Journal of Network and Systems Management (2021) 29:45
https://doi.org/10.1007/s10922-021-09611-x

Building an Intelligent Global IoT Reputation and Malicious Devices Detecting System

Qussai Yaseen[1] · **Yaser Jararweh**[2]

Received: 21 December 2020 / Revised: 29 May 2021 / Accepted: 9 June 2021 /
Published online: 17 June 2021

Abstract
The Internet of Things (IoT) applications are growing immensely. However, malicious IoT devices are major concerns that threaten the security of IoT applications. This paper proposes an intelligent reputation system for IoT devices using edge computing and cloud computing infrastructures. The proposed system can be used to mitigate the effect of malicious and malfunction IoT devices. Therefore, the proposed system can be used to enhance the effectiveness of IoT based systems such as smart cities, and reduce the risk of malicious IoT devices especially in sensitive systems, such as military applications, that leverage IoT devices. To achieve this goal, the paper proposes a new identification method for uniquely and globally identifying IoT devices wherever they move. Moreover, the paper proposes a new approach for computing the reputation of IoT devices, and calculating correct values based on these reputations. The results show that the proposed approach achieves very good results in detecting malicious IoT devices and computing very close values to the true values.

Keywords Internet of Things · Intelligent systems · Edge computing · Reputation systems · Trust systems · Information security

1 Introduction

The Internet of Things (IoT) integrates a huge number of autonomous and heterogeneous devices and sensors that send huge data to monitoring systems which analyze data and make decisions. IoT technology and devices are used in many applications;

✉ Qussai Yaseen
qmyaseen@just.edu.jo

[1] Department of Computer Information Systems, Jordan University of Science and Technology, Irbid, Jordan

[2] Department of Mathematics and Computer Science, Duquesne University, Pittsburgh, PA, USA

they are used in Smart Mobility (i.e VANETs), Smart Homes, Smart Grid, Public Safety and Environment Monitoring such as weather monitoring and water quality monitoring, Medical and Healthcare (Internet of Medical Things IoMT), Industrial Processing such as Californium (Cf) CoAP framework, Agriculture and Breeding such as Climate-Smart Agriculture (CSA), and connect vehicles (IoCV) [1, 2]. The usage of these applications and their benefits have an important role in enhancing the quality of nowadays life. Therefore, it is expected that the future of IoT devices and its technology and applications will shape our future [3].

There are different types of IoT sensors based on the type of connectivity [4], as shown in Fig. 1. First, non-IP direct to the server, which are sensors that are directly connected to the server without using IP, such as sea buoys that use radio modem links to a server. Second, non-Internet connected system, which are nodes connected to each other and to a base station using a non-IP radio network, where the base station sends their data to the internet such as environmental sensor networks. Third, virtually connected nodes, which are nodes that appear to be connected to the internet using a private non-IP radio network and a gateway for internet connection, such as Zigbee wireless sensors. Fourth, the indirectly connected IoT nodes use a gateway to link them to the internet as well, but they use IP in communication, which allows direct access to them, such as WiFi routers, 6LoWPAN compliant gateways, mobile IP that has many applications such as animal tracking. Finally, directly connected IoT devices such as IP cameras and mobile phones. Some IoT devices are mobile while others are not. For example, the directly connected IoT devices such as mobile phones can send and receive date in a mobile state. Sensors that may be attached

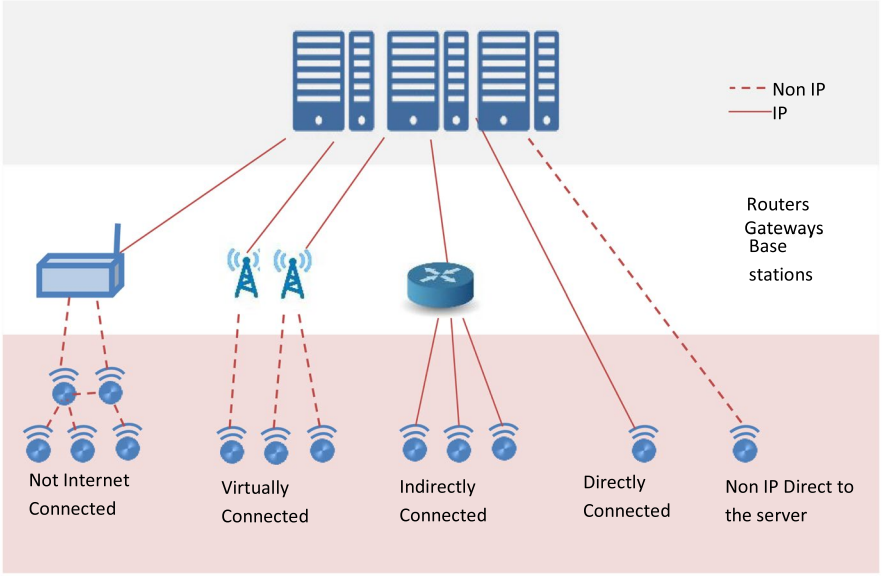

Fig. 1 Different Families for IoT devices

to mobile devices such as vehicles may send readings about pollution, temperature, jams, etc. in mobile states too.

