Security in IoT Mesh Networks Based on Trust Similarity

ATHOTA KAVITHA¹, (Senior Member, IEEE), VIJENDER BUSI REDDY², (Senior Member, IEEE), NINNI SINGH³, VINIT KUMAR GUNJAN⁴³, (Senior Member, IEEE), KURUVA LAKSHMANNA⁴, ARFAT AHMAD KHAN⁵, AND CHITAPONG WECHTAISONG⁶

¹JNTUH College of Engineering, JNTU University, Hyderabad, Telangana 500090, India
²Advanced Data Processing Research Institute, Secunderabad, Telangana 500009, India
³CMR Institute of Technology, Hyderabad, Telangana 500008, India
⁴School of Information Technology and Engineering, VIT, Vellore 632014, India
⁵Department of Computer Science, College of Computing, Khon Kaen University, Khon Kaen 40002, Thailand
⁶School of Telecommunication Engineering, Suranaree University of Technology, Nakhon Ratchasima 30000, Thailand

Corresponding authors: Arfat Ahmad Khan (arfatkhan@kkku.ac.th) and Chitapong Wechtaisong (chitapong@g.sut.ac.th)

This work was supported in part by the Department of Computer Science, College of Computing, Khon Kaen University, Thailand; and in part by the Suranaree University of Technology, Thailand.

ABSTRACT Internet of Things (IoT) Mesh networks are becoming very popular to enable IoT devices to communicate without relying on dedicated PC services. The Internet of Things (IoT) implicitly uses mesh networks. IoT connectivity to cloud and edge computing is in vogue. A Wireless Mesh Network (WMN) is a multi-hop and distributed wireless network with mesh routers and mesh clients. Data originating from mesh clients are forwarded to destinations through mesh routers. In IoT Mesh networks, mesh clients are IoT devices. The crucial security issue with these networks is the lack of a trusted third party for validation. However, trust between nodes is required for the proper functioning of the network. WMNs are particularly vulnerable as they rely upon cooperative forwarding. In this research work, a secure and sustainable novel trust mechanism framework is proposed. This framework identifies the malicious nodes in WMNs and improves the nodes’ cooperation. The proposed framework or model differentiates between legitimate and malicious nodes using direct trust and indirect trust. Direct trust is computed based on the packet-forwarding behavior of a node. Mesh routers have multi-radios, so the promiscuous mode may not work. A new two-hop mechanism is proposed to observe the neighbors’ packet forwarding behavior. Indirect trust is computed by aggregating the recommendations using the weighted D-S theory, where weight is computed using a novel similarity mechanism that correlates the recommendations received from different neighbors. Dynamic weight computation calculates the overall trust by using several interactions. We present the evaluations to show the effectiveness of the proposed approach in the presence of packet drop/modification attacks, bad-mouthing attacks, on-off attacks, and collusion attacks by using the ns-2 simulator.

INDEX TERMS Sustainable network, mesh networks, IoT, trust, similarity, recommendation based trust.

I. INTRODUCTION

Internet of Things (IoT) is a revolutionary technology in 21st century. A thing in IoT is an embedded computer with networking and sensing capabilities. As IoT networks are growing, the communication gap is also increasing with the Internet and more infrastructure is required to exchange data with the base station. When Wireless Mesh Network (WMN) infrastructure is used; mesh router(s) can be placed between IoT and Internet. So, many IoT networks can be connected to WMNs. A WMN gateway can be used to connect to the Internet. WMNs are increasingly deployed in IoT, machine-to-machine communication, and broadband Internet access. Mesh routers connect to heterogeneous networks including both wired and wireless networks [1]. A mesh network contains mesh routers, mesh clients and gateways [2].
Mesh clients are mostly IoT devices. Traditional IoT devices depend on the cloud to relay messages by using cellular or Wi-Fi connectivity. This works better in a standalone system but sometimes we want to establish a connection to the Internet and also create a local network to join other IoT devises [1]. Recently mesh networks reached a maturity level with approachable cost. So, Wireless mesh networking became a viable solution for industrial and commercial IoT applications such as smart cities, health care, smart home, farming, and industrial Internet [1]. WMNs are used as backbone networks for the Internet of Things and sensor networks [2].

Since IoT is characterized by different devices and these devices are connected to heterogeneous networks, security issues are possible. Research in IoT Security is getting priority in recent years and also trust computation has not matured enough in IoT [3]. A scalable framework is needed to deal with these security threats because IoTs are dynamic networks [4]. Authentication is used to prevent unauthorized access. Data protection can be done by encrypting the data. Trust is the main issue [5] because the data exchange between two IoT devices should be reliable. Fig. 1 shows a sample IoT Wireless Mesh Network (WMN) that contains mesh routers and IoT devices. Mesh routers are connected to each other and form a network. IoT devices are connected to mesh routers and get services from the network. IoT devices’ data will be sent to the cloud through WMN.

WMNs are classified into three categories [6]: Fully managed (nodes managed by ISP), Semi managed (Only few nodes managed by ISP) and Unmanaged networks (No management). As mesh networks are ad-hoc (semi-managed or unmanaged) no third-party authority manages mesh networks.

Semi-managed and unmanaged networks have several security issues with attacks originating from inside as well as outside the network. Some are [7] Packet dropping/modification attacks, On-Off attacks, Bad mouthing attacks, and Collusion attacks. In Packet dropping attack, malicious nodes drop packets with some probability. Badmouthing attack happens when the trust is computed based on the recommendation. When a node uses recommendations to compute the trust, badmouthing attacks are conceivable. Malicious nodes provide incorrect recommendations to lower a legitimate node’s trust values. In a collusion attack, a group of nodes collaborates and submit false suggestions about a target node to diminish the trust value.

