Trust Aspects of Internet of Things in the Context of 5G and Beyond

Evandro L. C. Macedo
High-Speed Networks Laboratory (RAVEL)
Federal University of Rio de Janeiro (UFRJ)
Rio de Janeiro, Brazil
evandro@ravel.ufrj.br

Renato S. Silva
High-Speed Networks Laboratory (RAVEL)
Federal University of Rio de Janeiro (UFRJ)
Rio de Janeiro, Brazil
renato@ravel.ufrj.br

Luís F. M. de Moraes
High-Speed Networks Laboratory (RAVEL)
Federal University of Rio de Janeiro (UFRJ)
Rio de Janeiro, Brazil
moraes@ravel.ufrj.br

Giancarlo Fortino
Department of Informatics, Modeling,
Electronics and Systems (DIMES)
University of Calabria (Unical)
Rende (CS), Italy
giancarlo.fortino@unical.it

***Abstract*—The Sixth-generation communication system (6G) relies on some groundbreaking technological enablers to provide IoT with its full realization. However, with a myriad of user equipment and IoT devices connected everywhere with different levels of capability, 6G will need a holistic approach to reconcile the strict security requirements with any Ultra-Reliable Low-Latency Communication (URLLC) among smart objects. As a key part of the 6G development, Blockchain is considered as an essential technology to simultaneously address both these stringent demands. In this paper, we consider a two-level approach, where trust is modeled by combining a high-level component based on Blockchain and Identity-Based Encryption (IBE) to manage device identities, and a low-level component based on a temporal decay and relative entropy components. Numerical results obtained from two different datasets substantiate our trust approach as a promising option aiming to shed some light on how the trust aspects should be considered in the context of 6G.**

***Index Terms*—IoT, 6G, security, trust**

I. Introduction

The standardization of 5G communications has been completed, and the system is being deployed worldwide. However, further challenges related to the spatial efficiency in the subterahertz spectrum has motivated industry and academia to start conceptualizing the next generation of communication system (6G). The sixth generation is expected to significantly improve the Key Performance Indicators (KPIs) of the fifth generation (5G), described on Table I [1], aiming to satisfy the requirements of the Internet of Things (IoT) applications. Technological trends such as ubiquitous and distributed artificial intelligence are being quickly developed to provide ultra-high reliability, ultra-low latency, and high-accuracy inter-device synchronicity [2].

With a myriad of user equipment and IoT devices connected with different levels of capability, 6G will need a systematic approach to secure the sheer volume of mobile data across a diverse set of platforms and comply with the strict privacy and security requirements, such as confidentiality, integrity and availability [3]. To provide IoT with its full realization, 6G should be hyper-secure with demanding requirements from industrial to high-end users, while simultaneously being low cost and low complex. Besides, IoT groundbreaking applications (*e.g.* opportunistic IoT services [4]) will require a safe communication platform with extremely low latency (< 0.1ms) to deal with the frequent interactions among devices moving very fast in aerial or even spatial environments [5], [6], as it is envisioned for 6G.

TABLE I
Key Performance Indicators (KPI) comparison between 5G and 6G [1]

KPI	5G	6G
Data rate	0.1Gbps–20Gbps	1Gbps–1Tbps
Reliability (error rate)	$< 10^{-5}$	$< 10^{-9}$
Density	$10^6/km^2$	$10^7/km^2$
Mobility	500km/h	1000km/h
Localization precision	10cm in 2D	1cm in 3D
Traffic capacity	10Mb/s/m^2	< 10Gb/s/m^3
Latency	1–5ms	10–100ns

6G IoT will be used to widen digital world boundaries in terms of sensing, understanding, and programming. As a result, in addition to the loss of information, loss of control over your device or host or loss of money, breach of information security can endanger the physical safety of people and cause loss of property [7]. Security keeps being one of the biggest challenges in IoT development [8]–[16], mainly because of the heterogeneity among platforms that IoT interconnects, the resource-constrained devices, and the different communication technologies. Resource constraints (in terms of computational power, memory, or energy) of typical IoT devices limit the implementation of sophisticated security techniques that can properly mitigate security risks. In particular, assigning trust

978-1-7281-9541-4/20/$31.00 ©2020 IEEE

metrics is a relevant issue, being considered as an open research area [17]–[19].

As a promising security solution for IoT, the emergent Blockchain (BC) is considered an indispensable technology to establish trust in future networks [20]. BC is an open database that maintains an immutably distributed ledger typically deployed in a peer-to-peer network. BC enables registering and updating transactions securely in a decentralized fashion without relying on a central intermediary. Thanks to the inherent advantage of the distributed ledger technology, BC will likely play a major role in securing and authenticating future communication systems [21]. BC has gained momentum in 6G development [3] to provide security, privacy, and reliability by design. Offerings of BC such as (*i*) decentralization by eliminating the need of central trusted third parties and intermediaries, (*ii*) transparency with anonymity, (*iii*) provenance and non-repudiation of the transactions made, (*iv*) immutability and tamper-proofing of the distributed ledger's content, (*v*) elimination of single-point-of-failure, improving resiliency and resistance to attacks like Distributed Denial of Service (DDoS), (*vi*) comparatively less processing delay as well as processing fee [22].

