Distributed Trust and Reputation Services in Pervasive Internet-of-Things Deployments

Borja Bordel[1] and Ramón Alcarria[2(✉)]

[1] Department of Computer Systems, Universidad Politécnica de Madrid, Madrid, Spain
borja.bordel@upm.es

[2] Department of Geospatial Engineering, Universidad Politécnica de Madrid, Calle Mercator 2, 28031 Madrid, Spain
ramon.alcarria@upm.es

Abstract. Cyberprotection in the context of Internet-of-Things (IoT) includes three basic areas: security, privacy and trust. Security and privacy technologies are related to mechanisms such as cryptography or authentication protocols that have been extensively explored and adapted to IoT requirements. However, new risks such as cyber-physical attacks and novel distributed, and pervasive architectures reveal new weaknesses where trust and reputation issues are the main challenges to be addressed. Nevertheless, both, trust and reputation, are intrinsically subjective and distributed, and algorithms guaranteeing a dynamic and efficient management of these properties tend to be computationally heavy and complex. In this context, new trust and reputation services for pervasive IoT deployments are needed. Therefore, in this paper we propose a new distributed architecture for the provision of trust and reputation services in IoT systems. The architecture is based on Blockchain technologies and the composition of different conceptual models (cognitive, computational, neurological, and game-theoretical) using stochastic functions. The resulting probability may be employed by nodes to create their own trustworthy subsystem. In order to validate the performance and usability of the proposal, an experimental validation based on simulation technologies is provided.

Keywords: Internet of Things · Blockchain · Cybersecurity · Stochastic models

1 Introduction

Internet-of-Things (IoT) [33] is one of the most powerful enabling technologies for new and promising paradigms such as Industry 4.0 [5], Cyber-Physical Systems [7] or Enhanced Living Environments [15]. In all these innovative solutions, software and hardware components manage large amounts of data which, in several cases, may be personal and (then) protected by international regulations

I. You et al. (Eds.): MobiSec 2021, CCIS 1544, pp. 16–29, 2022.
https://doi.org/10.1007/978-981-16-9576-6_2

such as the European GDPR (General Data Protection Regulation) [28]. Moreover, most of these new technical paradigms are envisioned to be implemented into critical infrastructures or applications [11], what makes them a potential focus [1] for many different attacks: from traditional cybercrime to the new cyber-physical risks [13] and cyber terrorism.

In this context, it is essential to protect IoT deployments using strong policies and mechanisms. Traditionally, a protected IoT deployment needs to implement technologies in three different areas: security, trust and privacy [16]. Security mechanisms [4] include authentication and integrity solutions, which are already highly adopted by current IoT technologies (mainly inherited from network technologies and protocols such as Bluetooth or ZigBee) [27]. On the other hand, privacy mechanisms, including cryptography and anonymization policies, although they are not fully adapted to the IoT deployments and requirements, they are also commonly implemented in many non-commercial IoT applications, especially lightweight versions of well-known algorithms such as The Onion Router (TOR) [12]. On the contrary, trust solutions face a totally different situation. Most common trust mechanisms nowadays are based on administrative schema, or on a social understanding of this concept [6]; what makes very difficult to integrate these technologies without deploying a large infrastructure or considering a relevant and constant human intervention. Trust mechanisms typically include two different aspects: intrusion detection and reputation. While intrusion detection requires, currently, large infrastructures and a great computational power (the most recent and successful solutions are based on mathematically complex algorithms such as artificial intelligence [20] and large data repositories); reputation mechanisms are usually supported through a direct human intervention, where users indicate those behaviors that are malicious, untrustworthy or, in general, dangerous (and, based on that input, the nodes' reputation is obtained). In that way, both areas are clearly facing open challenges, which prevents their massive use in the upcoming IoT deployments.

As a possible solution, new trust and reputation calculation frameworks and mechanisms are proposed. However, these proposals tend to be subjective and highly distributed, so innovative algorithms guaranteeing a dynamic and efficient management of trust and/or reputation are typically computationally heavy and complex [9]. Nevertheless, the increasing computational power of IoT nodes and single-board computers, together with the universal access to the global Internet granted by future 5G networks [29], are introducing a much more favorable scenario for those new proposals.

