A Reliable Lightweight Trust Evaluation Scheme for IoT Security

Hamad Aldawsari, Abdel Monim Artoli
Department of Computer Science, College of Computer and Information Sciences,
King Saud University, Riyadh 11543, Saudi Arabia

***Abstract*—The rapid development of smart devices and the consequent demand their reliability have posed many challenges limiting their versatility. One of the most significant challenges is safeguarding the widespread network of sensors and devices within harsh remote environments. Numerous trust schemes have been proposed to overcome related IoT security concerns. However, most of these schemes are not lightweight and consequently are not energy-efficient. This paper proposes a reliable lightweight trust evaluation scheme (RTE) to mitigate the malicious behavior of the nodes within IoT networks. The nodes are grouped into a set of clusters each having a cluster head while cluster members are categorized by evaluating their associated residual energy. Nodes with residual energy lower than the threshold (which is determined by the base station) are suspended until they recover and regain their activity. The computations are handled by the CH which is elected by an algorithm according to its energy and coverage degree in order to optimize the energy consumption in the network. For validation and performance evaluation, the proposed RTE scheme was compared to three of the recent schemes in its category. The obtained results have revealed that the proposed RTE scheme outperforms all of them in terms of detection rate, trust evaluation time, and energy efficiency.**

Keywords*—IoT security; clustering; trust; energy efficient algorithm

I. Introduction

The Internet of Things (IoT) is cumulatively improving the way of our life at a stunning pace. Basically, IoT can be referred to as the technology that provides a network allowing people, things, applications, and data to connect with each other through the Internet. This enables remote control, management, and interactive integrated services to be done easily, smoother, faster, and more reliable. IoT benefits several applications in different fields such as, but not restricted to, medical care, agriculture, and economics. IoT can be viewed as the smart infrastructure enabling numerous advantages while saving costs and ensuring efficiency. IoT things (Devices) should be able to control their resource access policy, for example, which device can gain access to its humidity resource. The hurdle is that the connected devices have limited resources that restrict their ability for storing and processing access policy information [1]. Another critical issue is that devices are dynamically added and deleted from IoT networks thus as a consequence, requiring the devices to update their access policy. Moreover, with this enormous number of connected devices, a highly scalable, secure, and reliable IoT management system is needed. Another crucial issue is the attacks which maybe initiated by some nodes participated in the network. One of the well-known attacks in this area is the brute force attack. This attack can be viewed as an attacker submitting numerous passwords or passphrases with the desire for in the long run speculating a blend accurately. In other words, the attacker is methodically checking every single imaginable password until the right one is caught. Then again, the attacker can endeavor to figure the key which is commonly made from the secret key utilizing a key inference work. This process is referred to as an exhaustive key search. Several attempts have been done in this direction but, however, they are based on centralized architecture assuming that devices are distributed statically. Specifically, most current IoT systems are built on a centralized client/server model, which requires all devices to be connected and authenticated through a centralized server. This model, however, would not be able to provide the need to disseminate the IoT system in the future which contradicts the real situations where devices are mobile like such as in IoT vehicle-to-vehicle scenarios which prevent IoT scalability. In this context, we provide a reliable light-weight trust evaluation (RTE) scheme able to maintain the trust between communicating devices to alleviate the risky effects of security-related issues. The main interesting point about RTE is its ability to achieve trust while consuming a very little amount of network energy which makes it a promising choice for scalable IoT-networks.

It is worth noting that IoT-WSN is paving its way as promising market segments [2]. The problem with IoT-WSN, however, is that all the involved sensor nodes have the permission to send data directly to BSs. This leads to consuming a large amount of stored energy, especially, with the nodes located far away from BSs. Clustering can be a solution to this problem wiht each cluster contains a set of sensor nodes while setting one of them as the cluster head (CH); aka coordinator. In this manner, CH is responsible for collecting the sensed data in its cluster and sends it to BS, while being the only permitted node to send to BS in its cluster. However, despite the phenomenal development of IoT-WSN, a number of issues still need more research work. The most hazardous issue, that comes in the first place, facing IoT-WSN is the security that threatens the deployment of IoT applications. In the second place, IoT is facing an energy efficiency issue. This is due to the usage of resource-constrained wireless sensors in several applications [3].

Despite the fact that there exists a large number of security techniques, it is indeed challenging to apply these technologies directly in IoT systems. This is due to following reasons [4]. First, the energy-sources limitation of sensor node which hamper the implementation of the security algorithms on the sensor node side [5]. Second, the potential physical risk due to installing the sensor node in harsh remote areas [6]. Third,

the security concerns as the sensor-people may have direct interaction with humans and the environment [7]. Finally, the heterogeneous of IoT network in which several types of sensor nodes are integrated in the IoT system [8]. This heterogeneity hinders the cooperative behavior between the sensor nodes [9]. These deficiencies deteriorate the performance of the IoT system which, in turn, exposes the system to serious attacks [10].

In literature, cryptography techniques made great efforts in mitigating security issues, for which the cryptographic-based systems are considered more effective with respect to the security concerns. However, these cryptography techniques depend on public-key schemes with powerful computing capabilities which lead, in turn, to higher energy consumption. This restricts the usage of such technique for achieving security in limited-resources sensor nodes. Still, the cryptographic technique requires a fixed infrastructure with centralized administration which, to some extent, contradicts with IoT concept of scalability; aiming to achieve a decentralized nature. This raises another security aspect known as internal attacks [11], where the attacks come from inside the network. As per the literature, trust-based technique [12] is considered the alternative that is able to resolve the security issue in IoT systems. Formally, trust is the level of confidence in a person or thing. In IoT systems, trust reflects the degree of belief or confidence about other nodes based on their past interaction and observation. Recently, it has been widely agreed that trust mitigates the problem of access control, providing reliable routing path and security mechanisms. Therefore, communication between nodes in the IoT system should be done under the supervision of trust. The problem with the trust technique, however, is twofold. First, the misleading information communicated from malicious nodes negatively impact the trust computation. This problem is exacerbated strongly if the network contains numerous illegitimate sensor nodes. To elaborate further, such nodes provide fake recommendations that confuse the task of CHs in evaluating trust. This problem, also, hurts the CH of BSs. Second, not all the involved sensor nodes provide recommendations to CH which results in an inaccurate trust computation. To elaborate further, sensor nodes with either low bandwidth or limited energy may prefer to preserve their resources; i.e., do not send recommendations, for actual data transfer. This results in a non-cooperative behavior among sensor nodes. Such bad-behavior not only compromises the network security but also deteriorates its limited resources and results in unbalanced energy consumption among nodes in the network.