In this article, we propose a trust modeling for IoT envisioning its use in the context of 6G. We discuss that using a trust model based on BC collaborates to reduce the overhead time spent to acquire before starting every IoT communication, which is especially important for optimizing network utilization in the critical environment envisioned to 6G. The approach is based on three components: (*i*) an initial trust component based on Identity-Based Encryption (*IBE*) and BC, (*ii*) a continuous analyzer component based on Information Theory, and (*iii*) a temporal decay component.

We consider using *IBE* [23] for managing device identities aiming to reduce the number of messages exchanged between IoT devices during authentication. To mitigate the IBE's vulnerability of enabling an IoT device being Private Key Generator (PKG), we propose using BC to decentralize the PKG and distribute the responsibility of inferring trust to network members. This infrastructure is going to be transparent to devices, acting as part of the network (the Internet), storing devices' keys. This way, trust about the transactions among devices will be provided by default – or by design – since it is intrinsic to the network. Thus, when a node wants to communicate with another node and needs to verify/validate whether the other node is in fact whom it claims to be, the identity of that node is verified along with the information stored in the BC. This information has a lot of computational effort invested in it, which indicates that the identity of the device is trustworthy.

We also consider the maintenance of trust during the communication between devices using Information Theory [24] to model the second component of our approach. We will discuss more this component in the following sections. As a third component, we take into account a temporal component that should decrease trust value as long as the devices stop communicating and cannot be sure about the other device trustworthiness, since it may have been compromised in the meantime. We show some numerical results that reinforce the effectiveness of our approach.

The rest of this paper is organized as follows. Section II provides a background to help understanding the proposal. Section III discourse about related work. Our trust model is presented in Section IV. Section V brings numerical results and some discussions about our findings. Finally, Section VI concludes the paper and indicates future work.

II. Background

Identity-based encryption (*IBE*) is a form of public-key cryptography in which a third-party server uses a simple identifier, such as an e-mail address, to generate a public key that can be used for encrypting and decrypting electronic messages. Compared with typical public-key cryptography, this scheme greatly reduces the complexity of the encryption process for both users and administrators. Although dismissing the need for a certificate authority, *IBE* depends upon a third-party server to generate private keys. Such a vulnerability enables Sybil attacks, in which a malicious IoT node pretends being the PKG server [25]. Figure 1 gives an overview of the *IBE* process.

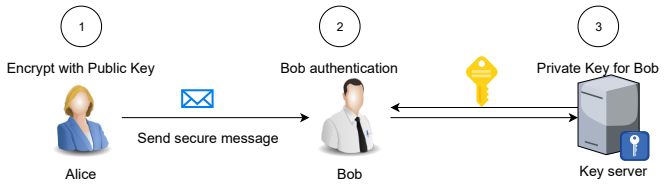

Fig. 1. (1) - Alice sends an encrypted message to Bob. (2) - Bob asks PKG server. (3) - PKG server sends a private key to Bob to permit him to decrypt Alice's message

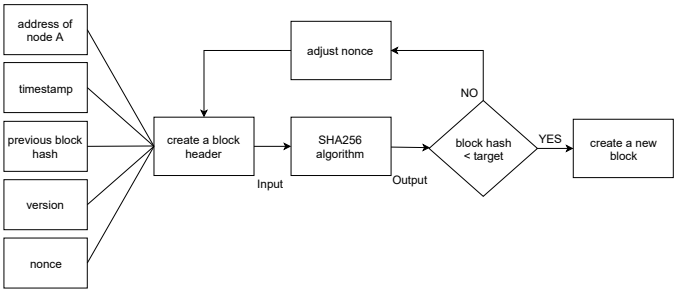

Fig. 2. PoW selects one node to create a new block in each round of consensus by computational power competition, in which the participating nodes need to solve a cryptographic puzzle

Another relevant technology is the Blockchain (BC), a growing distributed ledger based on append-only records (blocks) containing information about transactions such as date, time, and who is participating in transactions [26]. BC blocks are linked with each other through cryptographic hashes involving its previous block, a timestamp, and the transaction data. That is, BC can only be updated by consensus among participants in the system, and once new data is inserted,

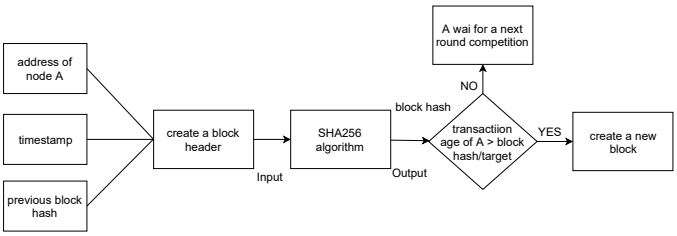

Fig. 3. PoS leverages a way of internal transaction incentive instead of consuming lots of computational power to reach a consensus

it can never be erased anymore. Instead of relying on a centralized authority, that can be seen as a vulnerability, the BC consensus-based mechanism distributes work for ensuring trust among all the network members, making them as part of such a trust [27].

The two most used consensus mechanism is the Proof-of-Work (PoW) and Proof-of-Stake (PoS) [28]. The PoW stands for a mechanism in which full nodes must apply a computational effort to solve a cryptographic problem (Figure 2). They compete to find a hash value that corresponds to the hash of a specific block. This mechanism provides the most secure and tamper-proof blockchain, although being the most energy-expensive one. The PoS, instead, is an energy-saving consensus protocol that is based on a random draw in which the more coins the more chances a node has to win the competition, depict in Figure 3.

