Computers, Materials & Continua
DOI: 10.32604/cmc.2022.029072
Article

Tech Science Press

TMTACS: Two-Tier Multi-Trust-Based Algorithm to Countermeasure the Sybil Attacks

Meena Bharti[1,*], Shaveta Rani[2] and Paramjeet Singh[2]

[1]Department of Computer Science and Engineering, I. K. Gujral Punjab Technical University, Kapurthala, 144603, Punjab, India
[2]Department of Computer Science and Engineering, Maharaja Ranjit Singh Punjab Technical University, Bathinda, 151001, Punjab, India
*Corresponding Author: Meena Bharti. Email: meenabharti89@gmail.com
Received: 23 February 2022; Accepted: 10 April 2022

Abstract: Mobile Ad hoc Networks (MANETs) have always been vulnerable to Sybil attacks in which users create fake nodes to trick the system into thinking they're authentic. These fake nodes need to be detected and deactivated for security reasons, to avoid harming the data collected by various applications. The MANET is an emerging field that promotes trust management among devices. Transparency is becoming more essential in the communication process, which is why clear and honest communication strategies are needed. Trust Management allows for MANET devices with different security protocols to connect. If a device finds difficulty in sending a message to the destination, the purpose of the communication process won't be achieved and this would disappoint both that device and all of your devices in general. This paper presents, the Two-Tier Multi-Trust based Algorithm for Preventing Sybil Attacks in MANETs (TMTACS). The TMTACS provides a two-tier security mechanism that can grant or revoke trust in the Nodes of the MANET. It's a smart way to identify Sybil nodes in the system. A proficient cluster head selection algorithm is also defined, which selects cluster head efficiently and does load balancing to avoid resource consumption from a single node only. Also, for routing efficient path is selected to deteriorate energy consumption and maximize throughput. The recent technique is compared with Secured QoS aware Energy Efficient Routing (SQEER), Adaptive Trust-Based Routing Protocol (ATRP), and Secure Trust-Aware Energy-Efficient Adaptive Routing (STEAR) in terms of Packet Delivery Ratio (PDR), consumption of energy etc. The simulation was performed on MATrix LABoratory (MATLAB) and the results achieved by the present scheme are better than existing techniques.

Keywords: Malicious node; sybil attack; MANET; trust management; security

1 Introduction

MANET is not centrally controlled and relies on wireless computers. They are becoming increasingly popular. These networks are usually formed by mobile devices, such as laptops, smartphones, and tablets [1]. MANETs are self-forming and self-healing [2]. The main advantage of MANETs is their ability to create networks in the absence of any pre-existing infrastructure [3]. This feature makes them an attractive choice for military communication networks. While this type of network has many benefits, it also has its drawbacks. One major drawback is the vulnerability of these networks to attacks [4]. Due to this vulnerability, MANETs can be easily compromised by a hacker and as a result, pose a major security risk. In a Manet, there are various kinds of attacks that attackers can utilize to interfere with the system or its users. Such attacks include Denial of Service (DoS), jamming, Sybil, black hole, gray hole, etc [5–11]. One of the dangerous attacks called Sybil has been elaborated on [12]. Sybil attack can be a real problem for systems that lack centralized and strong identity management and need to set up an individual and secure connection for each node in the network [13]. This attack is characterized by a node that tries to legitimize itself using multiple identities on the same physical device. Network entities that lack physical knowledge (and thus perceive each other as abstract IDENTITIES) are prone to Sybil attacks-where the one-to-one correspondence [6] between an entity and its ID ceases. They can be used to change your reputation score in a peer-to-peer network, and this might affect different aspects of an application [14]. For instance, if the attacker can freely revise their scores, then the reputation system may end up being flawed. In the worst-case scenario, an attacker could get hold of one device and create infinite forged identities [15].

A Sybil attack impacts the stability of the network [16,17]. Once there is a suspicion of a Sybil identity, all devices it's connected to should be disconnected from the network. Cryptographic-based-Authentication is a traditional way that is used to prevent Sybil attacks [18]. But this approach does have its limitations as it is very costly. On the other hand, Received Signal Strength (RSS) [19] is a lightweight solution for MANETs. This approach is cost-effective as this technique doesn't need any extra hardware like antennas or Global Positing System (GPS) etc. This is a protocol that allows node sharing of Sybil or Non-Sybil identities in the network. By doing this, it will reduce the stress on users who are constantly faced with logging in. As people are being urged to use secure networks, it is important to have reliable security mechanisms for MANET so it can continue trending over the next few years. With the recent growth of MANET, almost all devices are connected to the internet. This new approach comes with its own set of security challenges and privacy issues. One example of problems with communication networks is the risk of keys being extracted and confidential data being stolen. Now, a new issue is who or what can you trust? Managing trust in the MANET infrastructure is the main problem [20].

If you want to do things in the best possible way, your systems must rely on each other for assistance when necessary. Organizationally, one entity will always be the "front-facing" member of the group, but it is only linked to other entities at the back-end [21]. This is why it's so important to have a trustworthy object. To maintain credibility and protection, it must assure the best standards of trust management. TM ensures protection and safety for the interconnected nodes that contribute to a reliable and trustworthy service [22–32]. Smart technology has enabled many new ways to interact with our surroundings, but for MANET, there is the added worry of privacy and security. Many kinds of systems have problems with trust. One way to deal with this is through a distributed trust management scheme, which gets each device in the system to evaluate the trustworthiness of its neighbors. To reduce the issues with trust in systems in MANET, a trust algorithm is proposed which is consists of two tiers of security. Direct trust is based on multiple factors namely transmission trust, frequency trust and durability trust. The Proficient cluster head selection algorithm (PCHSA) is also used for

selecting an efficient cluster head. For a selection of route, trust value, residual energy and hop count is considered. Also, within-cluster routing tables are maintained which provides hybrid routing which causes an increase in throughput. In this research, we focus mainly on the smooth interaction of nodes and detection of Sybil nodes at cost of minimum energy consumption. We keep interactions between nodes in the system safe, private, and secure. This way, information can be safely exchanged between them without fear of being corrupted. With the proposed mechanism, existing trust management mechanisms are overcome and distributed security checks are employed to detect and prevent Sybil attacks. Here are the major objectives of the TMTACS:

(i) To provide a PCHSA algorithm for the efficient selection of cluster heads.
(ii) To provide a two-tier trust management system.
(iii) To detect Sybil nodes.
(iv) To provide a technique for selecting routing paths efficiently.