Several studies have been devoted to optimization of trust computation based on different methods and theories such as game theory [17], matrix theory [14], beta distribution [16], weighting [13], and Bayesian statistics [15]. However, it is worth mentioning that all attempts of the aforementioned studies results in increasing the energy consumption and network complexity. This, in turn, makes the network vulnerable to several attacks [18]. Thus, the idea is to design a less complex attestable lightweight trust evaluation scheme that alleviates the consequences of non-cooperative behavior of the nodes. Specifically, in this work we design a reliable trust evaluation (RTE) scheme for lightweight security, energy-efficient, free of the current trust evaluation schemes limitations. Several experiments were carried out to assess the performance of RTE. The end result is a promising security framework. For further vali-dation, a case study was carried out assessing the ability of RTE to ban the brute force attack. The results show its superiority.

The rest of this article is organized as follows. Section II covers related work. Section III describes the proposed Model. In Section IV, experimental work is presented to validate the approach and evaluate its performance. Finally, concluding remarks are presented in Section V.

II. Related Work

Trust evaluation is one of the prominent research directions in the IoT security, and it is characterized by two key issues: trust metrics and trust computational methods, [20]. Researchers in this field are challenged to achieve a balance between security requirements and energy efficiency in variant IoT environments. This section reviews the related attempts that have been done in the context of trust evaluation schemes in IoT networks. Khalil et al. [21] presented a framework based on a Fuzzy Logic model to evaluate the security trust level for each IoT node. The node is trusted if its trust level is greater than a threshold defined by the user. Only the trusted nodes are permitted to collect the critical information. Chen et al. [22] presented a trust architecture called IoTrust, integrating SDN with a cross-layer authorization protocol, and used two reputation evaluation schemes for node and organization. These schemes are efficient in defending against modification, replay, and message dropping attacks, with high detection accuracy. However, one of the main drawbacks of this technique is disregarding malicious user and organization behaviors, which could generate fake reputation values. Another research has been done to evaluate trust among devices in SDN-enabled home networks using a blockchain-based trust assessment framework. Boussard et al. [23] proposed such a system called STewARD which computes the trust score for each connected device based on its historical behavior. Then, this score is used to judge whether the node is permitted to connect to the crowd or not if it meets the required trust level assigned by the user. One drawback of this framework is that it has not yet proven the convergence of the underlying reputation system. However, it is still under development and its scalability problems should be solved. Other frameworks were conducted in the field of edge computing, Gao et al. [24] proposed a service-driven collaboration mechanism among IoT edge devices using multidimensional trust evaluation, in addition to a double-filtering design to filter the feedback from malicious devices in an efficient way. This mechanism applied low-overhead algorithms, which had an excellent performance in defeating malicious behaviors and improved the reliability of the IoT edge environment. However, the flexibility should be improved by optimizing the data aggregation technique. Another attempt was implemented for the security of Industrial IoT. Wang et al. [25] proposed an intelligent mobile edge computing-based trust evaluation scheme (MTES). The trustworthiness of sensor nodes has been evaluated by the mobile edge nodes which had relatively strong computation and storage ability. This mechanism could distinguish compromised and malicious nodes and decrease the energy consumption of the entire network. Dass et al. [26] proposed a trust evaluation model to compute the trustworthiness of the data generated from the participating nodes in an intelligent transport system. They

considered direct and indirect trust mechanisms for each of the sensor nodes and update their trust measures at regular intervals of time. They achieved a high detection rate and a low false detection rate. However, as all the operations are performed at the cloud server, it causes a delay in trust assessment, which do not suit real time scenarios. Recently, the deployment of machine learning algorithms in trust evaluation for IoT devices were widely investigated. Jayasinghe et al. [27] proposed a quantifiable trust assessment model based on machine learning principles. The model is consisted of three sub-models that classify the extracted trust features and combine them to produce a final trust value to be used for decision making. While Ma et al. [28] used a deep learning algorithm and adopted trust metrics based on comprehensive network behaviors in trust evaluation, to build a behavioral model for a given IoT device, and predict the trust status of this device which is used for decision making. These algorithms are still in their elementary stages, and need to be more flexible and practical, also the privacy issue of the training datasets needs to be considered. These algorithms consume are applicable for dedicated applications where the number of IoT devices is limited. They provide a high degree of security in the network, while consuming power heavily, and causing delay to the system due to complex computations. Therefore, the accomplishment of lightweight security algorithms is strongly demanded. Sedjelmaci et al. [29] proposed a light weight hybrid intrusion detection system, in which the game theory concept is employed to overcome the challenge of high-energy consumption in HIDS. For this purpose, the anomaly detection algorithm is activated just when a pattern of new attack is likely to happen. This technique achieved a good detection rate with a reduction of energy consumption. However, it still had many false positives. Therefore, Sedjelmaci et al. [30] enhanced the latter technique by adding an improved model on the basis of game theory to alleviate the rates of false positives. Another game theoretic approach has been used by Duan et al. [19] to establish an energy-aware trust derivation scheme to ensure sufficient security of WSNs by deriving the optimal number of recommendations. By using this scheme, the performance of the network has improved in terms of security, but it has still been affected by the increased overhead due to the trust requests. In view of the same, an energy efficient trust evaluation scheme (known as EETE) is introduced by Rani et al. [31].proposed another approach for trust evaluation in WSN-enabled IoT networks using game theory techniques for cluster creation. This scheme enabled the detection of malicious nodes while decreasing the needed communications between nodes. These algorithms will be compared to our proposed algorithm in Section IV. Lately, in a 2021 study, Rao et al. [32] proposed a novel method to attain security in wireless body area network based on fuzzy logic and considering the residual energy as the trust factor, and their results show that this metric has successfully improved the lifetime of the network. The study of the contemporary research in the trust evaluation for IoT systems illustrates the persistent need to obtain a reliable and lightweight algorithm that is flexible and applicable in different environments.

