Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.DOI

Security in IoT Mesh Networks based on Trust Similarity

ATHOTA KAVITHA[1], (Senior Member, IEEE), VIJENDER BUSI REDDY[2], (Senior Member, IEEE), NINNI SINGH[3], VINIT KUMAR GUNJAN[4], (Senior Member, IEEE) , KURUVA LAKSHMANNA[5], ARFAT AHMAD KHAN[6], and CHITAPONG WECHTAISONG[7]

[1]JNTUH College of Engineering, JNTU University, Hyderabad, Telangana, India (e-mail: athotakavitha@gmail.com)
[2]Advanced Data Processing Research Institute, Secunderabad, Telangana, India (e-mail: vijender@adrin.res.in)
[3]CMR Institute of Technology Hyderabad Telangana, India (e-mail: ninnisingh1991@gmail.com)
[4]CMR Institute of Technology Hyderabad Telangana, India (e-mail: vinitkumargunjan@gmail.com)
[5]School of Information Technology and Engineering, VIT, Vellore, India(e-mail: lakshman.kuruva@vit.ac.in)
[6]Department of Computer Science, College of Computing, Khon Kaen University, Khon Kaen 40002, Thailand(e-mail: arfatkhan@kku.ac.th)
[7]School of Telecommunication Engineering, Suranaree University of Technology, Nakhon Ratchasima 30000, Thailand(e-mail: chitapong@g.sut.ac.th)

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

ABSTRACT Internet of Things (IoT) Mesh networks are becoming very popular to enable IoT devices to communicate without relying on dedicated PC services. 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 a embedded computer with networking and sensing capabilities. As IoT networks are growing, communication gap is also increasing with the Internet and more infrastructure is required to exchange data with 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 with 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 cloud to relay messages by using cellular or Wi-Fi connectivity. This works better in standalone system but sometimes we want to establish a connection to Internet and also create a local network to join other IoT devices [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 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 the services from the network. IoT devices's data will be sent to 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 attack, On-Off attack, Bad mouthing attack and Collusion attack. 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 discuss a novel trust model to reduce the packet dropping/modification attacks, badmouthing attacks and collusion attacks. the proposed technoque does not require trusted third party and is dynamic. Mesh routers are Multi Radio and Multi Channel (MRMC) networks. A node may not be able to monitor neighbours' behaviour. The neighbor's behaviour is evaluated using a two-hop acknowledgement technique. The two-hop ACK mechanism to observe the neighbour's forwarding behaviour. 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 recommendation also contribute equally in the trust aggregation. Direct trust can be taken as weighting parameter for 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 similarity model is to compare the behaviour of two nodes' recommendations on common neighbouring nodes and compute the recommendation credibility of the node based on the error in 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 their neighbours. Since mesh nodes are MRMC capability, a two-hop ACK mechanism is used to observe the neighbour's packet forwarding behaviour.
- 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 suitable for aggregation. Here, weight refers to a node's recommendation credibility.
- The similarity between two nodes in the recommendation behaviour 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 upon 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 evaluate the performance based of 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 discuss the basic trust concepts as well as certain trust models that were developed for wireless mesh networks.

A. TRUST CONCEPTS

Trust is defined as individual belief about the future behaviour of a node which is based on the past experience [8]. 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

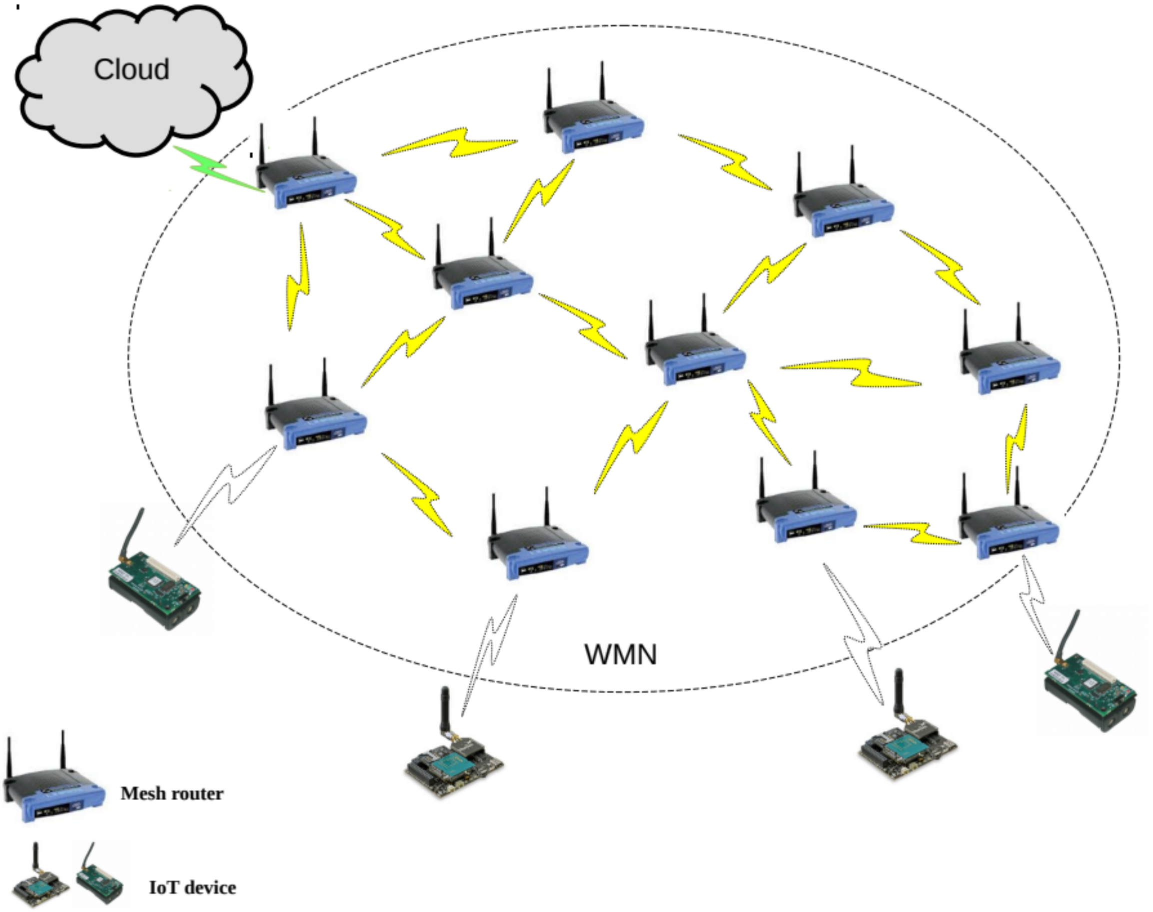


FIGURE 1. A sample IoT Wireless Mesh Network (WMN).

centralized model, trust is determined at central server and distributed to every network node, while in 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, node's behaviour may not be consistent. In 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 the selfish behaviour. Authors discuss selfish behaviour in different network stack layers and suggest 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 attack in WMNs. Authors propose a direct trust approach with watchdog mechanism. Watchdog mechanism is not possible in multi radio networks because node may not overhear its neighbouring node's activities in 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 attack. Authors use 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 behaviour of a node. Indirect trust is evaluated with direct trust parameter as weight. 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. CUSUM test is used to identify normal(H0) and abnormal behaviour(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 KS test. The trust value is computed using 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 effective use of energy. Authors used bandwidth usage and energy completion to derive trust. Game theory is used to make decisions based on trust replies received from neighbours.