This article discusses a novel trust model to reduce packet-dropping/modification attacks, badmouthing attacks and collusion attacks. The proposed technique does not require a trusted third party and is dynamic. Mesh routers are Multi-Radio and Multi-Channel (MRMC) networks. A node may not be able to monitor neighbors’ behavior. The neighbor’s behavior is evaluated using a two-hop acknowledgment technique. The two-hop ACK mechanism to observe the neighbor’s forwarding behavior. This is a unique feature of our contribution.

We aggregate the recommendations using weighted Dempster-Shafer (DS) theory. DS theory is one of the best aggregation methods when there is uncertainty in the values. Badmouthing and collusion attacks are possible in recommendation-based trust models. These attacks can be mitigated if the recommendations are weighted based on the node’s legitimacy in sending recommendations. If all recommendations are weighted equally then bad recommendations also contribute equally to the trust aggregation. Direct trust can be taken as a weighting parameter for the aggregation of recommendations. But this is always not feasible, as sometimes a node may forward the packets properly but gives wrong recommendations. Similarity-based models are best suitable for removing bad recommendations. The basic principle of the similarity model is to compare the behavior of two nodes’ recommendations on common neighboring nodes and compute the recommendation credibility of the node based on the error in the node’s recommendations. Incorporating security measures into the proposed framework ensures that multimedia data and IoT networks can continue to be trusted and kept private.

Following are the contribution of the proposed trust model.

- Every node uses packet forwarding to determine its neighbors. Since mesh nodes are MRMC capability, a two-hop ACK mechanism is used to observe the neighbor’s packet forwarding behavior.
- To determine indirect trust, the recommendations are combined using the weighted Dempster-Shafer (DS) theory. Since nodes are distributed, each node may not know about other nodes confidently. In this scenario, DS theory is best suited for aggregation. Here, weight refers to a node’s recommendation credibility.
- The similarity between two nodes in the recommendation behavior is used to calculate recommendation credibility.
- The weighted mean of indirect and direct trust is used to calculate the overall trust value. Weight is quantified depending on the frequency of interactions with that particular node. If interactions are more then direct trust will have more weight.
- The proposed methodology is amalgamated with AODV protocol [7] and evaluates the performance based on the parameters such as packet dropping, badmouthing, Collusion, and on-off attacks.

Following is the breakdown of this research article. Some of the common trust mechanisms in WMNs are briefly described in section 2. The system model and assumptions are described in Section 3. The proposed trust model’s security analysis and trust mechanism are presented in Section 4. The trust mechanism’s simulation results are shown in Section 5. In section 6, we finally conclude the paper.

II. TRUST IN IOT MESH NETWORKS

This section discusses the basic trust concepts as well as certain trust models that were developed for wireless mesh networks.
A. TRUST CONCEPTS
Trust is defined as an individual belief about the future behavior of a node which is based on past experience [8]. The reputation of a node is the trust that other nodes hold on this node. It is a global perception [8].

In this study, trust is evaluated on a continuous scale from 0 to 1, where 0 indicates distrust and 1 indicates complete trustworthiness. An individual node's trust may be computed either in centralized or distributed computation approaches. In the centralized model, trust is determined at the central server and distributed to every network node, while in a distributed model, trust is quantified individually by every node. Each approach has its own merits and demerits. IoT mesh networks are best adapted for the distributed model because the mesh network's nodes are independent. The two strategies employed in the distributed model, i.e., indirect trust and direct trust computing. Indirect trust is determined based on a neighbor's recommendation, while direct trust depends on experience. Direct and indirect trust computation models are both used in hybrid models.

The proposed distributed trust model quantifies the trust in IoT Mesh networks.

B. RELATED WORK
In this section, we briefly discuss some of the popular trust computation models in Mesh networks and IoT.

In a network, a node's behavior may not be consistent. In the case of nodes with limited resources (communication, capacity, battery power, computation, etc.), a node may turn 'selfish' in order to conserve resources. Bin Xie et al. [6] analyze a node's selfishness in WMNs, especially in presence of multi-operator networks. They also summarize various collaborative schemes to mitigate selfish behavior. The authors discuss selfish behavior in different network stack layers and suggest the replacement of promiscuous mode because of multi-radio networks.

A malicious node may modify or inject the packets into the network. SPAIS [9] is a novel mechanism to mitigate packet modification attacks in WMNs. The authors propose a direct trust approach with a watchdog mechanism.
mechanism is not possible in multi-radio networks because a node may not overhear its neighboring node’s activities in a promiscuous mode. Therefore in this work, we have proposed a novel approach to overcome this problem in section IV.

Heng et al. [10] proposed a trust model for wireless mesh networks to mitigate badmouthing attacks. Authors use the correlation method to filter out the bad recommendations. After filtering the recommendations D-S theory is used to aggregate the recommendations. Direct trust is computed based on the forwarding behavior of a node. Indirect trust is evaluated with the direct trust parameters as weight. The authors evaluate their method against entropy-based methods and probability-based methods.

Rida et al. [11] proposed a trust model for WMNs by using statistical detection methods. It uses CUSUM and KS tests to compute the trust. The CUSUM test is used to identify the normal (H0) and abnormal behavior (H1) of a node. KS test is used to compare the total packet loss with the control packets. Trust value is computed based on the result given by the KS test. The trust value is computed using the exponential average method to forget the older values [12], [13].