The rest of the paper is organized as Section 2 is about the literature review, and the work done previously by various authors is explained. Section 3 explains the proposed mechanism of detection and prevention of Sybil attacks. Section 4 is about the routing algorithm used for the present work. Section 4 is about the simulation and evaluation of a proposed method. Section 5 concludes the paper and future scope will be suggested.

2 Literature Review

Wang et al. [33] proposed a three-tier architecture to detect Sybil attacks. Firstly, they used RSSI value to differentiate between Sybil node and legitimate nodes in second layer energy-based methods were used for detection of Sybil node and finally, the base station will confirm about Sybil or legitimate node.

Uncertainty Analysis Framework (UAF) is a protocol that is used by Thorat et al. [34] for determining what happens when the device receives corrupt packets. There is an ad hoc on-demand routing protocol being used in the UAF. The values of uncertainty, disbelief, and belief can be determined by examining both the direct and indirect connections between a node and its neighbors.

Wang et al. [35] suggest that IoT devices in smart cities should establish a weighted information network to be able to safely communicate. The weight is calculated according to the network parameters, allowing trustworthy devices to be identified and protected. Each node will be classified into two lists: a white list and a black list. Nodes in a connected network will be added to the path based only on the category of a node. For example, we may add an IoT device if we have all of its information readily available and give it any type of profile. The level of trust in a certain device has been calculated by its expectation and fitness values. This allows the trust management system to keep tabs on and include various types of items utilized in an intelligent IoT-based smart city environment.

A model that is proposed by Rajbhandari et al. [36] combines fuzzy-trust ratings with the calculation of workflow. It is well suited for wireless sensor networks in an Internet of Things (IoT) environment. They used provenance information for capturing workflow.

A trust management scheme is proposed by Khatri et al. [37]. It's a fuzzy-based approach to dealing with ad hoc networks security. The authors have designed a Fuzzy Trust Algorithm to compute the trustworthiness of a device between source and destination. A node is judged by its previous actions as well as its current status. The Trust Factor type analysis plays an instrumental role in the process of routing nodes. This is because the measured level of trust between different nodes is used to determine which route is most appropriate. The approach also relies on other technological tools, including Public

Key Infrastructure (PKI) and graph categorization to identify bad nodes and the propagation of good nodes. Various lengths of keys influence the security and accuracy levels for each key. Thresholds vary per key, so it is necessary to find the right fit for your individual need. There are 2 levels to the fuzzy-based approach: The first level is deciding how many bits to drop, and the second level calculates the trust value for a node. This leads to significant performance increases as it introduces flexibility and maximizes stability. What makes a node trustworthy in this study is based on four core parameters, such as packets dropped, message replays, falsified messages sent to other nodes and messages being forwarded to the wrong destinations. In this, the trustworthiness of the node is evaluated by using input/output variables.

Piro et al. [38] proposed a method to detect Sybil nodes by looking at their behavior. According to this scheme, nodes that move together are classified as suspect Sybil nodes. Unrelated nodes are the ones that can move freely & amp; independently. These are classified as legitimate nodes. One must observe these suspect Sybil nodes for an extended period to discover their agenda and if necessary, neutralize them. This false-positive phenomenon is caused by the same movement of a group of virtual nodes.

Sethuraman et al. [39] coordinate a more efficient data transfer process by suggesting a redesigned version of the trust-based transmission scheme. In this computation of indirect and direct trust values based on the node's energy level. These metrics are considered while designing a trust system so that content reliability can be measured by the number of errors. It also helps to deal with ambiguity.

Desai et al. [40] have proposed a new approach to predictive modeling that is designed to stop security breaches before they happen. This paper explains how to spot routing attacks during route discovery. It is seen that the singular number attack is just one kind of routing attack-the proposed method here has an intelligent approach to detecting these attacks during route discovery. The predictive method is an ad hoc on-demand linear regression. The comparison of this formulation with the proposed scheme proves that, when applied to ad hoc on-demand applications, it improves service quality.

3 Proposed Work

An algorithm consists of two tiers and multiple trusts for the countermeasure of the Sybil attack. Two-tier multi-trust includes direct trust and indirect trust. Apart from this direct trust is based upon 3 parameters. To check the performance of our model we have used throughput and energy parameters. Trust value is calculated by observing nodes and keeping track of their behavior in terms of forwarding packets, frequency of contacts, etc.

3.1 Assumptions in Model

The clustered framework of MANET is shown in Fig. 1. Clusters are formed using a well-known algorithm [41]. There is a cluster head in each cluster which is responsible for sending packets outside the cluster and monitoring other Sensor Nodes (SNs) within the cluster. The cluster head (CH) is selected using the Proficient Cluster Head selection algorithm (PCHSA) explained in Section 3.2. Each CH is linked to Base Station (BS). The BS has unlimited resources and can remove the Sybil node. BS is uncompromisable by an attacker. It is also assumed that cluster heads are legitimate nodes. As in MANET, sensor nodes are moving so these nodes can change their cluster based on their geographical location. The sensor nodes can communicate with CH directly or through other sensor nodes. The base station initializes the trust value of all nodes. The trust value lies in the range of $[0,\ v-1]$ and the initial trust value assigned by BS is $[(v-1)/2]$. If the trust value $(\mathcal{J})$ of sensor nodes is greater or equal to

