A Two-level Integrated Approach for Assigning Trust Metrics to Internet of Things Devices

Evandro L. C. Macedo[1][a], Flavia C. Delicato[2][b], Luís F. M. De Moraes[1][c]
and Giancarlo Fortino[3][d]

[1]*Systems and Computing Engineering Program (PESC), Universidade Federal do Rio de Janeiro, Rio de Janeiro, RJ, Brazil*
[2]*Institute of Computing, Universidade Federal Fluminense, Niterói, RJ, Brazil*
[3]*Department of Informatics, Modeling, Electronics and Systems (DIMES), University of Calabria, Cosenza, Calabria, Italy*

Keywords: Blockchain, Entropy, IoT, Security, Trust.

Abstract: The Internet of Things (IoT) is the next step of the Internet evolution and it is paving the way for the development of Cyber-Physical Systems (CPS). It will enable the development of a plethora of new systems and applications. The massive, ubiquitous spread of interconnected IoT devices has increasingly exposed the vulnerability of data and related applications in an unprecedented way. If the security of any component in such systems gets compromised, an associated data leak may cause serious threats to privacy, material losses, and even put people's lives at risk. Therefore, studies on IoT security aspects have become increasingly important. This paper presents a proposal to deal with the still open issue related to trust aspects of IoT systems. The key idea consists of a two-level approach to simultaneously consider application and network characteristics, in which trust is modeled by combining a relative entropy measure of device's data rate (at the low level), and a reputation of a device provided by distributed-ledger (at the high level). Numerical results show the effectiveness of the proposed approach in isolating anomalous/untrusted devices based on their acquired reputation and on the respective changes in data rate behavior.

1 INTRODUCTION

The Internet of Things (IoT) (Atzori et al., 2010) represents a new stage in the evolution of the Internet, extending network communications to any type of intelligent object (*thing*). With an estimate of approximately 30 billion connected things by 2025 (Statista, 2021), the spread of IoT paves the way to a myriad of applications that can significantly impact the current society's way of life. Considerable benefits can be obtained, for instance, in the areas of healthcare, smart cities, smart home applications, intelligent transportation systems, and many other use cases based upon IoT devices (Casadei et al., 2019). The IoT will also enable the interoperability of heterogeneous technologies, through unprecedented data acquisition and exchange among diverse peer devices.

Taking advantage of the huge amount of data that can be collected by associated devices, several existing and envisaged IoT applications should also provide improvements to a variety of decision-making processes. However, harvesting such benefits will also imply tackling the task of providing security to each of the involved devices. In fact, achieving the full potential of IoT applications and services essentially depends on the trustworthiness of information and the protection of private data, especially in highly sensitive application domains such as healthcare, for instance. In IoT systems, if the security of any component becomes compromised, a data leak may cause serious privacy threats, bring about material losses, or even jeopardize people's lives. For example, a tampered sensor may expose private data, or deliver wrong measures for a patient's heart rate in healthcare IoT applications, leading to wrong-prescription errors. In another example, the malfunction caused by the disruption of any data supply-chain used to control traffic lights in an intelligent transport system may cause the occurrence of vehicle crashes. Thus, in this context, besides financial loss, a security flaw can lead to a violation of data privacy and, in the worst cases,

[a] https://orcid.org/0000-0001-5430-2168
[b] https://orcid.org/0000-0001-5334-8279
[c] https://orcid.org/0000-0002-4225-6296
[d] https://orcid.org/0000-0002-4039-891X

Macedo, E., Delicato, F., Moraes, L. and Fortino, G.
A Two-level Integrated Approach for Assigning Trust Metrics to Internet of Things Devices.
DOI: 10.5220/0010975800003194
In *Proceedings of the 7th International Conference on Internet of Things, Big Data and Security (IoTBDS 2022)*, pages 26-36
ISBN: 978-989-758-564-7; ISSN: 2184-4976

it may even incur physical damage to human beings. Therefore, new requirements and challenges need to be considered in the design of IoT systems and applications, especially in terms of security and trust (Paliszkiewicz, 2018; Sicari et al., 2015; Yan et al., 2014; Macedo et al., 2019; Bertino, 2019; Dedeoglu et al., 2019; Junior and Kamienski, 2021).

In this paper, we leverage the work proposed in (Macedo et al., 2020) by presenting a comprehensive evaluation and improving the model details. In such proposal, trust is modeled by gathering data from both the network and the application layers, which stand respectively for the *Low Level* and the *High Level*. For the High Level, the proposed model assumes the use of a distributed-record based on *blockchain*. This approach aims to provide an initial trust to devices that do not know each other previously. A relative entropy measure is adopted for the Low Level in order to capture data rate patterns changes. The key idea is to use the relative entropy of the data rate between communicating IoT devices to monitor the network behavior in order to detect anomalies. Additionally, it is also assumed a temporal decay of trust measured values to deal with the usual dynamism of IoT devices and their opportunistic interactions. The major advantage of such an integrated approach is that it exploits not only application information, but also network information to infer how much a device should be trusted. Different from our previous work (Macedo et al., 2020), we present: (i) a more detailed modeling with specific formulas according to the different cases of trust calculation; and (ii) more comprehensive results that show the effectiveness of the approach with different levels of malicious devices within the network.

The rest of this paper is organized as follows. In Section 2 we discourse about related works, presenting a comparative analysis between them and this proposal. Section 3 presents the two-level trust proposal and Section 4 its modeling. In Section 5 the experimental evaluation results are presented together with some discussions. Finally, Section 6 concludes the paper and foresees future work.

2 RELATED WORK

Dealing with security aspects is a major challenge in IoT (Stankovic, 2014; Atzori et al., 2010; Abomhara and Køien, 2014; Al-Fuqaha et al., 2015; Sicari et al., 2015; Prokofiev et al., 2017; Khan and Salah, 2018; Zhang et al., 2018; Macedo et al., 2019; Fortino et al., 2020b; Delicato and Pires, 2020), mainly because of the heterogeneity between the multiple components and platforms IoT interconnects, the resource-constrained devices, and the wireless communication technologies. In particular, the problem of assigning trust metrics to IoT devices is of a paramount importance and is currently considered as an open issue (Sato et al., 2016; Liu et al., 2016; Paliszkiewicz, 2018; Din et al., 2018; Sfar et al., 2018; Macedo et al., 2019; Fortino et al., 2020a; Babar et al., 2021; Wang and Zhang, 2016).