Yinpeng et al. [14] proposed a cluster-based trust model for WMNs. It computes direct reputation based on beta distribution and indirect reputation is computed based on recommendations from cluster members. Trust of cluster head and gateway is computed based on the risk factor of connecting nodes [15], [16]. Cluster head reputation is computed based on the risk factor of cluster members and gateway. However, authors consider only packet drop attacks. This model assumes all the recommendations are legitimate which is not possible in real scenarios.

Duan et al. [17] proposed a trust model for the effective use of energy. The authors used bandwidth usage and energy completion to derive trust. Game theory is used to make decisions based on trust replies received from neighbors.

Al-Hamadi et al. [18] proposed a decision-making system based on trust for health IoT systems. Reliability, loss of health probability, and risk classification are used to establish trust. Furthermore, this trust value is used to determine the risk of the node and the accuracy of the IoT devices. The value of these parameters is quantified depending on the IoT device’s query and response.

Zhu et al. [19] proposed a survey on recommender systems. The authors also explained the importance of similarity mechanisms such as Pearson correlation, Cosine correlation and Root Mean Squared difference.

The recommendations received from neighbors are uncertain. Aggregating these recommendations accurately require a good ensemble method. DS theory [23] is one of the best ensemble methods when data is uncertain. NBBTE [24] use DS evidence theory to combine the recommendations. They have not considered the credibility of recommendations and are susceptible to bad-mouthing attacks. They have not analyzed the performance in presence of malicious nodes. A trust management strategy for MANETs is proposed in the [25] using both recommendation and observation. The recommendations are combined using DS evidence theory. This model aggregates all recommendations with equal weight. This mechanism does not distinguish recommendations based on the node’s behavior, which leads to bad-mouthing attack [26], [27].

Before aggregating the recommendations, a node must verify the credibility of the recommender. Assigning same weight to each recommender may not be correct because all nodes may not give proper recommendations. If a malicious node sends wrong recommendations then assigns equal weight to all recommendations may give inaccurate indirect trust value. The weight of a recommendation can be computed based on the recommender’s behavior.

Yongmoo et al. [28] presents a survey on recommender systems where he explained the importance of similarity measure in recommender systems. The authors also explained the similarity mechanisms such as Pearson correlation, Cosine correlation and Root Mean Squared difference.

This section describes the pre-requisite of the proposed methodology. Every node in the mesh network has a similar configuration, such as communication hardware, memory, initial energy, and computational power. Every node in the mesh network has a unique Id that cannot change. The network is a flat model where the mesh client sends data to another mesh client.

A. ATTACK MODEL

There are many attacks in mesh networks [29], [30], [31]. We have concentrated on important attacks like packet dropping/ modification attacks, on-off attacks, bad-mouthing attacks, and collusion attacks. The malicious node modifies the contents of the packet before passing it on to the following node in a packet modification attack. A hostile node exhibits alternately good and poor behavior in an on-off attack. When a neighbor node’s trust value decreases, it exhibits positive behavior for a while to restore its trust value. Once its service is done, it acts in a bad-node manner. The detection of such on-off behavior is a challenging task. When recommendations on indirect trust computations are used, there is a chance of a collusion attack where nodes group and raise trust levels to become legitimate nodes [32], [33].
Direct trust is computed from the node’s forwarding behavior. Two-hop ACK is shown in Figure 3. The fields are similar to node can create this acknowledgment. The packet format of forwarded the packet. We are assuming that the acknowledg-

Two-hop Acknowledgment scenario.

FIGURE 3. Two-hop Acknowledgment packet format.

basis for computing indirect trust (IT). Indirect and direct trust are combined to calculate overall trust.

**Forwarding Acknowledgment**

An acknowledgment is a packet that traverses in the reverse direction, that is, destination to source, and indicates successful delivery of the packet. Two-hop acknowledgment (Two-hop ACK) is a special type of acknowledgment packet which traverses only two hops. Figure 2 shows the two-hop ACK scenario. When a node receives two-hop ACK from its two-hop neighbor, it assumes that the neighbor has successfully forwarded the packet. We are assuming that the acknowledgment is generated with its source signature so that no other node can create this acknowledgment. The packet format of Two-hop ACK is shown in Figure 3. The fields are similar to route-reply packet [7], [34], [35].

**A. DIRECT TRUST DT\(_B^A(t)\)**

Direct trust is computed from the node’s forwarding behavior. \(DT_B^A(t)\) is the direct trust on node \(B\) calculated by node \(A\). Since mesh routers have multi-radio and multi-channel wireless connectivity, promiscuous mode is not possible. So, we use two-hop ACK to compute direct trust.

Figure 2 shows four nodes \(A, B, C, D\), which are intermediate nodes in a route. Node \(A\) first sends data to node \(B\) then node \(B\) forwards data to node \(C\). Node \(C\) creates ACK and sends it to node \(A\). When node \(A\) receives ACK from node \(C\) it increases the forwarding count of the neighboring node \(B\). The forwarding Ratio computes the ratio between the number of packets correctly forwarded and a number of packets sent.

\[
\text{Forwarding ratio } FR_B^A(t) = \frac{p_t}{p_t + q_t} \tag{1}
\]

where
\(p_t=\text{Number of packets forwarded by node } B\) up to time \(t\).
\(q_t=\text{Number of packets dropped by node } B\) up to time \(t\).

The instantaneous changes of \(FR_B^A(t)\) is shown below. As the Forwarding ratio decreases \(\delta_t\) value increases otherwise it decreases.