III. The Proposed RTE Scheme

In this section, we propose the RTE model as a tool for applying trust between communicating nodes in an IoT network. The contribution of the RTE model is twofold. First, it applies trust management in intra-cluster and inter-cluster modes. Second, it is a light-weight model with an energy-efficient schema.

A. Network Model

Here, we consider an IoT sensor-network having M sensor nodes with limited energy sources along with limited radio range. A BS exists in the network with an unlimited energy source. The M nodes are grouped into N clusters. Each cluster has a different number of nodes. Each node $m_i,\ i = 1,\ \ldots,\ M$ is classified to either CH or CM. The hurdle is that these sensor nodes are operating in an open remote environment which makes it vulnerable to attacks. Additionally, some of the nodes may be initiating malicious attacks classified to either internal attacks like collusion attacks or external attacks like denial of service (DOS). In this context RTE model is used to observe the behavior of each node then evaluates the degree of trust in this node. The general components of the RTE scheme are depicted in Fig. 1.

B. Trust Model

Leaks of internal data of a specific organization may originate from its practitioners. It can be difficult sometimes to believe that a practitioner will intentionally sabotage their own business, and while it happens willfully often, it is strictly unintentional much of the time. Such behavior is referred to as internal attacks. The present work is an attempt to secure the network against such type of attacks. It should be noted that the RTE is controlled using a time slot S parameter; a user-defined parameter. Specifically, if the time slot is set to 60 seconds, then the RTE calculations, discussed below, are invoked every 60 seconds. Each time slot represents an iteration t in the algorithm. Therefore, we can say that iteration 1 starts at second 1 and iteration 2 starts at second 61, and so on.

1) Cluster Formation: At the very top level, RTE clusters the involved sensor nodes into N clusters as follows. Initially, the sensor nodes are deployed in a random manner while being kept static. Once the node starts up, it transmits a beacon signal to the BS. Afterward, the distance between each pair of sensor nodes is computed. The BS is responsible for computing the distance through evaluating the receiving signal strength which, in turn, can be translated into the distance. Let us comment on how the distance is computed. First, receive signal strength indicator (RSSI) is used to determine the signal strength measured in dBm. Note that higher dBm indicates higher signal strength. Second, according to the RSSI, the BS can calculate the distance to each node, for example, is the BS beacon signal broadcast range is 15 meters, it is widely known that if the RSSI is -50 dBm, then the distance is 1 meter. The task now is to find the N CHs. When a group of M sensor nodes runs in a network with a BS, naturally some nodes will perform better than others, basically by better aggregating data from neighboring nodes and transmit it to the BS. Let us call the few that excel at round $t = 1,\ 2,\ \ldots$ CHs, denote that $\mathbb{H}_t$, and the rest are CMs. The good thing about RTE is that at every round $t = 1,\ 2,\ \ldots$, the M nodes will share some information (discussed briefly below) with the BS who, in turn, uses this information to adjust the CHs. Accordingly, in the

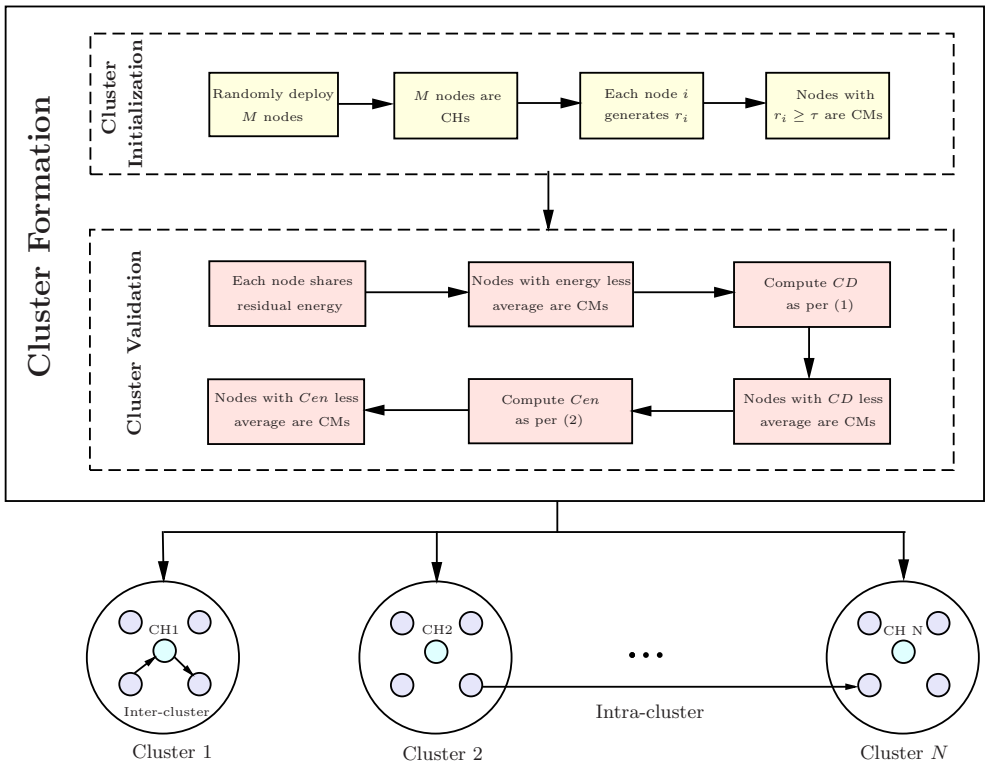

Fig. 1. The Main Components of RTE Scheme.