Fortino et al. (Fortino et al., 2019) designed a framework in which every IoT device was associated with a software agent capable to exploit its social attitudes to cooperate as well as to form complex agents social structures. The authors consider the reputation aspect by using a blockchain (Christidis and Devetsikiotis, 2016; Zhang and Zhou, 2020) implementation. In their approach, devices can use network services according to their reputation provided by blockchain. In (Fortino et al., 2020b) they also consider social aspects to provide a framework resilient to malicious activities.

In (Tang et al., 2019), Tang et al. use the passport analogy to propose a decentralized trust framework for cross-platform collaborations using blockchain technology. The authors highlight that an overall consensus framework for trust remains to be developed. In our approach, we focus on recording the devices' identities in blockchain to build devices' reputation (initial trust), but we improve such initial trust with information from the data rate behavior.

In (Hongjun et al., 2008), authors use Information Theory to build trust among devices. They represent the relationships among devices with a directional graph and compute the entropy of the capability of a device in performing an action. This way, they can detect malicious devices in the network. We also consider Information Theory in our work, but with a different perspective, focusing on the network level instead of the application level.

Khan et al. (Khan et al., 2017) propose a trust-based approach for managing the reputation of every device of an IoT network based on Routing Protocol for Low-Power and Lossy Networks (RPL). The approach generate the routing rules based on the reputation values of the devices. Authors' approach shows the ability to detect and also isolate malicious nodes from the network, resulting in better network resilience, as well as less number of misbehaving devices (bad devices) identified in the network after every RPL round. Our approach is independent of the routing protocol, since it relies on device to device communication to infer trust values.

Authors in (Caminha et al., 2018) introduce a smart trust management method based on machine learning which automatically assesses IoT trust by evaluating service provider attributes. In (Bernabe et al., 2016), authors use fuzzy logic to provide an end-to-end security solution through a lightweight authorization mechanism and a novel trust model that has been specially devised for IoT environments.

In (Zhou et al., 2018), authors consider an Identity-Based Encryption implementation together with a blockchain implementation. Authors split the devices in the chain to complete user authentication and private key protection. The results show the failure probability is stabilized with the number of cycles during which a device operates. We consider a two-level approach with not only application characteristics to infer trust values, but also network characteristics.

Authors in (Wang et al., 2021) considered building a distributed trust system for cooperative learning in edge computing. They propose a trusted consensus scheme for multi-party collaborative learning of edge artificial intelligence using a blockchain-based approach. Through experiments, the authors show that their proposal can be applied to such contexts with more safety and efficiency by reducing the probability of an attacker being chosen as the leader of the considered consensus protocol.

In (Hasan et al., 2019), authors assess the performance of several machine learning models to predict attacks and anomalies on the IoT systems accurately. Their study showed that the system obtained 99.4% test accuracy for Decision Tree, Random Forest, and ANN with a slightly better performance in other metrics for Random Forest.

The aforementioned proposals emphasize the importance and relevance of building trust-based approaches to provide security in the communication among IoT devices. In this paper, besides presenting a trust model that combines blockchain and Information Theory techniques, the key contribution of our work is the double perspective of both application level and network level, which allows capturing the dynamics of data rate behavior of devices and provides a comprehensive metric. Hence, our approach provides a more comprehensive trust metric that can deal with the particularities of IoT devices' data rate patterns.

3 TWO-LEVEL TRUST PROPOSAL

To perform device trust assignment, we consider an IoT system composed of three tiers, namely, the *Things* tier, the *Cloud* tier and an intermediate *Edge* tier (Li et al., 2017). Such an organization is driven by the recent paradigm of Edge Computing (Shi et al., 2016; Abbas et al., 2018), which aims to move (part of) computing, processing, and storage resources to the edge of the network, rather than centralizing them in remote cloud data centers. Considering such organization for an IoT system, we envision the High Level implementation at the Edge Tier to provide devices with lower latency than if it was at the Cloud Tier. We consider using blockchain since neither the Edge nor the Cloud Tiers provide the characteristics of immutability, traceability, and tamper-proof by design, which are native to blockchain platforms. Figure 3 illustrates a complete scenario considering both High and Low Levels in a three-tier architecture.

We propose modeling trust as a composition of application (High Level) and network (Low Level) characteristics that can be observed in a scenario with a device communicating with another device. We claim that, by using such characteristics, the device can calculate how much it trusts in the other device. The network characteristic that we consider is the data rate behavior of a device, while the application characteristic is the reputation that the identity of a device presents on the community (given by blockchain). In such a scenario, two devices at the Thing Tier do not know each other in a first contact, having little or no information required to infer an initial trust to start communicating. Then, to acquire the respective initial trust, the devices rely on the High Level to properly obtain the reputation of the related device's identity.

As Figure 1 depicts, initially, each IoT device queries the reputation (initial trust) of the other device's identity in a distributed-ledger-based infrastructure, which is at the High Level of our approach. Once the minimum initial trust is acquired, the communication can normally start over the Internet infrastructure. Another case of usage of the High Level is when the trust value drops below a certain predefined minimum trust (threshold) and the device needs to acquire again the last reputation value from the blockchain infrastructure. In particular, such threshold must be provided by the respective IoT application, depending on its specific security requirements. Applications with less stringent requirements will adopt lower thresholds, while applications more restrict will only accept high values of trust (high threshold). For analysis proposes, readers can notice in Section 5 that we considered a strict IoT application with a minimum trust of 0.8.

