Dynamic Trust-Based Device Legitimacy Assessment Towards Secure IoT Interactions

Vishwanath Garagad, and Nalini Iyer

Original scientific article

***Abstract*—Establishing trust-based interactions in heterogeneously connected devices appears to be the prominent mechanism in addressing the prevailing concerns of confidence, reliability and privacy relevant in establishing secure interactions among connected devices in the network. Trust-based assessment of device legitimacy is evolving given IoT devices' dynamic and heterogeneous nature and emerging adversaries. However, computation and application of trust level in establishing secure communications, access control and privacy domain are rarely discussed in the literature. To compute trust, based on the quality of service, direct interactions, and the relationship between devices, we introduce a multi-factor trust computation model that considers the multiple attributes of interactions in an IoT network of heterogeneous devices providing a wide range of data and services. Direct trust is estimated for quality of service considering the response time, reliability, consistency, and integrity attributes of devices. The time decay factor influences the credibility of computed trust over time. The policy-driven mechanism is employed to sift the devices and isolate the malicious ones. Extensive simulations validate the proposed model's effectiveness using Contiki's Cooja simulator for IoT networks.**

***Index Terms*—Privacy, Security, Internet of things, Trust, Recommendation, Maliciousness, Legitimacy, Convergence Time, Vehicular Network.**

I. Introduction

IoT is an emerging paradigm that changes the way humans and objects interact. It envisions a global network of devices interacting with each other. The edge devices can perform tasks like generating/collecting, storing, processing, infer and forwarding raw data or communicating sensitive and critical information over the network. The edge devices also function as service providers in various applications. Edge devices deal with essential data and services and are prone to vulnerabilities and threats. Edge devices in such models are ubiquitous, heterogeneous, mobile, dynamic, and resource-constrained in terms of processing capabilities, power, memory and bandwidth. Traditional security architecture needs to be tailored to meet the constraints of IoT and WSN models. Security for edge devices refers to protecting the CIA (Confidentiality, Integrity and Availability) of hardware, software and most importantly, data and information. The AAA model achieved these important security goals (Authentication, authorisation and Accounting).

Though authentication and authorization models lay strong security measures to ensure authenticated devices and users participate in the network, they are not adept enough to limit malicious activities of authenticated and authorized devices and users. IoT networks exposed to owners and devices may transform as potential adversaries and perform attacks on other devices for personal gain [1]. Deficiency and inefficiency of control mechanisms to ensure source validation and data accuracy may lead to information credibility issues. Further, misbehaving nodes with close social ties may contribute erroneous data, collude, and monopolize a class of services. With the advent of such threat, models arise the need for a mechanism that can dynamically evaluate the credibility and legitimacy of nodes and manage the access control rights of the nodes [5]. Data security is ensured by estimating the peer device's trustworthiness before interaction [6]. The model, governed by policies to evaluate the trustworthiness of the device and yet feasible enough to be deployed on the resource-constrained edge device [9].

Currently, access control mechanisms like token-based, key-based, role-based, attribute-based, and discretionary based models are employed in the networks of the Internet of Things [10]. Establishing an access control mechanism in IoT is vital to ensure only trusted devices participate in the interaction of data and services. Trust management is the fundamental approach in securing IoT networks [11]. Trust establishment between two interacting devices is achieved based on the observations, experience and recommendations [17]. Each edge device computes the trust of its neighbour. The proposed work proposes a dynamic access control mechanism that considers multiple factors for trust composition and evaluates the neighbour trust based on interaction context. Contributions of the proposed work are as follows:

1) Identifying the attributes of IoT devices in a dynamic infrastructure that can characterize device behaviour to compute trust scores.
2) Map the attributes and trust metrics to the interaction context and develop an interaction control mechanism.
3) Compute and aggregate the trust using multiple attributes to establish a consolidated context-based trust for neighbour edge devices.

The rest of the paper is organized as follows: Section II presents the related work to discuss the overview of trust fea-

Manuscript received February 1, 2022; revised June 6, 2022. Date of publication September 14, 2022. Date of current version September 14, 2022. The associate editor prof. Miljenko Mikuc has been coordinating the review of this manuscript and approved it for publication.

V. Garagad is with the School of Computer Science and Engineering, KLE Technological University, Hubballi, India (e-mail:vishwanath.garagad@gmail.com).

N. Iyer is with the School of Electronics and Electrical Engineering, KLE Technological University, Hubballi, India (e-mail: nalinic@kletech.ac.in).

Digital Object Identifier (DOI): 10.24138/jcomss-2021-0189

tures and trust models based on their nature of implementation and architecture as centralized, distributed and hybrid models. Section III explains the applied methodology and proposed approach. Evaluation and simulation results of the proposed model using Contiki's Cooja simulator is illustrated in section IV. Section VI concludes the paper with the research scope.

II. Related Work

Based on our review of the following literature [19], [24], we summarize, the overview and several characteristics of Trust in section II-A.

A. Overview of Trust

Marsh's Ph.D. Thesis in 1994 deemed the first publication merges the concept of trust with computers and introduces the consideration of trust in computers technology. Over the period, trust is conceptualized and discussed in diverse ways across various application domains in the literature [2], [5], [5], [10], [27]. Trust and reputation-based access control [21] and management are explored concerning various domains, including supply-chains, e-commerce, information systems, cloud systems, academic disciplines, including psychology, economics, and sensor networks [22], [23]. There is no concrete definition of trust despite decades of research on trust. Among the various reports in the literature, one common agreed-upon understanding for trust is a co-relationship between two parties referred to as "trustor" and "trustee". Trustor is an entity/party in need of certain services and thus relies on a second party "trustee" who can provide the service.