In the era of smart cities, many decisions are made based on the data received from IoT devices [5]. These devices send huge data that is filtered and analyzed to produce useful information, which is in turn used to make decisions. For example, the New York City Department of Transportation has an IoT based project called Midtown in Motion, which is a congestion management system used to improve travel times on Midtown's avenue. The system has improved travel times on Midtown's avenues by 10% [6].The sensitivity of situations that depend on these decisions varies from normal, such as traffic jam, to high and life threatening such as radio-active pollution. Therefore, the data accuracy is very important in these situations. Unfortunately, the data accuracy may be affected by intentional and unintentional incorrect values sent. Attacks on IoT data could be solo attacks, launched by single devices, or collusion attacks, launched by more than one IoT device. Both intentional and unintentional attacks are very risky. Therefore, using IoT devices reputation values, when extracting information from data sent by many IoT devices, mitigates the impact of incorrect values. However, the dynamic environment of IoT devices, where some devices are continuously moving, makes the using of IoT devices reputations and the detection and mitigation a hard process. Therefore, there is a need to build a robust reputation system for IoT devices that is not affected by the dynamic environment of IoT devices, and that helps in preventing malicious or unintentional attacks and mitigates their impact on the IoT system.

Assigning reputation values to IoT devices and using these values when taking decisions is a very useful solution to mitigate the problem of malicious or incorrect data. The reputation value of an IoT device, say X, may be calculated based on the votes of X's neighbors. However, mitigating the problem of incorrect data may be not an easy process in dynamic environments, where IoT devices are able to move continuously across many physical zones and change their neighbors. The challenge is to design a global collaborative reputation system that calculates, stores and updates the trustworthiness of IoT devices.The term 'global' means that the system covers the geographical area within which IoT devices move, such as a city or a country.

When designing the reputation system, we need to solve the following challenges:

1. How can the system keep persistent and distinct identities of IoT devices when moving across different zones and systems?
2. How the system may conduct punishment of reputation?
3. How the reputation values are computed, stored, used and synchronized across edge nodes?

This paper aims at designing, developing and testing a global reputation system using edge and cloud computing infrastructures facilities, which can be used to calculate reputation values, monitor the IoT devices while moving across different

edge zones, and update edge nodes with the reputation values of moving IoT devices. The contributions of the paper are summarized as follows.

1. The paper proposes a new identification system to uniquely and globally identifying IoT devices.
2. The paper proposes a new method to compute the reputation of IoT devices.
3. The paper proposes a new system to monitor IoT devices while moving through the environment, detect malicious devices and mitigate the effect of incorrect readings sent by those devices or malfunction devices.

The rest of paper is as follows. Next Section discusses some related work. Section 3 presents and explains the proposed system. Experiments and results are discussed in Sect. 4. Finally, Sect. 5 concludes the work.

2 Related Work

Leveraging edge and cloud computing in IoT applications has been proposed several times in research community. Andrafe et al. [7] proved that using edge computing improves the availability and improves the performance when edge nodes are not at full capacity. Moreover, proposing new protocols to enhance the security of IoT environment is another field for enhancing the applicability of IoT applications, such as the work performed by Hashemi and Shams [8], where they proposed a new protocol and fuzzy logic to calculate the trust of IoT devices.

There are some attempts to compute the reputation and trust of IoT machines and avoid malicious nodes. Nitti et al. [9] proposed two approaches for detecting malicious IoT devices. In the first approach, each object uses the direct interaction to calculate the trust values of other objects. The second approach used a distributed hash table to store and distribute the information, including behavior and feedback, about each node to all nodes. Similarly, Yan et al. [10] proposed an approach to compute the trust of IoT nodes and introduced two methods to protect the privacy and the feedback of participating nodes. The proposed methods are based on Public Key Cryptography, homomorphic and palliercrypto systems. However, their approaches have high computational cost.

Michalas and Komninos [11] used a cryptographic approach and a voting approach to compute the trustworthiness of IoT devices, and to protect the privacy and the anonymity of the participating nodes in the voting process.

In [12, 13], Hasan et al. proposed decentralized reputation aggregator and a privacy preserving protocols using a set of pre-trusted users, which is considered infeasible. Some authors used recommender systems, such as Asiri and Miri [14], who proposed a trust and reputation model based on recommender systems. They used probabilistic neural networks to compute reputations and classify devices. They avoided the cold start problem by predicting the rating of newly joining nodes, and maximized the approach availability using a distributed structure. However, they did not provide any experiments to prove their claims. Mendoza and Kleinshmidt [15]

used direct interaction approach, where nodes watch services requests, and indirect approach, where the trust is computed based on the recommendations from neighbors by exchanging trust tables, to build a distributed trust management model. However, their approach poses high traffic and consumes high levels of energy due to the high rate of updates.

Some research considered the contextual information while building the reputation of IoT devices, such as Hussein et al. [16]. The authors in [16] proposed a context-aware evaluation approach to evaluate the trustworthiness of users in an edge-based IoT model. To achieve their goal, they used a context-aware feedback and a crawler system that is based on feedback to make the trust evaluation process effective and unbiased.

Other researchers used some emerging technologies to enhance the computation of the reputation of IoT devices. For example, Chen et al. [17] used SDN and a behavior-based scheme to evaluate the trust of IoT devices. While Fortino et al. [18] used blockchain technology to build a local reputation system for IoT devices. In another work [19], Fortino et al. used cloud computing technology to build a local reputation based system for computing the reputation of IoT devices. Similarly, Debe et al. [20] used blackchain technology and smart contracts to build a decentralized reputation system. Zhang et al. [21] proposed a domain partition based approach to detect malicious nodes. The authors in [22] proposed an Anomaly Detection and Modeling in 802.11 Wireless Networks.

Djedjig et al.[23] worked on IoT in Low-power and Lossy Networks (RPL), and proposed a new Metric-based RPL Trustworthiness Scheme (MRTS) that uses and evaluates trust in secure routing topology construction. According to their experiments, their approach enhanced the packet delivery ratio, energy consumption and throughput. Similarly, Thulasiraman and Wang [24] worked on RLP and proposed a lightweight and trust-based methodology to secure the routing process in mobile IoT networks. The proposed approach selects the routing path based on a pre-computed node trust value as well as the average signal strength indicator (ARSSI) value across the IoT network. In the same context, Murali and Jamalipour [25] worked on enhancing RPL and securing IoT communication. However, they focused on Sybil attack and proposed an approach based on artificial bee colony (ABC).