III. Related Work

Even though the era of the 5G network has not yet fully arrived, the limitations of 5G security push up futurist designers to think about 6G [29]. 6G wireless networks are expected to enhance 5G, further increasing reliability, speeding up networks, and increasing available bandwidth. Several use cases, such as augmented reality and virtual reality, holographic telepresence and teleportation, eHealth, pervasive connectivity, Industry 4.0, Industrial IoT, and Unmanned mobility get being meant in advance for 6G [30]. However, such a desired improvement also brings additional security and privacy costs to be paid. When the physical and digital worlds merge closer in 6G, Internet level security will not suffice because of the tight dependence of physical safety on information security [31].

The work presented in [20] consider a tight combination of 6G and BC to outline challenges and opportunities derived from that. The 6G-BC combination is also considered in [32]. Adding BC with artificial intelligence, the work proposes a tier-based architecture aiming to tackle problems related to security, resource management, and orchestration. Challenges to match the envisaged demand surge for the 6G communication context is also addressed in [22] to speculate about research directions involving BC to surpass security issues and to unleash the potential of 6G systems. A BC radio access network architecture that could secure and effectively manage network access and authentication among trustless network entities is proposed in [33]. However, latency due to the BC-based networking services and the procedures of generating and confirming blocks has been a critical issue that restricts BC applications in delay-sensitive scenarios. The research in [34] outlines a solution to embed trust and DDoS mitigation into the networks by dividing the end to end connection on three parts: (a) originating customer network, (b) public wide area network, and (c) destination customer network.

Trust plays an important role in communications and interactions of objects in this world and is considered as a key factor in the success of online transactions [35]. However, although trust and reputation can participate together in several trust models, they have different meanings. When an entity infers about how much it can rely on another entity based on recommendations of a community, then we have reputation. On the other way, when an entity infers about the reliability of another entity based on its own observations, them we have trust [36]. We also can combine both concepts to build an embracing metric of trustworthiness.

Fortino *et al.* [37] designed a framework where every IoT device was associated with a software agent able to exploit its social attitudes to cooperate as well as to form complex agent social structures. In their approach, devices can use network services according to their reputation computed in BC. In [16] they also consider social aspects to provide a framework resilient to malicious activities. Other authors [38] used a passport model to propose a decentralized trust framework for cross-platform collaborations using BC technology. In this case, BC stores a combination of smart contracts, in which each interaction among devices, is signed by the participants. The work in [39] states that using BC to build trust is a relevant challenge. In this case, the authors replace the proof-of-work with a mechanism to establish the validity and integrity of transactions. Every agent creates his own genesis block and builds irrefutable historical transaction records that offer security and seamless scalability, without requiring global consensus. Agents who take resources from the community also contribute back using the authors' approach. In [40], the authors also considered social aspects with an agent-based approach (like [37]), proposing a novel reputation-oriented trust model, named StoRM, for the Internet of Things that combines social dimensions and microservice architecture with agent technology.

In [41], a trust model for wireless sensor networks (WSN) is developed using weighted averages to build data, behavior, and historical trust. Through simulations, authors show that their approach is aware of energy consumption with significant reduction of resource use and with higher detection rate in comparison with other approaches. In the same field, the work in [42] proposes using information theory to build trust among nodes in WSN. Malicious nodes are detected by using a relationship-based directional graph and entropy.

With a routing perspective, Khan *et al.* [43] proposes a trust-based approach for managing the reputation of every node of an IoT network based on IPv6 Routing Protocol for Low Power and Lossy Networks (RPL). The results show that the average delivery ratio grater than other approaches, as well as less number of bad nodes and number of bad

paths. Authors in [44] introduce a smart trust management method that automatically assesses the IoT resource trust, evaluating service provider attributes. They also use an elastic slide window feature that helps to differentiate broken or malfunctioning nodes among misbehaving devices.

Authors in [45] 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. They show that the performance of their approach is near the ground truth and define four regions of trust definition (distrust, untrust, trust, high trust).

In terms of an IBE implementation, [46] is one of the few works that consider this approach together with a BC implementation. The authors split the nodes in the chain to complete user authentication and private key protection. The results show that the failure probability is stabilized with the number of cycles a node works.

Different from the former works, our proposal relies on using a pre-acquired trust to achieve the security premises of IoT communication. Instead of using static information, we propose a dynamic trust model involving the individual device and its relationship with the network, and the neighborhood perception about his behavior. In the stringent low-latency context imposed by 6G, the proposed model can be used to simplify the security interactions between devices and third-party entities, expecting a reduced communication overhead.

IV. Trust Modeling

In particular, the concept of trust in interactions between human beings is linked to people's behaviors and experiences, as well as to attitudes of the individual himself who is establishing trust in others. In other words, the cultural aspects and the environment in which people are inserted influence the trust placed in others.

The concept of trust for IoT, as described in [47], is complex since it considers various aspects such as belief, integrity, reliability, among others. In this regard, the concept of trust becomes different from the concept previously mentioned. Building trust from one device to another may not consider the behavior and actions of the device itself (from a perspective of the sender device). For instance, a device that has become infected and behaves abnormally would want to transmit unconditionally to spread its malware. Hence, it won't take anything into account when it computes the trust of other devices, conversely, it will trust all of them. Thus, trust for IoT should be built only upon information that becomes from other devices (receivers). The question that arises is: Which information could be gathered to compose trust?