As the communication between the devices happens, the Low Level takes place (Figure 2). One device calculates the relative entropy of the other device's data rate (and vice versa) and uses this infor-

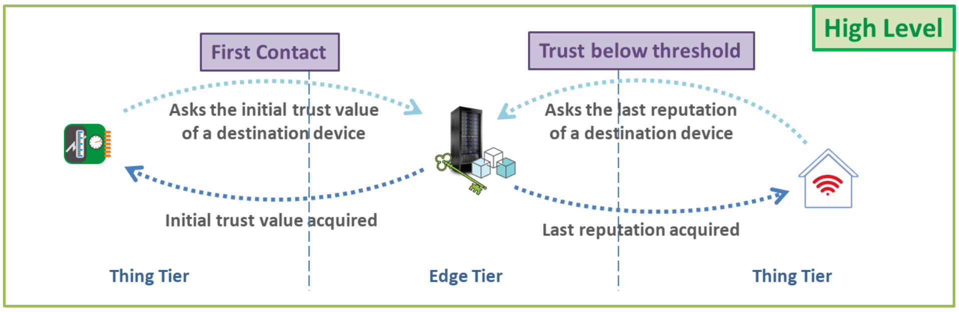
High Level
First Contact
Trust below threshold
Asks the initial trust value of a destination device
Initial trust value acquired
Asks the last reputation of a destination device
Last reputation acquired
Thing Tier
Edge Tier
Thing Tier

Figure 1: Two cases of the usage of High Level: when the first contact is established and an initial trust value needs to be acquired; and when the trust value drops below a predefined threshold (minimum trust).

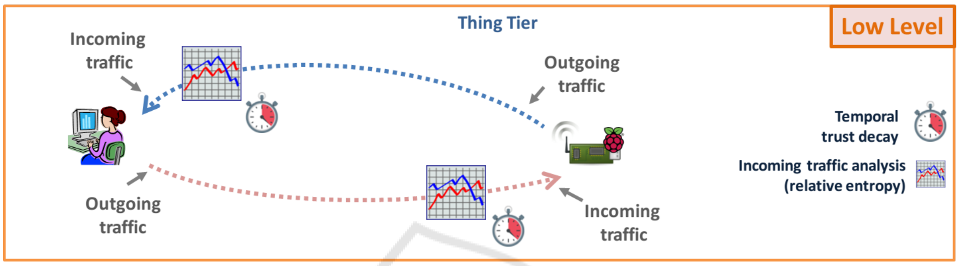

Figure 2: Example of the usage of Low Level: each device analyses the incoming data rate of the other device and builds its trust according to the relative entropy of such data rate.

mation to adjust the value of trust in the sender device over time. If the sender device starts behaving abnormally, this will negatively affect the trust and may cause communication to terminate if it decreases beyond a previously established threshold. In our case, an abnormal behavior means any data rate pattern that diverges from the estimated data rate distribution. If the communication is over, a temporal component reduces the trust value until it reaches the point that the devices will need to query the blockchain again and restart the whole process.

4 TRUST MODELING

In order to present the mathematical model, which can be used to obtain our proposed trust metric, let X_{ji} represent the data rate (in Bytes per second – Bps) that a device j receives from a device i, for any given pair of devices in an IoT network. X_{ji} is a non-negative, integer random variable that assumes values in the interval $\mathcal{S}_{ji} = [0, \Delta, 2\Delta, 3\Delta, \ldots, R_{ji}^{max}]$, where Δ is a positive integer and R_{ji}^{max} is the maximum received data rate. Thus, after observing sample values of the random variable X_{ji}, we obtain the respective sample distribution

$$P[X_{ji} = x] \triangleq p_{X_{ji}}(x), \quad x \in \mathcal{S}_{ji},$$

with which we derive information metrics based on Shannon's Information Theory formulas (Shannon, 1948), as we discuss afterward. More details about the samples used to obtain X_{ji} will be discussed in Section 5.

Let TR_{ji} be the trust of device j in device i. The trust values range from 0.0 (zero), which is the minimum trust value (or simply no trust), to 1.0 (one), which is the maximum value of trust. The TR_{ji} is based on the following three components:

1. TR_{ji} is initially computed based on the trust of the $i's$ identity, which is obtained from its reputation stored in a public-permissioned distributed ledger (*e.g.*, blockchain), expressed by C_1 (Equation 1). Such initial reputation values represented by the transactions in blockchain are populated through successfully past established communications, which the devices report at the end of an interaction. The number of confirmations a transaction has on the blockchain gives the reputation value provided by this component. We envision the implementation of full nodes at the Edge Tier, and not at the Things Tier, given that the IoT devices are known as being resource-constrained.

$$C_1 = \text{\# of confirmations the } i\text{'s identity has} \quad (1)$$

To establish consensus on a blockchain, it is essential to have a significant number of nodes (Paliszkiewicz, 2018). In addition, blockchain itself still has limitations, such as the transaction validation time and computational power required to

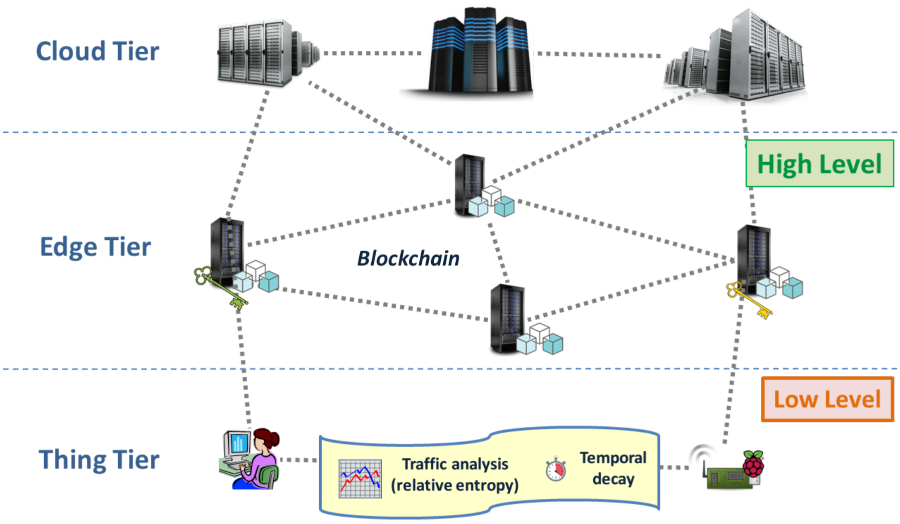

Figure 3: Trust scenario of two-level approach considering a tree-tier architecture.

form full nodes. Such aspects might incur an overhead in the communication between IoT devices. To overcome this issue, we propose building a blockchain infrastructure that can handle various application requirements and levels, from local applications associated with a local blockchain, to a global application with a blockchain in a large scale. In particular, we consider a consensus protocol based on proof-of-stake, which has the potential to better fit this context and can be implemented using, for instance, the Tezos Blockchain (Goodman, 2014).