The aforementioned related work introduced interesting approaches for building and using trust and reputation systems. However, they have some drawbacks such as working locally and do not considering dynamic environments, or working on specific systems such as peer-to-peer. This paper proposes an approach that considers the dynamic environment when building and using the reputation system, and leverages the infrastructure of edge computing by migrating the computation and storage of reputations to this layer instead of using intermediate nodes.

3 The Proposed Model

Figure 2 shows the proposed model for building a global IoT reputation system using edge and cloud computing infrastructures. The model consists of three layers, which are IoT layer, Edge layer, and Cloud layer. The IoT layer represents the

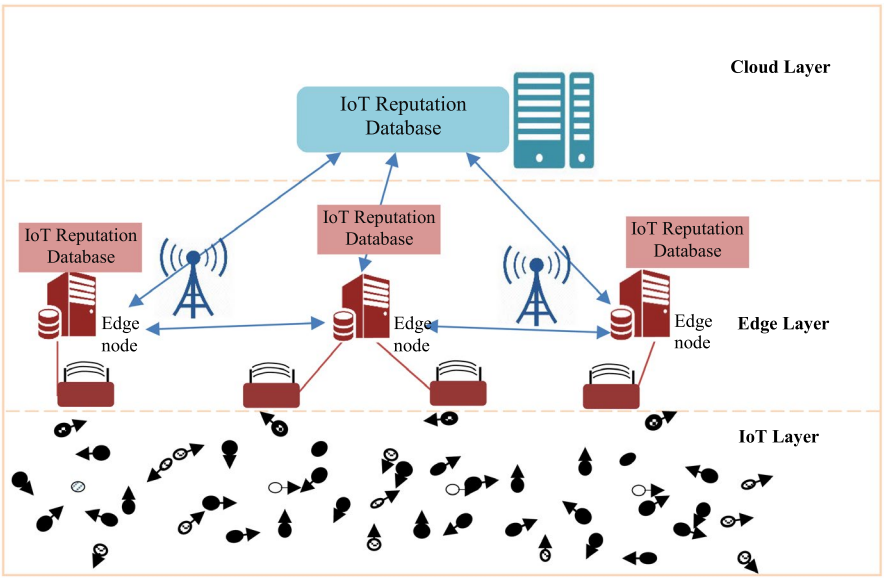

Fig. 2 An edge computing based model for reputation systems in Internet of Things

IoT devices that may move continuously and send data from different locations to base stations. The base stations, which are located at the edge layer, forward the data to edge nodes. Edge nodes, which are powerful devices and servers, analyze and filter the received data using special algorithms and store the reputation values of IoT devices. Moreover, they update the reputation values of IoT devices according to the received information from those devices. The reputation values of IoT devices at edge nodes are synchronized with the servers at the cloud layer. The synchronization process is important since the reputation values are sent from the cloud layer to edge nodes when needed. For example, the reputation values may be needed at edge nodes to detect collusion attacks in IoT layer. Hence, when an edge node needs the reputation value of an IoT device, it searches first at neighboring edge nodes asking them to send the information if exists. It supposes that the IoT devices move from the neighborhood to the new edge node area. However, if the requested values do not exist at neighboring edge nodes, the corresponding edge node contacts the cloud layer to get the missing reputation values. Searching for reputation values in neighboring edge nodes, instead of contacting the cloud directly, reduces the delay of getting reputation values and increases the speed of detecting malicious IoT nodes. Moreover, it reduces the traffic and computations on centralized cloud servers.

To make the proposed framework applicable, the following requirements should be met:

- IoT devices should be given unique identities.
- The readings sent by IoT devices should be monitored and checked to verify whether these readings are correct.

– The reputation values of IoT devices should be computed, stored and retrieved when needed with minimum delay.

The following sections show how the proposed approach meets these requirements.

3.1 Assigning IoT Identities

The IoT devices, such as smart phones and vehicles are subject to strong mobile capability. Therefore, the IoT infrastructure should guarantee that users can connect to services continuously, especially when moving. Moreover, IoT devices, regardless where they are located, need to be authenticated, and have access to services. Therefore, the Internet of Things calls for a new identity management paradigm to solve the existing identity security and privacy concerns on the Internet, and takes into account the native IoT unconventional characteristics.

Identifiers are crucial in IoT applications. They are used to uniquely identify entities for different purposes in different contexts. There are many standardized identifier schemes in use, which span from domain specific to generic schemes. Identification may be applied according to the device, application, network, etc. Therefore, the Alliance for Internet of Things Innovation AIOTI [26] classified identifiers into different categories as follows.

– Thing identifiers, which identify the entity of interest of the IoT application such as physical objects as machines or humans, or digital data as files. Examples of such identifiers are RFID tags, thing identifier in sensors non-volatile memory and Device ID in smart watches.
– Application and service identifiers, which identify software applications and services such as service unique identifier.
– Communication identifiers, which identify communication end points such as MAC addresses at the data link layer, IP address at the network layer and phone number in a phone network.
– User identifiers, which identify user of IoT application and services such as username and fingerprints.
– Data identifiers, which identify specific data instances such as metadata. Examples of such identifiers are Digital Twin and property types.
– Location identifiers, which identify the geographic area (GPS data) of things for tracking purposes.
– Protocol identifiers, which identify the type of protocol used in high level layers.