Let's suppose three situations revealing trust components:

- When the receivers do not know any information about the senders, they need a way to build an initial trust to start communicating;
- When the initial trust is set, the trust values should be dynamically adjusted so as to change it based on the behavior of the sender (more trust if the behavior is as expected, or less trust otherwise);
- When the communication ends, the devices do not know if the others were compromised or if they present any unexpected (malicious) behavior after some time, then the trust value should not endure perpetually, but decreased over idle time.

Trust can be understood as a local measure where one device assigns a value that represents how much it trusts in the other device. Each device will have a different perception about the other devices trustfulness, so that trust is not a global attribute with the same value for all devices. Hence, each device should compute the trust value of another device using contextual information that is directly related to that device.

An essential feature for trust is the guarantee of the uniqueness, veracity, and authenticity of the identity of an entity, an IoT device for example, in the network. Therefore, a device must know if the other device it is communicating with is the device it expects. This issue reveals the need for an IoT device identification mechanism that provides assurance of unique identities as well as protection against tampering, duplication, forgery, and impersonation. By combining the encryption technique of IBE to manage the identities of the communicating parties, with the distributed ledger of BC, it is possible to generate a common trust metric without using a centralized entity as a PKG server.

One of the objectives of this work is to propose the use of BC to store device's identities in the futuristic IoT environment of 6G, in which, rather than managing trade-offs, both security and latency should be addressed simultaneously. In such a security stringent scenario, IoT device identities will be stored almost inviolably, disabling any other device to tamper or corrupt and also prohibits multiple uses of such identification, since it would be necessary to obtain more than 50% of the computational power of BC network to change data.

Our approach is thought to be independent of the communication model, no matter if it is between devices, between a device and a gateway, or between a device and the cloud (considering a three-tier architecture as in [48]). Therefore, we consider the use of BC at different scales with local infrastructure (residential, for example), regional or global scale. Adding up to the initial trust offered by BC, it is also intended to address the maintenance of trust over time. For this, we propose metrics that use entropy as a way to adjust the trust between IoT devices.

An illustration of how the proposal works can be seen in Figure 4. In the illustrated scenario, initially, Alice and Bob do not know each other, having little or no information needed to infer an initial trust value to start communicating. The operating steps are as follows:

- **Step 1:** Each communication participant queries the other's identity in a High-Level Component based on a BC infrastructure that stores the identities of all network members. These identities can be obtained without the need for prior communication between members on account of the use of IBE
- **Step 2:** With the initial trust established, communication can start working over the Internet

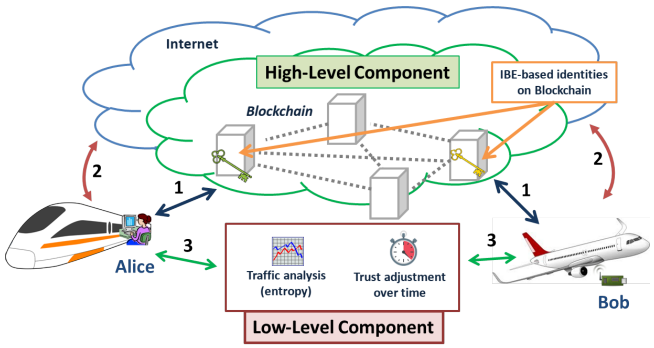

Fig. 4. 6G scenario of our Two-Levels Trust approach. Consider that Alice is on a super-fast train, while Bob (sensor) is on-board of an airplane. The communication between these two entities would only be possible upon a 6G platform

- **Step 3:** As the communication between Alice and Bob takes place, Alice calculates the entropy of Bob's traffic (and vice versa) and adjust trust in Bob over time. If Bob behaves abnormally[1], then it will negatively affect trust and may cause communication to terminate if it decreases beyond a previously established minimum. When the communication ends, a timer component (also part of the Low-Level Component) reduces the trust value until it reaches the point where Alice and Bob will have to consult the BC and start the whole process.

A. Trust Components

To perform device trust assignment, we propose dynamically combining contextual characteristics that can be observed by a particular device during its communication with another device. With these characteristics, the device can calculate how much it trusts in the other device.

Let $X(t)$ represent the incoming throughput[2] flowing into device j due to device i, at time t, for $t \in (0, T]$, where $T \in \mathbb{N}_{>0}$. If the traffic generated by a device is below the capacity of the data link connecting that device to the network (which we denote by C), then it is equal to the throughput. Therefore, for each t, $X(t)$ is assumed to be a random variable, with probability distribution function given by

$$P[\,X(t) \leq x] = F_X(x, t).$$

Under the hypothesis of stationarity we have:

$$P[\,X(t) \leq x] = P[\,X \leq x] = F_X(x).$$

Thus, from the given distribution of the random variable X, we are able to obtain information metrics (based on Shannon's Information Theory formulas), as we will discuss afterward.