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 patient health loss 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 three types of trust based models for Industrial IoT. The authors mainly focused on sensor cloud (SC). They proposed independent SC, Collaborative SC and Mutual SC to estimate the behaviour of sensor nodes and data centers. Authors also shown the performance improvement of IIoT due to trust mechanisms [20]–[22].

Recommendations received from neighbours are uncertain. Aggregating these recommendations accurately require a good ensemble method. DS theory [23] is one of the best ensemble method when data is uncertain. NBBTE [24] use DS evidence theory to combine the recommendations. They [24] have not considered credibility of recommendations and susceptible to bad mouthing attack. 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 distinguishing recommendations based on the node's behaviour, which leads to badmouthing 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 assigning equal weight to all recommendations may give inaccurate indirect trust value. Weight of a recommendations can be computed based on the recommender's behaviour.

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

III. SYSTEM MODEL AND ASSUMPTIONS

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 flat model where the mesh client send data to another mesh client.

A. ATTACK MODEL

There are many attacks in mesh networks [29]–[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 a legitimate nodes. [32], [33].

IV. PROPOSED METHODOLOGY

The objective of the proposed methodology is to offer an efficient trust technique for IoT mesh networks. Due to lack of range and visibility beyond the neighbours we have evolve a totally novel model to be able to gather and compute recommendations indirectly in IoT mesh networks. WThe trust computed from direct observation on the target node is known as direct trust (DT). Neighbor nodes send recommendations (R) regarding the target node. The recommendations are the basis for computing indirect trust (IT). Indirect and direct trust are combined to calculate overall trust.

Forwarding Acknowledgements

An acknowledgement is a packet that traverses in the reverse direction, that is, destination to source and indicates successful delivery of the packet. Two hop acknowledgement (Two-hop ACK) is a special type of acknowledgement 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 neighbour, it assumes that the neighbour has successfully forwarded the packet. We are assuming that the acknowledgement is generated with its source signature so that no other node can create this acknowledgement. The

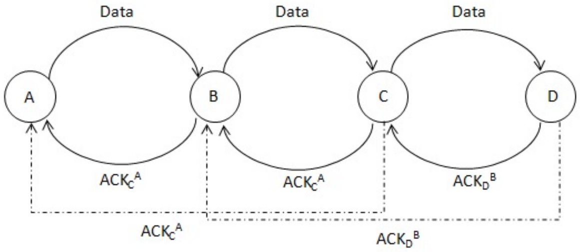
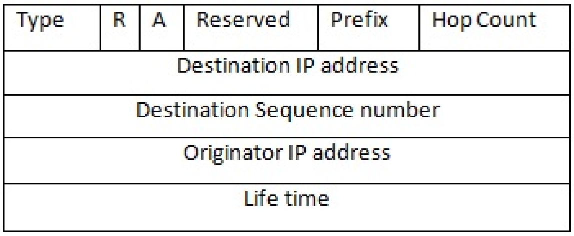


FIGURE 2. Two-hop Acknowledgement scenario.



Type	R	A	Reserved	Prefix	Hop Count
Destination IP address					
Destination Sequence number					
Originator IP address					
Life time					

FIGURE 3. Two-hop Acknowledgement packet format.

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 $DT_A^B(T)$:

Direct trust is computed from node's forwarding behaviour. $DT_A^B(t)$ 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 send it to node *A*. When node *A* receives ACK from node *C* it increases the forwarding count of the neighbouring node *B*. Forwarding Ratio computes the ratio between number of packets correctly forwarded and number of packets sent.

$$Forwarding\ ratio\ FR_A^B(t) = \frac{p_t}{p_t + q_t} \tag{1}$$

Where
p_t=Number of packets forwarded by node B upto time t.
q_t=Number of packets dropped by node B upto time t.

The instantaneous changes of $FR_A^B(t)$ is shown below. As Forwarding ratio decreases δ_t value increases otherwise it decreases.
If $FR_A^B(t-1) > FR_A^B(t)$
$$\delta_t = \delta_{t-1} + \alpha \times (FR_A^B(t-1) - FR_A^B(t))$$
If $FR_A^B(t-1) < FR_A^B(t)$
$$\delta_t = \delta_{t-1} + \beta \times (FR_A^B(t-1) - FR_A^B(t))$$
else
$$\delta_t = \delta_{t-1}$$
where $\alpha < \beta$

α is a punishment factor. β is encouragement factor. δ_t represents the momentary differences in a node's behaviour. Direct trust parameter is computed as follows. $DT_A^B(t)$ is the direct trust value computed on node *B* by node *A*.

$$DT_A^B(t) = FR_A^B(t) \times cos(\frac{\pi}{2} \times \delta_t) \tag{2}$$

In equation 5, δ_t shows the fluctuations in the node's behaviour. If fluctuations are high then δ_t increases. Therefore, $cos(.)$ function value decreases and thereby direct trust decreases. Direct trust assesses both forwarding behaviour as well as behaviour fluctuations of a node.

B. RECOMMENDATION CREDIBILITY (R)

Recommendation credibility gives the node's capability to send recommendations. We use root mean 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 neighbours to node A and node B. Then

$$D_A^B(t) = \sqrt{\frac{\sum\limits_{x\epsilon X_{AB}} (DT_A^x(t) - DT_B^x(t))^2}{|K_{AB}|}} \tag{3}$$

Where $DT_A^x(t)$ is the direct trust on node x at node A.
$D_A^B(t)$ represents the root mean square difference between the evaluation of node x by nodes A and B. The sensitivity to differences of $D_A^B(t)$ may reduce if there is more similarity in the DT values and if the number of common neighbours are high. Here this is a novel measure to compute dissimilarity in trust. The squared difference of trust is being normalized over the number of neighbours.

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

$$R_A^B(t) = (1 - D_A^B(t)) \times \frac{\sum\limits_{i\epsilon|K_{AB}|} (x_i \wedge y_i)}{n} \tag{4}$$

where n is the total number of recommendations. X is the set of direct trust values on neighbouring nodes. Y is the set of recommendations sent by a particular neighbour, B. $x_i \epsilon X$, $y_i \epsilon Y$. $x_i \wedge y_i$ is *1* if both sets show similar legitimate neighbour behaviour 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 neighbouring nodes. These are useful to judge the trustworthiness of neighbour nodes. The recommendations received from neighbours are independent and uncertain. One of the best way 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-Shaffer(DS) theory

[23] DS theory use 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 Ω 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 Ω is a power set contains $\{Legitimate, Malicious\}$ where Hypothesis $H = \{Legitimate\}$, $\overline{H} = \{Malicious\}$ and $U = \Omega$. Let m_x^B and m_y^B 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_x^B. The trust values from different sources are independent to 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

$$m_p^q(H) = \frac{R_p^x \times T_x^q}{\sum\limits_{x \epsilon W-\{p\}} R_p^x}$$

$m_p^q(\overline{H}) = 0.$

$$m_p^q(U) = 1 - \frac{R_p^x \times (T_x^q)}{\sum\limits_{x \epsilon W-\{p\}} R_p^x}$$

Where W is the set of neighbours to q and $x \epsilon W$.