IoT device should get a unique identifier in order to trace and check the IoT authentication globally. This paper proposes a new identification system that helps in creating a unique reputation profile for IoT devices. The proposed identification model links profile ID to Local Identification to produce global identification. To guarantee that the Global ID is unique, each edge node should have a unique ID that is used to set its IoT devices ID (Edge node ID-IoT local ID), which represents the Global ID of the IoT device. Moreover, an IoT device once launched and used should get a

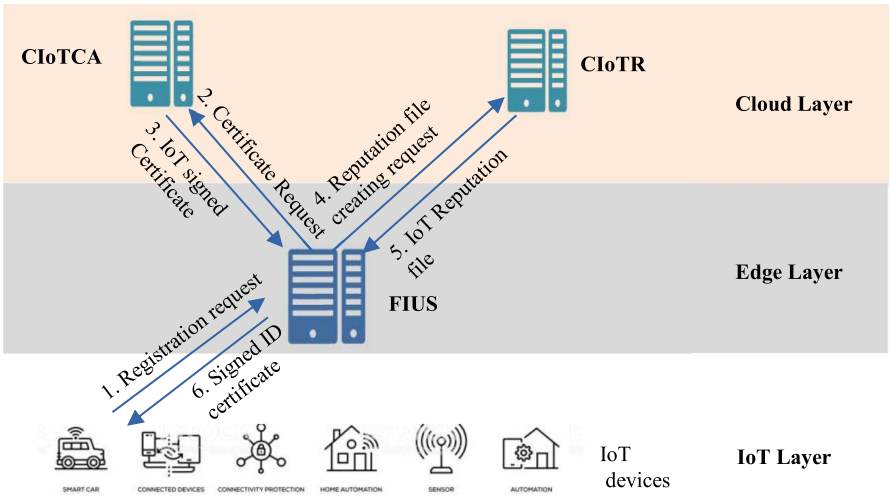

Fig. 3 IoT registration

profile with an ID stored and registered at the corresponding edge node. When moving to other zones, the IoT device should provide this ID to the new zone controller. Furthermore, the identification scheme should ensure that IoT devices cannot duplicate profiles.

Figure 3 below shows the proposed identification system. Each Edge Zone should have a globally unique Identifier. Within each edge zone, an IoT device should register itself to the Identification and Authentication Server (FIUS) in that zone. The ID that an IoT gets consists of two parts, which are the Edge Zone ID and the IoT unique identifier (e.i. UUID, GSM phone number, etc.). We call the new globally identification number of the IoT device as IoT Reputation ID (IoTRID). The IoTRID should be globally unique for each IoT device. Moreover, an IoT device should be prevented from having more than one IoTRID. To achieve this purpose, the FIUS at the edge zone issues a signed certificate for each IoT device as follows.

1. The IoT device sends a registration request to the FIUS at the edge node. The request should contain the IoT unique identifier (i.e. UUID, GSM phone number, etc.).
2. The FIUS at the edge zone prepares a new request to send it to the Cloud IoT Certificate Authority CIoTCA. The new request consists of the previous IoT request with a modified ID, which consists of the edge zone ID followed by the IoT device ID (EdgeID-IoTID).
3. The CIoTCA checks whether the EdgeID-IoTID (and IoTID) has no existing reputation profiles. If the EdgeID-IoTID (and IoTID) has no profile, the CIoTCA issues a certificate for the IoT device with the EdgeID-IoTID and signs it using its private key, and sends it back to the FIUS.

4. The FIUS sends a new request to the Cloud IoT Reputation server (CIoTR) server containing the signed certificate from the CIoTCA to create a new reputation profile for the IoT device.
5. The CIoTR server creates the new profile, stores it in the Reputation Database, and sends a copy to the FIUS.
6. The FIUS stores the profile copy and sends the signed certificate to the IoT device.

The unique identity of an IoT device guarantees the monitoring process of the IoT device when moving across different edge zones. Therefore, the IoT device should be prevented from getting more than one identity. The proposed identification scheme guarantees this purpose by issuing a digital certificate containing the unique identity of any IoT device. Strictly speaking, the CIoTCA checks the digital certificate database before issuing a digital certificate for an IoT device, which prevents identity duplication.

Assigning a unique ID for each edge zone and using it in the IoT identification accelerates finding and getting the reputation profile of an IoT device when the IoT device moves across edge zones. Clearly, after an IoT device registers itself in an edge zone and moves to another edge zone, the new edge zone needs the reputation profile of the IoT device to use it be-fore trusting the data sent by the IoT device. In other words, the edge ID helps in routing reputation profiles across edge zones to reduce latency and not contacting cloud to get these files.

3.2 Computing the Reputation Values of IoT Devices

Reputation values are crucial in maximizing the correctness of the received readings from IoT devices. This Section introduces the proposed approach in calculating the reputation values of IoT devices. Figure 4 shows the proposed reputation values range. The symbol δ represents the estimated correct value among received readings, β represents the reputation values of IoT devices that send readings equals to δ, α is used to measure how far a reading is from δ, and λ represents the decrease in reputation value that should be considered when a readings is far by α from δ . This paper uses the following values: $\beta = 1, \alpha = 1, \lambda = 1$. That is, the IoT device that sends a correct reading is given a reputation of 1, while the IoT device that sends a reading greater or smaller than δ by δ (2δ or δ- δ) is given a reputation 0. We should mention here that the range of reputation value in this paper is $[-1, +1]$, therefore, the smallest reputation value given to an IoT device is -1 even if the sent reading is far from the optimal reading by more than twice the correct value. Moreover, to fix the cold start problem, δ is set to the median, and the reputation values of all IoT devices in the system are set to 0, because of no history of readings from IoT devices. This avoids using the sent readings from fresh IoT devices at the beginning, but it allows fresh IoT devices to build their reputations according to the closeness of their first readings from the estimated correct value (Fig. 4).