For modeling purposes, we chose for this component to follow a Gaussian distribution with parameters mean $\mu = 1$ and variance $\sigma^2 = 1$ to have samples of the number of confirmations normally distributed.

The more confirmations a transaction has, the harder it is to tamper such a transaction. Thus, based on the number of confirmations we can consider the transaction is strongly agreed upon by blockchain members and the tampering probability can be considered negligible;

2. TR_{ji} is also influenced by the relative entropy of the data rate, which changes when the current data rate behavior of the device deviates from the estimated data rate behavior due to any type of anomalous condition. The estimated data rate distribution X_{ji} can be obtained through an initial observation of the data rate behavior of the peering device, in which the device learns the "true" distribution. To obtain such metric, we discuss the following concepts. The self-information of the event $\{X_{ji} = x\}$ is defined as $I(x) = -\log p_{X_{ji}}(x)$ (Shannon, 1948; Gallager, 1968). The average of the self-information is the entropy of the random variable X_{ji}, given in Equation (2).

$$H(X_{ji}) = E[I(X_{ji})] = -\sum_{x \in \mathcal{S}_{ji}} p_{X_{ji}}(x) \log p_{X_{ji}}(x) \tag{2}$$

In the same way, we define the non-negative, integer random variable Y_{ji}, which represents the observed data rate flowing into a device j generated by a device i. Y_{ji} also assume values in $\mathcal{S}_{ji}$ and its distribution is defined as:

$$P[Y_{ji} = y] \triangleq q_{Y_{ji}}(y), \quad y \in \mathcal{S}_{ji}.$$

Using previous definitions, we can calculate the relative entropy described in Equation (3), which stands for the Kullback-Leibler (Kullback, 1959; Principe, 2010) divergence, a type of "distance" between two distributions.

$$D(p||q) = \sum_{x \in \mathcal{S}_{ji}} p_{X_{ji}}(x) \log \frac{p_{X_{ji}}(x)}{q_{Y_{ji}}(x)} \tag{3}$$

Therefore, $p_{X_{ji}}(x)$ is the estimated distribution of the data rate received by j sent by i. The $q_{Y_{ji}}(x)$ is also the distribution of the respective data rate, but is the actually observed during data transmission. As $q_{Y_{ji}}(x)$ approximates $p_{X_{ji}}(x)$ in Equation 3, the relative entropy ("distance") $D(p||q)$ decreases. So, based on previous conclusions, we model data rate behavior when the observed distribution differs from the true (estimated) distribution, and adjust the trust of a specific device. In order to capture the essence of the divergence concept and bring it into the context of trust calculation, we define the component C_2 with the following strategy:

- if the obtained divergence value $D(p||q)$ is less than 1, then the calculated trust value follows the formula:

$$C_2 = 1.0 - D(p||q)$$

- for divergence values $D(p||q)$ greater than 1, the calculated trust value follows the formula:

$$C_2 = -0.5 + \left(\frac{1}{D(p||q)}\right)$$

The rationale behind such a strategy is to assign greater trust values to devices which present divergence values below 1 and penalize others that exceed 1. Divergence values below 1 (close to zero) indicate a ”proximity” of the distributions (little divergence), or even, little information gain (mutual information close to zero, little reduction in uncertainty about a random variable when observing another) (Principe, 2010; Gallager, 1968).

3. IoT is a highly dynamic and opportunistic environment. Devices constantly move around, sometimes over long distances. As a device is not able to know where the peering device moved to, or which networks it has joined in, or which people had access to it, so maintaining an unchanged trust value over time will not effectively represent how much the device is trustworthy. That is, since the context in which the interactions take place is prone to change, it is necessary to have an expiration of the trust value from the moment the communication ends. A possible analogy is the case of a web service session that expires if there is no user activity after a while, making it necessary to start a new session. Hence, for the third component, we considered a temporal decay that works like a timeout by decreasing the trust value from the moment devices stop communicating. When the trust value falls below a predefined threshold, the devices will need to restart the trust establishment process, i.e., the devices will need to obtain a minimum trust from blockchain again. In our model we consider a proportional temporal decay (C_3) as described in Equation (4).

$$C_3 = TR_{ji} \times d \tag{4}$$

where d is the decay factor.

The trust calculation is updated as the data rate samples from the devices are collected and the communication between them evolves over time. Each device recalculates its trust in other peering devices based on the respective current calculated trust. To do so, the device considers the following cases:

1. If the trust value is below the defined threshold, then the new trust value is calculated using the High Level component according to the following formula (Equation 5):

$$TR_{ji}^{\text{updated}} = TR_{ji}^{\text{current}} + C_1 \tag{5}$$

2. If the current trust value is above the related threshold, then the updated trust value is calculated through the Low Level component according to Equation 6:

$$TR_{ji}^{\text{updated}} = TR_{ji}^{\text{current}} + C_2 \tag{6}$$

3. Finally, in the case where there is no communication, then the temporal decay component takes effect, according to Equation 7:

$$TR_{ji}^{\text{updated}} = TR_{ji}^{\text{current}} - C_3 \tag{7}$$

5 EXPERIMENTAL EVALUATION AND DISCUSSION

In this section, we evaluate the potential of our approach to translate network data rate behavior of IoT devices into a meaningful trust metric. We perform experiments using real traces obtained from the dataset found in (Sivanathan et al., 2017) to validate our approach with data coming from a real IoT application. All dynamism that is typical of such a context is reflected into traces. For example, the connectivity disruption due to mobility causes zero data to be received by a device.