next round, the node that was a CM in the last round may become a CH. Each node has a number $i = 1,\ 2,\ \ldots, M$ and a tag: CH or CM. The numbers are permanent, but the tags may change from round to round. The BS transmits a threshold τ to all the sensor nodes to guide the task of electing the CHs. Each node $m_i,\ i = 1,\ 2,\ \ldots,\ M$ generates a random number r_i. Then r_i is compared against τ, if $r_i \geq \tau$, then node m_i is considered CH. Otherwise, it is an ordinary CM. Now, it is the BS turn to evaluate the validity of the elected CHs. The BS evaluates the CHs $\mathscr{H}_j \in \mathbb{H}_t$ according to three metrics. First, the residual energy of each CH is computed. This parameter must be high for a competitor CH. Second, the CH coverage degree (CD) is evaluated. This parameter indicates the ratio of the neighboring nodes (nbr) of the CH to the total number of nodes M. Neighboring nodes to a CH are those nodes that are located in either 1-hop or 2-hop from that CH. The CD of a given CH is evaluated by:

$$CD(\mathscr{H}_j) = \frac{|nbr(\mathscr{H}_j)|}{M}, \tag{1}$$

Where $|\mathscr{X}|$ is the cardinality of set $\mathscr{X}$. This parameter must be high for a competitor CH. Third, the CH centrality CH_Cen is evaluated. Contradicting with the other two metrics, CH centrality should be of low value. This parameter indicates energy consumption of a CH during the data aggregation and is given by:

$$CH\_Cen(\mathscr{H}_j) = \frac{\sqrt{\frac{\sum_{k \in nbr(\mathscr{H}_j)} d^2(\mathscr{H}_j, m_k)}{|nbr(\mathscr{H}_j)|}}}{A}, \tag{2}$$

Where $d(\mathscr{H}_j, m_k)$ is the distance between the CH $\mathscr{H}_j$ and node m_k and A is the area of the network. The CHs that pass the three metrics are considered confirmed ones while the others are considered CMs.

2) RTE Intra-cluster Evaluation: After electing the CHs, it is now the responsibility of each CH $\mathscr{H}_j \in \mathbb{H}_t$ to maintain the trust of the CMs $m_{i_j} \in \mathscr{H}_j$ in its cluster. To this end, the trust is represented as a continuous number in the interval [0,1], in which 0 indicates malicious, 1 indicates complete trust, and 0.5 indicates suspicious. For achieving trust in the case of intra-cluster, two direct and indirect trust concepts are employed. The degree of belief of CH $\mathscr{H}_j$ in a node m_{i_j} represents the direct trust (DT) which is computed according to the direct communication between node m_{i_j} with its CH $\mathscr{H}_j$. On the other hand, indirect trust (IT) is the degree of belief in node m_{i_j} from its neighbors. The idea is that each CM m_{i_j} preserves the trust of its neighbors and transmits these values to the CH $\mathscr{H}_j$. Both the DT and IT withstand against internal attacks. The trust T_t of a CM m_{i_j} with respect to its CH $\mathscr{H}_j$. at round $t = 1,\ 2,\ \ldots$ is given by:

$$\begin{aligned} T_t(\mathscr{H}_j, m_{i_j}) =& \alpha DT_t(\mathscr{H}_j, m_{i_j}) \\ &+ \beta \frac{\sum_{k \in nbr(m_{i_j})} IT_t(m_{k_j}, m_{i_j})}{|nbr(m_{i_j}) - 1|}, \end{aligned} \tag{3}$$

where $\alpha > 0$ and $\beta > 0$, chosen afresh at each round, are weight factors such that $\alpha + \beta = 1$. $DT_t(\mathscr{H}_j, m_{i_j})$ represents the direct trust of CH $\mathscr{H}_j$ in node m_{i_j} at round t and $IT_t(m_{k_j}, m_{i_j})$ is the indirect trust of node m_{k_j} in node m_{i_j}. Before elaborating on computing both the DT and

IT, we provide some preliminaries. Given a node m_{i_j}, let us define the positive well-behaved $P(m_{i_j})$ activity and the negative malicious $N(m_{i_j})$ activity. Consider that $E_{\max}(m_{i_j})$ is the maximum energy attained by node m_{i_j}, $\Delta_t(m_{i_j})$ is the residual energy of node m_{i_j} after communications in round t and $E_{th} \in [0,1]$ is an energy threshold chosen by the BS. If the node is doing some malicious communications at round t, then it is expected that by the end of the round, the node would consume a lot of energy. Therefore, the strategy is as follows. If $\Delta_t(m_{i_j})/E_{\max}(m_{i_j}) < E_{th}$, then node m_{i_j} well-behaved at round t, i.e. $P(m_{i_j}) = \Delta_t(m_{i_j})/E_{\max}(m_{i_j})$ and $N(m_{i_j}) = 0$. Otherwise, node m_{i_j} maliciously-behaved at round t, i.e. $N(m_{i_j}) = \Delta_t(m_{i_j})/E_{\max}(m_{i_j})$ and $P(m_{i_j}) = 0$. Each node m_{i_j} starts out at round 1 by a suspended direct trust, i.e. $DT_1(\mathscr{H}_j, m_{i_j}) = 0.5$. In the next round $t+1$, the node m_{i_j} updates its direct trust as follows.

$$DT_t(\mathscr{H}_j, m_{i_j}) = P(m_{i_j}) DT_{t-1}(\mathscr{H}_j, m_{i_j}) - N(m_{i_j}) DT_{t-1}(\mathscr{H}_j, m_{i_j}). \quad (4)$$

It should be noted that if $\alpha \geq \beta$, it means that node n_i has a higher trust of DT than that of IT. Otherwise, node n_i has a higher trust of IT than that of DT.

Finally, with the above in mind, the indirect trust of node m_{i_j} is given by:

$$IT_t(m_{k_j}, m_{i_j}) = P(m_{i_i}) \sum_{k \in nbr(m_{i_j}), k \neq i} DT_{t-1}(m_{k_j}, m_{i_j}) - N(m_{i_i}) \sum_{k \in nbr(m_{i_j}), k \neq i} DT_{t-1}(m_{k_j}, m_{i_j}). \quad (5)$$

3) RTE Inter-cluster Evaluation: A satisfactory observation about the RTE model is its ability to evaluate the trust between two different clusters using the inter-cluster evaluation schema. This is achieved with the employment of CHs $\mathscr{H}_j \in \mathbb{H}_t$ and BS. Specifically, the trust value T between two nodes belonging to different clusters $(\mathscr{H}_j, \mathscr{H}_k)$ is basically established by the trust between the two cluster heads, i,e. $T_t(\mathscr{H}_j, \mathscr{H}_k)$. The inter-cluster trust evaluation between node m_{i_j} from CH $\mathscr{H}_j$ and node m_{l_k} from CH $\mathscr{H}_k$ is expressed mathematically by:

$$T_t(m_{i_j}, m_{l_l}) = T_t(\mathscr{H}_j, \mathscr{H}_k) \times T_t(\mathscr{H}_k, m_{l_k}). \quad (6)$$

The RTE model shown in Algorithm 1 employs the above calculations.