The Dempster's combination rule of m_x^B and m_y^B is [25] :

$$m_x^B(H) \bigoplus m_y^B(H) = \frac{1}{K}[m_x^B(H) m_y^B(H) + m_x^B(H) m_y^B(U) + m_x^B(U) m_y^B(H)]$$

$$m_x^B(\overline{H}) \bigoplus m_y^B(\overline{H}) = \frac{1}{K}[m_x^B(\overline{H}) m_y^B(\overline{H}) + m_x^B(\overline{H}) m_y^B(U) + m_x^B(U) m_y^B(\overline{H})]$$

$$m_x^B(U) \bigoplus m_y^B(U) = \frac{1}{K} m_x^B(U) m_y^B(U)$$

Where

$$K = m_x^B(H) m_y^B(H) + m_x^B(H) m_y^B(U) + m_x^B(U) m_y^B(U) + m_x^B(U) m_y^B(H) + m_x^B(U) m_y^B(\overline{H}) + m_x^B(\overline{H}) m_y^B(\overline{H}) + m_x^B(\overline{H}) m_y^B(U)$$

The trust value of node *B* is $bel(H) = m_x^B(H) \bigoplus m_y^B(H)$. Indirect Trust $IT_A^B(t)$ is the indirect trust on node B calculated by node A.

$IT_A^B = m_x^B(H) \bigoplus m_y^B(H) ... \bigoplus m_y^B(H)$

the order of combination does not have any impact on the result due to transitivity and commutative property of Dempster's combination.

D. OVERALL TRUST

Overall trust is computed based on a node's packet forwarding behaviour with the neighbour. $OT_A^B(t)$ is the overall trust on node B at node A.

$$OT_A^B(t) = \tau \times DT_A^B(t) + (1-\tau) \times IT_A^B(t) \qquad (5)$$

Where τ is the weight of direct trust which can be calculated as follows.

$$\tau = \frac{I_t(A,B)}{I_t(A,B) + M_t(A,B)} \qquad (6)$$

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.

As number of interactions $(I_t(A,B))$ increase, τ also increases. So, weight of the direct trust increases. The node become more experienced and increases the belief on its own judgement.

$M_t(A,B)$ is the average of total number of packets forwarded by node *B* other than node *A*'s packets. Similar to the recommendation sharing, neighbours may also send 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 τ is used to give weightage to direct and indirect trust as per Equation 5 and computation of τ value as given in Equation 6. When there are more number of direct interactions the direct trust will give significant information about neighbor. If direct interactions are low then τ 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 which contain other neighbor nodes trust values and are shared periodically. Recommendations are used to computer 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.

$$M_t(A,B) = \frac{\sum\limits_{x \epsilon K_B - A} (R_A^x \times I_t(x,B))}{|K_B| - 1} \qquad (7)$$

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 neighbouring node

2 When a node receives two hop ACK from the neighbouring 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 neighbours.

F. SPACE REQUIREMENTS:

Trust table contains trust parameters of the neighbouring node. *neighbour 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* neighbours and *i* recommenders for each neighbour then space requirement for 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 neighbours' behaviour 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 become k for one data packet from destination to source.

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

Assume that the size of two-hop ACK is φ and data packet is ϑ then the total over head in one session due to two-hop ACKs will be

$$\text{Overhead due to two-hop ACK is} = k \times \frac{\varphi}{\vartheta} \tag{8}$$

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

V. EVALUATION

In this section, we present the performance of the proposed model. We analyzed the recommendation credibility computation, direct trust computation, accuracy of the trust and finally performance of the network in presence of malicious nodes. We also analyze the strength of trust model in presence of packet dropping, on-off, bad mouthing and collusion attacks. 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 value in DATA-I (in Figure 4) but PCC showing lower value. The data sets X and Y are independent to each other so PCC may not give accurate value. DATA-II (in Figure 4) shows cosine similarity is high. PCC is not possible on DATA-V (in Figure 4) because Y set has same values. Cosine similarity shows highest value in all the cases. RMS similarity (*RMS_sim*) is low when more number of values are not similar. It is observed that no similarity mechanism works perfectly on all kinds of data. The proposed parameter R_A^B shows better value for all six types of data sets. It is shown that the proposed recommendation credibility accurately computing the similarity value between two nodes.

Parameter	value
Simulation Time	*600 sec*
Number of nodes	*25*
Area	*1200×900*
Transmission Range	*150m*
Transport protocol	*UDP*
Application protocol	*CBR*
Radio interfaces	*4*

TABLE 1. Simulation parameters for WMNs simulations

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 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 the packets randomly with *Packet dropping rate (Pr)=n*, defined as one packet is dropped *randomly* in every *n* packets. The successful packet delivery to the destination also depends on the number of malicious nodes present in the path.

Assume that 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:

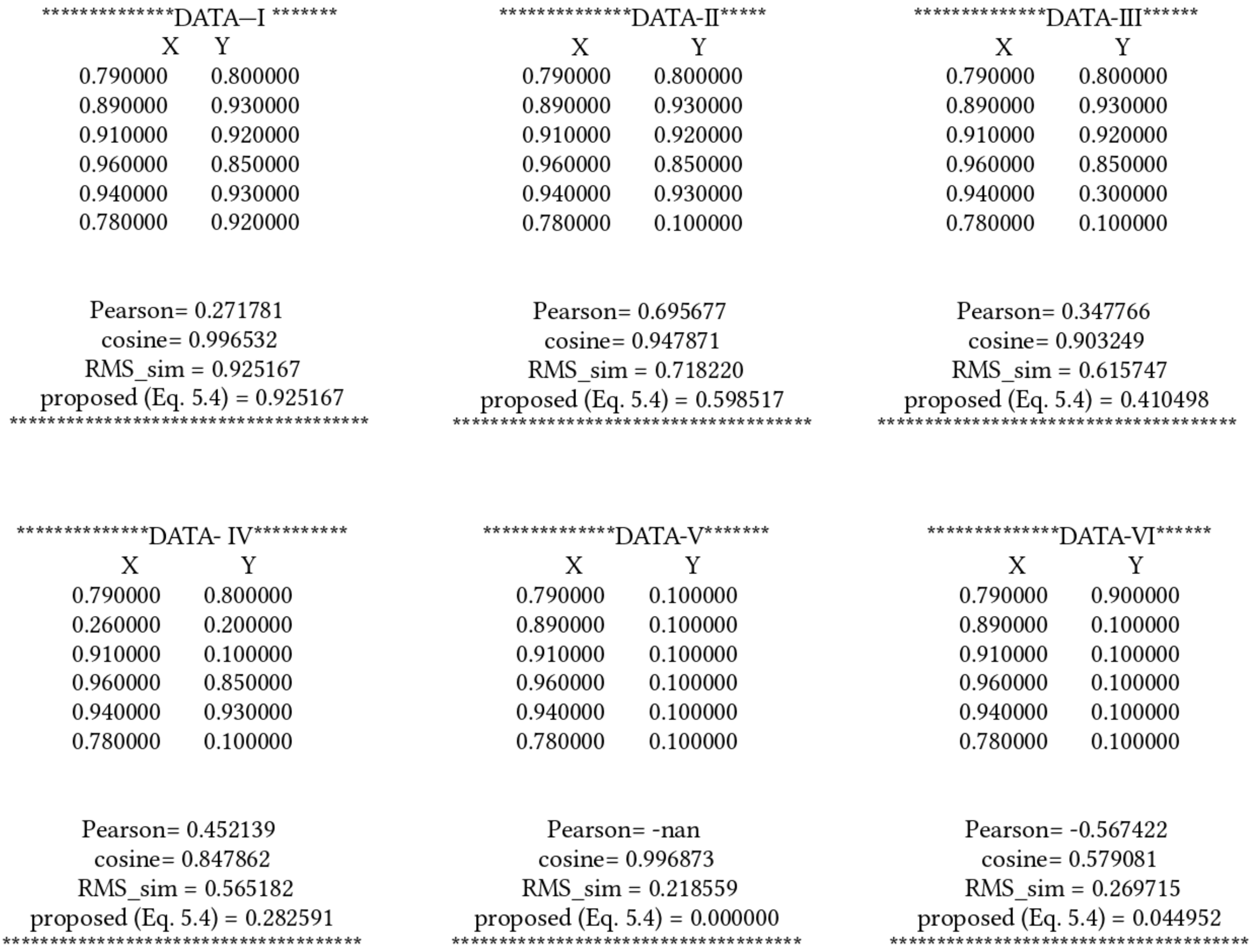
$$p + (1 - p) \times p + (1 - p)^2 \times p + ... + (1 - p)^{k-1} \times p \tag{9}$$

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

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

$$(1 - p)^k \tag{10}$$

Figures 5-9 show the trust values of TWMN and ratio methods [25], [43], [44] with $\gamma = 1$ and $\gamma = 3$ val-



```
**************DATA–I *******
           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= 0.271781
         cosine= 0.996532
      RMS_sim = 0.925167
  proposed (Eq. 5.4) = 0.925167
*************************************
```

```
**************DATA-II*****
        X           Y
   0.790000   0.800000
   0.890000   0.930000
   0.910000   0.920000
   0.960000   0.850000
   0.940000   0.930000
   0.780000   0.100000


        Pearson= 0.695677
         cosine= 0.947871
      RMS_sim = 0.718220
  proposed (Eq. 5.4) = 0.598517
*************************************
```

```
**************DATA-III******
        X           Y
   0.790000   0.800000
   0.890000   0.930000
   0.910000   0.920000
   0.960000   0.850000
   0.940000   0.300000
   0.780000   0.100000


        Pearson= 0.347766
         cosine= 0.903249
      RMS_sim = 0.615747
  proposed (Eq. 5.4) = 0.410498
*************************************
```

```
**************DATA- IV**********
        X           Y
   0.790000   0.800000
   0.260000   0.200000
   0.910000   0.100000
   0.960000   0.850000
   0.940000   0.930000
   0.780000   0.100000


        Pearson= 0.452139
         cosine= 0.847862
      RMS_sim = 0.565182
  proposed (Eq. 5.4) = 0.282591
*************************************
```

```
**************DATA-V*******
        X           Y
   0.790000   0.100000
   0.890000   0.100000
   0.910000   0.100000
   0.960000   0.100000
   0.940000   0.100000
   0.780000   0.100000


        Pearson= -nan
         cosine= 0.996873
      RMS_sim = 0.218559
  proposed (Eq. 5.4) = 0.000000
*************************************
```

```
**************DATA-VI******
        X           Y
   0.790000   0.900000
   0.890000   0.100000
   0.910000   0.100000
   0.960000   0.100000
   0.940000   0.100000
   0.780000   0.100000


        Pearson= -0.567422
         cosine= 0.579081
      RMS_sim = 0.269715
  proposed (Eq. 5.4) = 0.044952
*************************************
```

FIGURE 4. PCC, Cosine correlation, RMS similarity and proposed similarity method(R_A^B) values of example data sets.

ues. 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 ratio method, TWMN is reducing in all scenarios whereas ratio method is stable at one value in all scenarios

Figure 10 and figure 11 shows the trust values of TWMN with different punishment factors i.e $\alpha = 2$ and $\alpha = 4$. It is evident that as punishment factor α increases, trust value reduces drastically because of $cos(.)$. 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 expected trust values. The expected trust value for legitimate

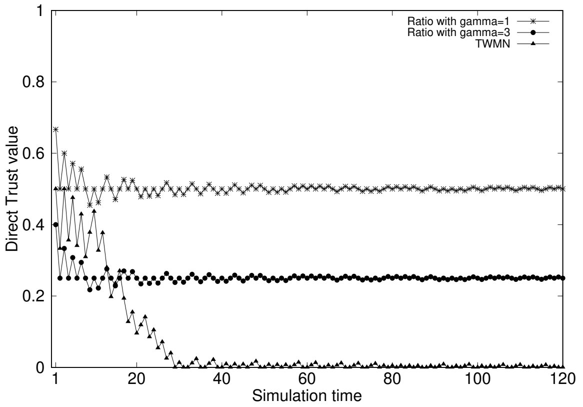


FIGURE 5. Packet drop attack mitigation at Pr=2.

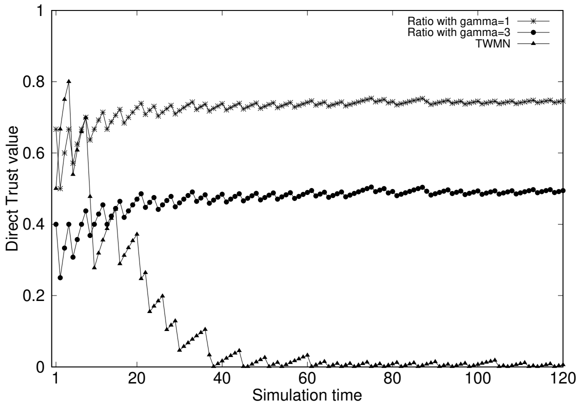


FIGURE 6. Packet drop attack mitigation at Pr=4.