Let $TR_{ij}(t)$ represent the trust of a i device in a j device at time t. The $TR_{ij}(t)$ is defined as follows:

1) Initially, $TR_{ij}(t)$ is computed based on the trust of the $j's$ identity in the BC, expressed by $BC(j, t)$. This component gives a trust value based on the number of confirmations that a transaction has on the BC. As the community suggests, the recommended number of confirmations is around 6 confirmations [49]. The more confirmations a transaction has, the harder it is to reverse. Hence, with this number of confirmations we can consider that the information of that transaction is strongly agreed upon BC members and the probability of tampering it is nearly impossible;
2) $TR_{ij}(t)$ is also influenced by the variation of the relative entropy of the traffic, which occurs when the expected traffic behavior deviate from the current behavior of the device due to any type of anomaly condition. The self-information of the variable X is given by Equation (1), and the average of the self-information is the entropy of the random variable, given in Equation (2):

$$I(X) = -\log p_X(x) \tag{1}$$

$$H(X) = E[-\log p_X(x)] = -\sum_{x \in (0,C]} p_X \log p_X \tag{2}$$

Using this we can calculate the relative entropy (Equation (3)), which stands for the Kullback-Leibler [50] divergence, a type of "distance" of two distributions.

$$\begin{aligned} D(p||q) &= \sum_{x \in (0,C]} p_X(x) \log \frac{p_X(x)}{q_X(x)} = \\ &= E_{p_X(x)} \left[\log \frac{p_X(x)}{q_X(x)} \right] \end{aligned} \tag{3}$$

As stated before, $p_X(x)$ is the expected distribution of the incoming throughput (or traffic) from a sender j to a receiver i. The $q_X(x)$ is also the distribution of this throughput but empirically observed. As $q_X(x)$ approximates $p_X(x)$, then the relative entropy ("distance") $D(p||q)$ decreases. So, we model the behavior when the observed distribution differs from the true (expected) distribution and adjust the trust of the specific device with the inverse function of $D(p||q)$ as Equation (4).

$$RE(X) = \frac{1}{D(p||q)} \tag{4}$$

Thus, $RE(X, t)$ is the component based on the relative entropy of the random variable $X(t)$ previously defined.
3) The third component we consider is a timeout component that decreases the initial trust from the moment devices stop communicating. After that, the devices will need to obtain a novel initial trust from BC. In our model we consider both a proportional time decay (TD) as described in Equation (5).

$$TD(t) = TR_{ij}(t) \times d \tag{5}$$

where d is the decay factor.

The Equation 6 presents the proposed composition with all three components together.

$$TR_{ij}(t) = BC(j, t) + RE(X, t) - TD(t) \tag{6}$$

[1]divergence of the expected traffic distribution from the observed one
[2]Throughput here is given in Bytes per second (Bps)

V. Results and Discussion

An implementation of the trust analytic model was developed in order to analyze its behavior over time. The results presented use the dataset found in [51] and also a synthetic dataset. This dataset is composed by traffic traces from a smart-campus environment instrumented with a diversity of IoT devices which includes cameras, lights, sensors, and health-monitors. The traffic obtained from the dataset was slightly changed adding some spikes during a short and a long period to observe how the approach might behave.

There are relevant implementation assumptions to highlight:

- Taking into consideration the common resource-constraints of IoT devices, the results were obtained considering three different configurations of the size of the sliding window (200, 600, 1000), which contains the traffic values used in the calculations. Also, the sliding window is used to accommodate different time scales that can have impact on the trust calculation;
- For the sample distribution of traffic we consider a fixed amount of bins (10) and a fixed maximum value of traffic (100 KBytes/s);
- The expected traffic value used to compare with the received one is calculated using a Kalman Filter, since it closely tracked the received traffic and does not require a lot of resources;
- When the communication is established for the first time between two nodes, only the High-Level Component (application information-based) actuates, which obtains the reputation of the node in the community;
- When there is traffic (i.e., the incoming throughput is greater than zero and less than the transmission capacity), only the Low-Level Component (network information-based) actuates to change the trust value;
- When the incoming throughput is zero, only the Timing Component (also part of Low-Level Component) actuates by constantly decreasing the trust value according to a predefined rate (e.g. - 0.1 trust/s).

For the following results, we just consider the Low-Level Component to observe what is the real impact of the network characteristics on the trust metric, therefore the High-Level Component does not take place.

As the analysis evolves each component of the Equation 6 is computed. For instance, a device j generates traffic to a device i according to a distribution. This means that in each time interval τ (*e.g.*, one second), a value of bytes per τ is generated. In the same manner, device i also sends traffic to device j, but changes its behavior during an interval of the experimentation and starts sending traffic according to other distribution. What we want to demonstrate is the dynamicity of the trust metric as the behavior of the traffic changes.

In Figure 5 we can see the traffic history over time that an IoT node *i* sent to node *j*. We slightly changed the original traces to consider some spike variations using the day 2016-09-28 of the dataset from [51], which resumes in the spikes on the 10000s and 23000s, respectively. Figure 6 depicts the results of the trust values, which increases as soon as the traffic pattern begins to stabilize. Then, when the first spike is reached, the trust value drops, with different depths depending on the size of the sliding window (more depth the broader the window is). Then, as the spike turns to be the new pattern, the trust starts to increase again. These changes are due to the Low-Level Component, produced by the variations on the traffic distribution over time, captured by the relative entropy.