IV. Experimental Work

In this section, the performance of the proposed algorithm RTE is evaluated in IoT sensor-based network using the NS-3 simulator. This network has a number of nodes behave in a malicious manner. We compute and compare the detection rate, energy consumption, and trust evaluation time of RTE with three benchmark schemes TDDG [19], LHIDS [30] and EETE [31]. Then, to verify the resilience of RTE we measured the detection rate under brute force attack. The simulation keeps running for 50 iterations, which was good enough for accurate results.

Algorithm 1: reliable lightweight trust evaluation scheme (RTE)

Input : N //Number of sensor nodes
S //Time slot
Output: T //Trust of the sensor nodes

$t := 1$ //Iteration number representing the number of the time slot S
//Cluster the nodes
Deploy the N sensor nodes randomly.
foreach *node* $m_i \in N$ **do**
  Transmit becaon signal to the BS.
  Compute the distance to the BS.
end
do
  BS transmits a threshold τ to the N sensor nodes.
  $\mathbb{H}_t := \emptyset$. //Set of all CHs.
  foreach *node* $m_i \in N$ **do**
    Generate random number r_i.
    if $r_i \geq \tau$ **then**
      Node m_i declares it self a temporary CH.
      Node m_i is added to $\mathbb{H}_t$.
      else
        Node m_i is declared as a CM.
      end
    end
  end
  //Evaluation of the permanent CHs
  foreach *CH* $\mathscr{H}_j \in \mathbb{H}_t$ **do**
    Compute the residual energy of CH $\mathscr{H}_j$.
    Compute $CD(\mathscr{H}_j)$ of CH $\mathscr{H}_j$ as per (1).
    Compute $CH\_Cen(\mathscr{H}_j)$ of $\mathscr{H}_j$ as per (2).
  end
  BS generates a CH threshold $C\tau$ in the interval [0,N].
  Keep the best performing $C\tau$ CHs in $\mathbb{H}_t$ and switch the rest to CMs.
  BS transmits the energy threshold $E_{th} \in [0,1]$.
  foreach *Ch* $\mathscr{H}_j \in \mathbb{H}_t$ **do**
    foreach *node* $m_{i_j} \in \mathscr{H}_j$ **do**
      Compute $E_{\max(m_{i_j})}$ of node m_{i_j}.
      Compute $\Delta_t(m_{i_j})$ of node m_{i_j}.
      if $\Delta_t(m_{i_j})/E_{max(m_{i_j})} < E_{th}$ **then**
        $P(m_{i_j}) := \Delta_t(m_{i_j})/E_{\max(m_{i_j})}$.
        $N(m_{i_j}) := 0$.
        else
          $N(m_{i_j}) := \Delta_t(m_{i_j})/E_{\max(m_{i_j})}$.
          $P(m_{i_j}) := 0$.
        end
      end
      Compute the DT of node m_{i_j} as per (4).
      Compute the IT of node m_{i_j} as per (5).
      Compute the trust T as per (3).
    end
  end
  Wait until the end of the time slot.
  $t := t + 1$.
while *the network is running*;

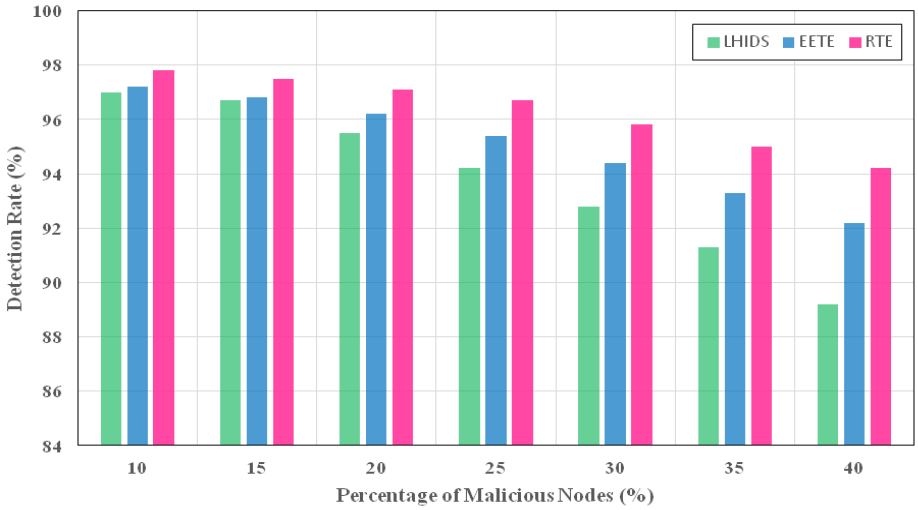

Fig. 2. Detection Rate Comparison between RTE Algorithm and other 2 Algorithms, while Increasing the Number of Misbehaving Nodes in the Network.

TABLE I. SIMULATION PARAMETERS

Parameter	Value
Network area, A	500×500 m^2
Node number, N	300
Number of iterations, R	50
Packet size	1024-bits
Communication range	100 m
Percentage of malicious nodes	$10 - 40\%$
Hop limit	2
Initial DT	0.5 (suspend)
Max. number of nodes in a cluster, K	10
Initial energy	$10J$
Node transmission range	$25m$

A. Experimental Setup

We consider that we have a network of 500×500 m^2, with 300 nodes randomly deployed. The propagation delay is calculated using constant speed propagation. Moreover, the radio energy model are utilized for initial energy distribution. We assume that we have a 1024-bits packet length. In all the experiments, we use the following values in Table I, which proved good enough for accurate and fast results:

B. Evaluation Metrics

For validating the proposed RTE algorithm, the following validation measures are employed.

1) Detection rate, $D_t(W)$: Given an IoT-network W, the detection rate ($D_t(W)$) is the ratio between the number of correctly detected malicious nodes $\mathbb{M}_t$ at iteration t to the total number of predefined malicious nodes $\mathscr{M}$ and is given by

$$D_t(W) = \frac{\mathbb{M}_t}{\mathscr{M}}.$$

2) Average energy consumption, $Avg(C_i)$: Given a cluster C_i with K sensor nodes, the average energy consumption ($Avg(C_i)$) is the average consumed energy, in Joule (J), by the active nodes in Cluster C_i, and is given by

$$Avg(C_i) = \frac{\sum_{j=2}^{K} E_j}{K},$$

where E_j is the consumed energy by node j in cluster i. The reason why the summation start by 2 is that the CH is not considered while computing the average consumed energy.

