load up to 100. Then they show slight variation in the throughput performance.

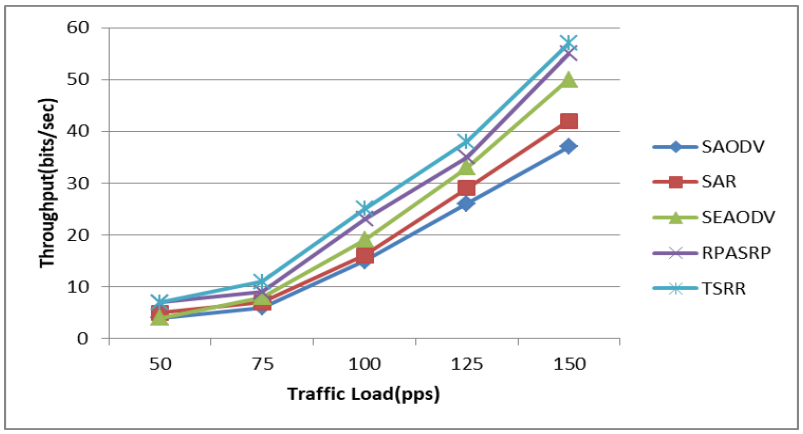

Fig. 8. Throughput with varying Traffic Load (20% malicious nodes)

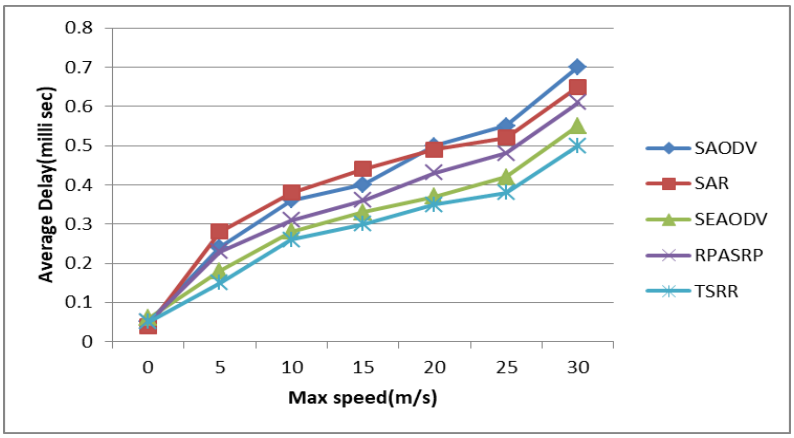

Fig. 9. Average end-to-end delay (20% malicious nodes)

The end-to-end delay in the presence of malicious nodes is shown in **Fig. 9**. It can be observed that, TSRR protocol has less end-to-end delay compared to the other protocols. Since it has chosen trust based secured reliable routing path with less time by minimizing the control packet overheads, the packet transmission can be faster and the end-to-end delay is considerably reduced. Although TSRR protocol performs both the authentication process and computation of trust metrics, the time required for route discovery is less since it selects the better link quality path. **Fig. 9** also shows that SEAODV shows better performance in delay than RPASRP, SAR and SAODV since SEAODV uses Message Authentication Code (MAC) and small size routing messages. Hence, the average end-to-end delay is considerably lower compared to the other three routing protocols. Since SAODV and SAR have implemented security mechanisms to discover secured routing path, the end-to-end delay is more, compared to the other protocols. RPASRP shows increase in end-to-end delay compared to the proposed protocol because of the computation required for reputation evaluation and other cryptographic computations done at each node during route discovery and packet transmission phase. TSRR protocol consumes less end-to-end delay by choosing secured, reliable route and minimizing control packet overheads.