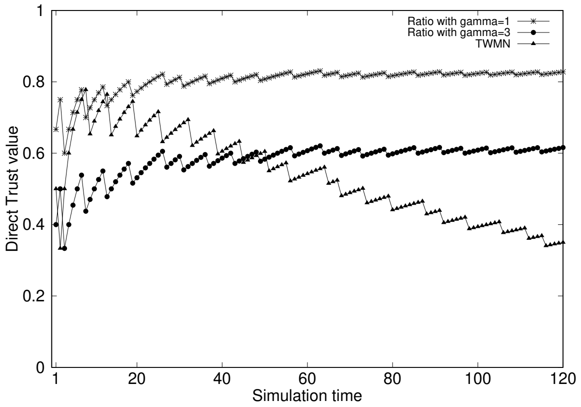


FIGURE 7. Packet drop attack mitigation at Pr=6.

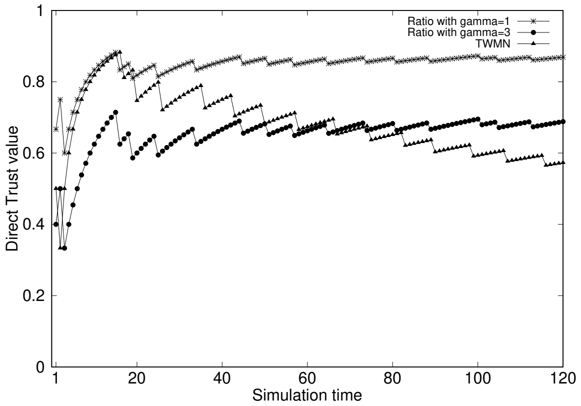


FIGURE 8. Packet drop attack mitigation at Pr=8.

node is 1 and for malicious node is 0.

In this simulation, nodes in the network start behaving in a malicious manner at random. These nodes send bad recommendations on legitimate nodes in a non-collusive manner (mode). In collusive mode, malicious nodes form a group and send good recommendations on group members, bad recommendations on 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 on neighbours present in the trust table. Figure 12 shows the trust computation error in presence of collusive and non-collusive mode. In both modes trust computation error is low i.e. the trust model accurately identifying the malicious nodes.

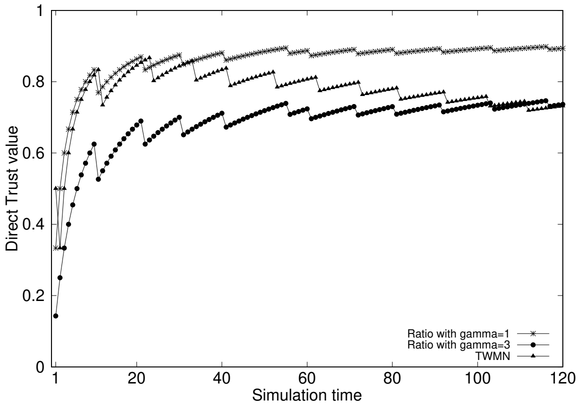


FIGURE 9. Packet drop attack mitigation at Pr=10.

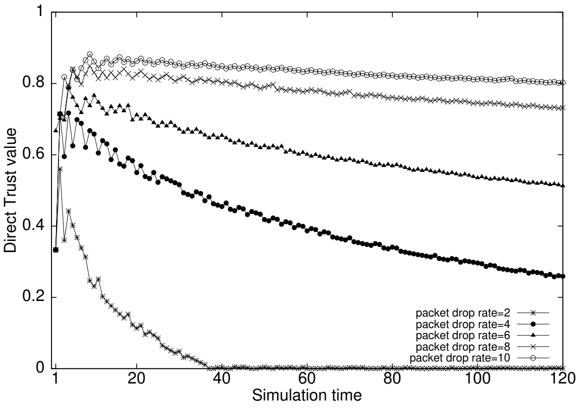


FIGURE 10. Direct trust computation with α=2.

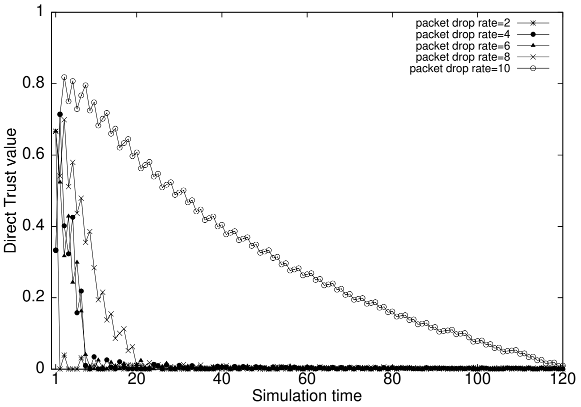


FIGURE 11. Direct trust computation with α=4.

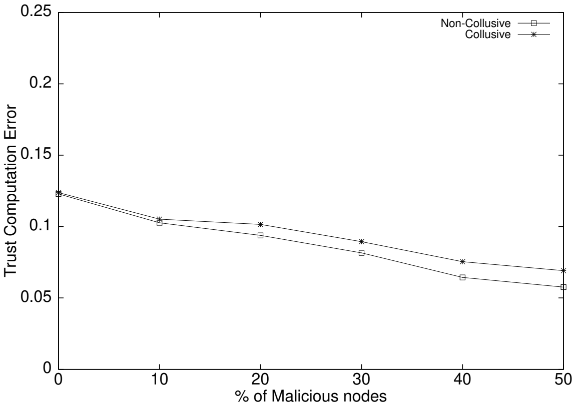


FIGURE 12. Trust accuracy in presence of collusive and non-collusive attack.

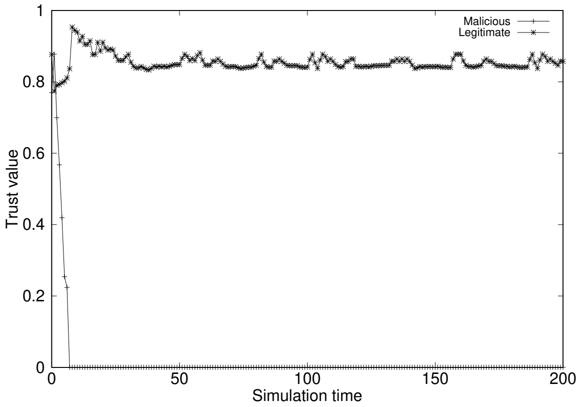


FIGURE 13. Trust value computation by TWMN.

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. Legitimate node performs well so trust value is high. Malicious node shows bad behaviour so trust value decreases and reaches zero.

Figure 14 and 15 shows 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 $(1 - actual\, trust\, value)$. In both circumstances, TWMN quantifies the recommendation credibility value with high accuracy.

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

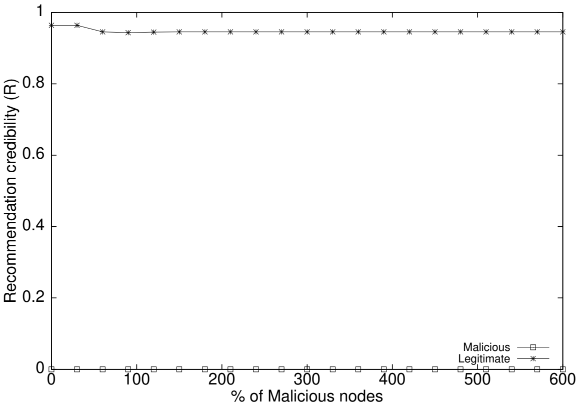


FIGURE 14. Recommendation trust computation by TWMN with constant bad recommendation.