3) Trust Evaluation time: It is the time taken by the algorithm to evaluate the trust since receiving the request to computing the direct and indirect trust of the node. This is computed using the concept of elapsed seconds.

C. Experiment 1: Detecting Malicious Nodes and Detection Rate

In this experiment, the detection rate of our proposed algorithm RTE was tested to validate its reliability, this metric is important and should be as high as possible. The experiment is run several times in a nested format according to varying percentages of malicious nodes start from 10% to 40%, with a step of 5%. Figure 2 illustrates the comparison of detection rate between LHIDS, EETE, and RTE. The detection rate decreases when the number of malicious nodes increases. However, the detection rates of LHIDS and EETE start decreasing significantly when the ratio of misbehaving nodes exceeds 20%, while the chart of RTE keeps decreasing slightly and never falls below 94.6%, this value is in the worst case when 40% of the nodes in the network behaving illegitimately, which shows a reliable performance unaffected by the high numbers of malicious nodes. The results show the superiority of RTE clearly which is justified by the two following reasons. The first one is the accurate calculations carried out by RTE, specifically, RTE inter-cluster and intra-cluster trust evaluation

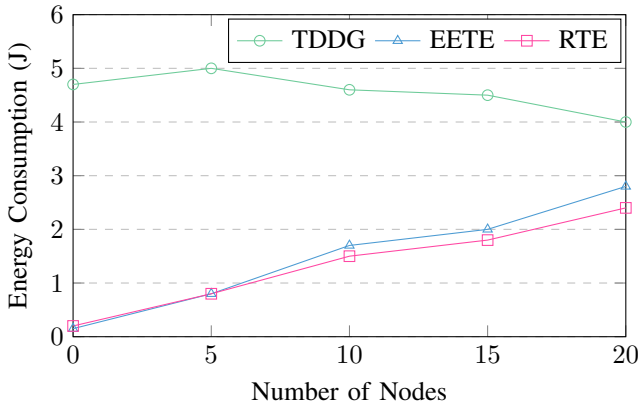

Fig. 3. Average Energy Consumption Comparison between RTE Algorithms and other 2 Algorithms, while Increasing the Number of Nodes in the Network.

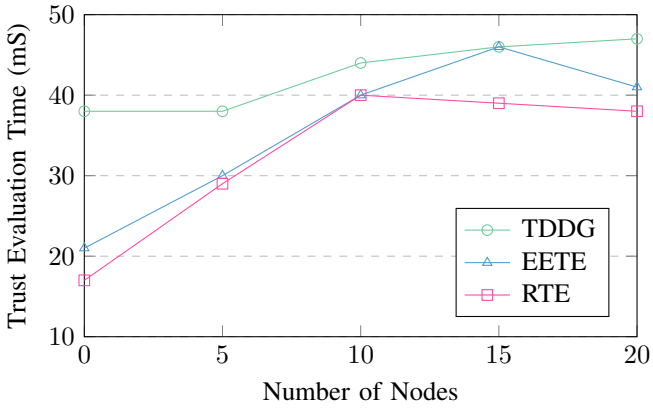

Fig. 4. Trust Evaluation Time Comparison between RTE Algorithm and other 2 Algorithms, while Increasing the Number of Nodes in the Network.

by the CHs. For which, the nodes are classified upon their past behaviors into trusted, suspicious, or malicious. Moreover, the malicious nodes are immediately excluded from the network which helps efficiently in mitigating the malicious behavior in the network. The second reason is the consistent validation of the clusters by the BS each iteration, which provides an additional monitoring to the network and improves the security by keeping the CHs trusted.

D. Experiment 2: Average Energy Consumption ($Avg(C_i)$)

In this experiment, the efficiency of the proposed algorithm is validated by the measurement of the average energy consumed by the algorithm to evaluate the trust of the participating nodes in the network. As mentioned earlier, the nodes in the IoT environment are power constrained, so the trust evaluation algorithm should be as light as possible and consume the minimum amount of energy. The experiment is run several times with a varying number of participating nodes starting from 0 to 20, with a step of 5. Fig. 3 shows the results of this experiment for three lightweight algorithms TDDG, EETE, and RTE. At the beginning of the chart EETE and RTE consume similar amount of energy. However, when the number of nodes increases, our algorithm needs less energy than the other two models. When the number of nodes is 20, it consumes $0.40J$ less than the EETE algorithm. It is observed that RTE gives the best performance. This optimization in energy consumption is resulted from the reduction of the trust calculations in the network, where only the CHs are responsible for the trust computations while the other CMs concentrate in the process of packets transmission. Another reason for the efficiency of our algorithm, is the role of BS in evaluation the clusters each iteration and elect the appropriate CHs, which helps in maintaining a steady amount of energy in the network.

E. Experiment 3: Trust Evaluation Time

In this experiment, we assess the robustness of the algorithm by investigating the required time for trust evaluation of the participating nodes. The algorithm should be performed as fast as possible to protect the network from the dangerous consequences of the presence of misbehaving nodes. The experiment is run several times with a varying number of nodes from 0 to 20 nodes, with a step of 5. Fig. 4 We can see that RTE's curve is the least deviating curve from the others, but this ideal behavior is practically hard to attain due to nodes interaction overhead in computing the indirect trust. However, we can observe that the curve of RTE is the least deviating curve from the others, and this algorithm requires the least amount of time to evaluate the trust between nodes. This results rationally match the results of the previous experiment, as the proposed algorithm limits the computations and implement them only in the CHs and BS, which also reduces the needed communication overhead for the process. Therefore, we can say that RTE is unaffected by increasing the number of participating nodes in the network.