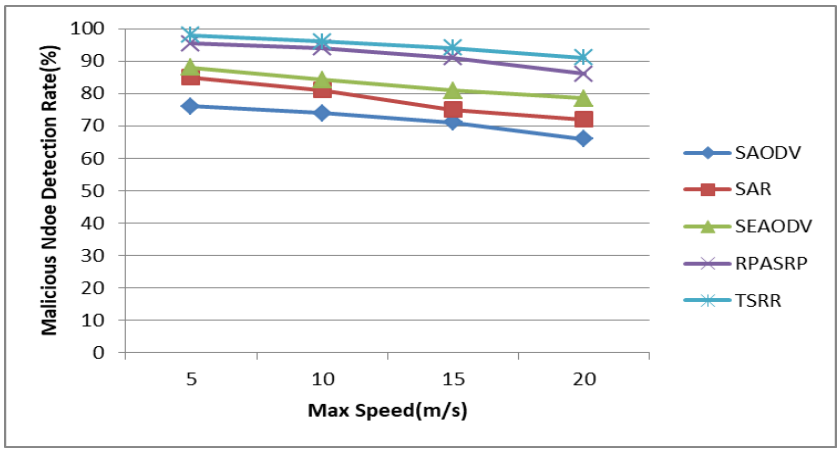

Fig. 10. Detection Rate (20% malicious nodes)

Fig. 10 shows the malicious node detection rate of the proposed scheme TSRR, RPASRP, SAODV, SAR and SEAODV with variable speed in the presence of 20% of malicious nodes in a network. TSRR and RPASRP protocols show similar performance in the detection of malicious nodes since both the protocols have implemented an efficient subject logic based dynamic reputation evaluation mechanism for detecting and isolating the malicious nodes in a better way. TSRR protocol provides better detection rate than RPASRP since it applies a novel security tag model to choose the authenticated nodes to participate in the route discovery and packet transmission phases. It also introduces a cross layer based reputation evaluation mechanism to choose secured, reliable routes by considering efficient routing metrics. Hence, the proposed protocol TSRR detects and isolates the malicious nodes in a more effective manner than the other protocols taken for comparison. Compared to SAR and SAODV, SEAODV provides better detection rate as the node speed increases. This is due to the fact that it provides better authentication and strong security mechanism for route discovery and packet transmission, which in turn increases the detection rate of malicious nodes. From **Fig. 10**, it is also observed that, SAODV shows less performance in the detection rate of malicious nodes compared to all the other secured routing protocols since it lacks a proper authentication mechanism and trust models for detecting and isolating the malicious nodes.

6. Conclusion

In this work, a new Trust based Secured Reliable Route Discovery scheme (TSRR) has been proposed for Wireless Mesh Network. This routing scheme provides optimal performance since it employs the security mechanisms of tag based authentication, implements Cross Layer and Subject Logic based Dynamic Reputation (CLSL-DR) to compute Trust Metrics. Therefore, it minimizes the control packet overhead during the route discovery and separates the malicious nodes. Comparison of the proposed routing scheme TSRR with a similar trust based secure routing protocol Role based Privacy Aware Secure Routing Protocol (RPASRP) and other Secure routing protocols such as SAODV, SAR and SEAODV is carried out using ns-2 simulation. The metrics used in this work for comparison are packet delivery ratio, throughput, average delay, routing overhead and detection rate of malicious nodes. From the experiments conducted, it is observed that, the proposed protocol provides better performance in terms of Packet Delivery Ratio (PDR), Throughput, End-to-end delay and Detection rate compared to all the other protocols taken for comparison. The number of packets dropped is

reduced since the purposeful packet drops by malicious nodes are avoided by choosing only the trusted nodes. The proposed protocol considers both security capabilities of the routing and effectiveness of the routing in terms of choosing high performance secured, reliable routing path. Performance and security analysis are also carried out in this work. It shows that our proposed protocol is efficient and is able to defend the packet dropping attacks such as sybil, sink hole and hello flood attacks. Future works in this direction can be the use of fuzzy logic to handle the uncertainty in trust computation effectively.