$(v-1)/2$ SN is considered as an honest node. For purpose of routing proactive routing, techniques are used within a cluster in the case of proactive routing, routing tables are maintained, so routing is fast and less energy is consumed. While communication in inter-cluster is done using a reactive approach. When nodes transmit packets, their energy is consumed which is known as transmission energy. Let's assume a node has to send k bits/packet to another node which is d meters away then Eq. (1) can be used to calculate transmission energy as [42]

$$E_{T,X}(k,d) = \left\langle \begin{array}{l} k \times E_{elec} + k \times \in_{fs} \times d^2 \\ k \times E_{elec} + k \times \in_{amp} \times d^4 \end{array} \middle| \begin{array}{l} d \le d_0 \\ d > d_0 \end{array} \right\rangle \tag{1}$$

where, E_{elec} is the energy used per bit in transmission or receiving of packets, $\in_{amp}$, and $\in_{fs}$ are multipath fading model and free space model respectively. Similarly, the energy consumed in receiving a k bits/packet can be defined in Eq. (2)

$$E_{RX}(k) = k \times E_{elec} \tag{2}$$

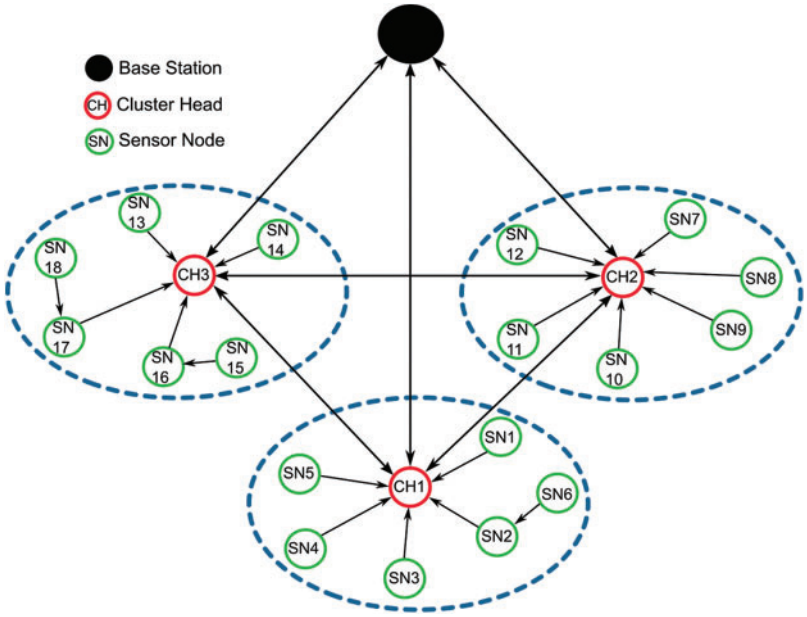

Figure 1: Clustered network

The SNs having an energy of more than 20% of initial energy can take part in routing or communication while SNs with energy less than 20% can perform basic tasks only.

3.2 Proficient Cluster Head Selection Algorithm (PCHSA)

The researchers mainly use distance parameters to select cluster heads. We have considered energy and link quality parameters too for the selection of cluster heads as usage of energy is more than other nodes. So, cluster heads are used in rotation. In PCHSA, apart from distance, we have taken residual energy and link quality into consideration. PCHSA provides a robust approach to select cluster heads so that there is an equal balance of load on all SNs and also to enhance networks life. CH plays an important role in data forwarding and monitoring of nodes. If CH has low energy, it will not be able to perform its task. So, energy is taken into consideration for the selection of CH to have an efficient network. The detailed PCHSA is shown in Algorithm 3.1.

Algorithm 3.1: Proficient Cluster Head Selection Algorithm (PCHSA)

Input: Sensor nodes, coordinates and energy of SNs.

Output: Cluster heads (CHs)

1) for each $i \in N$, calculate the distance of the sensor node with BS using the formula

$$d_i = \sqrt{(S_i(x) - BS(x))^2 + (S_i(y) - BS(y))^2}$$

and store the distance of each node in the array

$d = \{d_1, d_2, d_3 \ldots\ldots\ldots d_N\}$

2) Update the residual energy of each node after a certain interval of time (t) and energy is stored in an array

$e = \{e_1, e_2, e_3 \ldots\ldots\ldots e_N\}$

3) for each $i \in N$, calculate link quality (Q)

$$Q_i = \frac{number\ of\ packets\ send\ by\ S_i}{number\ of\ packets\ recieved\ by\ BS}$$

4) for each $i \in N$, calculate the cluster value (CV)

$$CV_i = w_1 * \frac{1}{d_i} + w_2 * e_i + w_3 * Q_i$$

where $w_1 + w_2 + w_3 = 1$

5) For proficient cluster head (CH) $= \max\{CV_1, CV_2, CV_3 \ldots\ldots CV_4\}$

Repeat steps 1 to 5 after time t to select new cluster heads (CHs)

3.3 Direct Trust

Direct Trust is calculated from the history of a node. Direct trust helps monitor sensor nodes in terms of correct forwarding of the packet, frequency and durability of contacts with other nodes. Whenever a node says SN(A) wants to send information to another node say SN(B) the path selected by them will be based on the trust value of neighbor nodes. To calculate direct trust following parameters will be computed.

3.3.1 Transmission Trust

Transmission trust is based on the correct packets forwarded by a node. To find transmission trust among SN(A) and SN(B) at a time (Δt) ($\mathcal{J}^C_{A,B}(\Delta t)$) is computed using Eq. (3).

$$\mathcal{J}^C_{A,B}(\Delta t) = \left[v \times \left(\frac{C^C_{A,B}(\Delta t) + 1}{C^C_{A,B}(\Delta t) + I^C_{A,B}(\Delta t) + 2} \right)^{\left(\frac{I^C_{A,B}(\Delta t)}{C^C_{A,B}(\Delta t) + I(\Delta t) + 2} \right)} \right] \tag{3}$$

Here, Δt is a time slot for which we have to calculate transmission trust. $C^C_{A,B}$ are the number of correct packets of A which are forwarded by B. $I^C_{A,B}(\Delta t)$ are the number of packets of A not forwarded by B. v is a domain of range.

3.3.2 Frequency Trust

Frequency represents the frequency of contacts between sensor nodes. The greater the frequency of contacts more the node is social and hence can be trusted. The frequency of nodes SN(A), SN(B) with the destination SN(D) is shown in Eq. (4)

$$\mathcal{J}^{F}_{A,B}(\Delta t) = \left[v \times \left(\frac{C^{F}_{A,B}(\Delta t) + C^{F}_{B,D}(\Delta t)}{\sum_{i=1}^{\eta_A} C^{F}_{A,i}(\Delta t) + \sum_{i=1}^{\eta_B} C^{F}_{B,i}(\Delta t)} \right) \right] \tag{4}$$

Here $C^{F}_{A,B}(\Delta t)$ is several contacts between A & B in time interval Δt, $C^{F}_{B,D}(\Delta t)$ are several contacts between B & D, η_A is the total number of neighbors of node A and η_B is a total number of neighbors of node B.