Authors in the literature outlines the following properties of trust: [5], [19], [20]

- Trust is dynamic
  The trust between two entities at any instant of time is a result of past interactions and is valid for a certain time frame and is time-dependent. An entity "A" trusting another entity "B" at time (t), may or may not carry the same level of trust at time (t+δt). Trust value of A on B at time (t+δt) is influenced by the interactions between A and B during the period (δt) in addition to its previous trust value at time (t). Hence it can be postulated that trust value evaluated at a certain point of time does not necessarily retain the same value over the indefinite period, and instead, decays over time.
- Trust is asymmetric
  Consider a state where, an entity A trusts B with a trust value of τAB, and B trusts A with a trust value of τBA, then τAB need not be equal to τBA.
- Trust need not be transitive
  Consider a state where an entity A trusts B with a trust value of τAB, and B trusts C with a trust value of τBC, then there exists no condition that A also trusts C, with the same trust value τBC. Although it should be noted that A's trust value computation on C: τAC may be influenced by τBC.
- Trust is context dependent
  Trust value computation of an entity A on B in a certain context C1 need not have the same credence in another context C2.

Referring to the features, trust computation at any point in time, in general, is based on the factors such as sensor data irregularity, past experiences, reliability, computation time, frequency of Interactions, the context of interactions, indirect/recommendation trust and, the credibility of recommending entity [5].

The research community has acknowledged the importance of trust computation and management, and there exist many approaches that pursue the creation of functional systems. However many approaches do not consider the features of IoT devices and their ecosystem [24]. IoT integrates wide range of smart devices(things) with different characteristics to collate, collaborate, and share their services and information to accomplish a task. The devices in IoT are distributed, dynamic, and decentralized. Trust-based access control and management approach proposed in literature are broadly classified into centralized [3], [4], [12] and distributed models [6], [7], [27], [36].

A centralized trust model enhances security by introducing a centralized entity referred as super device in literature. Super device undertakes the complex and computationally intense task of trust computation, evaluation, and storage. Central entity may be a trusted third party (TTP), gateway, broker, or dedicated IoT device. It collects the trust-related information periodically, computes trust value of the device, and stores trust value of all the devices based on their functional and performance attributes. It communicates the trust value of a service provider to a seeker. Centralized model of trust management successfully protects against trust related threats. However concerns associated with centralized models are, firstly how can the central entity be trusted? And secondly how the central entities can trust another devices and communicate?. Such a model is prone to attacks such as Distributed Denial of Service (DDOS), Man in the Middle attack (MIM), and wormhole attack [1]. Some of the prominent consequences of centralized model for trust computation and management are as follows,

- Leads to huge network traffic to address trust related information gathering and handle [2],
- Attacks targeting the central device may disrupt the entire network,
- Memory and computation overhead in the central device.

Distributed trust model employs trust computation mechanisms that are distributed across the network. Sensor devices in a wireless sensor network have a limited communication range limiting direct interaction with the destination node. Hence the information is relayed through other devices. In the process, it is critical to make decisions to identify the trusted route for information transfer. The devices compute the trust of its neighbour and maintain a repository of the computer trust against the neighbouring nodes. The computed trust value is propagated to nodes that want to evaluate the trust of the neighbouring and non-neighbouring nodes. The distributed model decentralizes the computation and storage mechanism. The memory requirement is optimized since every node stores

the trust values of immediate neighbouring nodes only. The neighbour relationship is defined by the communication range of each node. Hybrid trust models are discussed in the literature that tend to implement the computationally intense operations on a central device and lightweight modules. Some prominent trust models reviewed from literature are discussed in section II-B.

B. Trust Models

Application of trust assessment model in data fusion is proposed in [8]. Weighted Trust is considered for trust score computation, using data trust, behavioural trust and historical trust.

Nguyen, et al. [9] proposes a challenge-response approach for initial trust establishment and a trust assessment model is employed to reconsider the trust value over a period of time. The challenge-response(CR) session results to an uncertainty level through information entropy that is transformed to initial trust value. The proposed CR mechanism creates knowledge about a device by investigating its behaviour towards challenges, where uncertainty level is measured based on the probability of the device to provide expected response. Then dynamic trust is evaluated and the initial trust value is considered to be threshold, which in turn ensures to retain or terminate the access session, based on the uncertainty level or trust value.

Access cotrol system is appended by Trust Aware Role-based model to authenticate a new dynamic human user by B. Gwak, et al. [10]. Initial trust establishment is done based on the psychological concept of I-sharing. TARAS follows the reasoning that users with similar roles are more likely to respond in a similar way. TARAS employs the protocol of two-steps Authentication by a Trusted Third Party (TTP) via Two-Factor Authentication method and Role-Identification via Social Networking Service (SNS) account. This protocol limits the applicability of TARAS for cyber-physical systems, where the probability of the service provider and service requester to be human user is minimum. Additionally, it mandates the need for service requester (human user) to possess a mobile phone for TTP authentication and SNS account to gain access, limiting its application for cyber-physical systems. The concept of trust transferability and trust value management can be explored to investigate its applicability for devices in cyber-physical systems to prevent and mitigate the DoS and Data integrity attacks [30].