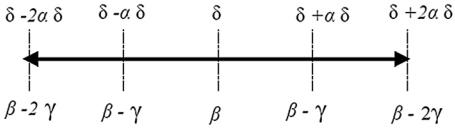

Fig. 4 Reputation range

The proposed approach uses Formula 1 to compute the preliminary reputation value, denoted by P_0, which is based on the current reading sent by the corresponding IoT device. The formula guarantees assigning reputation values according to the closeness of the sent reading from the correct value, denoted by δ. For example, given the values $\beta = 1$, $\alpha = 1$, $\lambda = 1$ used by this paper, suppose that the correct value $\delta = 30$, and two IoT devices, say X and Y, sent the values 10 and 60 respectively. In this case, $P_0(IoT_x) = +0.33$ and $P_0(IoT_y) = 0.0$.

$$P_0(IoT_x) = \beta - (|r_x - \delta|/\alpha\delta) \tag{1}$$

3.3 Updating the Reputation Values of IoT devices

Formula 2 is used to update the stored reputation value of an IoT device after computing the reputation value based on the new reading. The old reputation value, denoted by P_{old} , and the new computed value based on the new reading, denoted by P_{new}, are assigned weights, which are used to compute the updated reputation value. Hence, $P_{new} + P_{old} = 1$. In this paper, P_{old} is given a weight of 0.8, while P_{new} is given a weight of 0.2. These values may differ according to the given system. That is, some systems may prefer to give high weight to stored value and minimize the effect of the new computed values.

Selecting the appropriate weight values, P_{new} and P_{old}, is important in avoiding malicious or malfunction IoT devices. Assigning a very high value to P_{new} (very low value to P_{old}) may enable some IoT devices, which were considered as malicious IoT devices in the past in other locations, to get a high reputation fast when moving to new locations. This enables them to send malicious or incorrect readings without detection at the beginning. Meanwhile, assigning a high value to P_{old} (very low value to P_{new}) may prohibit some benign nodes that suffered malfunctions in the past from getting back quickly and participating in sending readings. Therefore, this trade off should be considered when assigning weights to get the highest performance.

$$P(IoT_x) = w * P_{old}(IoT_x) + (1 - w) * P_{new}(IoT_x) \tag{2}$$

3.4 Computing the Correct Reading

There are different families of IoT devices, as discussed in Sect. 3. These devices may send different readings such as weather conditions, pollution, traffic jam, humidity, ratings of services such as edge and cloud services or other types of ratings, etc. The readings may be sent from different IoT devices about a specific object in the same location, such as pollution percentage sent from a group of sensors in the same location and time window, or traffic jam readings sent from a group of vehicles in the same location and same time window. These readings may be different because of the type of sensors, sensitivity, battery, malfunction, etc. Thus, how can we estimate the correct reading among the different readings sent? The estimate

of the correct reading should consider malfunction and malicious IoT devices. Moreover, some benign IoT devices may be more accurate than others in measuring and taking a reading. Therefore, the readings sent by accurate and benign IoT devices should be considered more in estimating or computing the correct reading. To achieve this purpose, the weight of readings should be different according to the trustworthiness of IoT devices. The trustworthiness depends on the reputation of an IoT device, which are computed based on the history of correct (or how close) sent by the IoT device.

Formula 3 is used to compute the correct reading among the sent readings with considering the reputation of IoT devices. However, the readings sent by IoT devices with positive reputation values only are considered. That is, the readings sent by IoT devices with negative reputation values are excluded. These devices should prove that they can be trusted by sending correct readings or close correct readings and get a positive reputation in order to consider their readings afterward.

$$\delta = \sum_{x=1}^{n} r_{xt} * P(IoT_x) / \sum_{x=1}^{n} P(IoT_x), P(IoT_x)\, 0 \tag{3}$$

where $IoT_x \in \{IoT_1, IoT_2, IoT_3, ..., IoT_n\}$, r_{xt} is the reading r sent by the IoT_x during the time window t, $P(IoT_x)$ is the reputation value of IoT_x.

3.5 The Algorithm

Algorithm 1: Computing correct readings and reputation values

Given $G_x = \{IoT_1, IoT_2, IoT_3, \ldots, IoT_n\}$ a set of IoT devices, $R_{xt} = \{r_{1t}, r_{2t}, r_{3t}, \ldots, r_{nt}\}$ the readings sent by G_x during a time window t, P = $\{p_1, p_2, p_3, \ldots, p_n\}$ the reputation values of G_x.
for *i=1 to n* **do**
  $p_i \leftarrow 0$ `// Assign a reputation of 0 for all IoT devices`
end
Set m $\leftarrow$ median ($\{r_{10}, r_{20}, r_{30}, ..., r_{n0}\}$) `//compute the median for the first set of sent readings`
for *x=1 to n* **do**
  $P_0(IoT_x) = 1$–(| $r_x - m$ | /m)`//compute the first reputation value of each IoT device`
end
for *t= 1 to k* **do**
  $\delta = \sum_{x=1}^{n} r_{xt} * P(IoT_x) / \sum_{x=1}^{n} P(IoT_x), P(IoT_x) > 0$ `//Compute the correct value using sent readings and stored reputations`
  for *x=1 to n* **do**
    $P_{new}(IoT_x) = \beta - (|r_x - \delta| / \alpha\delta)$ `//compute the new reputation value of the given IoT based on the sent reading`
    $P(IoT_x) = 0.8 * P_{old}(IoT_x) + 0.2 * P_{new}(IoT_x)$ `//update the stored reputation value (old)`
  end
end

The proposed approach can be used for all IoT devices families. To explain the approach, suppose that $G_x = IoT_1, IoT_2, IoT_3, ..., IoT_n$ is a set of IoT devices located in a location l during the time window t. Now, suppose that all devices have sent readings $R_{xt} = r_{1t}, r_{2t}, r_{3t}, \ldots, r_{nt}$, where r_{it} is a reading r sent by IoT_i during time window t. Now, to estimate the correct value among sent readings, the reputation of IoT devices should be considered. Suppose that the $P = p_1, p_2, p_3, \ldots, p_n$ is the set of reputations values of the set G_x, where $-1 \leq p_i \leq +1$. Algorithm 1 shows how the proposed approach compute correct readings, and compute and update the reputation values.