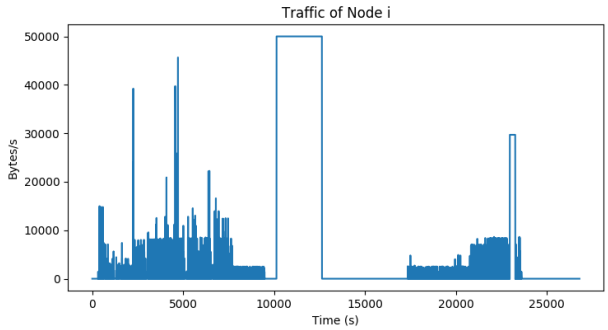

Fig. 5. Traffic produced by an IoT node using the day 2016-09-28 of the dataset from [51] with a slightly manual modification (spikes on the 10000s and 23000s)

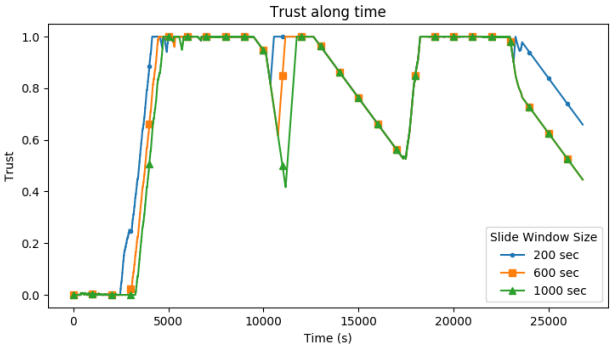

Fig. 6. Trust values obtained with our trust model using the traffic from the dataset [51]

Figure 7 shows the synthetic traffic pattern with periodic variations. We highlight the traffic actually received by node j (square-dot orange curve) and the expected traffic by node j (triangle-dot green curve), which stands for the ground truth of the traffic the node j should receive. With this type of pattern, in Figure 8 we can realize that the size of the sliding window has significant impact on the results, which is clearly explained by its relationship with the size of the period of changes in this traffic pattern. Still in this figure, we can also see that when the received traffic matches the expected one the trust value increases, whilst trust is penalized when the received traffic diverges from the expected. Considering these results it is possible to see that the Low-Level Component is able to capture the changes in the traffic pattern of the nodes, which helps to compose the trust metric and assures its effectiveness.

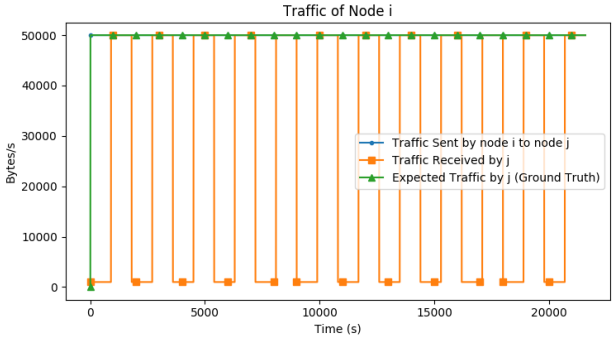

Fig. 7. Synthetic traffic pattern with periodic variations

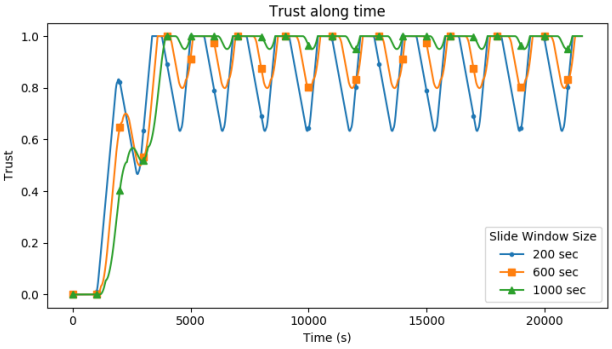

Fig. 8. Trust values using a synthetic traffic pattern with periodic variations

VI. Concluding Remarks and Future Work

The approach we present in this article considers a High-Level and a Low-Level Components, mixing application and network characteristics of the devices to compose a comprehensive trust metric able to capture and isolate misbehaving nodes. We envision the use of our trust approach in the context of 6G since we consider using Blockchain as one of the components, which is a building block technology of 6G.

As one of the main pillars of the 6G development as a whole, Blockchain presents itself as a promising technology to tackle the trust aspects of IoT. Its distributed ledger address two critical issues related to the stringent 6G ecosystem that supports IoT communication. First, using BC infrastructure to store initial trust dismisses a third-party PKG, which mitigates a relevant vulnerability point of the system. Second, assuming the BC response time similar to the traditional keys exchanging time, the two-level trust model we proposed reduces the overhead time spent to acquire trust before starting every IoT communication, which helps optimizing network utilization. With the results obtained from two different datasets previously shown, we can see that the Low-Level Component behaves according to the expectations, including for the synthetic spikes purposely inserted into the first dataset. Therefore, we show that our approach is promising to capture behavior changes and adjust trust under it.

Our future work involves completing tests including the initial trust provided by BC as the High-Level Component considering the perspective of Fog/Edge Computing and its security [15], [52]. Particularly taking into account the BC overhead time to reply to the initial trust, it is part of our plans studying the BC consensus protocol that better fit the requirements of our trust model, considering the 6G commitment points related to URLLC for IoT communications.

We also plan to improve the relative entropy factor that composes the low-level component of our trust model by combining throughput with other features such as average packet length and mean time interval between packets. Inputting more information into the relative entropy factor will aim basically to stabilize the entropy behavior by attenuating potential outstanding intervals.

The results obtained from the datasets show that the Low-Level Component behaves according to expectations, even considering the synthetic spikes inserted into the first dataset.

Acknowledgment

We would like to acknowledge the support from Fundação de Amparo à Pesquisa do Estado do Rio de Janeiro (FAPERJ), Rede-Rio (the state academic backbone network), and Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) that partially funded this study. The research was also partially funded by the Italian MIUR, PRIN 2017 Project "Fluidware" (CUP H24I17000070001).