On the other hand, centralised trust based decision making system for health IoT proposed in [12] uses risk classification, reliability and loss of health probability for building the trust. Trust management is used to effectively collect various geo-tagged health data for making reliable diagnosis and decisions Trust value computed is used to assess the reliability of health data provided by the IoT device. Query/response model is employed in the approach of trust computation. Proposed model claims to address bad-mouthing attack by malicious member but does not considers the immunity against collusion based attacks.

Further, for IoT systems, M. N. Aman, et al. [13] used physical unclonable functions(PUF) to establish mutual authentication.Challenge-response approach is employed between the two entities and facilitates secure session establishment between edge-nodes and edge-node to a server. The session key is generated by the hash function of random numbers generated by both the entities during mutual authentication, which are permanently erased from the memory after session establishment, hence ensures the privacy of challenge-response pair.

Further, trust model for social IoT is introduced by Truong, et.al [15] using recommendation, reputation and knowledge trust metrics to establish trust model. Trust score is estimated for the system entities using fuzzy-based approach. In addition to this adaptive trust management system [27] uses dynamic weighted sum method to assess the trust of the entities in the community of common interests for social IoT.

Trust and Energy Awareness Secure Routing Protocol (TESRP) proposed for WSN [14] employs a distributed approach for trust establishment. TESRP considers the trust level, residual energy and hops to implement a multi-faceted routing strategy in making routing decisions. TESRP channels data through trusted nodes traversing through shorter paths and balancing out energy consumption among trusted nodes. Proposed work in [14] lacks addressing the scalability issues and approaches for mitigating the malicious activities.

Survey conducted [27] by Bao et.al classifies the literature relating to trust management models to summarize the advantages, disadvantages and effectiveness in developing a defense mechanism against infected nodes. The survey identifies the gaps in the literature work but lacks focus on scalability of trust management approaches for IoT applications.

III. Proposed Methodology

This section discusses the proposed methodology for developing, computing and evaluating trust model using direct peer to peer interactions and their behaviour for IoT system. Exhaustive literature review is conducted to develop the understanding the state of art trust models and threat models across various network architecture and to study the change in the behaviour of various attributes of an infected IoT device. Based on the review, metrics are identified that are used in the dynamic computation of direct trust of devices in the IoT network. Considering the classification of [26], our proposed model is characterised as distributed in nature, uses QoS attributes for trust composition, aggregates the trust scores using context and time-decay weighted sum to obtain a single trust. The trust update employed considers a hybrid approach which includes event driven and time-driven updates. The model considers that the devices in the network are able to manage the trust scores of other devices by evaluating the data and services provided by peer devices. The model identifies the behaviour of the peer devices to be malicious or legitimate in order to isolate or engage the device within the network. The implemented model is distributed in nature with all devices of similar features. However, each device in the network is autonomous in its behaviour and independent in the trust computation as discussed in the following section III-A.

A. Trust Computation

Trust computation model constitutes of following phases: neighbour discovery, trust composition, trust propagation, trust aggregation, trust update and trust formation [27].

1) Neighbour Discovery: The primary phase in any network based model is to discover the neighbour participants in the network. This phase is termed as neighbour discovery in the current work. In the proposed technique of neighbour discovery every device identifies its neighbours based on the single hop wireless communication range of the discovering device. The discovering device broadcasts a HELLO message in the network. The neighbour devices that receive the HELLO message acknowledge the message to register itself in the neighbour table or database of the broadcasting device. The process of neighbour discovery is scheduled at periodic intervals to list and de-list the dynamic devices in the network. Newly joined device is registered and listed in the neighbour table and device that fails to acknowledge is de-listed from the neighbour table. Algorithm 1 shows the details of neighbour discovery and database creation:

Algorithm 1 Implementing neighbour table construction

```
for node n:i to N
    open neighbour table
    for node j to N(j!=i)
        if receive acknowledgement message
            insert the value of ID_j in the neighbour table
        end if
    end for
end for
```

2) Trust Composition: Trust composition refers to what components, attributes and factors to be considered for trust computation. behaviour of the IoT device needs to be considered to evaluate the device trust and is measured in terms of attributes like competence, cooperativeness, reliability, honesty, consistency, unselfishness, response time [3], [4], [27], [36]. In the proposed work, we compute direct trust by self experience of device with the neighbouring device by considering the factors as consistency, response time and honesty. The direct trust is computed using weighted aggregation of trust score with reference to multiple attributes of the device. The weights for trust score obtained from consistency, response time and honesty is referred to as α, β and γ as shown in equation 1. Consistency and Honesty together attribute the context of reliability and response time attributes the context of availability.

$$T_{direct}{}_A^B = X + Y + Z \tag{1}$$

where,

$$X = \alpha * Con_{Trust}{}_A^B$$
$$Y = \beta * Hon_{Trust}{}_A^B$$
$$Z = \gamma * Rt_{Trust}{}_A^B$$

Such that,

$$\alpha + \beta + \gamma = 1$$
$$\{\alpha, \beta, \gamma\} \in [0, 1]$$

The values of α, β and γ are context dependent and can be used to evaluate the trustworthiness of the device in a specific context of choice by the truster device. In general case, as considered in this paper the values of weights are considered to be of equal weight of 0.33 each.