If \(FR_B^A(t - 1) > FR_B^A(t)\)

\[
\delta_t = \delta_{t-1} + \alpha \times (FR_B^A(t-1) - FR_B^A(t)) \tag{2}
\]

Else

\[
\delta_t = \delta_{t-1} + \beta \times (FR_B^A(t-1) - FR_B^A(t)) \tag{3}
\]

where \(\alpha < \beta\)

\(\alpha\) is a punishment factor. \(\beta\) is the encouragement factor.
\(\delta_t\) represents the momentary differences in a node’s behavior.

The direct trust parameter is computed as follows. \(DT_A^B(t)\) is the direct trust value computed on node \(B\) by node \(A\).

\[
DT_A^B(t) = FR_B^A(t) \times \cos(\frac{\pi}{2} \times \delta_t) \tag{4}
\]

In equation 5, \(\delta_t\) shows the fluctuations in the node’s behavior. If fluctuations are high then \(\delta_t\) increases. Therefore, the \(\cos(\cdot)\) function value decreases, and thereby direct trust decreases. Direct trust assesses both forwarding behavior as well as behavior fluctuations of a node.

**B. RECOMMENDATION CREDIBILITY (R)**

Recommendation credibility gives the node’s capability to send recommendations. We use root mean the square difference to compute the similarity between two recommendations.

\(R_A^B(t)\) is the recommendation credibility of node \(B\) at node \(A\), computed as follows:

Let \(K_{AB}\) is a set of common neighbors to node \(A\) and node \(B\). Then

\[
DR_A^B(t) = \sqrt{\sum_{i \in K_{AB}} (DT_A^B(t) - DT_B^A(t))^2} \tag{5}
\]

where \(DT_A^B(t)\) is the direct trust on node \(x\) at node \(A\).

\(DR_A^B(t)\) represents the root mean square difference between the evaluation of node \(x\) by nodes \(A\) and \(B\). The sensitivity to differences of \(DR_A^B(t)\) may reduce if there is more similarity in the \(DT\) values and if the number of common neighbors is high. Here this is a novel measure to compute dissimilarity in trust. The squared difference of trust is normalized over the number of neighbors.

Thus recommendation credibility \(R_A^B(t)\) which is dependent upon the difference error \(DR_A^B(t)\) is computed as follows:

\[
R_A^B(t) = (1 - DR_A^B(t)) \times \frac{\sum_{i \in |K_{AB}|} (x_i \land y_i)}{n} \tag{6}
\]

where \(n\) is the total number of recommendations. \(X\) is the set of direct trust values on neighboring nodes. \(Y\) is the set
of recommendations sent by a particular neighbor, $B$. $x_i \in X$, $y_i \in Y$. $x_i \land y_i = I$ if both sets show similar legitimate neighbor behavior otherwise the value is 0 which is similar to binary AND operation.

**C. INDIRECT TRUST**

Indirect trust is computed based on the recommendations received from the neighboring nodes. These are useful to judge the trustworthiness of neighbor nodes. The recommendations received from neighbors are independent and uncertain. One of the best ways to aggregate uncertain recommendations is Dempster-Shafer (DS) evidence theory. Instead of using simple DS theory on recommendations, we use weight in recommendation aggregation. Here weight is Recommendation credibility value.

**Dempster-Shafer(DS) Theory [23]:**

DS theory use the belief function to represent the evidence received from each recommender. These belief functions are combined using Dempster’s combination rule.

**Definition (36):** A mass function is defined over a frame $\Omega$ is a function $m : 2^\Omega \rightarrow [0, 1]$ such that the following two conditions hold

1. $m(\phi) = 0$
2. $\sum_{A \subseteq \Omega} m(A) = 1$

$m(A)$ is a measure of the belief that is assigned to exactly the set $A$. The belief function $Bel$ on $m$ is $\forall A \subseteq \Omega, Bel(A) = \sum_{B \subseteq A} m(B)$

Let $\Omega$ is a power set contains {Legitimate, Malicious} where Hypothesis $H = \{Legitimate\}$, $\bar{H} = \{Malicious\}$ and $U = \Omega$. Let $m^B_i$ and $m^B_y$ be the mass functions of the Bel of node $x$ and Bel of node $y$ respectively. Each hypothesis assigned a value between $[0, 1]$.

Let the trust value of $B$ at $x$ is $T^B_x$. The trust values from different sources are independent of each other and the recommendations from each recommender on target may be uncertain. There must be some weight to represent the credibility of the recommender. Here we are calling weight as recommendation credibility($R$).

If node $p$ and node $q$ are neighbours then the value of mass function is

$$m^B_p(H) = \frac{R^B_x \times T^B_q}{\sum_{x \in W - \{p\}} R^B_x}$$

$$m^B_p(\bar{H}) = 0.$$  

$$m^B_p(U) = 1 - \frac{R^B_x \times (T^B_q)}{\sum_{x \in W - \{p\}} R^B_x}$$

where $W$ is the set of neighbors to $q$ and $x \in W$.