First, all IoT devices are assigned a reputation of 0 (steps 2–4) since all IoT devices are fresh at the beginning. Hence, this reputation excludes the readings sent by these IoT devices from consideration when computing the correct reading. However, these readings are considered when computing the reputation values of these devices. That is, fresh IoT devices that send close readings to the correct reading get a positive reputation, which helps them to be considered when computing correct readings afterwards. Next, after fresh IoT devices send their readings, the median of these readings is considered the correct value (step 5). Based on this value, the reputation of fresh IoT devices is computed using Formula 1 (steps 6–8). In subsequent readings sent by IoT devices, the correct reading is computed (for every preset time window) using Formula 3 (step 10). The reputation of IoT devices are updated after each time window using Formula 1 and Formula 2 (steps 11–14). Notice that the weights of old reputation and new reputation values used in this paper is 0.8 and 0.2 respectively. Hence, the P_{old} means the stored reputation value, P_{new} means the reputation value computed based on the current sent reading, and the updated reputation value means the update on the stored reputation value.

4 Experiments and Analysis

The experiments were conducted using Cooja contiki Simulator 3.0 on Ubuntu Operating System [27]. The Network area was set to 1000 X 1000 m2. One cloud node, ten edge nodes and hundred IoT devices were generated in the experiments.

Table 1 Simulation parameters

Parameter	Value
Operating system	Ubuntu 18.04
Simulator	Cooja contiki simulator 3.0
Network area	1000 X 1000 m2
Number of cloud nodes	1
Number of edge nodes	10
Number of IoT devices	100
Number of mobile IoT devices	Differs according to the experiment
Number of malicious devices	Differs according to the experiment

The IoT devices used are mobile, where the percentage of mobile devices differs in the experiments. The IoT devices generated consists of malicious and benign IoT devices, and the percentage of malicious IoT devices differs in the experiments. Table 1 shows the simulation parameters. The value of the true correct reading of the monitored phenomena, event, etc. that IoT devices sends readings about is set to 60. Each IoT devices were set to send two to three readings in the edge zone before moving to other zones. Malicious IoT devices were set to send a reading of a random value between 0 and 30, while benign IoT devices were set to send a reading of a random value between 58 and 62.

The conducted experiments compare between two methods, which are the proposed method in this paper and a baseline method. The properties of the baseline method are as follows. It sets the reputation value to 1 for fresh IoT devices, and updates the reputation value of the IoT device according to the formulas provided in the paper. However, it does not keep the reputation values of IoT devices when moving to other edge zones. That is, an IoT device gets a fresh reputation value of 1 when it moves to new zones. The following experiments compare between the two methods.

Figure 5 compares between the computing of correct value by both the proposed approach and the baseline approach given many readings about a specific condition received from many IoT devices in the same location and time window. The experiment were conducted given variable percentage of malicious IoT devices. The Benign IoT devices and Malicious IoT devices sent two readings in each edge zone they visit before moving to different zones. The correct values shown in the figure are average of correct values that were computed in all edge zones. The mobility of IoT devices in this experiments was set to 100%. As shown in the figure, the computed correct values by the proposed system are very close to the true correct value, which is 60. The percentage of malicious IoT devices and the high mobility of IoT devices did not affect the computed correct value in the proposed system. This is due to the fact that the proposed system assign reputation values to IoT devices according to how close their readings from the computed correct value. The low reputation of malicious IoT devices assigned very low weight to the readings they sent, which reduce their effect in the overall

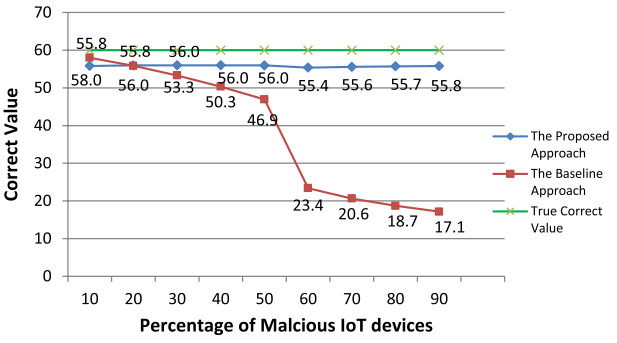

Fig. 5 The computation of correct values with variable percentage of malicious IoT devices

computation of correct values. This process was not affected by the high rate of mobility as the proposed system keeps the reputation values and updates them as the the IoT devices move from one edge zone to another. However, this is not situation in the case of the tradition approach.

The results of the baseline approach are not encouraging as shown in Figure 5. The computed correct values of the baseline approach are far from the true correct value, which is 60. This poor performance in computing the correct value by the baseline approach become very poor as the percentage of malicious nodes increases as shown in the figure. This is due to the fact that the baseline approach does not keep the reputation of IoT device while moving from edge zone to another, and gives full reputation of 1 for fresh IoT devices at the beginning.