Consistency(*ConTrust*) is the ability of the edge device to respond on request. The response to the request may either be in the form of availability or denial of resource, data or service based on the type of request. Approval or denial of service is considered as success or failure [27]. The consistency in term of data is computed using the packet delivery ratio (PDR) and service response ratio (SSR) based on context of interaction.

Honesty(*HonTrust*) is the measure of integrity behaviour of edge device with respect to the data/service. HonTrust is used to quantify the reliability of a device/user on other regarding the correctness of information or service rendered in a given context. The ideology and interpretation of the concept of honesty is adopted from [28], [29]. In the proposed context, trust based on honesty is computed by the evaluating device for the device under observation based on how the device responds to a data or service request. Ensuring the integrity of data and service by assuring non-disclosure and non-tampering [30], maps to the honesty factor. Honesty attribute of the device is characterized by its nature to retain the integrity of the packet data. It is quantified by correlating the packets received by truster for coherence as shown in equation 2.

$$Hon_{Trust}{}_A^B = \frac{\left\|CP_A^B\right\|}{\left\|CP_A^B + NCP_A^B\right\|} \tag{2}$$

where,

CP_A^B : Number of packets with coherency above threshold
NCP_A^B : Number of packets with coherency below threshold

Response time(*RtTrust*)is the measure of availability of the device and the average time taken by the neighbouring devices to respond to a request. Requesting device 'A' keeps track of the response time of device 'B' for all the request generated in within an interval of T (60 seconds). Every request initiates a local timer in requesting device to track the response time. The average of all the response times is used to compute RtTrust as shown in algorithm 2 .

3) Trust Propagation: Trust propagation refers to communication of trust values computed by each device to the neighbouring devices that can possibly also belong to different cluster, community and type. Proposed work in this paper implements a distributed trust propagation mechanism for wireless sensor network where devices maintain the trust forwarding information of their neighbouring devices. Distributed model eliminates the need for a centralised entity. The trust propagation is interaction based where the device shares its trust table entry to the peer device with which it interacts.

Algorithm 2 Implementing neighbour table construction

```
for node n_Req
Initialize respCount to 0
Initialize totalRespTime to 0
    Start Timer1
    while Timer 1 ≤ 60
        if requestSent_#i
            Start TimerResp_#i
            Increment respCount
        end if
        if respReceived_#i
            Stop TimerResp_#i
            totalRespTime += TimerRespVal_#i
            Reset TimerResp_#i
        end if
    end while
    Reset Timer1
    Compute AvgRespTime
        AvgRespTime = totalRespTime / respCount
    if AvgRespTime ≥ δ_Thres
        RtTrust = 1
    else
        RtTrust = (δ_Thres - AvgRespTime)/δ_Thres
    end if
end for
```

4) Trust Aggregation: Trust aggregation is combining all the trust values computed by self and collected from neighbouring devices in the form of recommendation trust. The truster device estimates the trustworthiness of trustee based on it 'A' s self experience and direct interactions with the trustee 'B' and computes the trust scores referred to as ${T_{direct}}_A^B$. Reliability of the trust computation is improved by considering the peer recommendations for the trustee. The recommendations of the mutual neighbour peers is used to compute the indirect trust score referred to as ${T_{indirect}}_A^B$. Trust aggregation is an important phase of trust computation and should counter the recommendation based threats in trust based model [31]. Major trust aggregation techniques discussed in the literature include simple average, weighted sum, credibility weighted average, Bayesian inference, fuzzy logic [32] and belief theory [33], [34]. Trust aggregation in the presented work includes credibility weighted recommendations from neighbouring device with context of interaction as an additional factor as shown in Equation 3 and 4. The trustworthiness computed by the truster towards recommending peer is considered to estimate the credibility of its recommendations towards other peer devices in Equation 4. Each device maintains a trust table in the network for its neighbouring devices. Trust table tabulates the number of interactions and respective trust values computed using each factor *ConTrust, HonTrust, RtTrust* and respective weightages based on the context of trust evaluation.

$$wTrust_i^B = A + B + C \tag{3}$$

where,

$$A = \alpha * {Con_{Trust}}_i^B$$
$$B = \beta * {Hon_{Trust}}_i^B$$
$$C = \gamma * {Rt_{Trust}}_i^B$$

$${T_{indirect}}_A^B = \frac{\sum_{i=1}^{N} {Cred_{Factor}}_A^i * wTrust_i^B}{(N)} \tag{4}$$

where,

$${Cred_{Factor}}_A^i = {T_{indirect}}_A^B$$
$$\alpha + \beta + \gamma = 1$$

5) Trust Update: Trust update refers to the instant at which the trust score computed is updated. Literature demonstrates event driven and time driven trust update schemes. We propose a hybrid approach for trust update that includes both event based and time based trust update schemes. The trust scores for consistency and honesty are updated event based and time based update is followed for response time trust scores. The response time based trust score and overall trust of neighbouring devices is computed at a regular frequency.