The Dempster’s combination rule of $m^B_x$ and $m^B_y$ is [25]:

$$m^B_x(\bar{H}) \oplus m^B_y(\bar{H}) = \frac{1}{K} [m^B_x(H)m^B_y(\bar{H}) + m^B_x(\bar{H})m^B_y(H) + m^B_x(H)m^B_y(U) + m^B_x(U)m^B_y(H)]$$

$$m^B_x(U) \oplus m^B_y(U) = \frac{1}{K} [m^B_x(U)m^B_y(U)]$$

where

$$K = m^B_x(H)m^B_y(H) + m^B_x(H)m^B_y(U) + m^B_x(U)m^B_y(H) + m^B_x(U)m^B_y(U) + m^B_x(H)m^B_y(\bar{H}) + m^B_x(\bar{H})m^B_y(H) + m^B_x(H)m^B_y(U) + m^B_x(U)m^B_y(U)$$

The trust value of node $B$ is $bel(H) = m^B_x(H) \oplus m^B_y(H)$. Indirect Trust $IT^B_A(t)$ is the indirect trust on node $B$ calculated by node $A$.

$$IT^B_A(t) = \tau \times DT^B_A(t) + (1 - \tau) \times IT^B_A(t)$$

where $\tau$ is the weight of direct trust which can be calculated as follows.

$$\tau = \frac{I_t(A, B)}{I_t(A, B) + M_t(A, B)}$$

where

$I_t(A, B)$ = Number of packets forwarded by node $B$ of node $A$.

$M_t(A, B) =$Mean of total number of packets forwarded by $B$ except $A$’s packets.

A number of interactions ($I_t(A, B)$) increase, $\tau$ also increases. So, the weight of the direct trust increases. The node becomes more experienced and increases the belief on its own judgment.

$M_t(A, B)$ is the average of the total number of packets forwarded by node $B$ other than node $A$’s packets. Similar to recommendation sharing, neighbors may also send a wrong number of interactions. So, the number of interactions are normalized by using recommendation credibility to compute $M_t(A, B)$. The importance of variable $\tau$ is used to give weightage to direct and indirect trust as per Equation 5 and computation of $\tau$ value as given in Equation 6. When there is more direct interaction direct trust will give significant information about neighbors. If direct interactions are low then $\tau$ value is computed through periodic information (recommendations) received from other neighbor nodes. So when direct interactions are more, high priority is given to direct trust otherwise indirect trust is given high priority. In the implementation, recommendations are the special packets that contain other
neighbor nodes’ trust values and are shared periodically. Recommendations are used to compute the indirect trust. Direct trust is computed based on the number of packets forwarded by the neighbor. Overall trust is computed as per Equation 5.

\[ M_t(A, B) = \sum_{x\in K_B} (R_A^x \times I_p(x, B)) \]

\[ K_B \] is the set of nodes that have communicated with node \( B \), and \( |K_B| \) is the cardinality.

### E. COMPUTATION COST

Overall Trust is computed in two scenarios

1. When a node receives recommendations from the neighboring node
2. When a node receives two hop ACK from the neighboring node.

Trust value is updated in the trust table after computing the overall trust. The worst case complexity of updating the trust value is \( O(m) \) where \( m \) is the number of neighbors.

### F. SPACE REQUIREMENTS

Trust table contains the trust parameters of the neighboring node. neighbor id, direct trust, indirect trust, \( Itpq \), \( Mtpq \), \( OT \) occupies \( x \) bytes of each parameter. Recommender’s parameters like recommender id, trust, \( Itpq \) occupies \( x \) bytes of each parameter. If there are \( m \) neighbors and \( i \) recommenders for each neighbor then the space requirement for the trust table at every node is \( m \times [6 \times x + i \times (3 \times x)] \) bytes.

### G. OVERHEAD ANALYSIS

We use two-hop ACKs to assess the neighbors’ behavior in the proposed trust model. The number of ACKs in the path depends on the path length. Let us assume that path length from source to destination is \( k \) hops. The number of two-hop ACKs becomes \( k \) for one data packet from destination to source.

If there are \( p \) packets in one session then the total number of two-hop ACKs will be \( p \times k \).

Assume that the size of two-hop ACK is \( \varphi \) and the data packet is \( \vartheta \) then the total overhead in one session due to two-hop ACKs will be

\[ \text{Overhead due to two-hop ACK is} = k \times \frac{\varphi}{\vartheta} \]

We have discussed computation cost, space requirement, and overhead analysis for better understanding however we can minimize the overhead by using optimization mechanisms such as piggybacking and cumulative acknowledgments.

### V. EVALUATION

In this section, we present the performance of the proposed model. We analyzed the recommendation credibility accurately computes the similarity value between two nodes. We also analyze the strength of the trust model in presence of packet dropping, on-off, bad-mouthing, and collusion attacks. The proposed trust model is integrated with AODV in ns-2 [37] and named as TWMN.

### A. RECOMMENDATION CREDIBILITY EVALUATION

We have analyzed the performance of recommendation credibility with some popular similarity measures. The similarity measures used for evaluation are: Pearson correlation (PCC), Cosine correlation and Root Mean Squared difference (RMS) [28], [38], [39].

Figure 4 gives PCC, Cosine similarity, RMS similarity, and proposed recommendation credibility values of six example data sets. Even though \( X \) and \( Y \) sets are showing similar values in DATA-I (in Figure 4) but PCC shows a lower value. The data sets \( X \) and \( Y \) are independent of each other so PCC may not give an accurate value. DATA-II (in Figure 4) shows cosine similarity is high. PCC is not possible on DATA-V (in Figure 4) because the \( Y \) set has the same values. Cosine similarity shows the highest value in all the cases. RMS similarity (RMS_sim) is low when more values are not similar. It is observed that no similarity mechanism works perfectly on all kinds of data. The proposed parameter \( R_2 \) shows the better value for all six types of data sets. It is shown that the proposed recommendation credibility accurately computes the similarity value between two nodes.