3.3.3 Durability Trust

Durability represents the duration of contact between sensor nodes. If a node is connected with other nodes for a longer period, it means the node is better connected to other nodes and is good for communication. The durability of SN(A) for SN(B) with the destination SN(D) is shown in Eq. (5)

$$\mathcal{J}^{D}_{A,B}(\Delta t) = \left[v \times \left(\frac{D^{D}_{A,B}(\Delta t) + D^{D}_{B,D}(\Delta t)}{\sum_{i=1}^{\eta_A} D^{D}_{A,i}(\Delta t) + \sum_{i=1}^{\eta_B} D^{D}_{B,i}(\Delta t)} \right) \right] \tag{5}$$

Here $D^{D}_{A,B}(\Delta t)$ is the duration of contact between A & B in time interval Δt, $D^{D}_{B,D}(\Delta t)$ is the duration of contact between B & D.

A combination of communication trust, frequency trust and durability trust are used for the detection of Sybil nodes which is computed using Eq. (6)

$$\mathcal{DJ}_{A,B}(\Delta t) = \alpha \times \mathcal{J}^{C}_{A,B}(\Delta t) + \beta \times \mathcal{J}^{F}_{A,B}(\Delta t) + \gamma \times \mathcal{J}^{D}_{A,B}(\Delta t) \tag{6}$$

α, β, γ are weights such that $\alpha + \beta + \gamma = 1$. The weights are adjustable as per application to nullify the effect of the Sybil attack. For example, in military-related services, the weight of α will be high. The trustworthiness status of SNs can be decided according to Eq. (7).

$$S\left(\mathcal{DJ}_{A,B}(\Delta t)\right) = \left\{ \begin{array}{c|c} \left(\left[\frac{v-1}{2} \right] + 1 \right) & \textit{Highly trusted} \\ \left(0; \left[\frac{v-1}{2} \right] \right) & \textit{Sybil Node} \\ \left(\left[\frac{v-1}{2} \right]; \left[\frac{v-1}{2} \right] + 1 \right) & \textit{Legitimate Node} \end{array} \right\} \tag{7}$$

3.3.4 Indirect Trust

Indirect trust is used to prolong the network's life span and also to prevent a network from being bad-mouthing by the Sybil node. In direct trust node, A checks the trust value for node B. When A finds trust value ($\mathcal{DJ}_{A,B}(\Delta t)$) for node B is low or in the category of Sybil node, it will send a message to the cluster head. The cluster head will check indirect trust within a cluster. CH collects information from all SNs within a cluster to get confirmation about the Sybil node. The indirect trust within a cluster for node B at time interval Δt ($\mathcal{IJ}_{CH,B}(\Delta t)$) can be computed using Eq. (8)

$$\mathcal{IJ}_{CH,B}(\Delta t) = \sum_{i=1}^{i=\eta_C} \frac{\mathcal{DJ}_{i,B}(\Delta t)}{\eta_C} \tag{8}$$

Here η_C is the total number of SNs in a cluster for which indirect trust has to be calculated. The trustworthiness of SNs can be decided using Eq. (9).

$$S\left(\mathcal{IJ}_{CH,B}(\Delta t)\right) = \left\{ \begin{array}{l|l} \left(\left[\frac{v-1}{2}\right]+1\right) & \textit{Highly trusted} \\ \left(0;\left[\frac{v-1}{2}\right]\right) & \textit{Sybil Node} \\ \left(\left[\frac{v-1}{2}\right];\left[\frac{v-1}{2}\right]+1\right) & \textit{Legitimate Node} \end{array} \right\} \tag{9}$$

The complete algorithm of TMTACS is shown in Algorithm 3.2

Algorithm 3.2: Trust-Based Sybil Attack Detection

Input–Set of Sensor nodes SNs S $=\{S_1, S_2, \ldots\ldots S_n\}$,

Output–Detection of Sybil Attack in MANET

1. Initialize sensor nodes SNs with coordinates, speed of their movement and direction of movement and trust value $\frac{v-1}{2}$
2. Using Algorithm 1 PCHSA selects CHs
3. Find neighbors for SNs
4. SNs start communicating and forwarding data.
5. Upon encountering nodes share Exchange_List.
6. If energy_of_node> $\mathbb{E}$
   Node will take part in communication
   Else
   Node will perform basic operations only
7. Check energy of nodes after periodic intervals of time
8. Compute transmission trust using Eq. (3)
$$\mathcal{J}^C_{A,B}(\Delta t) = \left[v \times \left(\frac{C^C_{A,B}(\Delta t)+1}{C^C_{A,B}(\Delta t)+I^C_{A,B}(\Delta t)+2} \right) \left(\frac{I^C_{A,B}(\Delta t)}{C^C_{A,B}(\Delta t)+I(\Delta t)+2} \right) \right]$$
9. Compute frequency trust using Eq. (4)
$$\mathcal{T}^F_{A,B}(\Delta t) = \left[v \times \left(\frac{C^F_{A,B}(\Delta t)+C^F_{B,D}(\Delta t)}{\sum_{i=1}^{\eta_A} C^F_{A,i}(\Delta t)+\sum_{i=1}^{\eta_B} C^F_{B,i}(\Delta t)} \right) \right]$$
10. Compute durability trust using Eq. (5)
$$\mathcal{T}^D_{A,B}(\Delta t) = \left[v \times \left(\frac{D^D_{A,B}(\Delta t)+D^D_{B,D}(\Delta t)}{\sum_{i=1}^{\eta_A} D^D_{A,i}(\Delta t)+\sum_{i=1}^{\eta_B} D^D_{B,i}(\Delta t)} \right) \right]$$
11. Check whether data sent by SN A through SN B is delivered to the destination successfully or not
$$\left| R^D_A(\Delta t) - R^D_B(\Delta t) \leq \mathfrak{E} \right|$$

(Continued)