Traces from a smart-campus environment compose the dataset in (Sivanathan et al., 2017) with over 20 IoT devices, including cameras, smart lights, activity sensors, and health-monitors. These traces include raw packets and flow information, annotated with specific device attributes, over a period of 3 weeks. In our experiments, we consider the period of one day of the dataset and extract the data rate in bytes/s from flows for each pair of devices according to the tuple (Source IP, Destination IP) by summing the amount of bytes transmitted in one second. During the experiments, we used the data rate of some of those devices, such as smart lights and activity sensors, considering a scenario of smart city IoT application. In such scenario, interactions between devices may take place in order to accomplish cooperative tasks, such as a network of drones that cooperate to expand communication over an area of a disaster. With this, we envision that our approach can detect changes in data rate pattern and adjust the trust in the respective IoT device correctly (by increasing or penalizing it).

We run experiments considering the data rate between any two devices identified inside the dataset through their respective flows. Throughout the text, we use device i and device j to refer to those devices, where "devices i" denotes the devices sending data to "devices j" (receivers). The experiments consist in playing data rate values obtained from the dataset and calculating the trust metric according to Equations 5, 6, and 7. Relevant assumptions regarding the implementation should be highlighted:

- We consider a sliding window with size of 600 seconds to compose the data rate distribution estimation;
- For the sample distribution of the data rate, following the definitions presented in Section 4, we compute the relative frequencies of data rate considering $\Delta = 10000$ and we simplified the $R_{ji}^{max} = 100$ KBps for all devices, therefore $S_{ji} = [0, 10KBps, 20KBps, ..., 100KBps]$;
- The value for the estimated data rate, used to compare with the value for the actually received data rate, is calculated using a Kalman Filter with $mean = 0$ and $covariance = 1$, since it closely tracks the received data rate and does not require too many resources;
- When the communication is established for the first time between two devices, only the component at the High Level (application-based) actuates, obtaining the reputation of the device in the community;
- When the received data rate is greater than zero, only the Low Level component (network-based) actuates to change the trust value;
- When there is no data rate, only the temporal component (also bellowing to the Low Level) actuates by constantly decreasing the trust value according to a predefined rate (e.g., -0.1 trust/s).

We chose to obtain the initial trust values from the High Level synthetically from a Gaussian distribution with parameters $\mu = 1$ and $\sigma^2 = 1$. The initial trust values are provided by the blockchain (High Level) whenever a device makes a trust request. Queries to the blockchain are made in two situations: in the beginning of a new communication; and when the trust value drops below the established threshold.

Our approach is aware of resource consumption and only requires sufficient memory to keep the data rate history of peering devices. The size of the time window of the data rate history might depend on which granularity is desired (defined by the application). The larger the window, the longer the data rate history and, consequently, more memory will be used.

We vary the number of pairs of devices up to 4 pairs (total of 8 devices), each pair with a different data rate pattern for the respective sender device, as it can be seen in Figure 4. Devices 1 and 2 are labeled as licit sender devices with data rate patterns as estimated, while devices 3 and 4 are labeled as malicious devices with distribution of data rate different from the estimated. Figure 5 depicts the respective calculated trust values for each data rate pattern previously presented in Figure 4. For devices 1 and 2, the trust values in the first seconds rise from zero trust to the minimum trust set at 0.8 according to the values obtained from the High Level (Figure 6). The Low Level starts taking place as the trust value surpassed the established threshold, which allows the devices to communicate. Meanwhile, neither device 3 nor 4 could surpass the threshold, which indeed protects the other devices (and consequently the network) from these malicious devices, since their communication is not allowed in such a situation. We emphasize that devices are only allowed to establish communications when their respective trust values are above the predefined minimum trust (threshold). Therefore, our approach indeed provides IoT applications with more security by protecting licit devices from malicious ones. Table 1 summarizes the parameters used in the experiment.

The trust values obtained by the High Level from the computation of Equation 5 is illustrated in Figure 6. Figure 7 depicts the trust values calculated by the Low Level from the Equation 6. The behavior of each component is depicted for each device in the experiment. In Figure 6, we see the queries to the High Level to obtain the initial trust values when they are below the threshold. Again, this means the High Level is queried only when the Low Level cannot be applied. The opposite occurs for the Low Level, as it can be seen in Figure 7. The relative entropy score is computed by the receiver device when the trust values

Table 1: Parameter setup of the experiment.

Parameter	Value
Number of samples	21600
Number of IoT devices	8 (4 pairs); 60 (30 pairs)
Sliding window size	600 s
Fraction of malicious devices	10%, 50%, 90%
High Level component	$N(1,1)$
Trust threshold	0.8
Temporal component	- 0.1 trust/s
Estimated data rate	Kalman Filter, mean = 0, cov = 1
Size of the interval that contains a sample (Δ)	10000
Maximum data rate (R_{ji}^{max})	100 KBps
Number of intervals	10

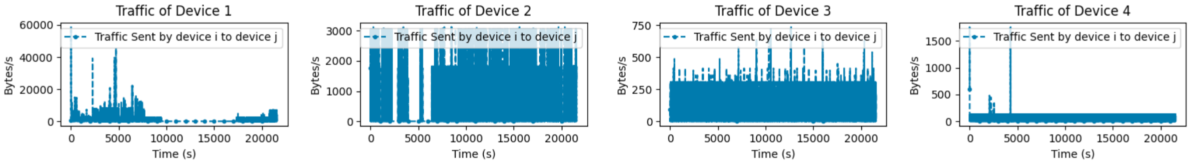

Figure 4: Traces from dataset (Sivanathan et al., 2017) for each sender device *i*. The first two graphs (devices 1 and 2) are traces from licit devices, while the last two graphs (devices 3 and 4) come from malicious devices. The data rate samples are given over a period of 21600 seconds (6 hours).

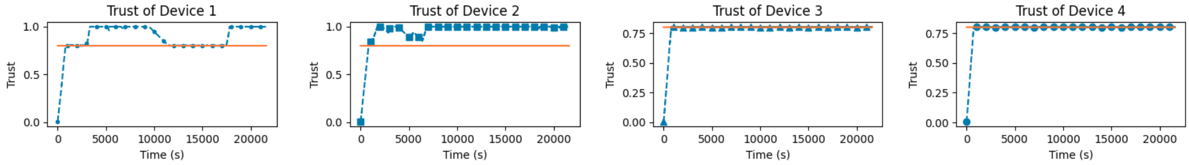

Figure 5: Calculated trust over time for each device according to the respective data rate patterns shown in Figure 4.