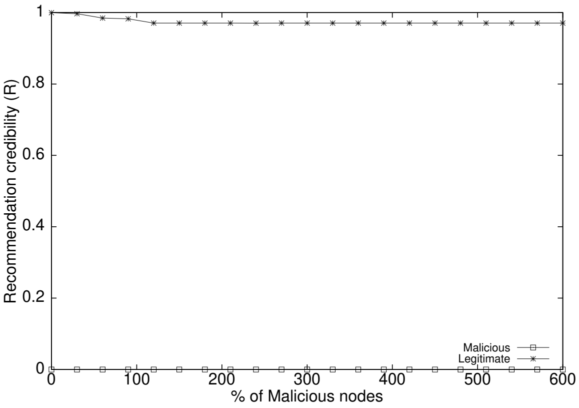


FIGURE 15. Recommendation trust computation by TWMN with dynamic bad recommendation.

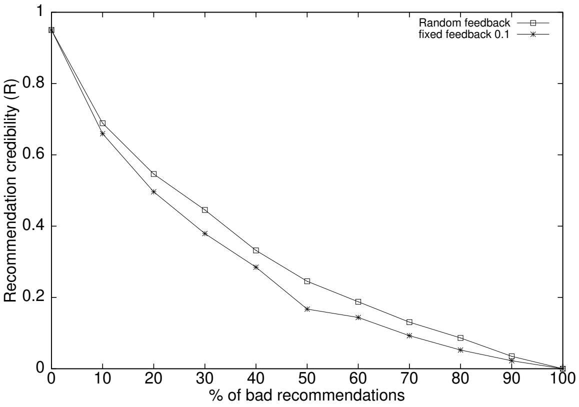


FIGURE 16. Recommendation trust computation by TWMN with different number of bad recommendations.

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 perfor-

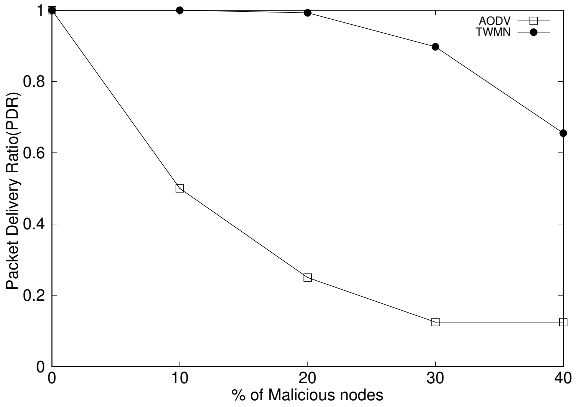


FIGURE 17. Packet Delivery Ratio in presence of malicious nodes.

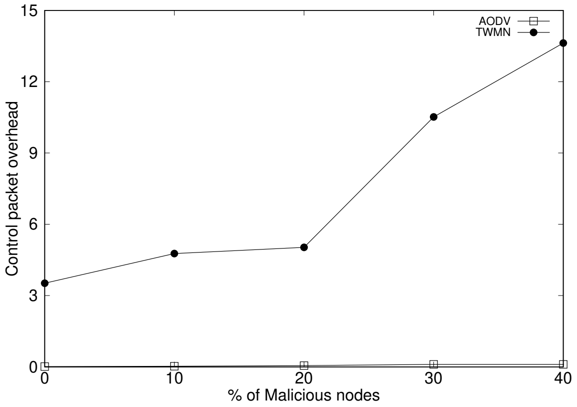


FIGURE 19. Control packet overhead of TWMN and AODV in presence of malicious nodes.

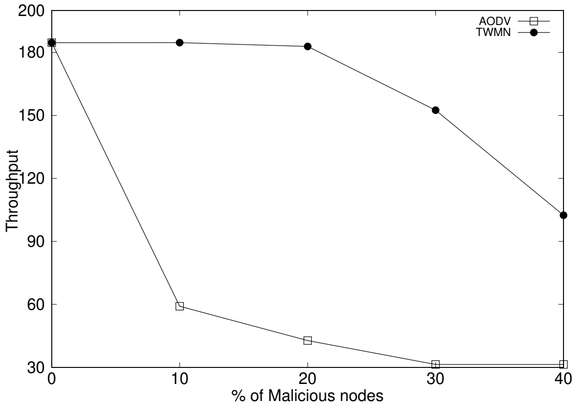


FIGURE 18. Throughput in presence of malicious nodes.

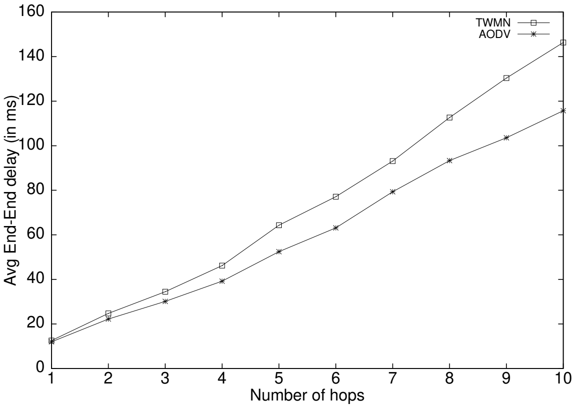


FIGURE 20. Average end-end delay computation with different path lengths.

mance evaluation scope is to compare the network efficiency with and without 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 simulations 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. As number of malicious nodes increases PDR of AODV is decreases drastically due to packet drops. TWMN successfully identifies malicious nodes so, 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 exists in the new route hence the PDR reduces after the malicious nodes cross 30%. Throughput is directly proportional to PDR so throughput of TWMN is high compared to AODV. Figure 18 shows throughput analysis. Due to MRMC, interference is also less compare 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 acknowledgement. As number of malicious nodes increases the route length increases so number of two-hop ACKs increase.

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

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 behaviour in the mesh network. TWMN gives a robust approach to compute recommendations in a distributed manner. TWMN uses similarity mechanism to remove the malicious recommendations. Indirect trust is aggregated by using weighted DS Theory. TWMN trust accuracy is better and also accurately computes the recommendation credibility. We have shown that TWMN successfully identifies the malicious nodes and ensures packets delivery to destination in presence of packet drop/modification attack, badmouthing attack, collusion attack and on-Off attack. 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 trust mechanism. Sensors' data is also very important in IoT networks. Data Trust [19] also can be integrated to verify the consistency and reliability of the IoT device. We are working on a logical extension to apply the proposed trust model for channel assignment in MRMC so that legitimate nodes get more Quality of Service.

FUNDING STATEMENT

This study was supported by College of Computing, Khon Kaen University, Thailand.

ACKNOWLEDGEMENT

We would like to thank College of Computing, Khon Kaen University, Thailand.