F. Case Study: RTE Performance under Brute Force Attack

To prove the efficiency of the RTE algorithm, it was tested for computing the trust of the involved nodes in an IoT sensor-based network, while assuming the presence of some malicious nodes behaving badly and initiating brute force attack. This section is dedicated mainly for analyzing the performance of RTE under brute force attack. RTE was run several time slots. Each time slot takes number of second that vary from slot to another. The time slot ends when all nodes sense and transmit the data, along the path, to the BS. In each slot, we categorize the nodes as follows: normally behaving nodes, malicious nodes, attacked nodes, and dead nodes. The node is considered dead when its energy is less than threshold (user-defined value), in our case it is assumed 60% of the average energy of the nodes in the slot. On the other hand, malicious nodes are those initiating brute force attack. Fig. 5 illustrates the performance of RTE under brute force attack in terms of False Positive Rate (FPR) and False Negative Rate (FNR), while increasing the percentage of malicious nodes in the network. The graph shows that when the percentage of malicious node is 10%, the FPR is 11%. By increasing the number of malicious nodes, the performance of the RTE will not be highly affected. We observe that if half of the network is infected, the FPR approaches 21%. The FPR has increased 10% when the percentage of malicious nodes has increased 40%. This proves the highly efficient performance of the proposed algorithm in such highly malicious environment.

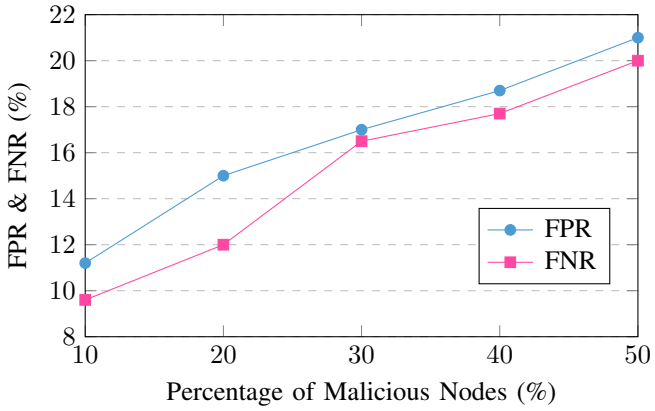

Fig. 5. Performance (2 metrics) of RTE with Respect to Varying Ratio of Misbehaving things under Brute Force Attack.

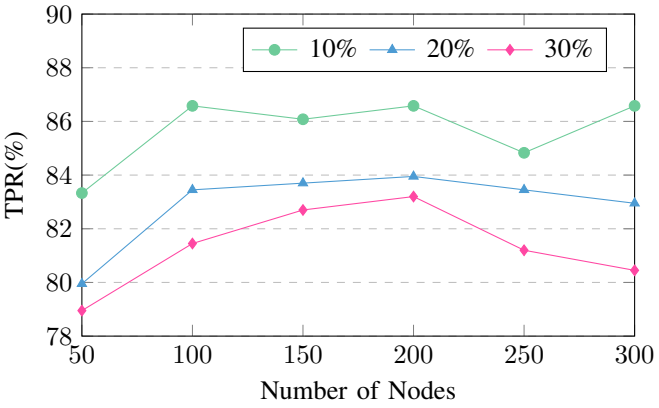

Fig. 6. Performance (TPR) of RTE under Brute Force Attack.

G. Performance Investigation

The performance results of RTE would have been greatly affected with varying percentages of malicious nodes. In other words, as the percentage of malicious node in the network increases, the performance of RTE, or any competitor algorithm for that matter, naturally affected. With this in mind, to the end of the experiment, we validate RTE performance with respect to three scenarios, each with a different percentage of malicious nodes. Specifically, scenario 1 assumes 10% malicious nodes, scenario 2 assumes 20% malicious nodes, and scenario 3 assumes 30% malicious nodes. That is to expose the operational range of RTE.

The TPR results of RTE with respect to the three scenarios is depicted in Fig. 6. It gives a vivid picture on the evolution of the algorithm with respect to the three scenarios. It can be easily noticed that as the number of nodes increase, the RTE performance, TPR, increases. This is attributed mainly to the accurate design of the algorithm in computing the trust.

V. Conclusion

This paper proposes a novel reliable lightweight trust evaluation (RTE) scheme to improve the security of clustered-sensor IoT-network in presence of some malicious illegitimate nodes. The model considers both the trustworthiness of nodes and network energy efficiency thus differentiating it from peers in the literature. In contrast with other trust evaluation schemes, RTE reduces the needless transmissions. RTE aggregates the nodes in a set of clusters, controlled by a set of CHs. Two scenarios are used to evaluate trust. First, intra-cluster evaluation is carried out by the CH to trust any communication between nodes in its cluster. Second, inter-cluster evaluation is carried out to trust any communication between nodes in different clusters. The CHs are responsible for evaluating the trust while CMs send/receive data which, in turn, increases the network lifetime. Simulation results of the RTE scheme show its superiority over current trust evaluation schemes in terms of detection rate and time of malicious nodes, energy efficiency, and trust evaluation time. What is more, RTE is abilities are tested in detecting brute force attack with varying percentage of attack and varying number of nodes. As the number of attacks increases, RTE detection rate for malicious nodes increases. This reflected RTE ability in achieving promising results for FPR, TPR, TNR and FNR. In future works, our goal is to extend the RTE scheme to be able to detect several kinds of external attacks like DoS, black-hole attack, and wormhole attack.

Acknowledgment

The authors would like to thank Deanship of scientific research for funding and supporting this research through the initiative of DSR Graduate Students Research Support (GSR), King Saud University

Abbreviations

The following abbreviations are used in this manuscript:

RTE	Reliable lightweight trust evaluation scheme
CH	Cluster head
CM	Cluster member
IoT	Internet of thing
BS	Base station
FPR	False Positive Rate
TPR	True Positive Rate
FNR	False Negative Rate
DR	Detection Rate

References

[1] Lim, J.; Keum, D.; Ko, Y. B. A Stepwise and Hybrid Trust Evaluation Scheme for Tactical Wireless Sensor Networks. *Sensors* 2020, 20(4), 1108.

[2] Chitanya, M. Robustness, Security and Privacy in Location-Based Services for Future IoT. *Research and Reviews: Advancement in Robotics* **2018**, 1(2), 1-5.

[3] Bhushan, B.; Sahoo, G. Requirements Protocols, and Security Challenges in Wireless Sensor Networks: An Industrial Perspective. In Handbook of Computer Networks and Cyber Security, Springer, Cham, 2020; pp. 683–713.