Figure 6 shows the final reputation values of both benign and malicious IoT devices in the proposed system. This experiment was performed by allowing IoT devices to send three readings in each edge zone before moving to another zone. The mobility in this experiment was set to 100%. The reputation values were extracted after the experiment ended.As mentioned before, benign IoT devices were set to send readings from the range [58–62], and the malicious IoT devices was set to send readings from the range [0–30]. As shown in the figure, the reputations of benign IoT devices are very close to 1 (the highest possible reputation value).However, the reputation values of malicious IoT devices varies from 0 to around 50. Keeping the reputation values on edge nodes and in the cloud helped the proposed system to move the reputation values while IoT devices move. Moreover, the synchronization process between edge nodes and the cloud node allowed edge nodes to retrieve the updated reputation values and to use them in the computation process of correct readings.

Figure 7 shows how the proposed approach and the baseline approach compute the correct value of reading given different percentage of mobility of IoT devices. As shown in the figure, the baseline approach behaves badly when increasing the percentage of mobile devices, meanwhile, the performance of the proposed approach is stable while increasing the percentage of mobile IoT devices.

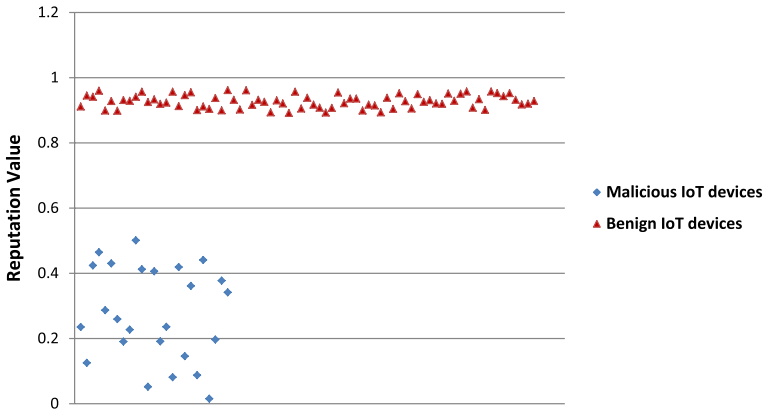

Fig. 6 The final reputations of IoT devices

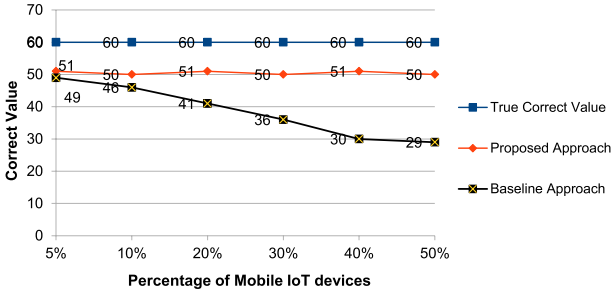

Fig. 7 Computing correct values vs variable IoT mobility

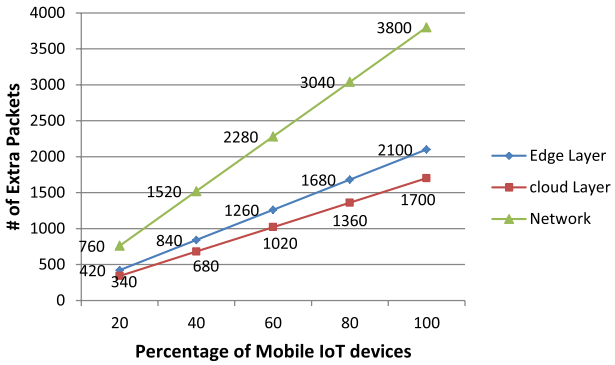

Fig. 8 Network overhead

Figure 8 shows the network overhead of the proposed system. Clearly, the proposed approach adds some overhead on the network because of the transferring of IoT profiles among edge nodes and the cloud node. Moreover, the figure shows that the overhead posed on edge nodes is larger than the cloud node. This is due to the fact that the experiment was set to allow IoT devices to move from one edge zone to another and to send two readings in each edge zone they moved to. This allowed edge zones to find the IoT profiles in neighboring edge nodes, and eliminated the need to contact the cloud to retrieve the updated IoT profile. The overhead on the cloud node was posed because of the synchronization process between edge nodes and the cloud node.

5 Conclusions and Future Work

The applications of IoT are growing immensely. Trusting the data gathered from IoT devices is mandatory for the applicability and usability of IoT application. Therefore, measuring the reputation of IoT devices to build a trust metric is crucial. However, the heterogeneity and mobility of IoT devices makes this mission harder. This

paper has proposes a global reputation system that assign global identities to IoT devices regardless of their heterogeneity. Moreover, it has proposed a method to compute the reputations of IoT devices to be used in computing the correct values of readings. The proposed model has leveraged edge computing and cloud computing capabilities to achieve its purpose. The experiments have shown that the proposed approach achieves very good results in estimating the true value of readings in contrary to the baseline approach. Furthermore, the experiments have shown that proposed model reduces the effect of malicious and malfunction IoT devices greatly by assigning very low reputation to such devices. As future work, we plan to apply the proposed model in larger environment, and check the scalability of our model and how it deals with large amount of received data.

Acknowledgements This work was supported in part by Jordan University of Science and Technology, Research Award #20190150.