6) Trust Formation: Trust formation refers to the process of computing the overall trust as shown in Equation 5 considering the self experienced trust computed in Equation 1 with weight w1 and neighbour device recommendations with weight w2 as shown in Equation 4. The final trust value of A on B is computed as in Equation 6, considering the past history of trust value as $HistTrst_A^B$ with the weightage W_{his} which considers the impact of time decay, where $T_{interval}$ is the interval between last update and current update. The devices are prone to demonstrate extrement good or bad behaviour under circumstances such as malicious behaviour or some operational issues. Such sudden behavioural change may influence the trust computation in an abrupt way. Consideration of $HistTrst_A^B$ in the computation of $Trust_A^B$ regulates the influence of such behaviour.

$$CurrentTrust_A^B = w1 * {T_{direct}}_A^B + w2 * {T_{indirect}}_A^B \tag{5}$$

$$Trust_A^B = W_{his} * HistTrst_A^B + (1 - W_{his}) * CurrTrst_A^B \tag{6}$$

$$W_{his} = r1 * T_{interval} * e^{(-r2 * T_{interval})} \tag{7}$$

where,

$$w1 + w2 = 1,$$
$$(w1, w2) \in R,$$
$$(0 < w1 < 1) and$$
$$(0 < w2 < 1).$$

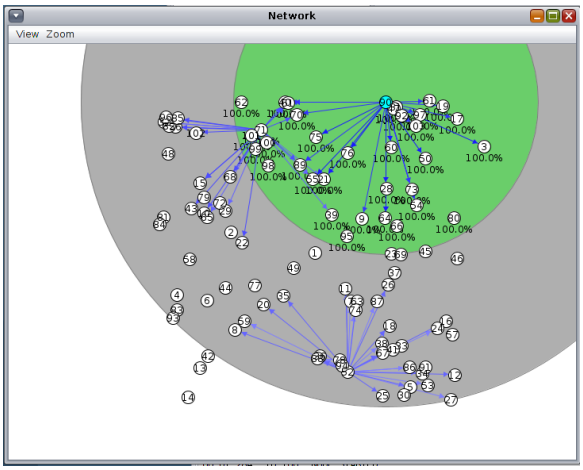

Fig. 1. Network Topology in Announcement Mode for Neighbour Discovery.

IV. Results

Numerous simulation based experiments are conducted on Contiki's Cooja simulator [25] to study the behaviour of node in case of attacks. The experiments are conducted with various run times of the computation model and inducing varied number of malicious nodes in the network to determine the efficiency and performance of model in terms of convergence time to detect the malicious/infected node. Table 1 shows the simulation environment parameters.

TABLE I
Simulation Parameters

Parameter	Value
Network Size	400m x 400m
Number of Nodes	5-500
Malicious Nodes	2-400
Simulation Time	3600 s
Trust Computation Run Time	30s to 90s

In the current work, the proposed model for computing trust for direct observations commences with the discovery of neighbour devices, where devices are capable to interact via unicast, multicast and broadcast communications. Neighbour device discovery and service discovery is implemented using the announcement primitive and updated in the neighbour database. as shown in Figure. 1.

The discovered devices are registered and retained for a defined time period T_{ret}, if available for interaction. The entry corresponding to the device is cleared, if the device don't respond or interact during a defined schedule. The neighbour discovery table update and entry of neighbouring devices is shown in figure 2.

Trust scores are being computed in terms on consistency, honesty and response time as shown in Figure. 3. Output window of simulator for response time trust using turn around time is shown in Figure.4.

In the experimentation phase, we have deployed nodes in the 400m x 400m rectangular flat space with random distribution of identical Tmote/skymote devices. Following experiments were conducted:

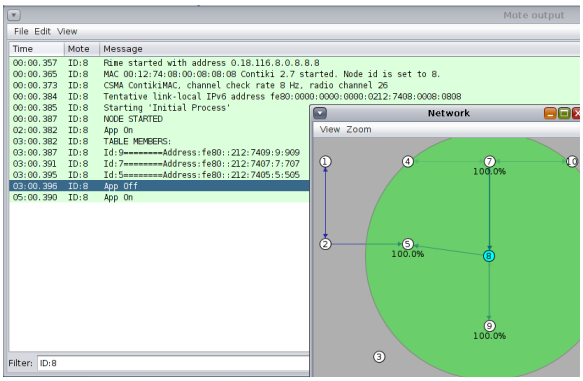

Fig. 2. Network Discovery Table Entry of neighbours.

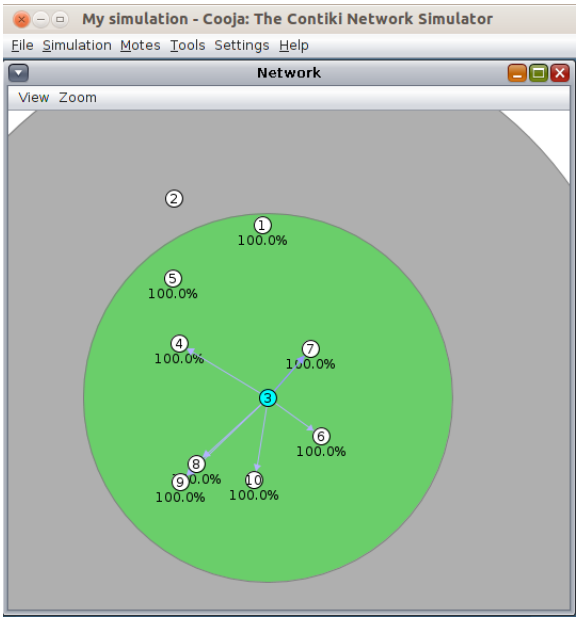

Fig. 3. Trust Computation.