[4] Um, T. W.; Lee, E.; Lee, G.M.; Yoon, Y. Design and Implementation of a Trust Information Management Platform for Social Internet of Things Environments. *Sensors* **2019**, 19(21), 4707.

[5] Ram, M.; Kumar, S.; Kumar, V.; Sikandar, A.; Kharel, R. Enabling Green Wireless Sensor Networks: Energy Efficient T-MAC Using Markov Chain Based Optimization. *Electronics* **2019** 8(5), 534.

[6] Halder, S.; Ghosal, A.; Conti, M. LiMCA: an optimal clustering algorithm for lifetime maximization of internet of things. *Wireless Networks* **2019**, 25(8), 4459–4477.

[7] Derder, A.; Moussaoui, S.; Doukha, Z.; Boualouache, A. An online target tracking protocol for vehicular Ad Hoc networks. *Peer-to-Peer Networking and Applications* **2019**, 12(4), 969–988.

[8] Rani, R.; Katti, C.P. End-to-end security in delay tolerant mobile social network. In International Conference on Application of Computing and Communication Technologies, 2019; pp. 45–54.

[9] Bica, I.; Chifor, B.C.; Arseni, Ş.C.; Matei, I. Multi-Layer IoT Security Framework for Ambient Intelligence Environments. *Sensors* **2019**, 19(18), 4038

[10] Fu, H.; Liu, Y.; Dong, Z.; Wu, Y. A Data Clustering Algorithm for Detecting Selective Forwarding Attack in Cluster-Based Wireless Sensor Networks. *Sensors* **2020**, 20(1), 23.

[11] Bypour, H.; Farhadi, M.; Mortazavi, R. An Efficient Secret Sharing-based Storage System for Cloud-based Internet of Things. *International Journal of Engineering* **2019** 32(8), 1117–1125.

[12] Alnumay, W.; Ghosh, U.; Chatterjee, P. A Trust-Based predictive model for mobile ad hoc network in internet of things. *Sensors* **2019** 19(6), 1467.

[13] Ullah, I.; Youn, H.Y. A novel data aggregation scheme based on self-organized map for WSN. *The Journal of Supercomputing* **2019**, 75(7), 3975–3996.

[14] Vijayan, R.; Jeyanthi, N. Trust Management Approaches in Mobile Adhoc Networks. In Ubiquitous Computing and Computing Security of IoT, 2019; pp. 69-99.

[15] Yin, X.; Li, S. Trust evaluation model with entropy-based weight assignment for malicious node's detection in wireless sensor networks. *EURASIP Journal on Wireless Communications and Networking* **2019**, 198.

[16] Wu, X.; Huang, J.; Ling, J.; Shu, L. BLTM: beta and LQI based trust model for wireless sensor networks. *IEEE Access* **2019**, 7, 43679–43690.

[17] Mohsenzadeh, A.; Bidgoly, A.J.; Farjami, Y. A novel reward and penalty trust evaluation model based on confidence interval using Petri Net. *Journal of Network and Computer Applications* **2020**, 102533.

[18] Malik, N.A.; Rai, M. Enhanced Secure and Efficient Key Management Algorithm and Fuzzy With Trust Management for MANETs. Available at SSRN 3565898

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

[20] Kolias, C.; Kambourakis; G., Stavrou, A.; Voas, J. DDoS in the IoT: Mirai and other botnets. *Computer* **2017**, 50(7), 80-84.

[21] Khalil, A.; Mbarek, N.; Togni, O. Fuzzy Logic based security trust evaluation for IoT environments. In *2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA)*,**2019**; (pp. 1-8).

[22] Chen, J.; Tian, Z.; Cui, X.; Yin, L.; Wang, X. Trust architecture and reputation evaluation for internet of things. *Journal of Ambient Intelligence and Humanized Computing* **2019**, 10(8), 3099–3107.

[23] Boussard, M.; Papillon, S.; Peloso, P.; Signorini, M.; Waisbard, E. STewARD: SDN and blockchain-based Trust evaluation for Automated Risk management on IoT Devices. In IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2019; pp. 841–846.

[24] Gao, Z.; Zhao, W.; Xia, C.; Xiao, K.; Mo, Z.; Wang, Q.; Yang, Y. A Credible and Lightweight Multidimensional Trust Evaluation Mechanism for Service-Oriented IoT Edge Computing Environment. In 2019 IEEE International Congress on Internet of Things (ICIOT), 2019; pp. 156–164.

[25] Wang, T.; Luo, H.; Jia, W.; Liu, A.; Xie, M. MTES: An intelligent trust evaluation scheme in sensor-cloud enabled industrial Internet of Things. *IEEE Transactions on Industrial Informatics*.

[26] Dass, P.; Misra, S.; Roy, C. T-safe: Trustworthy service provisioning for IoT-based intelligent transport systems. *IEEE Transactions on Vehicular Technology* **2020**, 69(9), 9509-9517.

[27] Jayasinghe, U.; Lee, G. M.; Um, T. W.; Shi, Q. Machine learning based on trust computational model for IoT services. *IEEE Transactions on Sustainable Computing* **2018**, 4(1), 39-52.

[28] Ma, W.; Wang, X.; Hu, M.; Zhou, Q. Machine Learning Empowered Trust Evaluation Method for IoT Devices. *IEEE Access* **2021**, 9, 65066-65077.

[29] Sedjelmaci, H.; Senouci, S. M.; Al-Bahri, M. A lightweight anomaly detection technique for low-resource IoT devices: A game-theoretic methodology. In *2016 IEEE international conference on communications (ICC)* **2016** (pp. 1-6).

[30] Sedjelmaci, H.; Senouci, S. M.; Taleb, T. An accurate security game for low-resource IoT devices. *IEEE Transactions on Vehicular Technology* **2017**, 66(10), 9381–9393.

[31] Rani, R.; Kumar, S.; Dohare, U. Trust evaluation for light weight security in sensor enabled internet of things: game theory oriented approach. *IEEE Internet of Things Journal* **2019**, 6(5), 8421–8432.

[32] Rao, J. D.; Sridevi, K. Novel security system for wireless body area networks based on fuzzy logic and trust factor considering residual energy. *Materials Today: Proceedings* **2021**, 45, 1498-1501.