References

[1] Akyildiz, I. F., Wang, X. and Wang, W, "Wireless mesh networks: a survey," *Computer networks*, vol. 47, no. 4, pp. 445-487, 2005. Article (CrossRef Link)

[2] Waharte, S., Boutaba, R., Iraqi, Y.,and Ishibashi, B. "Routing protocols in wireless mesh networks: Challenges and design considerations," *Multimedia Tools and Applications*, vol. 29, no. 3, pp. 285–303, 2006. Article (CrossRef Link)

[3] Campista, M. E. M., Esposito, P. M., Moraes, I. M., Costa, L. H. M., Duarte, O. C. M., Passos, D. G., and Rubinstein, M. G., "Routing metrics and protocols for wireless mesh networks," *IEEE network*, vol. 22, no. 1, pp. 6-12, 2008. Article (CrossRef Link)

[4] Mogaibel, H. A and Othman, M., "Review of routing protocols and it's metrics for wireless mesh networks," in *Proc. of 2010 Second Pacific-Asia Conference on Circuits, Communications and System*, pp. 27-30, 2010. Article (CrossRef Link)

[5] Lin, H., Hu, J., Ma, J., Xu, L. and Nagar, A., "A role based privacy-aware secure routing protocol for wireless mesh networks". *Wireless Personal Communications*, vol. 75, no. 3, pp. 1611-1633, 2014. Article (CrossRef Link)

[6] Lin, H., Ma, J., Hu, J., and Yang, K., "PA-SHWMP: a privacy-aware secure hybrid wireless mesh protocol for IEEE 802.11 s wireless mesh networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2012, p. 69, 2012. Article (CrossRef Link)

[7] Paris, S., Nita-Rotaru, C., Martignon, F. and Capone, A, "Cross-layer metrics for reliable routing in wireless mesh networks," *IEEE/ACM Transactions on Networking (TON)*, vol. 21, no. 3, pp. 1003-1016, 2013. Article (CrossRef Link)

[8] Mahmoud, M. M., Lin, X. and Shen, X. S. "Secure and reliable routing protocols for heterogeneous multihop wireless networks," *IEEE Transactions on Parallel & Distributed Systems*, vol. 26, no. 4, pp. 1140-1153, 2015. Article(CrossRef Link)

[9] Yu, Y., Ning, Z. and Guo, L., "A secure routing scheme based on social network analysis in wireless mesh networks," *Science China Information Sciences*, vol. 59, 122310, 2016. Article (CrossRef Link)

[10] Lin, H., Hu, J., Xu, L., Tian, Y., Liu, L. and Blakeway, S., "A trustworthy and energy-aware routing protocol in software-defined wireless mesh networks," *Computers & Electrical Engineering*, vol. 64, pp. 407-419, 2017. Article(CrossRef Link)

[11] Bhanu, M. S., "A Survey of Secure Routing Protocols for Wireless Mesh Networks," *International Journal of Computer Applications*, vol. 97, no. 6, 2014.

[12] Zapata, M. G., & Asokan, N., "Securing ad hoc routing protocols," in *Proc. of the 1st ACM workshop on Wireless security, ACM*, pp. 1-10, September 2002. Article (CrossRef Link)

[13] Yi, S., Naldurg, P. and Kravets, R., "A security-aware routing protocol for wireless ad Hoc networks," *Urbana*, 51, 61801, 2002.

[14] Khan, S., & Loo, J., "Cross layer secure and resource-aware on-demand routing protocol for hybrid wireless mesh networks," *Wireless Personal Communications*, vol.62, no. 1, pp. 201-214, 2012. Article(CrossRef Link)

[15] Azhari, S. V., Afshari, N. and Nassiri, M, "Novel lifetime routing metric for IEEE 802.11 wireless mesh networks," *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 28, no. 1, pp. 1-12, 2018. Article(CrossRef Link)