### VI. EXPERIMENTAL EVALUATION

In this section, we present the performance of the proposed model. We have implemented the proposed trust model in ns-2 [37] and integrated it with AODV [7], [40], [41] routing protocol. 26 nodes are placed randomly in an area of \( 1200 \times 900 \) \( m^2 \) by using NSG [42] topology generator. Malicious nodes are deployed randomly in the network. The results are taken in presence of badmouthing and collusion attacks. Malicious nodes form groups and send bad recommendations on legitimate nodes and good recommendations on collusive nodes. Simulation parameters are given in Table 1.

### A. ANALYSIS ON PACKET DROPPING ATTACK

The objective of this simulation is to show the TWMN’s effectiveness in presence of packet-dropping attacks. Malicious node drops packets randomly with Packet dropping rate \( (Pr)=n \), defined as one packet is dropped randomly in every \( n \) packet. The successful packet delivery to the

| Parameter                  | value  |
|----------------------------|--------|
| Simulation Time            | 600 sec|
| Number of nodes            | 25     |
| Area                       | 1200 x 900 |
| Transmission Range         | 150m   |
| Transport protocol         | UDP    |
| Application protocol       | CBR    |
| Radio interfaces           | 4      |
destination also depends on the number of malicious nodes present in the path.

Assume that the malicious node drops the packet with probability $p$

If there are two malicious nodes in the path then the probability is $p + (1 - p) \times p$

If there are three malicious nodes then the probability is $p + (1 - p) \times p + (1 - p)^2 \times p$ similarly, for $k$ malicious nodes, the packet drop probability is:

$$p + (1 - p) \times p + (1 - p)^2 \times p + \ldots + (1 - p)^{k-1} \times p \quad (9)$$

The eq. 12 evaluates to $1 - (1 - p)^k$

Therefore the probability of successful delivery of the packet if $k$ malicious nodes are present in the path is:

$$(1 - p)^k \quad (10)$$

Figures 5-9 show the trust values of TWMN and ratio methods [25], [43], [44] with $\gamma = 1$ and $\gamma = 3$ values. TWMN is effectively computing the trust values for selective packet droppings also. Simulations show that as packet dropping rate $n$ increases the trust value convergence time also increases. So, malicious node identification time increases. Compared to the ratio method, TWMN is reducing in all scenarios whereas the ratio method is stable at one value in all scenarios

Figure 10 and figure 11 show the trust values of TWMN with different punishment factors i.e $\alpha = 2$ and $\alpha = 4$. It is evident that as punishment factor $\alpha$ increases, trust value reduces drastically because of $\cos(\cdot)$. The trust value is reducing minimum 60% and maximum 90% for $\alpha = 2$ to $\alpha = 4$.

**B. TRUST ACCURACY**

The objective of this simulation is to show the accuracy of the trust model, TWMN. We use Trust Computation Error to denote the accuracy. Trust Computation Error is computed as the Root Mean Square error between the actual trust and

| DATA-I   | DATA-II  | DATA-III  |
|----------|----------|-----------|
| X Y      | X Y      | X Y       |
| 0.790000 | 0.800000 | 0.790000  |
| 0.890000 | 0.930000 | 0.890000  |
| 0.910000 | 0.920000 | 0.910000  |
| 0.960000 | 0.850000 | 0.960000  |
| 0.940000 | 0.930000 | 0.940000  |
| 0.780000 | 0.920000 | 0.780000  |

Pearson= 0.271781
Cosine= 0.996532
RMS_sim = 0.925167
proposed (Eq. 5.4) = 0.925167

| DATA-IV  | DATA-V   | DATA-VI   |
|----------|----------|-----------|
| X Y      | X Y      | X Y       |
| 0.790000 | 0.800000 | 0.790000  |
| 0.260000 | 0.200000 | 0.890000  |
| 0.910000 | 0.100000 | 0.910000  |
| 0.960000 | 0.850000 | 0.960000  |
| 0.940000 | 0.930000 | 0.940000  |
| 0.780000 | 0.100000 | 0.780000  |

Pearson= 0.452139
Cosine= 0.847862
RMS_sim = 0.565182
proposed (Eq. 5.4) = 0.282591

| DATA-VII | DATA-VIII | DATA-IX  |
|----------|-----------|----------|
| X Y      | X Y       | X Y      |
| 0.790000 | 0.800000  | 0.790000 |
| 0.890000 | 0.100000  | 0.890000 |
| 0.910000 | 0.100000  | 0.910000 |
| 0.960000 | 0.100000  | 0.960000 |
| 0.940000 | 0.100000  | 0.940000 |
| 0.780000 | 0.100000  | 0.780000 |

Pearson= -nan
Cosine= 0.996873
RMS_sim = 0.218559
proposed (Eq. 5.4) = 0.000000

| DATA-X   | DATA-XI  |
|----------|----------|
| X Y      | X Y      |
| 0.790000 | 0.800000 |
| 0.890000 | 0.930000 |
| 0.910000 | 0.920000 |
| 0.960000 | 0.850000 |
| 0.940000 | 0.930000 |
| 0.780000 | 0.920000 |

Pearson= 0.695677
Cosine= 0.947871
RMS_sim = 0.718220
proposed (Eq. 5.4) = 0.598517

| DATA-XII | DATA-XIII |
|----------|-----------|
| X Y      | X Y       |
| 0.790000 | 0.800000 |
| 0.890000 | 0.930000 |
| 0.910000 | 0.920000 |
| 0.960000 | 0.850000 |
| 0.940000 | 0.930000 |
| 0.780000 | 0.920000 |

Pearson= 0.347766
Cosine= 0.903249
RMS_sim = 0.615747
proposed (Eq. 5.4) = 0.410948

**FIGURE 4.** PCC, Cosine correlation, RMS similarity and proposed similarity method ($\beta^3_A$) values of example data sets.
expected trust values. The expected trust value for a legitimate node is 1 and for a malicious node is 0.