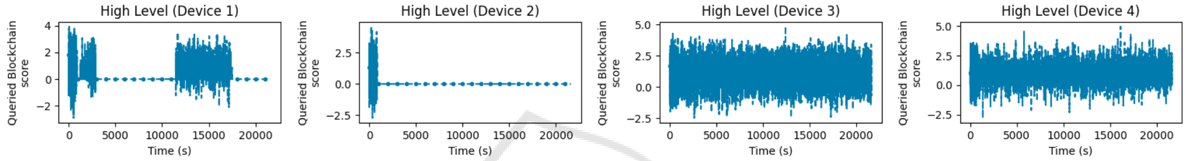

Figure 6: Blockchain score at the High Level when queried by each receiver device. Notice that C_1 score is only queried in cases where trust values of the sender device remain below the threshold.

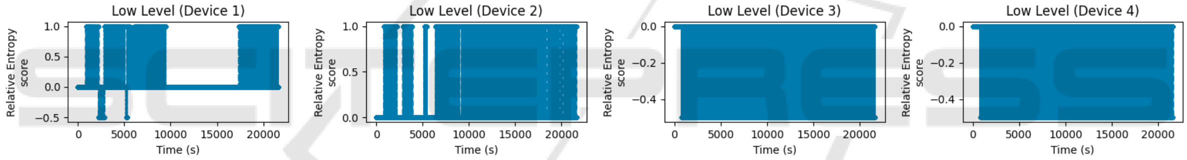

Figure 7: Relative entropy score at the Low Level computed by each receiver device. Notice that C_2 score is only computed in cases where trust values remain above the threshold.

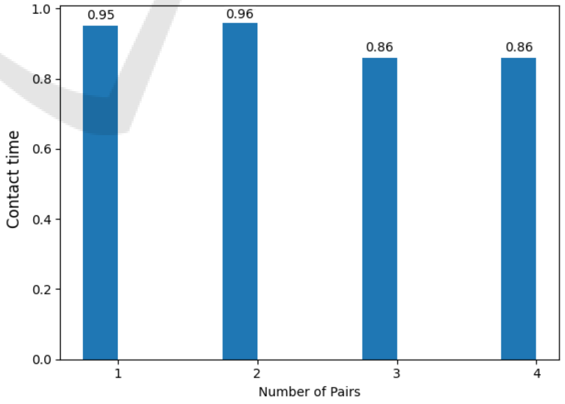

Figure 8: Histogram of contact time over the number of pairs of devices.

are above the threshold and when the devices are actually communicating, which means there is data being transferred. For example, for device 2, the High Level presents values only in the beginning when the devices start to establish connectivity, then the Low Level takes place and keeps active til the end of the experiment since the trust values remain above the threshold. On the other hand, for device 4 (labeled as malicious) the High Level is constantly queried and the Low Level only returns negative values (penalize the trust value) since there is no data to send.

To observe if our approach is working properly, we analyze the behavior of generated trust values when the number of malicious devices in the network increases. As our approach only allows the communication of devices that present a minimum trust value, we calculate the time that such devices keep on communicating. This way, we define the *contact time* metric according to the following equations. Let *NW* (Equation 8) be a binary function that assumes 1 (one) when a device *i* wants to transmit to the device *j*, i.e., the observed data rate is positive; or 0 (zero) otherwise.

$$NW = \begin{cases} 1, & \text{if } y > 0, \quad y \in \mathcal{S}_{ji} \quad \text{(cf. Section 4)} \\ 0, & \text{otherwise} \end{cases} \tag{8}$$

Let also *NT* (Equation 9) be another binary function that assumes 1 (one) when transmission is allowed, i.e., the calculated trust value TR_{ji} is greater than or equal to the established threshold; or 0 (zero) otherwise.

$$NT = \begin{cases} 1, & \text{if } TR_{ji} \geqslant \text{threshold} \\ 0, & \text{otherwise} \end{cases} \qquad (9)$$

Then, we define the *contact time* as the sum described in Equation 10, with *NS* as the number of data rate samples in the experiment. We assume that at least one device will present intention to transmit, i.e, $y > 0$, hence the denominator in Equation 10 is always greater than zero.

$$ContactTime = \frac{\sum_{k=1}^{NS} NT_k}{\sum_{k=1}^{NS} NW_k}, \qquad \sum_{k=1}^{NS} NW_k > 0 \qquad (10)$$

Therefore, the *contact time* is the fraction of time during which the trust in a device remains above a certain threshold during the experiment. During such time, devices are allowed to communicate (establish contact). Otherwise, when trust values fall below the threshold, there is no more contact between devices. The threshold depends on the application, which can accept lower trust values (less restrict) or only higher trust values (more restrict).

In Figure 8 we show the average *contact time* for one pair up to four pairs of devices. During the first two sets of experiments (one and two pairs), only licit devices are considered, so the *contact time* remains high. For the following sets, with 3 and 4 pairs, we see that the average *contact time* reduces, which confirms that the introduction of malicious devices had an impact on the *contact time*, and also reveals the effectiveness of the trust approach in containing malicious devices on the network.

We also analyzed the scalability and the stability of our approach, considering a configuration with numerous devices according to Table 1. We vary the number of pairs from 1 to 30 and, with 30 pairs of devices, i.e., 60 devices in total, we obtained a *contact time* of 0.84 for a network configuration with 10% of malicious devices. With 50% of malicious devices, we obtained 0.73 of *contact time* and 0.58 with 90% of malicious devices. The higher the rate of malicious devices, the shorter the *contact time*, which means that such malicious devices are not being able to communicate. This confirms that our approach prevents potential security attacks from being successful. Figure 9 illustrates the *contact time* according to the number of pairs and the rate of malicious devices.