REFERENCES

[1] Jeffrey Lee. Mesh networking and iot, May 2018.

[2] WeilinWang Ian F.Akyildiz, XudongWang. Wireless mesh networks: a survey. Elsevier joural on Computer Networks, 47(4):445–487, 2005.

[3] J. López R. Román-Castro and S. Gritzalis. Evolution and trends in iot security. IEEE Computer, 51(7):16–25, July 2018.

[4] BrunoCrispo Mahmoud Ammar, Giovanni Russello. Internet of things: A survey on the security of iot frameworks. Elsevier Journal of Information Security and Applications, 38:8–27, February 2018.

[5] Athanasios V.Vasilakos Zheng Yan, Peng Zhang. A survey on trust management for internet of things. Elsevier Journal of Network and Computer Applications, 42:120–134, 2014.

[6] Bin Xie Lakshmi Santhanam and Dharma P. Agrawal. Selfishness in mesh networks: wired multihop manets. IEEE Wireless Communications, 15(4):1536–1284, August 2008.

[7] C. Siva Ram Murthy and B. S. Manoj. Ad Hoc Wireless Networks: Architectures and Protocols. Prentice Hall, 2004.

[8] K. Govindan and P. Mohapatra. Trust computations and trust dynamics in mobile adhoc networks: A survey. IEEE Communications Surveys and Tutorials, Vol. 14 issue 2:Pp 279–298, 2012.

[9] Xinyu Yang Donghai Zhua and Wei Yub. Spais: A novel self-checking pollution attackers identification scheme in network coding-based wireless mesh networks. Elsevier Computer Networks, 91:376–389, 2015.

[10] Heng Chuan Tan, Maode Ma, Houda Labiod, Peter Han, Joo Chong, and Jun Zhang. A non biased trust model for wireless mesh networks. International journel of communication systems, wiely, 30(9):1–8, 2016.

[11] Rida Khatoun, Youcef Begriche, Juliette Dromard, Lyes Khoukhi, and Ahmed Serhrouchni. A statistical trust system in wireless mesh networks. Annals of Telecommunications, 71(5):187–199, 2016.

[12] G Thippa Reddy, M Praveen Kumar Reddy, Kuruva Lakshmanna, Rajesh Kaluri, Dharmendra Singh Rajput, Gautam Srivastava, and Thar Baker. Analysis of dimensionality reduction techniques on big data. IEEE Access, 8:54776–54788, 2020.

[13] Vijender Busi Reddy, Sarma Venkataraman, and Atul Negi. Communication and data trust for wireless sensor networks using d–s theory. IEEE Sensors Journal, 17(12):3921–3929, 2017.

[14] Yinpeng Yu Yao Yu, Yuhuai Peng and TianyuRao. A new dynamic hierarchical reputation evaluation scheme for hybrid wireless mesh networks. Elsevier Journal on Computers and Electrical Engineering, 40, Issue 2:663–672, February 2014.

[15] Vankadhara Rajyalakshmi and Kuruva Lakshmanna. A review on smart city-iot and deep learning algorithms, challenges. International Journal of Engineering Systems Modelling and Simulation, 13(1):3–26, 2022.

[16] Kuruva Lakshmanna, Rajesh Kaluri, Nagaraja Gundluru, Zamil S Alzamil, Dharmendra Singh Rajput, Arfat Ahmad Khan, Mohd Anul Haq, and Ahmed Alhussen. A review on deep learning techniques for iot data. Electronics, 11(10):1604, 2022.

[17] J. Duan, D. Gao, D. Yang, C. H. Foh, and H. Chen. An energy-aware trust derivation scheme with game theoretic approach in wireless sensor networks for iot applications. IEEE Internet of Things Journal, 1(1):58–69, 2014.

[18] H. Al-Hamadi and I. R. Chen. Trust-based decision making for health iot systems. IEEE Internet of Things Journal, 4(5):1408–1419, 2017.

[19] C. Zhu, J. J. P. C. Rodrigues, V. C. M. Leung, L. Shu, and L. T. Yang. Trust-based communication for the industrial internet of things. IEEE Communications Magazine, 56(2):16–22, Feburary 2018.

[20] Ninni Singh, Vinit Kumar Gunjan, Gopal Chaudhary, Rajesh Kaluri, Nancy Victor, and Kuruva Lakshmanna. Iot enabled helmet to safeguard the health of mine workers. Computer Communications, 2022.

[21] Vijender Busi Reddy, Atul Negi, S Venkataraman, and V Raghu Venkataraman. A similarity based trust model to mitigate badmouthing attacks in internet of things (iot). In 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), pages 278–282. IEEE, 2019.

[22] Vijender Busi Reddy, S Venkataraman, and Atul Negi. A dynamic trust evolution model for manets based on mobility. International Journal of Ad Hoc and Ubiquitous Computing, 28(4):230–246, 2018.

[23] Frans voorbraak. Dempster-shafer theory.

[24] X. Zhou R. Feng, X. Xu and J. Wan. A trust evaluation algorithm for wireless sensor networks based on node behaviors and d-s evidence theory. Sensors(Basel), 11, No. 2:1345–1360, 2011.

[25] Zhexiong Wei, Helen Tang, F Richard Yu, Maoyu Wang, F Richard Yu, Maoyu Wang, and Peter Mason. Security enhancements for mobile ad hoc networks with trust management using uncertain reasoning. IEEE Transaction on Vehicular Technolgy, 63, NO. 9:4647–4658, 2014.

[26] Kuruva Lakshmanna, R Kavitha, BT Geetha, Ashok Kumar Nanda, Arun Radhakrishnan, and Rachna Kohar. Deep learning-based privacy-preserving data transmission scheme for clustered iiot environment. Computational Intelligence and Neuroscience, 2022, 2022.

[27] Jiaming Pei, Zhi Yu, Jinhai Li, Mian Ahmad Jan, and Kuruva Lakshmanna. Tkagfl: A federated communication framework under data heterogeneity. IEEE Transactions on Network Science and Engineering, 2022.

[28] Yongmoo Suh Keunho Choi. A new similarity function for selecting neighbors for each target item in collaborative filtering. Elsevier Knowledge-Based Systems, 37:146–153, 2013.

[29] Yanli Yu, KeqiuLi, Wanlei Zhou, and PingLi. Trust mechanisms in wireless sensor networks:attack analysis and countermeasures. Elsevier Journal of Network and Computer Applications, 35:867–880, 2012.

[30] Himanshu Sahu and Ninni Singh. Software-defined storage. In Innovations in Software-Defined Networking and Network Functions Virtualization, pages 268–290. IGI Global, 2018.

[31] Ninni Singh, Vinit Kumar Gunjan, and Moustafa M Nasralla. A parametrized comparative analysis of performance between proposed adaptive and personalized tutoring system "seis tutor" with existing online tutoring system. volume 10, pages 39376–39386. IEEE, 2022.