Algorithm 3.2: Continued

12. Compute final direct trust value using Eq. (6)
$$\mathcal{DJ}_{A,B}(\Delta t) = \alpha \times \mathcal{J}^{C}_{A,B}(\Delta t) + \beta \times \mathcal{J}^{F}_{A,B}(\Delta t) + \gamma \times \mathcal{J}^{D}_{A,B}(\Delta t)$$
13. Update new trust values after each predefined slot by assigning $\frac{100 + 10 * \mathcal{DJ}_{A,B}(\Delta t)}{2}$ weight to recent $(\Delta t + 1)$ trust value and $\frac{100 - 10 * \mathcal{DJ}_{A,B}(\Delta t)}{2}$ weight to older (Δt) trust value.
14. While $\mathcal{DJ}_{A,B}(\Delta t) \geq \left[\frac{v-1}{2}\right]$ & $\left|R^{D}_{A}(\Delta t) - R^{D}_{B}(\Delta t) \leq \mathfrak{E}\right|$
    Communication will continue to take place
15. If $\mathcal{DJ}_{A,B}(\Delta t) < \frac{v-1}{2}$
    Node A will tell CH about node B
16. CH will calculate cluster level trust using Eq. (8)
$$\mathcal{IJ}_{CH,B}(\Delta t) = \sum_{i=1}^{i=\eta_C} \frac{\mathcal{DJ}_{i,B}(\Delta t)}{\eta_C}$$
17. If $\mathcal{IJ}_{CH,B}(\Delta t) \geq \frac{v-1}{2}$
    CH will continue to communicate with the SN(B).
    Else
    SN(B) is a Sybil node. CH will send this information to BS.
18. BS will remove that node from the network.

Each SN contains a unique ID and location. As communication starts in-network sensor node starts a logical time slot. Based on successful packet delivery, frequency of contact and duration of contact direct trust values are computed using Eqs. (3)–(6). If a node is suspicious then indirect trust values are calculated using Eq. (8). The table for range of domain (v) for trust estimation w.r.t. v = 4 is given in Tab. 1.

Table 1: Trust estimation (w.r.t. v = 4)

Range of trust values	Sensor node classification
(0, 2)	Sybil node
[2, 3)	Legitimate node
[3, 4]	Highly trusted node

4 Routing Algorithm

In the routing algorithm used for TMTACS the decision to choose a path for transmission of packets is known as Minimal path cost (MPC) which is based on Eq. (10) [41]

$$MPC = w_{\mathcal{J}} \times \mathcal{J}^{D}_{A,B}(\Delta t) + w_e \times Node_{Energy} + w_{hop} \times hop\_count \tag{10}$$

where, $w_{\mathcal{J}} + w_e + w_{hop} = 1$, MPC takes into consideration of trust value, energy, & hop count for the intermediate node. When say node A sends an RREQ frame to node B then if the trust value of node A is high and energy is low node B will ignore the RREQ frame while if the trust value of B is low & energy is high node A will itself discard RREP frame. Hence route selected by TMTACS will be more

efficient. Also, in TMTACS routing tables are maintained inside the cluster which will reduce wait time hence packet delivery ratio & packet delay ratio will improve Routing Algorithm for TMTACS is provided in Algorithm 4.1 and Algorithm 4.2

5 Simulation and Evaluation

The effectiveness of TMTACS is checked using MATLAB R2018a. The proposed scheme is compared with SQEER [43], ATRP [44] and STEAR [45] in terms of severity, packet delivery ratio, Sybil Node detection, Average energy of network and throughput. The performance of a network is also checked by increasing the malicious node percentage. The simulation parameters used for the experiment are shown in Tab. 2.

Algorithm 4.1: Route Discovery

Input: Sensor nodes, threshold_energy ($\mathbb{E}$)
Output: Route discovery

1. Initialize routing tables inside clusters.
2. Update routing tables after a specific interval of time.
3. While ($RREQ_{TTL}>0$)
   Broadcast RREQ frames
4. If ($\mathcal{DT}(\Delta t) \geq \frac{v-1}{2}$ & $Node_{energy} < \mathbb{E}$)
   Discard the RREQ frame by the current node
5. ElseIf ($\mathcal{DT}(\Delta t) < \frac{v-1}{2}$ & $Node_{energy} \geq \mathbb{E}$)
   Reject RREP frame by predecessor node.
6. EndIF
7. If ($node_{current} == node_{destination}$)
   Send RREP and return
   Else
   $RREQ_{TTL} = RREQ_{TTL}-1$
8. End while.

Algorithm 4.2: Forwarding packet

Input: Sensor nodes
Output: Forwarding of message

1. Check if the destination node is in the same cluster

If (source_node.RoutingTable.contains(Destination_node)
Forward message through a predefined path

2. Else
   Find route using Algorithm 4.1
3. Endif

Table 2: Parameter's list used for simulation

List of parameters	Values
Area of network	1000 m × 1000 m
Simulation time	1000 s

(Continued)

Table 2: Continued

List of parameters	Values
Number of sensor nodes	100–500
Radio range of sensor nodes	20 m
Initial energy	5 J
Range of trust (r)	4
Size of packet	512 bytes
Number of sybil nodes	10%–60%

5.1 Packet Delivery Ratio (PDR)

It can be defined as the ratio of the number of packets delivered to the total number of packets sent [46]. It includes RREP and RREQ packets. The network should have a high PDR. High PDR means a more reliable network. The comparative analysis of the proposed scheme with existing techniques is shown in Fig. 2. It can be depicted that the Packet delivery ratio of the proposed scheme is better than existing techniques because in the proposed scheme hybrid routing is used. Routing tables are maintained at the cluster level which improves the packet delivery ratio. Also, while selecting the routing path in the proposed scheme shortest path is selected using hop count which also reduces wait time and thus improves the packet delivery ratio.