References

[1] W. Saad, M. Bennis, and M. Chen, "A vision of 6g wireless systems: Applications, trends, technologies, and open research problems," *CoRR*, vol. abs/1902.10265, 2019.

[2] B. Stiller, T. Bocek, F. Hecht, G. Machado, P. Racz, and M. Waldburger, "Mobile Systems IV," University of Zurich, Department of Informatics, Tech. Rep., 01 2010.

[3] F. Tariq, M. R. A. Khandaker, K. Wong, M. A. Imran, M. Bennis, and M. Debbah, "A speculative study on 6g," *CoRR*, vol. abs/1902.06700, 2019.

[4] R. Casadei, G. Fortino, D. Pianini, W. Russo, C. Savaglio, and M. Viroli, "Modelling and simulation of opportunistic iot services with aggregate computing," *Future Generation Computer Systems*, vol. 91, pp. 252 – 262, 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X18307246

[5] G. Gui, M. Liu, N. Kato, F. Adachi, and F. Tang, "6G: Opening New Horizons for Integration of Comfort, Security and Intelligence," *IEEE Wireless Communications*, 1 2020.

[6] M. H. Alsharif, A. H. Kelechi, M. A. Albreem, S. A. Chaudhry, M. S. Zia, and S. Kim, "Sixth generation (6g) wireless networks: Vision, research activities, challenges and potential solutions," *Symmetry*, vol. 12, no. 4, 2020.

[7] M. Ylianttila, R. Kantola, A. Gurtov, L. Mucchi, I. Oppermann, Z. Yan, T. Nguyen, F. Liu, T. Hewa, M. Liyanage, I. Ahmad, J. Partala, R. Abbas, A. Hecker, S. Jayousi, A. Martinelli, S. Caputo, J. Bechtold, I. Morales, and J. Röning, "6g white paper: Research challenges for trust, security and privacy," 6G Flagship, University of Oulu, Tech. Rep., 04 2020.

[8] J. A. Stankovic, "Research directions for the internet of things," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 3–9, 2014.

[9] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787 – 2805, 2010. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128610001568

[10] M. Abomhara and G. M. Køien, "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)*, 2014, pp. 1–8.

[11] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[12] S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: The road ahead," *Computer Networks*, vol. 76, pp. 146 – 164, 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128614003971

[13] A. O. Prokofiev, Y. S. Smirnova, and D. S. Silnov, "The internet of things cybersecurity examination," in *2017 Siberian Symposium on Data Science and Engineering (SSDSE)*, 2017, pp. 44–48.

[14] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, pp. 395–411, 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X17315765

[15] P. Zhang, M. Zhou, and G. Fortino, "Security and trust issues in fog computing: A survey," *Future Generation Computer Systems*, vol. 88, pp. 16 – 27, 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X17329722

[16] G. Fortino, F. Messina, D. Rosaci, and G. M. L. Sarne, "Resiot: An iot social framework resilient to malicious activities," *IEEE/CAA Journal of Automatica Sinica*, vol. 7, no. 5, pp. 1263–1278, 2020.

[17] J. Paliszkiewicz, *Trust: A Multifaceted Notion*. Springer International Publishing, 2018, pp. 9–23.

[18] A. R. Sfar, E. Natalizio, Y. Challal, and Z. Chtourou, "A roadmap for security challenges in the internet of things," *Digital Communications and Networks*, vol. 4, no. 2, pp. 118 – 137, 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2352864817300214

[19] E. L. C. Macedo, E. A. R. de Oliveira, F. H. Silva, R. R. Mello, F. M. G. França, F. C. Delicato, J. F. de Rezende, and L. F. M. de Moraes, "On the security aspects of internet of things: A systematic literature review," *Journal of Communications and Networks*, vol. 21, no. 5, pp. 444–457, Oct 2019.

[20] T. Nguyen, N. Tran, L. Loven, J. Partala, M. Kechadi, and S. Pirttikangas, "Privacy-aware blockchain innovation for 6g: Challenges and opportunities," in *2020 2nd 6G Wireless Summit (6G SUMMIT)*, 2020, pp. 1–5.

[21] E. C. Strinati, S. Barbarossa, J. L. Gonzalez-Jimenez, D. Kténas, N. Cassiau, and C. Dehos, "6g: The next frontier," *CoRR*, vol. abs/1901.03239, 2019.

[22] T. Hewa, G. Gür, A. Kalla, M. Ylianttila, A. Bracken, and M. Liyanage, "The role of blockchain in 6g: Challenges, opportunities and research directions," in *2020 2nd 6G Wireless Summit (6G SUMMIT)*, 2020, pp. 1–5.

[23] J. C. Barbosa, "A proposal of using elliptic curve in identity based cryptography and its application for secure message exchange," M.S. thesis, Federal University of Rio de Janeiro, 2005.

[24] C. E. Shannon, "A mathematical theory of communication," *Bell System Technical Journal*, vol. 27, no. 3, pp. 379–423, 1948.

[25] A. Hezam, D. Konstantas, and M. Mahyoub, "A comprehensive iot attacks survey based on a building-blocked reference mode," *International Journal of Advanced Computer Science and Applications*, vol. Vol. 9, 04 2018.

[26] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[27] S. Zhang and J.-H. Lee, "Analysis of the main consensus protocols of blockchain," *ICT Express*, vol. 6, no. 2, pp. 93 – 97, 2020.