07 : 21 . 288	ID: 2	debug Tag:	1 :: (2.0)	<->	(3.0) TAT	: 66
11 : 00 . 895	ID: 3	debug Tag:	1 :: (3.0)	<->	(4.0) TAT	: 46
14 : 40 . 895	ID: 3	debug Tag:	2 :: (3.0)	<->	(4.0) TAT	: 46
14 : 41 . 305	ID: 4	debug Tag:	1 :: (4.0)	<->	(3.0) TAT	: 15
18 : 20 . 893	ID: 3	debug Tag:	3 :: (3.0)	<->	(4.0) TAT	: 46
18 : 21 . 305	ID: 4	debug Tag:	2 :: (4.0)	<->	(3.0) TAT	: 15
22 : 01 . 305	ID: 4	debug Tag:	3 :: (4.0)	<->	(3.0) TAT	: 15
25 : 40 . 895	ID: 3	debug Tag:	4 :: (3.0)	<->	(4.0) TAT	: 46
25 : 41 . 306	ID: 4	debug Tag:	4 :: (4.0)	<->	(3.0) TAT	: 15
29 : 20 . 769	ID: 3	debug Tag:	5 :: (3.0)	<->	(4.0) TAT	: 30
29 : 21 . 306	ID: 4	debug Tag:	5 :: (4.0)	<->	(3.0) TAT	: 15
33 : 01 . 017	ID: 3	debug Tag:	6 :: (3.0)	<->	(4.0) TAT	: 62
33 : 01 . 305	ID: 4	debug Tag:	6 :: (4.0)	<->	(3.0) TAT	: 15
36 : 40 . 767	ID: 3	debug Tag:	7 :: (3.0)	<->	(4.0) TAT	: 30
36 : 41 . 305	ID: 4	debug Tag:	7 :: (4.0)	<->	(3.0) TAT	: 15
40 : 20 . 767	ID: 3	debug Tag:	8 :: (3.0)	<->	(4.0) TAT	: 30
40 : 21 . 305	ID: 4	debug Tag:	8 :: (4.0)	<->	(3.0) TAT	: 15
44 : 00 . 894	ID: 3	debug Tag:	9 :: (3.0)	<->	(4.0) TAT	: 46

Fig. 4. Response Trust Computation using Turn Around Time (TAT)

1) The deployed nodes had fixed positions during the entire simulation period. Random nodes were added and removed to validate the neighbour discovery and update process. The neighbour table update for listing and de-

TABLE II
CONVERGENCE TIME (IN SECONDS) OF PROPOSED MODEL WITH VARIED NETWORK SIZE AND INFECTED DEVICES

	Total Device Count						
Infected Device Count	5	10	50	100	200	300	500
2	32	38	47	58	67	72	91
5	65	57	65	69	72	76	97
8	*	62	67	72	79	82	98
10	*	81	73	75	81	87	101
50	*	*	82	79	87	91	116
100	*	*	*	91	89	98	127
200	*	*	*	*	102	107	164
400	*	*	*	*	*	*	228

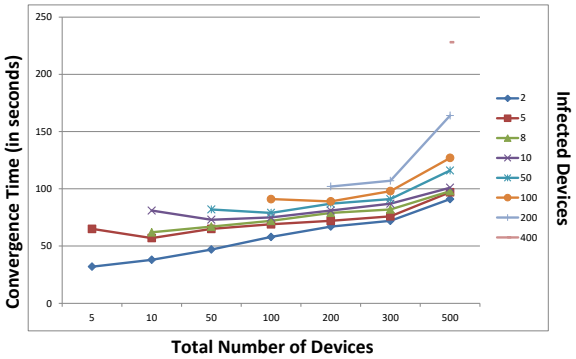

Fig. 5. Convergence time to identify infected device count against total device count.

listing the devices is validated.

2) Randomly some devices were selected as infected and their behaviour was maligned. Malicious sensors were programmed to deviate from the expected behaviour in the case of data sourcing and forwarding at timed frequencies. The sensors tend to infuse malicious data or try to modify the forwarded data packets. The malicious behaviour impacts the integrity of the data. This experiment simulated the situation that a device is captured, infected or a infected device is induced in the network. Convergence time of identifying the infected device is measured for a fixed run time of 60 seconds, 120 second by varying the number of infected devices in the network. The observations are summarised in Table 2:

Convergence time is an important assessment metric of the correctness of trust model and also indicate the effectiveness of the mechanism [35]. Convergence time in the context of detecting the malicious devices is the time taken to arrive at a consensus about the trustworthiness of a trustee device based on the self-assessment and peer recommendation aggregations. Convergence is the rate at which the model arrives at a consensus for varied total network density and malicious device ratio as compared to network density. To obtain the convergence behaviour of the model, we have simulated the model for network size N=5,10,50,100,200,300 and 500 and malicious node count M=2,5,8,10,50,100,200 and 400 as shown in table 2. Figure. 5 depicts the convergence rate of the model for above mentioned experimental set-up. The results obtained demonstrate a reasonable improvement in the convergence time as compared to global convergence time (GCT) demonstrated in [36] by using broker devices for trust aggregation for network size of 1000. Yet, the concern is with the increasing network size. The convergence time is observed to be very high with the increasing network size as the aggregation algorithm get computationally time consuming to process for multiple neighbouring devices. Further experimentation's with highly scaled network size as demonstrated by [36] will yield comparable results.

Experimental results depicted in Figure. 5 represent peak convergence time in cases where majority participants in the network are infected or malicious. In such scenarios, the decision making process in computationally complex and results into in-appropriate conclusions. In some iterations the model did not converge to a stable state for the entire period of simulation. The results are presented here based on averages of multiple iterations.