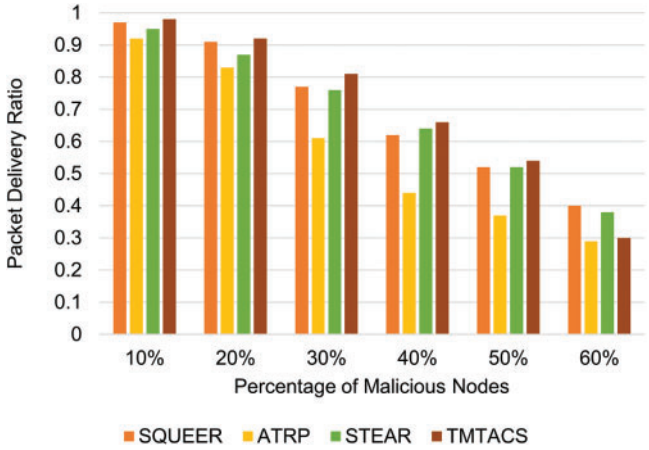

Figure 2: Packet delivery ratio with varying percentages of malicious nodes

5.2 Average Energy Consumed

It is the ratio of the sum of energy consumed by all nodes to the total number of nodes. The average energy consumed for proposed and existing schemes by varying numbers of nodes is shown in Fig. 3. If we consider unit energy is consumed in the transmission of a packet, the average energy consumed by the network directly depends upon the number of transmissions. In the proposed scheme shortest path is chosen hence reducing the number of transmissions and overall consumption of energy. Moreover, using routing tables in clusters will also reduce energy consumption which is used in finding paths every time.

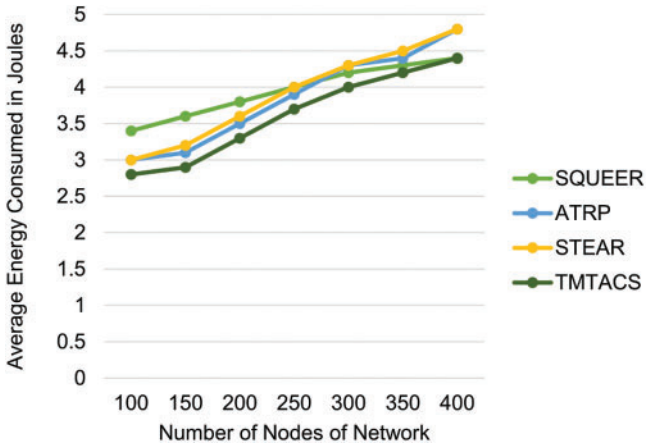

Figure 3: Average energy consumed under attack conditions by a varying number of nodes of the network

5.3 Network Throughput

The ratio of packets received at a destination is network throughput [47]. One might confuse PDR with throughput. To clear the difference between these both consider a case in which packets are added to the buffer in the initial phase due to wait time it will not affect PDR as packets have not entered the system yet but it will affect throughput. On the other hand, if packet delivery is failed 2 or more times there will not be much effect on throughput but PDR will become low. The comparative analysis of network throughput with SQEER, STEAR and ATRP is shown in Fig. 4. TMTACS provides better throughput than existing techniques. TMTACS is better because it chooses an effective path for routing keeping the trust value, energy and hop count of a path. It is efficient in removing faulty nodes. Moreover, the TMTACS trust function is dynamic. CH is selected based on good link quality. Hence throughput of TMTACS is better than existing techniques.

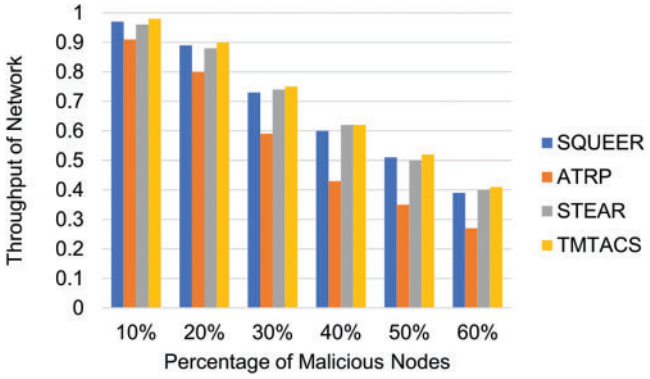

Figure 4: Network throughput by varying percentage of malicious nodes

5.4 Identification of Sybil Nodes

To check the identification of Sybil nodes, the Sybil nodes are injected in-network at a different percentage. Fig. 5 shows several Sybil nodes identified at a varying percentage of malicious nodes. The dynamic trust function is a reason behind the minimal impact on trust value. It is because TMTACS

employs 2 levels of trust value and direct trust is based on 3 factors. Apart from this TMTACS provides an adjustable time slot.

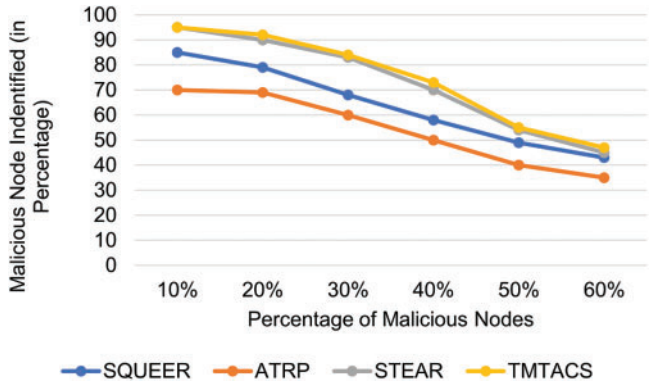

Figure 5: Identification of malicious nodes at various percentage

Figs. 2–5 show that TMTACS is better than existing techniques in terms of PDR, average energy consumed, network throughput and identification of malicious nodes. It is because the TMTACS is dynamic as it detects trust in time slot due to which the nodes which firstly show appropriate behavior to remain undetected are also got detected. Also, in the case of selecting a route for sending a packet the trust value, minimum hop count and residual energy are taken into consideration due to which efficient short path is selected which is robust also.

6 Conclusion

Sensitive data is transferred using sensor nodes in MANET. So, the security of this data is a major concern. In a recent study, a complete security solution, as well as efficient routing with minimum hops, is provided. Firstly, an algorithm to select cluster heads efficiently is explained. Also, the cluster head selected is changed after a periodic time interval to maintain load balancing. Then trust functions are explained in which there are two tiers of security by employing direct trust and indirect trust. There are 3 factors in the case of direct trust namely communication trust, frequency trust and durability trust. Afterward, if direct trust is low for some nodes cluster head will calculate indirect trust. If the indirect trust will be below the base station be informed and the Sybil node will be removed by the Base station. The performance of a proposed scheme is checked with existing schemes in terms of severity, packet delivery ratio, Sybil Node detection, Average energy consumption of network and throughput. The results show that the proposed scheme is better in terms of packet delivery ratio, average energy consumed and network throughput. Also, the impact of malicious nodes on trust value is minimum in TMTACS. So, it is highly suitable for many applications. In the future, we want to modify TMTACS so that it can be used for IoT-based applications.