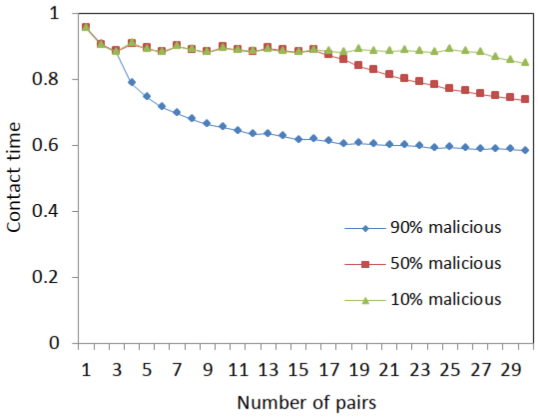

Figure 9: Contact time variation according to the number of pairs of devices and the rate of malicious devices.

We calculate performance metrics for the case of 10% of malicious devices in the network and obtained 0.84 of accuracy, with precision of 0.94, and 0.88 of recall. With 50% of malicious devices, we obtained 0.70 of accuracy, 0.67 of precision, and 0.89 of recall. With 90% of malicious devices we obtained 0.5 of accuracy, 0.15 of precision, and 0.88 of recall. The accuracy and precision drop with the increase in the number of malicious devices, given that we focus on classifying licit devices and not malicious ones. Therefore, licit samples become rarer, which reduces the number of true positives and false negatives. Despite the variations presented in accuracy and precision, the recall remained stable. Table 2 resumes all performance metrics.

Table 2: Performance metrics with different percentages of malicious devices.

% of malicious devices	Accuracy	Precision	Recall
10%	0.84	0.94	0.88
50%	0.7	0.67	0.89
90%	0.5	0.15	0.88

6 CONCLUDING REMARKS AND FUTURE WORK

In this paper, we presented a mathematical model to define trust in the context of IoT. We proposed a two-level approach to model trust aspects, enabling IoT devices to infer trust among themselves. We mixed characteristics of Low Level (network perspective) and High Level (application perspective) to compound a meaningful trust metric capable of capturing data rate behavior changes.

With results obtained using real datasets, the Low

Level behaves according to the expectations, even in extreme scenarios caused by spikes of data rate. By using data rate distribution, it was possible to capture the essence of traffic, which makes the approach robust. Furthermore, since the approach has two-levels, computing a trust value not only based on the network aspects, but also on the application aspects offered by the High Level component, it is very difficult for a malicious device to tamper it considering the inherent characteristics of blockchain. Therefore, we show the effectiveness of our approach in (i) relying on reputation values provided by the High Level component when the devices do not know each other or with not sufficient acquired trust value, and (ii) in capturing network behavior changes, adjusting trust according to that, and protecting the licit devices from malicious ones.

In the future, we plan to extend this work with Artificial Intelligence to improve the learning of new traffic behaviors IoT devices might present. We also envision a real deployment considering devices virtualization with digital twins in a Multi-access Edge Computing context to provide results from a real deployment.

ACKNOWLEDGMENT

We would like to acknowledge the support from Fundação de Amparo à Pesquisa do Estado do Rio de Janeiro (FAPERJ) and Rede-Rio (the state academic backbone network), and Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES), which partially funded this study. Also, this work is partially funded by FAPESP (grant 2015/24144-7), and by the Italian MIUR, PRIN 2017 Project “Fluidware” (CUP H24I17000070001). Flavia C. Delicato is a CNPq Fellow.

REFERENCES

Abbas, N., Zhang, Y., Taherkordi, A., and Skeie, T. (2018). Mobile Edge Computing: A Survey. *IEEE Internet of Things Journal*, 5(1):450–465.

Abomhara, M. and Køien, G. M. (2014). Security and privacy in the Internet of Things: Current status and open issues. In *2014 International Conference on Privacy and Security in Mobile Systems (PRISMS)*, pages 1–8.

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., and Ayyash, M. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Communications Surveys Tutorials*, 17(4):2347–2376.

Atzori, L., Iera, A., and Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, 54(15):2787 – 2805.

Babar, S., Mahalle, P., et al. (2021). Trust management approach for detection of malicious devices in siot. *Tehnički glasnik*, 15(1):43–50.

Bernabe, J. B., Ramos, J. L. H., and Gomez, A. F. S. (2016). TACIoT: Multidimensional Trust-Aware Access Control System for the Internet of Things. *Soft Computing*, 20(5):1763–1779.

Bertino, E. (2019). Iot security a comprehensive life cycle framework. In *2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC)*, pages 196–203.

Caminha, J., Perkusich, A., and Perkusich, M. (2018). A Smart Trust Management Method to Detect On-Off Attacks in the Internet of Things. *Security and Communication Networks*, 2018:1–10.

Casadei, R., Fortino, G., Pianini, D., Russo, W., Savaglio, C., and Viroli, M. (2019). Modelling and simulation of opportunistic iot services with aggregate computing. *Future Generation Computer Systems*, 91:252 – 262.

Christidis, K. and Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*, 4:2292–2303.

Dedeoglu, V., Jurdak, R., Putra, G. D., Dorri, A., and Kanhere, S. S. (2019). A trust architecture for blockchain in iot. In *Proceedings of the 16th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, pages 190–199.

Delicato, F. C. and Pires, P. F. (2020). Challenges in developing collaborative iot systems. In *2020 IEEE 6th International Conference on Collaboration and Internet Computing (CIC)*, pages 25–33. IEEE.

Din, I. U., Guizani, M., Kim, B.-S., Hassan, S., and Khan, M. K. (2018). Trust management techniques for the internet of things: A survey. *IEEE Access*, 7:29763–29787.

Fortino, G., Fotia, L., Messina, F., Rosaci, D., and Sarné, G. M. L. (2020a). Trust and Reputation in the Internet of Things: State-of-the-Art and Research Challenges. *IEEE Access*, 8:60117–60125.

Fortino, G., Messina, F., Rosaci, D., and Sarne, G. M. L. (2019). Using Blockchain in a Reputation-Based Model for Grouping Agents in the Internet of Things. *IEEE Transactions on Engineering Management*, pages 1–13.