V. CONCLUSION

This paper aims to introduce the concept of trust in establishing distributed security in IoT through the existing trust management models and propose a dynamic and distributed trust assessment model. The primary contribution of this work is the development of dynamic trust model using multi factor based trust computation to identify and isolate the infected devices in an IoT network. Weighted averaging is applied to consider and aggregate the independent recommendation from the neighbour devices. Malicious node were implemented to perform bad-mouthing to analyze effectiveness of model. The experiments conducted in the presented work shows improvement in the performance and efficiency of the model with an improvement in the convergence time and run time to detect the infected/malicious devices as compared to Global Convergence Time (GCT) in [36] for trust aggregation in a network of 1000 devices. Validating the efficacy of proposed model on real IoT network such as vehicular network and exploring the aggregation techniques to combine the recommendations are the future research directions.

However many open issues persist and further refinements need to be applied to trust forwarding and aggregation techniques. Aggregation of subjective and independent agents for decision making provides huge scope for improvement in the aggregation algorithm and paves path for research opportunities in the domain of trust management models. IoT and Edge computing are providing contemporary dimensions for research in the domain SAMIE. Lack of proven and accepted trust management models in IoT is retarding the emergence of IoT edge computing.

REFERENCES

[1] A. Tandon and P. Srivastava. "Trust-based Enhanced Secure Routing against Rank and Sybil Attacks in IoT," *Twelfth International Conference on Contemporary Computing (IC3)*, Noida, India, pp. 1-7, 2019.

[2] Noshina Tariq, Muhammad Asim, Zakaria Maamar, M. Zubair Farooqi, Noura Faci, Thar Baker, "A Mobile Code-driven Trust Mechanism for detecting internal attacks in sensor node-powered IoT",*Journal of Parallel and Distributed Computing*,Volume 134,Pages 198-206, ISSN 0743-7315,2019.