Acknowledgement: The authors wish to thank many anonymous referees for their suggestions to improve the paper. Meena Bharti would like to thank I.K. Gujral Punjab Technical University for offering the Ph.D. course in Computer Science & Engineering and providing support to access the resources for research.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] H. Nishiyama, M. Ito and N. Kato, "Relay-by-smartphone: Realizing multihop device-to-device communications," *IEEE Communications Magazine*, vol. 52, no. 4, pp. 56–65, 2014.

[2] C. E. Fossa and T. G. Macdonald, "Internetworking tactical manets," in *2010-Milcom 2010 Military Communications Conf.*, San Jose, CA, USA, pp. 611–616, 2010.

[3] P. Ghosekar, G. Katkar and P. Ghorpade, "Mobile ad hoc networking: Imperatives and challenges," *IJCA Special Issue on MANETs*, vol. 3, pp. 153–158, 2010.

[4] B. Pourghebleh, K. Wakil and N. J. Navimipour, "A comprehensive study on the trust management techniques in the internet of things," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 9326–9337, 2019.

[5] P. Shah and T. Kasbe, "Detecting sybil attack, black hole attack and DoS attack in VANET using RSA algorithm," in *2021 Emerging Trends in Industry 4.0 (ETI 4.0)*, Raigarh, India, pp. 1–7, 2021.

[6] J. R. Douceur, "The sybil attack," in *Int. Workshop on Peer-to-Peer Systems*, Berlin, Heidelberg, pp. 251–260, 2002.

[7] S. Ali, M. A., Khan, J., Ahmad, A. W., Malik and ur. A., Rehman, "Detection and prevention of black hole attacks in IOT & WSN," in *2018 Third Int. Conf. on Fog and Mobile Edge Computing (FMEC)*, Barcelona, Spain, pp. 217–226, 2018.

[8] M. Arifeen, A. Al Mamun, T. Ahmed, M. S. Kaiser and M. Mahmud, "A blockchain-based scheme for sybil attack detection in underwater wireless sensor networks," in *Proc. of Int. Conf. on Trends in Computational and Cognitive Engineering*, Singapore, pp. 467–476, 2021.

[9] C. Pu and K. -K. R. Choo, "Lightweight sybil attack detection in IoT based on bloom filter and physical unclonable function," *Computers & Security*, vol. 113, pp. 102541, 2022.

[10] X. Zhang, W. Zhang, W. Sun, X. Sun and S. K. Jha, "A robust 3-D medical watermarking based on wavelet transform for data protection," *Computer Systems Science and Engineering*, vol. 41, no. 3, pp. 1043–1056, 2022.

[11] X. Zhang, X. Sun, X. Sun, W. Sun and S. K. Jha, "Robust reversible audio watermarking scheme for telemedicine and privacy protection," *Computers Materials & Continua*, vol. 71, no. 2, pp. 3035–3050, 2022.

[12] J. Newsome, E. Shi, D. Song and A. Perrig, "The sybil attack in sensor networks: Analysis & defenses," in *Third Int. Symp. on Information Processing in Sensor Networks, 2004. IPSN 2004*, Berkeley, CA, USA, pp. 259–268, 2004.

[13] A. Nadeem and M. P. Howarth, "A survey of MANET intrusion detection & prevention approaches for network layer attacks," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 4, pp. 2027–2045, 2013.

[14] M. Gupta, P. Judge and M. Ammar, "A reputation system for peer-to-peer networks," in *Proc. of the 13th Int. Workshop on Network and Operating Systems Support for Digital Audio and Video*, Monterey, California, USA, pp. 144–152, 2003.

[15] K. Venkatraman, J. V. Daniel and G. Murugaboopathi, "Various attacks in wireless sensor network: Survey," *International Journal of Soft Computing and Engineering (IJSCE)*, vol. 3, no. 1, pp. 208–212, 2013.

[16] J. Dinger and H. Hartenstein, "Defending the sybil attack in P2P networks: Taxonomy, challenges, and a proposal for self-registration," in *First Int. Conf. on Availability, Reliability and Security (ARES'06)*, Vienna, Austria, pp. 8–763, 2006.

[17] M. A. Jan, P. Nanda, X. He and R. P. Liu, "A sybil attack detection scheme for a centralized clustering-based hierarchical network," in *2015 IEEE Trustcom/BigDataSE/ISPA*, Helsinki, Finland, pp. 318–325, 2015.

[18] O. B. Baban, "Survey on literature detection methods of sybil attack in WSN," *International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)*, vol. 4, no. 10, pp. 67–72, 2017.