In this simulation, nodes in the network start behaving in a malicious manner at random. These nodes send bad recommendations to legitimate nodes in a non-collusive manner (mode). In collusive mode, malicious nodes form a group and send good recommendations to group members, and bad recommendations to legitimate nodes. Simulations are run with different source-destination pairs. After 600 seconds a legitimate node is selected and its trust accuracy is computed based on the trust assessments of neighbors present in the trust table. Figure 12 shows the trust computation error in presence of collusive and non-collusive modes. In both modes, trust computation error is low i.e. the trust model accurately identifies the malicious nodes.
C. TRUST VALUE COMPUTATION

This simulation aims to demonstrate how the TWMN computes trust values for both malicious and legitimate nodes. Figure 13 shows the trust values of the legitimate and malicious nodes. A legitimate node performs well so the trust value is high. Malicious node shows bad behavior so the trust value decreases and reaches zero.

Figure 14 and 15 show the recommendation credibility value of legitimate and malicious nodes. The recommendation credibility value is quantified in two badmouthing attack scenarios. Figure 14 demonstrates the credibility score of a malicious and legitimate node. Malicious node relay 0.1 recommendation score to a legitimate node. Figure 15 illustrates the credibility score, which complements the trust value i.e \((1 - \text{actual trust value})\). In both circumstances, TWMN quantifies the recommendation credibility value with high accuracy.

Figure 16 shows recommendation credibility against a number of bad recommendations. As the percentage of bad recommendations increases, recommendation credibility decreases. The contribution of recommendations is reduced based on the correct recommendations received from that neighbor (recommender).

D. PERFORMANCE EVALUATION

The proposed trust mechanism identifies the malicious nodes in mesh networks based on packet forwarding. Two-hop ACK is used to identify whether a node has forwarded the packet or not. We have evaluated the proposed model trust
computations in presence of malicious nodes. However, our performance evaluation scope is to compare the network efficiency with and without the trust model. This shows the significance of the proposed trust model for wireless mesh networks. Some of the model parameters are already evaluated in our paper [22] for wireless sensor networks. Due to the above-mentioned scope, we have evaluated the proposed model in wireless mesh network model parameters. The objective of this simulation is to show the performance of the network in presence of malicious nodes.

Figure 17 shows the PDR analysis of TWMN in presence of malicious nodes. A number of malicious nodes increase PDR of AODV decreases drastically due to packet drops. TWMN successfully identifies malicious nodes so, the path will be established through legitimate nodes. When malicious nodes are increased there may be chances of malicious nodes which are not evaluated previously may exist in the new route hence the PDR reduces after the malicious nodes cross 30%. Throughput is directly proportional to PDR so the throughput of TWMN is high compared to AODV. Figure 18 shows the throughput analysis. Due to MRMC, interference is also less compared to SRSC so, TWMN shows higher PDR.

Control packet overhead is the average number of control packets for one data packet received. Figure 19 shows network overhead in presence of malicious nodes. The overhead of TWMN is high compared to AODV due to two-hop acknowledgment. As the number of malicious nodes increases the route length increases so the number of two-hop ACKs increases.

We have evaluated the average end-end delay without malicious nodes to analyze the delay due to two-hop ACKs. Figure 20 shows the delay with the different numbers of hops. Delay is increased as the number of hops are increasing between the source and destination. The Delay of TWMN is
higher than AODV because TWMN sends two-hop ACKs in the reverse path which consumes the network resources.

VII. CONCLUSION

In this paper, a secure and sustainable two-hop ACK mechanism framework was proposed here to build trust information. The scheme proposed is called TWMN which successfully identifies malicious nodes in the network. The two-hop mechanism allows verification of the packet forwarding behavior in the mesh network. TWMN gives a robust approach to computing recommendations in a distributed manner. TWMN uses a similarity mechanism to remove malicious recommendations. Indirect trust is aggregated by using the weighted DS Theory. TWMN trust accuracy is better and also accurately computes the recommendation’s credibility. We have shown that TWMN successfully identifies the malicious nodes and ensures packet delivery to the destination in presence of packet drop/modification attacks, badmouthing attacks, collusion attacks, and on-Off attacks. The scheme proposed has more network overhead compared to AODV because of two-hop ACK packets. PDR is high because of MRMC as well as the trust mechanism. Sensors’ data is also very important in TWMN because of the reverse path which consumes the network resources.