[16] Nanda, A., Nanda, P., He, X., Jamdagni, A. and Puthal, D., "A hybrid encryption technique for Secure-GLOR: The adaptive secure routing protocol for dynamic wireless mesh networks," *Future Generation Computer Systems*, 2018. Article(CrossRef Link)
[17] Mahmoud, M. M., Taha, S., Misic, J. and Shen, X., "Lightweight privacy-preserving and secure communication protocol for hybrid ad hoc wireless networks," *IEEE Transactions on Parallel & Distributed Systems*, vol. 25, no. 8, pp. 2077-2090, 2014. Article(CrossRef Link)
[18] Khan, S., Loo, K. K., Mast, N. and Naeem, T, "SRPM: secure routing protocol for IEEE 802.11 infrastructure based wireless mesh networks," *Journal of Network and Systems Management*, vol. 18, no. 2, pp. 190-209, 2010. Article(CrossRef Link)
[19] Li, C., Wang, Z. and Yang, C., "Secure Routing for Wireless Mesh Networks," *IJ Network Security*, vol. 13, no. 2, pp.109-120, 2011.
[20] Siddiqui, M. S., "Security issues in wireless mesh networks," in *Proc. of International Conference on Multimedia and Ubiquitous Engineering, MUE'07, IEEE*, pp. 717-722, April, 2007. Article(CrossRef Link)
[21] Siddiqui, M. S., Amin, S. O., Kim, J. H., & Hong, C. S., "MHRP: A secure multi-path hybrid routing protocol for wireless mesh network," in *Proc. of Military Communications Conference, MILCOM 2007, IEEE*, pp. 1-7, October 2007. Article (CrossRef Link)
[22] Bansal, D., Sofat, S., & Singh, G., "Secure routing protocol for hybrid wireless mesh Network (HWMN)," in *Proc. of International Conference on Computer and Communication Technology (ICCCT), IEEE*, pp. 837-843, 2010. Article(CrossRef Link)
[23] You, Z. and Wang, Y. "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.
[24] Konwar, S., Paul, A. B., Nandi, S. and Biswas, S., "MCDM based trust model for secure routing in Wireless Mesh Networks," in *Proc. of Information and Communication Technologies (WICT), 2011 World Congress, IEEE*, pp. 910-915, December 2011. Article(CrossRef Link)
[25] Matam, R. and Tripathy, S, "THWMP: trust based secure routing for wireless mesh networks," in *Proc. of the 2011 International Conference on Communication, Computing & Security*, ACM, pp. 40-45, February 2011. Article(CrossRef Link)
[26] Hwang, R. J. and Hsiao, Y. K., "A secure and reliable routing protocol for wireless mesh networks," *Journal of Shanghai Jiaotong University (Science)*, vol. 19, no. 4, pp. 466-475, 2014. Article (CrossRef Link)
[27] Yu, M. and Leung, K. K., "A trustworthiness-based QoS routing protocol for wireless ad hoc Networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 4, pp. 1888-1898, 2009. Article (CrossRef Link)
[28] Popalyar, F. and Yaqini, A., "A trust model based on evidence-based subjective logic for Securing wireless mesh networks," in *Proc. of 21st Conference on Innovation in Clouds, Internet and Networks and workshops (ICIN), IEEE*, February 2018. Article (CrossRef Link)
[29] Tan, H. C., Ma, M., Labiod, H., Chong, P. H. J. and Zhang, J., "A non-biased trust model for wireless mesh networks," *International Journal of Communication Systems*, vol. 30, no. 9, e3200, 2017. Article (CrossRef Link)
[30] Shafer, G., "A mathematical theory of evidence," *Princeton university press*, vol. 42, 1976.
[31] Sen, J., "Secure routing in wireless mesh networks," *arXiv preprint* arXiv:1102.1226, 2011.

Navamani T.M. received her Ph.D and M.E. (CSE) at Anna University Chennai. She has 21 years of teaching experience and currently she is working as Associate Professor in School of Computer Science and Engineering, VIT University, Vellore. She has published more than 26 papers in International , national journals and conferences. Her area of interest is Wireless Ad Hoc Networks, Security and Mobile Computing. She is a life member of Indian Society of Technical Education (ISTE) and member of CSI, IET.

Yogesh P received his M.E(CSE) at Manonmaniam Sundaranar University and PhD at Anna University, Chennai in 1998 and 2007, respectively. Currently he is working as Professor, Department of Information Science and Technology, College of Engineering, Guindy, Anna Univeristy, Chennai. He is having 5 years of Industry experience and 28 years of teaching experience in Engineering Colleges and Technical universities. He has guided 11 PhD scholars and now he is guiding 7 active PhD candidates in the area of Wireless Networks, Computer Networks and Multimedia Communications. His current research interests include Computer Networks, Mobile Computing. Multimedia Communications and security in Computing. He has very good publication record with 90 papers in International Journals and more than 75 papers in International Conferences and National conferences. He is currently lifetime member of CSI and ISTE.