[19] S. Abbas, M. Merabti, D. Llewellyn-Jones and K. Kifayat, "Lightweight sybil attack detection in manets," *IEEE Systems Journal*, vol. 7, no. 2, pp. 236–248, 2012.
[20] K. A. Awan, I. U. Din, M. Zareei, M. Talha, M. Guizani *et al.,* "Holitrust-a holistic cross-domain trust management mechanism for service-centric internet of things," *Special Section on Mobile Edge Computing and Mobile Cloud Computing: Addressing Heterogeneity and Energy Issues of Compute and Network Resources, IEEE Access*, vol. 7, pp. 52191–52201, 2019.
[21] A. Arabsorkhi, M. S. Haghighi and R. Ghorbanloo, "A conceptual trust model for the internet of things interactions," in *2016 8th Int. Symp. on Telecommunications (IST)*, Tehran, Iran, pp. 89–93, 2016.
[22] N. Alsaedi, F. Hashim, A. Sali and F. Z. Rokhani, "Detecting sybil attacks in clustered wireless sensor networks based on energy trust system (ETS)," *Computer Communications*, vol. 110, pp. 75–82, 2017.
[23] R. Priyadarshi, P. Rawat, and V. Nath, "Energy dependent cluster formation in heterogeneous wireless sensor network," *Microsystem Technologies*, vol. 25, no. 6, pp. 2313–2321, 2019.
[24] D. Xie, Q. Zhou, X. You, B. Li and X. Yuan, "A novel energy-efficient cluster formation strategy: From the perspective of cluster members," *IEEE Communications Letters*, vol. 17, no. 11, pp. 2044–2047, 2013.
[25] I. D. Chakeres and E. M. Belding-Royer, "AODV routing protocol implementation design," in *24th Int. Conf. on Distributed Computing Systems Workshops, 2004. Proc.*, Tokyo, Japan, pp. 698–703, 2004.
[26] G. D'Angelo, F. Palmieri and S. Rampone, "Detecting unfair recommendations in trust-based pervasive environments," *Information Sciences*, vol. 486, pp. 31–51, 2019.
[27] Y. Sun and Y. Zhao, "Dynamic adaptive trust management system in wireless sensor networks," in *2019 IEEE 5th Int. Conf. on Computer and Communications (ICCC)*, Chengdu, China, pp. 629–633, 2019.
[28] A. Boukerch, L. Xu and K. El-Khatib, "Trust-based security for wireless ad hoc and sensor networks," *Computer Communications*, vol. 30, no. 11–12, pp. 2413–2427, 2007.
[29] J. U. Kim, M. J. Kang, J. M. Yi and D. K. Noh, "A simple but accurate estimation of residual energy for reliable WSN applications," *International Journal of Distributed Sensor Networks*, vol. 11, no. 8, pp. 107627, 2015.
[30] J. Zheng, M. Z. A. Bhuiyan, S. Liang, X. Xing, and G. Wang, "Auction-based adaptive sensor activation algorithm for target tracking in wireless sensor networks," *Future Generation Computer Systems*, vol. 39, pp. 88–99, 2014.
[31] W. Liang, J. Long, T. H. Weng, X. Chen, K. C. Li *et al.,* "TBRS: A trust based recommendation scheme for vehicular CPS network," *Future Generation Computer Systems*, vol. 92, pp. 383–398, 2019.
[32] R. S. Bali and N. Kumar, "Secure clustering for efficient data dissemination in vehicular cyber–physical systems," *Future Generation Computer Systems*, vol. 56, pp. 476–492, 2016.
[33] H. Wang, "A Three-tier scheme for sybil attack detection in heterogeneous IWSN," in *MATEC Web of Conf.*, Sanya, China, pp. 1–8, 2020.
[34] S. A. Thorat and P. J. Kulkarni, "Uncertainty analysis framework for trust based routing in MANET," *Peer-to-Peer Networking and Applications*, vol. 10, no. 4, pp. 1101–1111, 2017.
[35] B. Wang, M. Li, X. Jin and C. Guo, "A reliable IoT edge computing trust management mechanism for smart cities," *IEEE Access*, vol. 8, pp. 46373–46399, 2020.
[36] S. Rajbhandari, O. F. Rana and I. Wootten, "A fuzzy model for calculating workflow trust using provenance data," in *Proc. of the 15th ACM Mardi Gras Conf.: From Lightweight Mash-Ups to Lambda Grids: Understanding the Spectrum of Distributed Computing Requirements, Applications, Tools, Infrastructures, Interoperability, and the Incremental Adoption of Key Capabilities*, NewYork, NY, USA, pp. 1–8, 2008.
[37] P. Khatri, S. Tapaswi and U. P. Verma, "Fuzzy based trust management for wireless ad hoc networks," in *2010 Int. Conf. on Computer and Communication Technology (ICCCT)*, Allahabad, India, pp. 168–171, 2010.
[38] C. Piro, C. Shields and B. N. Levine, "Detecting the sybil attack in mobile ad hoc networks," in *2006 Securecomm and Workshops*, Baltimore, MD, USA, pp. 1–11, 2006.
[39] P. Sethuraman and N. Kannan, "Refined trust energy-ad hoc on demand distance vector (ReTE-AODV) routing algorithm for secured routing in MANET," *Wireless Networks*, vol. 23, no. 7, pp. 2227–2237, 2017.

[40] A. M. Desai and R. H. Jhaveri, "Secure routing in mobile ad hoc networks: A predictive approach," *International Journal of Information Technology*, vol. 11, no. 2, pp. 345–356, 2019.
[41] T. Khan, K. Singh, M. H. Hasan, K. Ahmad, G. T. Reddy *et al.,* "ETERS: A comprehensive energy aware trust-based efficient routing scheme for adversarial WSNs," *Future Generation Computer Systems*, vol. 125, pp. 921–943, 2021.
[42] T. M. Behera, U. C. Samal and S. K. Mohapatra, "Energy-efficient modified LEACH protocol for IoT application," *IET Wireless Sensor Systems*, vol. 8, no. 5, pp. 223–228, 2018.
[43] T. Kalidoss, L. Rajasekaran, K. Kanagasabai, G. Sannasi and A. Kannan, "QoS aware trust based routing algorithm for wireless sensor networks," *Wireless Personal Communications*, vol. 110, no. 4, pp. 1637–1658, 2020.
[44] N. A. Khalid, Q. Bai and A. Al-Anbuky, "Adaptive trust-based routing protocol for large scale WSNs," *IEEE Access*, vol. 7, pp. 143539–143549, 2019.
[45] B. M. Thippeswamy, S. Reshma, V. Tejaswi, K. Shaila, K. R. Venugopal *et al.,* "STEAR: Secure trust-aware energy-efficient adaptive routing in wireless sensor networks," *Journal of Advances in Computer Networks*, vol. 3, no. 2, pp. 146–149, 2015.
[46] A. Tsirigos and Z. J. Haas, "Analysis of multipath routing-part I: The effect on the packet delivery ratio," *IEEE Transactions on Wireless Communications*, vol. 3, no. 1, pp. 138–146, 2004.
[47] A. B. Malany, V. S. Dhulipala and R. M. Chandrasekaran, "Throughput and delay comparison of MANET routing protocols," *International Journal of Open Problems Computational Math*, vol. 2, no. 3, pp. 461–468, 2009.