References

1. Venkatraman, B., Aloqaily, M., Reisslein, M.: An SDN architecture for time sensitive industrial IoT. J. Comput. Netw. **186**, 107739 (2021)
2. Ridhawi, I. Al., Aloqaily, M., Boukerche, A., Jararweh Y.: Enabling intelligent IoCV services at the edge for 5G networks and beyond. IEEE Trans. Intell. Transp. Syst. (2021)
3. Khanna, A., Kaur, S.: Internet of Things (IoT), applications and challenges: a comprehensive review. J. Wirel. Pers. Commun. **114**, 1687–1762 (2020)
4. Hart, J., Martinez, K.: Toward an environmental Internet of Things. J. Earth Space Sci. **2**(5), 194–200 (2015)
5. Jararweh, Y., Otoum, S., Ridhawi, I.Al.: Trustworthy and sustainable smart city services at the edge. J. Sust. Cities Soc. **62**, 102394 (2020)
6. Midtown Congestion Management System. https://www1.nyc.gov/html/dot/html/pr2012/pr12_25.shtml
7. Andrade, E., Nogueira, B., Farias, I., Araújo, D.: Performance and availability trade-offs in fog-cloud IoT environments. J. Netw. Syst. Manag. **29**, 2 (2021)
8. Hashemi, S., Shams, F.: Fuzzy, dynamic and trust based routing protocol for IoT. J. Netw. Syst. Manag. **28**, 1248–1278 (2020)
9. Nitti, M., Girau, R., Atzori, L.: Trustworthiness management in the social Internet of Things. IEEE Trans. Knowl. Data Eng. **26**(5), 1253–1266 (2014)
10. Yan, Z., Ding, W., Niemi, V., Vasilakos, A.V.: Two schemes of privacy preserving trust evaluation. J. Future Gener. Comput. Syst. **62**, 175–189 (2016)
11. Michalas, A., Komninos, N.: The lord of the sense: a privacy preserving reputation system for participatory sensing applications. In: Proceedings of the 2014 IEEE Symposium on Computers and Communications (ISCC), pp. 1–6 (2014)
12. Hasan, O., Brunie, L., Bertino, E., Shang, N.: A decentralized privacy preserving reputation protocol for the malicious adversarial model. IEEE Trans. Inf. Forensics Secur. **8**(6), 949–962 (2013)
13. Hasan, O., Brunie, L., Bertino, E.: Preserving privacy of feedback providers in decentralized reputation systems. J. Comput. Secur. **31**(7), 816–826 (2012)
14. Asiri S., Miri, A.: An IoT trust and reputation model based on recommender systems. In: Proceedings of the 14th Annual Conference on Privacy, Security and Trust (PST), Auckland, pp. 561–568 (2016)
15. Mendoza, C.V.L., Kleinschmidt, J.H.: A distributed trust management mechanism for the Internet of Things using a multi-service approach. J. Wirel. Pers. Commun. **103**(3), 2501–2513 (2018)
16. Hussain, Y., Zhiqiu, H., Akbar, M., Alsanad, A., Alsanad, A.A., Nawaz, A., Khan, I., Khan, Z.: Context-aware trust and reputation model for fog-based IoT. J. IEEE Access **8**, 31622–31632 (2020)

17. Chen, J., Tian, Z., Cui, X., Yin, L., Wang, X.: Trust architecture and reputation evaluation for Internet of Things. J. Ambient Intell. Humaniz. Comput. **10**(8), 3099–3107 (2019)
18. Debe, M., Salah, K., Rehman, M.H.U., Svetinovic, D.: IoT public fog nodes reputation system: a decentralized solution using Ethereum blockchain. J. IEEE Access **7**, 178082–178093 (2019)
19. Fortino, G., Messina, F., Rosaci, D., Sarne, G.M.L.: Using blockchain in a reputation-based model for grouping agents in the Internet of Things. IEEE Trans. Eng. Manag. 1231–1243 (2020)
20. Fortino, G., Messina, F., Rosaci, D., Sarnń, G.L.: Using trust and local reputation for group formation in the Cloud of Things. J. Future Gener. Comput. Syst. **89**, 804–815 (2018)
21. Zhang, P., Kong, Y., Zhou, M.: A domain partition-based trust model for unreliable clouds. J. IEEE Trans. Inf. Forensics Secur. **13**(9), 2167–2178 (2018)
22. Allahdadi, A., Ricardo, M.: Anomaly detection and modeling in 802.11 wireless networks. J. Netw. Syst. Manag. **27**(1), 3–38 (2019)
23. Djedjig, N., Tandjaoui, D., Medjek, F., Romdhani, I.: Trust-aware and cooperative routing protocol for IoT security. J. Inf. Secur. Appl. 52 (2020)
24. Thulasiraman, P., Wang Y.: A lightweight trust-based security architecture for RPL in mobile IoT networks. In: Proceedings of the 16th IEEE Annual Consumer Communications and Networking Conference (CCNC), Las Vegas, NV, USA (2019)
25. Murali, S., Jamalipour, A.: A lightweight intrusion detection for Sybil attack under mobile RPL in the Internet of Things. J. IEEE Internet Things **7**(1), 379–388 (2020)
26. Alliance for Internet of Things Innovation AIOTI. https://aioti.eu/
27. Cooja Simulator. http://anrg.usc.edu/contiki/index.php/Cooja_Simulator

Qussai Yaseen received his Ph.D. in Computer Science from the University of Arkansas, USA in 2012. He is currently an Associate professor at Jordan University of Science and Technology, Jordan. He published many papers in prestigious journals and conferences in fields related to networks security, security analytics, insider threat, and IoT security. Moreover, he is an active member in many events in information technology in the fields of information security, computer networks, mobile computing, etc. such as DDSW, EDI40, SECUREWARE, MobiSPC, ICICS.

Yaser Jararweh received his Ph.D. in Computer Engineering from the University of Arizona, USA in 2010. He is currently a professor of computer sciences at Duquesne University, USA. He has co-authored several technical papers in established journals and conferences in fields related to machine learning applications, blockchain, edge-cloud computing, HPC, SDN, security and data intensive computing. He is co-chairing many IEEE events such as FMEC, SDS, IoTSMS, SNAMS, AICCSA and CCSNA.