[32] Balmukund Mishra, Ninni Singh, and Ravideep Singh. Master-slave group based model for co-ordinator selection, an improvement of bully algorithm. In 2014 International Conference on Parallel, Distributed and Grid Computing, pages 457–460. IEEE, 2014.

[33] Ninni Singh and Neelu Jyothi Ahuja. Bug model based intelligent recommender system with exclusive curriculum sequencing for learner-centric tutoring. International Journal of Web-Based Learning and Teaching Technologies (IJWLTT), 14(4):1–25, 2019.

[34] N Singh, A Kumar, and NJ Ahuja. Implementation and evaluation of personalized intelligent tutoring system. Int. J. Innov. Technol. Explor. Eng.(IJITEE), 8:46–55, 2019.

[35] Ninni Singh and Neelu Jyothi Ahuja. Implementation and evaluation of intelligence incorporated tutoring system. Int. J. Innov. Technol. Explor. Eng.(IJITEE), 8:4548–4558, 2019.

[36] Uwe Kay Rakowsky. Fundamentals of the dempster-shafer theory and its applications to reliability modelling. International Journal of Reliability, Quality and Safety Engineering, 14, Issue 06:579–601, December 2007.

[37] Network simulator 2. "http://www.isi.edu/ns".

[38] Puja S Prasad, B Sunitha Devi, M Janga Reddy, and Vinit Kumar Gunjan. A survey of fingerprint recognition systems and their applications. In International Conference on Communications and Cyber Physical Engineering 2018, pages 513–520. 2018.

[39] Santosh Kumar, Mohd Dilshad Ansari, Vinit Kumar Gunjan, and Vijender Kumar Solanki. On classification of bmd images using machine learning (ann) algorithm. In ICDSMLA 2019, pages 1590–1599. Springer, 2020.

[40] G SuryaNarayana, Kamakshaiah Kolli, Mohd Dilshad Ansari, and Vinit Kumar Gunjan. A traditional analysis for efficient data mining with integrated association mining into regression techniques. In ICCCE 2020, pages 1393–1404. Springer, 2021.

[41] Syed Musthak Ahmed, B Kovela, and Vinit Kumar Gunjan. Iot based automatic plant watering system through soil moisture sensing—a technique to support farmers' cultivation in rural india. In Advances in Cybernetics, Cognition, and Machine Learning for Communication Technologies, pages 259–268. Springer, 2020.

[42] Peng-Jung Wu. Nsg2.

[43] Mohd Dilshad Ansari, Vinit Kumar Gunjan, and Ekbal Rashid. On security and data integrity framework for cloud computing using tamper-proofing. pages 1419–1427, 2021.

[44] Amita Kashyap, Vinit Kumar Gunjan, Amit Kumar, Fahimuddin Shaik, and Allam Appa Rao. Computational and clinical approach in lung cancer detection and analysis. volume 89, pages 528–533. Elsevier, 2016.

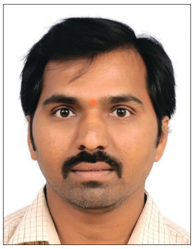
KAVITHA ATHOTA (SENIOR MEMBER, IEEE) is working as an Associate Professor in the Department of Computer Science and Engineeirng, Jawaharlal Nehru Technological University Hyderabad, Telangana, India. Dr. Kavitha has received her Ph.D. degree in Computer Science from University of Hyderabad, M.Tech. and B.Tech. degrees from Jawaharlal Technological University Hyderabad.

Her research interests include Wireless Networks Communication Protocols, Network Security, IoT and Algorithms. She has handled a research project funded by AICTE under research promotion scheme titled "QoS support for real-time traffic in MANETs". Dr.Kavitha was a principal investigator for the project titled "Centre of Excellence on Disaster Management" funded under TEQIP. She has supervised Masters Theses and currently guiding two research scholors. Dr.Kavitha serverd on Technical Program Committee of several conferences and she is also reviewer of serveral prominent journals. Dr.Kavitha is an active member and volunteer of IEEE, ACM and ISTE.

VIJENDER BUSI REDDY was born in Hyderabad, India, in 1982. He received the M.Tech. degree in information technology from IIT Roorkee, Roorkee, in 2006. He has completed Ph.D. from University of Hyderabad. He is working for Advanced Data Processing Research Institute, Secunderanad, India, since 2008 as scientist. His research areas are security in IoT, Deep Learning,Target detections in Remote sensing. He is a permanent member of ASI and IEEE SeniorMember. He received the Best Project Achievement Award from ISRO.

NINNI SINGH, PHD. is an Associate Professor at the Department of Computer Science Engineering at CMR Institute of Technology, Hyderabad (Affiliated to Jawaharlal Nehru Technological University, Hyderabad). She has published research papers in IEEE, Elsevier and Springer conferences, authored several research article most of which are indexed in the SCOPUS database. She joined the academic teaching profession in January 2015. She held the SRF (Senior Research Fellow) position on DST sponsored project funded by Govt. of India total period of 3 years. She served as Assistant Professor at University of Petroleum and Energy Studies Dehradun Uttarakhand.

VINIT KUMAR GUNJAN, PHD. (SENIOR MEMBER, IEEE) is an Associate Professor at the Department of Computer Science and Engineering at CMR Institute of Technology, Hyderabad (Affiliated to Jawaharlal Nehru Technological University, Hyderabad). He has published research papers in IEEE, Elsevier and Springer conferences, 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 a senior member of IEEE, an active volunteer in the IEEE Hyderabad section, and was 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 honour of working with top IEEE leaders. He was received the best IEEE Young Professional award in 2017 from the IEEE Hyderabad Section.



KURUVA LAKSHMANNA has received his B-Tech in Computer Science and Engineering from Sri Venkateswara University College of Engineering -Tirupathi, India in the year 2006, M-Tech in Computer Science and Engineering(Information Security) from National Institute of Technology Calicut, Kerala, India in the Year 2009, and Ph.D from VIT, India in the year of 2017. He is working as an Associate professor in VIT, India. He was a visiting professor in Guangdong University of Technology, China in 2018. He has published research papers in IEEE, Elsevier and Springer, most of which are indexed in the SCOPUS database. His research interests are Machine learning, Data Mining in DNA sequences, IoT, Data Science and Security etc.

ARFAT AHMAD KHAN received the B.Eng. degree in electrical engineering from the University of Lahore, Pakistan, in 2013, the M.Eng. degree in electrical engineering from the Government College University Lahore, Pakistan, 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, UAE. From 2018 to 2022, he worked as a lecturer and senior researcher with the Suranaree University of Technology. Currently, he is working as a senior lecturer and researcher at 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 B.Eng. in Telecommunication Engineering int 2008, M.Eng. in Telecommunication Engineering in 2014 from Suranaree University of Technology, Thailand and Ph.D. in the field of Information and Communication Engineering, from Shibaura Institute of Technology, Japan in 2016. Currently he is an assistant professor at the School of Telecommunication Engineering, Institute of Engineering, Suranaree University of Technology, Thailand. His research interests include wireless network design and optimization, network traffic localization and global engineering education.

• • •