Fortino, G., Messina, F., Rosaci, D., and Sarne, G. M. L. (2020b). ResIoT: An IoT social framework resilient to malicious activities. *IEEE/CAA Journal of Automatica Sinica*, 7(5):1263–1278.

Gallager, R. G. (1968). *Information Theory and Reliable Communication*. John Wiley & Sons, Inc., New York, NY, USA.

Goodman, L. (2014). Tezos a self-amending crypto-ledger. *Whitepaper*.

Hasan, M., Islam, M. M., Zarif, M. I. I., and Hashem, M. (2019). Attack and anomaly detection in iot sensors in iot sites using machine learning approaches. *Internet of Things*, 7:100059.

Hongjun, D., Zhiping, J., and Xiaona, D. (2008). An Entropy-based Trust Modeling and Evaluation for Wireless Sensor Networks. In *2008 International Conference on Embedded Software and Systems*, pages 27–34.

Junior, F. M. R. and Kamienski, C. A. (2021). A survey on trustworthiness for the internet of things. *IEEE Access*, 9:42493–42514.

Khan, M. A. and Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, 82:395–411.

Khan, Z. A., Ullrich, J., Voyiatzis, A. G., and Herrmann, P. (2017). A Trust-Based Resilient Routing Mechanism for the Internet of Things. In *Proceedings of the 12th International Conference on Availability, Reliability and Security*, ARES '17, New York, NY, USA. Association for Computing Machinery.

Kullback, S. (1959). *Information Theory and Statistics*. Wiley, New York.

Li, W., Santos, I., Delicato, F. C., Pires, P. F., Pirmez, L., Wei, W., Song, H., Zomaya, A., and Khan, S. (2017). System modelling and performance evaluation of a three-tier Cloud of Things. *Future Generation Computer Systems*, 70:104 – 125.

Liu, L., Loper, M., Ozkaya, Y., Yasar, A., and Yigitoglu, E. (2016). Machine to machine trust in the iot era. In *Proceedings of the 18th International Conference on Trust in Agent Societies - Volume 1578*, TRUST'16, page 18–29, Aachen, DEU. CEUR-WS.org.

Macedo, E. L. C., de Oliveira, E. A. R., Silva, F. H., Mello, R. R., França, F. M. G., Delicato, F. C., de Rezende, J. F., and de Moraes, L. F. M. (2019). On the security aspects of Internet of Things: A systematic literature review. *Journal of Communications and Networks*, 21(5):444–457.

Macedo, E. L. C., Silva, R. S., de Moraes, L. F. M., and Fortino, G. (2020). Trust Aspects of Internet of Things in the Context of 5G and Beyond. In *2020 4th Conference on Cloud and Internet of Things (CIoT)*, pages 59–66.

Paliszkiewicz, J. (2018). *Trust: A Multifaceted Notion*, pages 9–23. Springer International Publishing, Cham.

Principe, J. C. (2010). *Information theoretic learning: Renyi's entropy and kernel perspectives*. Springer Science & Business Media, USA.

Prokofiev, A. O., Smirnova, Y. S., and Silnov, D. S. (2017). The Internet of Things cybersecurity examination. In *2017 Siberian Symposium on Data Science and Engineering (SSDSE)*, pages 44–48.

Sato, H., Kanai, A., Tanimoto, S., and Kobayashi, T. (2016). Establishing Trust in the Emerging Era of IoT. In *2016 IEEE Symposium on Service-Oriented System Engineering (SOSE)*, pages 398–406.

Sfar, A. R., Natalizio, E., Challal, Y., and Chtourou, Z. (2018). A roadmap for security challenges in the Internet of Things. *Digital Communications and Networks*, 4(2):118 – 137.

Shannon, C. E. (1948). A Mathematical Theory of Communication. *Bell System Technical Journal*, 27(3):379–423.

Shi, W., Cao, J., Zhang, Q., Li, Y., and Xu, L. (2016). Edge Computing: Vision and Challenges. *IEEE Internet of Things Journal*, 3(5):637–646.

Sicari, S., Rizzardi, A., Grieco, L., and Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, 76:146 – 164.

Sivanathan, A., Sherratt, D., Gharakheili, H. H., Radford, A., Wijenayake, C., Vishwanath, A., and Sivaraman, V. (2017). Characterizing and classifying IoT traffic in smart cities and campuses. In *2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pages 559–564.

Stankovic, J. A. (2014). Research Directions for the Internet of Things. *IEEE Internet of Things Journal*, 1(1):3–9.

Statista (2021). IoT and non-IoT connections worldwide 2010-2025 . Technical report, Statista.

Tang, B., Kang, H., Fan, J., Li, Q., and Sandhu, R. (2019). IoT Passport: A Blockchain-Based Trust Framework for Collaborative Internet-of-Things. In *Proceedings of the 24th ACM Symposium on Access Control Models and Technologies*, SACMAT '19, page 83–92, New York, NY, USA. Association for Computing Machinery.

Wang, K., Xu, S. P., Chen, C.-M., Islam, S. H., Hassan, M. M., Savaglio, C., Pace, P., and Aloi, G. (2021). A trusted consensus scheme for collaborative learning in the edge ai computing domain. *IEEE Network*, 35(1):204–210.

Wang, P. and Zhang, P. (2016). A Review on Trust Evaluation for Internet of Things. In *Proceedings of the 9th EAI International Conference on Mobile Multimedia Communications*, MobiMedia '16, pages 34–39, ICST, Brussels, Belgium, Belgium. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).

Yan, Z., Zhang, P., and Vasilakos, A. V. (2014). A survey on trust management for Internet of Things. *Journal of network and computer applications*, 42:120–134.

Zhang, P. and Zhou, M. (2020). Security and trust in blockchains: Architecture, key technologies, and open issues. *IEEE Transactions on Computational Social Systems*, 7(3):790–801.

Zhang, P., Zhou, M., and Fortino, G. (2018). Security and trust issues in fog computing: A survey. *Future Generation Computer Systems*, 88:16 – 27.

Zhou, B., Li, H., and Xu, L. (2018). An Authentication Scheme Using Identity-based Encryption Blockchain. In *2018 IEEE Symposium on Computers and Communications (ISCC)*, pages 00556–00561.