[28] L. M. Bach, B. Mihaljevic, and M. Zagar, "Comparative analysis of blockchain consensus algorithms," in *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 2018, pp. 1545–1550.

[29] M. Wang, T. Zhu, T. Zhang, J. Zhang, S. Yu, and W. Zhou, "Security and privacy in 6g networks: New areas and new challenges," *Digital Communications and Networks*, 2020.

[30] M. Giordani, M. Polese, M. Mezzavilla, S. Rangan, and M. Zorzi, "Toward 6g networks: Use cases and technologies," *IEEE Communications Magazine*, vol. 58, no. 3, pp. 55–61, 2020.

[31] C. Greer, M. Burns, D. Wollman, and E. Griffor, "Cyber-physical systems and internet of things," *NIST Special Publication*, vol. 202, no. 2019, p. 52, 1900.

[32] Y. Dai, D. Xu, S. Maharjan, Z. Chen, Q. He, and Y. Zhang, "Blockchain and deep reinforcement learning empowered intelligent 5g beyond," *IEEE Network*, vol. 33, pp. 10–17, 05 2019.

[33] X. Ling, J. Wang, T. Bouchoucha, B. C. Levy, and Z. Ding, "Blockchain radio access network (b-ran): Towards decentralized secure radio access paradigm," *IEEE Access*, vol. 7, pp. 9714–9723, 2019.

[34] R. Kantola, "6g network needs to support embedded trust," in *Proceedings of the 14th International Conference on Availability, Reliability and Security*, ser. ARES '19. New York, NY, USA: Association for Computing Machinery, 2019.

[35] A. Arabsorkhi, M. Sayad Haghighi, and R. Ghorbanloo, "A conceptual trust model for the internet of things interactions," in *2016 8th International Symposium on Telecommunications (IST)*, 2016, pp. 89–93.

[36] Y. Wang and J. Vassileva, "Trust and reputation model in peer-to-peer networks," in *Proceedings Third International Conference on Peer-to-Peer Computing (P2P2003)*, 2003, pp. 150–157.

[37] G. Fortino, F. Messina, D. Rosaci, and G. M. L. Sarne, "Using blockchain in a reputation-based model for grouping agents in the internet of things," *IEEE Transactions on Engineering Management*, pp. 1–13, 2019.

[38] B. Tang, H. Kang, J. Fan, Q. Li, and R. Sandhu, "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*, ser. SACMAT '19. New York, NY, USA: Association for Computing Machinery, 2019, p. 83–92. [Online]. Available: https://doi.org/10.1145/3322431.3326327

[39] P. Otte, M. de Vos, and J. Pouwelse, "Trustchain: A sybil-resistant scalable blockchain," *Future Generation Computer Systems*, vol. 107, pp. 770 – 780, 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X17318988

[40] K. Kravari and N. Bassiliades, "Storm: A social agent-based trust model for the internet of things adopting microservice architecture," *Simulation Modelling Practice and Theory*, vol. 94, pp. 286 – 302, 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1569190X19300322

[41] Z. Chen, L. Tian, and C. Lin, "Trust model of wireless sensor networks and its application in data fusion," *Sensors*, vol. 17, no. 4, 2017. [Online]. Available: https://www.mdpi.com/1424-8220/17/4/703

[42] D. Hongjun, J. Zhiping, and D. Xiaona, "An entropy-based trust modeling and evaluation for wireless sensor networks," in *2008 International Conference on Embedded Software and Systems*, July 2008, pp. 27–34.

[43] Z. A. Khan, J. Ullrich, A. G. Voyiatzis, and P. Herrmann, "A trust-based resilient routing mechanism for the internet of things," in *Proceedings of the 12th International Conference on Availability, Reliability and Security*, ser. ARES '17. New York, NY, USA: Association for Computing Machinery, 2017. [Online]. Available: https://doi.org/10.1145/3098954.3098963

[44] J. Caminha, A. Perkusich, and M. Perkusich, "A smart trust management method to detect on-off attacks in the internet of things," *Security and Communication Networks*, vol. 2018, pp. 1–10, 04 2018.

[45] J. Bernal Bernabe, J. L. Hernandez Ramos, and A. F. Skarmeta Gomez, "Taciot: Multidimensional trust-aware access control system for the internet of things," *Soft Comput.*, vol. 20, no. 5, p. 1763–1779, May 2016. [Online]. Available: https://doi.org/10.1007/s00500-015-1705-6

[46] B. Zhou, H. Li, and L. Xu, "An authentication scheme using identity-based encryption blockchain," in *2018 IEEE Symposium on Computers and Communications (ISCC)*, June 2018, pp. 00 556–00 561.

[47] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for internet of things," *Journal of network and computer applications*, vol. 42, pp. 120–134, 2014.

[48] W. Li, I. Santos, F. C. Delicato, P. F. Pires, L. Pirmez, W. Wei, H. Song, A. Zomaya, and S. Khan, "System modelling and performance evaluation of a three-tier cloud of things," *Future Generation Computer Systems*, vol. 70, pp. 104 – 125, 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X16302047

[49] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Working Paper*, 2008.

[50] S. Kullback, *Information Theory and Statistics*. New York: Wiley, 1959.

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

[52] M. G. R. Alam, M. M. Hassan, M. Z. Uddin, A. Almogren, and G. Fortino, "Autonomic computation offloading in mobile edge for iot applications," *Future Generation Computer Systems*, vol. 90, pp. 149 – 157, 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X18303996