REFERENCES

[1] J. Lee, (May 2018). Mesh Networking and IoT. Accessed: Nov. 10, 2022. [Online]. Available: https://downloads.com/articles/how-mesh-networking-will-make-iot-real
[2] I. F. Akyildiz, X. Wang, and W. Wang, “Wireless mesh networks: A survey,” Comput. Netw., vol. 47, no. 4, pp. 445–487, Mar. 2005.
[3] R. Román-Castro, J. López, and S. Gritzalis, “Evolution and trends in IoT security,” Computer, vol. 51, no. 7, pp. 16–25, Jul. 2018.
[4] M. Ammar, G. Russello, and B. Crispo, “Internet of Things: A survey on the security of IoT frameworks,” J. Inf. Secur. Appl., vol. 38, pp. 8–27, Feb. 2018.
[5] Z. Yan, P. Zhang, and A. V. Vasilakos, “A survey on trust management for Internet of Things,” J. Netw. Comput. Appl., vol. 42, pp. 120–134, Jun. 2014.
[6] B. X. L. Santhanam and P. D. Agrawal, “Selfishness in mesh networks: Wired multihop MANETs,” IEEE Wireless Commun., vol. 15, no. 4, pp. 1284–1536, Aug. 2008.
[7] C. S. R. Murthy and B. S. Manoj, Ad How Wireless Networks: Architectures and Protocols. Upper Saddle River, NJ, USA: Prentice-Hall, 2004.
[8] K. Govindan and P. Mohapatra, “Trust computations and trust dynamics in mobile adhoc networks: A survey,” IEEE Commun. Surveys Tuts., vol. 14, no. 2, pp. 279–298, 2nd Quart., 2012.
[9] D. Zhu, X. Yang, and W. Yu, “SPAS: A novel self-checking pollution attackers identification scheme in network coding-based wireless mesh networks,” Comput. Netw., vol. 91, pp. 376–389, Nov. 2015.
[10] H. C. Tan, M. Ma, H. Labiod, P. Han, J. Chong, and J. Zhang, “A non biased trust model for wireless mesh networks,” Int. J. Comput. Syst., vol. 30, no. 9, pp. 1–8, 2016.
[11] R. Khatoun, Y. Bgeiriche, J. Dromard, L. Khoukhi, and A. Serhrouchni, “A statistical trust system in wireless mesh networks,” Ann. Telecommun., vol. 71, nos. 5–6, pp. 187–199, Jun. 2016.
[12] G. T. Reddy, M. P. K. Reddy, K. Lakshmana, R. Kaluri, D. S. Rajput, G. Srivastava, and T. Baker, “Analysis of dimensionality reduction techniques on big data,” IEEE Access, vol. 8, pp. 54776–54788, 2020.
[13] V. Busi Reddy, S. Venkataraman, and A. Negi, “Communication and data trust for wireless sensor networks using D-S theory,” IEEE Sensors J., vol. 17, no. 12, pp. 3921–3929, Jun. 2017.
KUNJA KAVITHA (Senior Member, IEEE) received the B.Tech. and M.Tech. degrees from Jawaharlal Nehru Technological University, Hyderabad, and the Ph.D. degree in computer science from the University of Hyderabad. She is currently a Professor with the Department of Computer Science and Engineering, Jawaharlal Nehru Technological University Hyderabad, Telangana, India. She has handled a research project funded by AICTE under research promotion scheme titled “QoS support for real-time traffic in MANETs.” She was a principal investigator for the project titled “Centre of Excellence on Disaster Management” funded under TEQIP. She has supervised master’s theses and currently guiding two research scholars. She has served on technical program committee for several conferences. Her research interests include wireless networks communication protocols, network security, the IoT, and algorithms.

She is an Active Member and Volunteer of IEEE, ACM, and ISTE. She is also a reviewer of several prominent journals.

VINOD KUMAR GUNJAN (Senior Member, IEEE) received the Ph.D. degree. He is currently an Associate Professor with the Department of Computer Science and Engineering, CMR Institute of Technology, Jawaharlal Nehru Technological University, Hyderabad. He has published research papers in IEEE, Elsevier, and Springer Conferences. He has authored several books and edited volumes of Springer Series, most of which are indexed in the SCOPUS database. In 2016, he received the prestigious Early Career Research Award from the Science Engineering Research Board, Department of Science and Technology, Government of India. He was an Active Volunteer of the IEEE Hyderabad Section, and the Treasurer, Secretary, and Chairperson of the IEEE Young Professionals Affinity Group and IEEE Computer Society. He has been involved in organizing several technical and non-technical workshops, seminars, and conferences, where he had the honor of working with top IEEE leaders. He was received the Best IEEE Young Professional Award from the IEEE Hyderabad Section, in 2017.

KURUVAKALAKSHMANNA received the B.Tech. degree in computer science and engineering from the Sri Venkateswara University College of Engineering, Tirupati, India, in 2006, the M.Tech. degree in computer science and engineering (information security) from the National Institute of Technology at Calicut, Kerala, India, in 2009, and the Ph.D. degree from VIT, India, in 2017. He was a Visiting Professor with the Guangdong University of Technology, China, in 2018. He is currently working as an Associate professor with VIT. He has published research papers in IEEE, Elsevier, and Springer, most of which are indexed in the SCOPUS database. His research interests include machine learning, data mining in DNA sequences, the IoT, data science, and security.

ARFAT AHMAD KHAN received the B.Eng. degree in electrical engineering from the Government College University Lahore, Pakistan, in 2013, the M.Eng. degree in electrical engineering from the University of Petroleum and Energy Studies in 2015, and the Ph.D. degree in telecommunication and computer engineering from the Suranaree University of Technology, Thailand, in 2018. From 2014 to 2016, he was an RF Engineer with Etisalat, United Arab Emirates. From 2018 to 2022, he worked as a Lecturer and Senior Researcher with the Suranaree University of Technology. He is currently working as a Senior Lecturer and Researcher with Khon Kaen University, Thailand. His research interests include optimization and stochastic processes, channel and the mathematical modeling, wireless sensor networks, Zigbee, green communications, massive MIMO, OFDM, wireless technologies, signal processing, and the advance wireless communications.

CHITAPONG WECHTAISONG received the B.Eng. and M.Eng. degrees in telecommunication engineering from the Suranaree University of Technology, Thailand, in 2008 and 2014, respectively, and the Ph.D. degree in information and communication engineering from the Shibaura Institute of Technology, Japan, in 2016. He is currently an Assistant Professor with the School of Telecommunication Engineering, Institute of Engineering, Suranaree University of Technology. His research interests include wireless network design and optimization, network traffic localization, and global engineering education.