[3] Saied, Y. Ben, A. Olivereau, D. Zeghlache, and M. Laurent. (2013) "Trust Management System Design for The Internet of Things: A Context-Aware And Multi-Service Approach," *Computers Security*, 351–365.
[4] Saied, Y. Ben, A. Olivereau, D. Zeghlache, and M. Laurent. (2014) "Lightweight Collaborative Key Establishment Scheme for the Internet of Things." *Computer Networks*, 273–295.
[5] Y. Yang, L. Wu, G. Yin, L. Li and H. Zhao. "A Survey on Security and Privacy Issues in Internet-of-Things," in *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1250-1258, 2017.
[6] Chen, I. R., J. Guo, and F. Bao., "Trust Management for SOA-Based IoT and Its Application to Service Composition." *IEEE Trans.Serv. Comput.*, 482–495.
[7] [20] Chen, I. R., F. Bao, and J. Guo (2016) "Trust-Based Service Management for Social Internet of Things Systems." *IEEE Trans. Dependable Secur. Comput.*, 684–696.
[8] Chen Z, Tian L, Lin C. Trust Model of Wireless Sensor Networks and Its Application in Data Fusion. Sensors (Basel). 2017 Mar 28;17(4):703. doi: 10.3390/s17040703. PMID: 28350347; PMCID: PMC5421663.
[9] T. Nguyen, D. Hoang, D. Nguyen and A. Seneviratne, 2017. "Initial trust establishment for personal space IoT systems," *IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, Atlanta, GA, pp. 784-789, 2017.
[10] B. Gwak, J. Cho, D. Lee and H. Son. "TARAS: Trust-Aware Role-Based Access Control System in Public Internet-of-Things,". *17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, New York, NY, pp. 74-85, 2018.
[11] Alshehri, M.D., Hussain, F.K. Hussain, O.K. Clustering-Driven Intelligent Trust Management Methodology for the Internet of Things (CITM-IoT). *Mobile Netw Appl 23*, 419–431 (2018).
[12] I. R. C. H. Al-Hamadi, "Trust-based decision making for health iot systems," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1408–1419, 2017.
[13] M. N. Aman, K. C. Chua and B. Sikdar, "Mutual Authentication in IoT Systems Using Physical Unclonable Functions," in *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1327-1340, Oct. 2017, doi: 10.1109/JIOT.2017.2703088.
[14] Ahmed, A., Bakar, K.A., Channa, M.I. et al. A Secure Routing Protocol with Trust and Energy Awareness for Wireless Sensor Network. *Mobile Netw Appl 21*, 272–285 (2016). https://doi.org/10.1007/s11036-016-0683-y
[15] Truong, N.B., Um, T.W., Lee, G.M.: A Reputation and Knowledge Based Trust Service Platform for Trustworthy Social Internet of Things. —textslInnovations in Clouds, Internet and Networks (ICIN), Paris (2016).
[16] J. Yuan and X. Li. "A Reliable and Lightweight Trust Computing Mechanism for IoT Edge Devices Based on Multi-Source Feedback Information Fusion," in *IEEE Access*, vol. 6, pp. 23626-23638, 2018. doi: 10.1109/ACCESS.2018.28318986
[17] S. Asiri and A. Miri. "An IoT trust and reputation model based on recommender systems," in *Proc. 14th Annu. Conf. Privacy, Secur. Trust (PST)*, pp. 561568, 2016.
[18] F. Bao, Chen, R., Guo, J., "Scalable, Adaptive and Survivable Trust Management for Community of Interest Based Internet of Things Systems," in *11th International Symposium on Autonomous Decentralized System*, Mexico City, Mexico, 2013.
[19] Pranata, I., G. Skinner, and R. Athauda. (2012) "A Holistic Review on Trust and Reputation Management Systems for Digital Environments." *Int. J. Comput. Inf. Technol.*, 44–53.
[20] Grandison, T., and M. Sloman. (2000) "A Survey of Trust in Internet Applications." *IEEE Communication Surveys Tutorials*, 2–16.
[21] Abdelmuttlib I., Siti H., Abdullah G., Suleman K., Muhammad K.,. Trust and reputation for Internet of Things: Fundamentals, taxonomy, and open research challenges, *Journal of Network and Computer Applications*, Volume 145, 102409, ISSN 1084-8045, 2019.
[22] Y. Yu, K. Li, W. Zhou, and P. Li, "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures," *Journal of network and computer applications*, vol. 35, pp. 867-880, 2012.
[23] G. Caronni, "Walking the web of trust," in Proceedings of textsl9th IEEE International Workshops on Enabling Technologies (WETICE), 2000.
[24] I. Ud Din, M. Guizani, B. Kim, S. Hassan and M. Khurram Khan. "Trust Management Techniques for the Internet of Things: A Survey," in *IEEE Access*, vol. 7, pp. 29763-2978, 2019. doi: 10.1109/ACCESS.2018.2880838
[25] Contiki, http://www.contiki-os.org/, [Online; accessed 02-April-2019].
[26] Guo, J., Chen, I., Tsai, J. P. (2017). A survey of trust computation models for service management in Internet of Things systems. *Computer Communications*, 97(1), 1–14.
[27] F. Bao, Chen, R., Guo, J., "Scalable, Adaptive and Survivable Trust Management for Community of Interest Based Internet of Things Systems," in *11th International Symposium on Autonomous Decentralized System*, Mexico City, Mexico, 2013.
[28] Azzedin, F.A. "Trust Modeling and Its Applications for Peer-to-Peer Based Systems". *Ph.D. Thesis*, University of Manitoba, Winnipeg, Manitoba, 2004.
[29] Azzedin, F. "Taxonomy of reputation assessment in peer-to-peer systems and analysis of their data retrieval". *The Knowledge Engineering Review*, 29(4), 463-483. doi:10.1017/S026988891400017
[30] V. G. Garagad , N. C. Iyer , and H. G. Wali , "Data Integrity: A security threat for internet of things and cyber-physical systems," *2020 International Conference on Computational Performance Evaluation (ComPE)*, 2020.
[31] V. Busi Reddy, A. Negi, S. Venkataraman and V. R. Venkataraman, 2019, "A Similarity based Trust Model to Mitigate Badmouthing Attacks in Internet of Things (IoT)," *IEEE 5th World Forum on Internet of Things (WF-IoT)*, Limerick, Ireland, pp. 278-282, 2019.
[32] D. Chen, 2011. "TRM-IoT: A trust management model based on fuzzy reputation for Internet of Things," *Comput. Sci. Inf. Syst.*, vol. 8, no. 4, pp. 1207–1228.
[33] V. Busi Reddy, S. Venkataraman and A. Negi, 2017. "Communication and Data Trust for Wireless Sensor Networks Using D–S Theory," in *IEEE Sensors Journal*, vol. 17, no. 12, pp. 3921-3929.
[34] R. Feng, X. Xu, X. Zhou, and J. Wan,. "A trust evaluation algorithm for wireless sensor networks based on node behaviors and D-S evidence theory," *Sensors*, vol. 11, no. 2, pp. 1345–1360, 2011.
[35] X. Li, F. Zhou, and X.Yang, "Scalable feedback aggregating (SFA) overlay for large-scale P2P trust management", *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 10, pp. 1944-1957, Oct. 2012.
[36] J. Yuan and X. Li, "A Reliable and Lightweight Trust Computing Mechanism for IoT Edge Devices Based on Multi-Source Feedback Information Fusion," in *IEEE Access*, vol. 6, pp. 23626-23638, 2018.
[37] F. Samie, V. Tsoutsouras, L. Bauer, S. Xydis, D. Soudris, and J. Henkel, "Computation offloading and resource allocation for low-power IoT edge devices," in *Proc. IEEE 3rd World Forum Internet Things (WF-IoT)*, pp. 7-12, Dec. 2016.

Vishwanath Garagad is a research scholar and assistant professor at KLE Technological University, Hubli, Karnataka, India(2016). He obtained Bachelor Degree in Electronics and Communication Engineering from B.V.Bhoomaraddi College of Engineering and Technology, VTU Belgaum(2009) and Masters Degree in VLSI Design and Embedded Systems from VTU Belgaum(2014). His researches are in fields of image processing, IoT security, electronics, digital systems, and embedded systems.

Nalini Iyer is currently heading School of Electronics and Communication Engineering at KLE Technological University, Hubli, Karnataka, India. She obtained Ph.D. in Electronics and Communication (Information Security Algorithm Optimization and Architectures, VTU Belgaum) in 2014. Her researches are in fields of Cryptography, Hardware Security, Embedded systems for autonomous functions(Autonomous Vehicle), Vehicular Communication and VLSI Design.
She is affiliated with IEEE and has served as in-vited reviewer. Besides, she is also involved in student associations, curriculum design and outcome based education pedagogy development activities in the university.