Therefore, in this paper we are proposing a service-based trust and reputation calculation solution. The proposed calculation algorithm considers four different approaches or understandings of trust: cognitive, computational, neurological, and game-theoretical. Trust, in or proposal, is not a fixed value but a probability distribution, what represents in a better manner the intrinsic uncertainty of the observations. Local calculations are then integrated into a global trust value, which is obtained and updated using a distributed Blockchain network.

From a market perspective, the proposed solution shows a high applicability as it can be implemented in all kinds of devices and IoT nodes (only common mathematical operations are employed). On the other hand, several lightweight implementations of brokers and Blockchain networks can be found, which also facilitates the applicability of the proposed architecture in all kinds of commercial scenarios.

The rest of the paper is organized as follows: Sect. 2 describes the state of the art on trust solutions for IoT deployments; Sect. 3 describes the proposed solution, including the proposed architecture and the trust calculation framework; Sect. 4 presents an experimental validation using statistical techniques; and Sect. 5 concludes the paper.

2 State of the Art on Trust Solutions for IoT Systems

As one of the most relevant open problems nowadays, related to IoT systems, trust and reputation calculation and management have received a lot of attention in the last ten years. Many different proposals may be found, although in general six different categories are typically identified [32].

The first group of works propose the introduction of Trusted Third Parties (TTP) and authentication protocols [17]. In these schemes, trustworthy components are those which are authenticated by a very secure middleware or components known as TTP or secure enclaves [23]. Standard ciphers, keys and protocols are deployed among all components [26]. In hierarchic network architectures, trust domains may be created and TTP may be built as trustworthy gateways [21]. Although this scheme is very useful in client-server architectures, in very distributed IoT deployments is very inefficient.

The second group of trust solutions for IoT deployments is composed of recommender systems. A recommender system may be of three types: content-based filtering [30], collaborative filtering [8], and a hybrid system [19]. In general, in all these approaches, nodes receive and analyze recommendations to decide with which other nodes they stablish a connection (as people do in societies). These systems can take advantage of the network structure, but they are totally reactive and cannot be employed as a prevention solution. Moreover, this approach requires a large human intervention and can be barely automated.

Works in the third group address behavior-based mechanisms. In this approach, nodes monitor the behavior of other components and decide about the connections they want to maintain or prune [31]. Although this scheme allows nodes to perform simple local evaluations [8], (as in the previous case) it can be difficult to employ this technology in prevention policies as collected data are not enough for supporting predictions. Besides, this approach lacks a global understating of trust for the entire system of the particular nodes.

In order to solve this challenge and enable the option of implementing prevention policies and making predictions, in the fourth group of trust solutions, mechanisms are based on metadata. Information such as the geographical location of the ownership of nodes is employed to determine which nodes are untrustworthy and malicious [25]. This scheme is totally proactive, as malicious nodes

may be removed before they start operating, just knowing their metadata. However, the percentage of false positives in this approach is higher than in any other previous approach (what reduces the system performance).

In the last five years, the Blockchain revolution has also affected the IoT technologies, and different proposals to provide and support trust in IoT deployments based on Blockchain may be found [3,18,28] (fifth category). However, in general, in this approaches all data from the nodes is exchanged through the Blockchain network to secure it and make it trustworthy [2]. Although this mechanism may provide certain level of trust, some works have reported different attacks and problems associated to this solution [10,22]. Furthermore, the delay of transactions communicated through Blockchain networks grows up exponentially, reducing the network performance in a very relevant manner.

Finally, and sixth category, many different hybrid approaches have been reported. These schemes try to combine the advantages of different mechanisms. One of the most common proposals includes a behavior-based solution together with a TTP or middleware (in order to store local calculations and get a global value) [14]. However, these solutions are still very weak against manipulations, contrary to Blockchain-based mechanisms.

Table 1 shows a summary with the main state of the art proposals.

Table 1. Main state-of-the-art solutions

References	Short description	Main problems
[17,21,26]	Trusted Third Parties and authentication protocols	In very distributed IoT deployments is very inefficient
[8,19,30]	Recommender systems	They are totally reactive and cannot be employed as a prevention solution
[8,31]	Behavior-based mechanisms	Difficult to employ in prevention policies
[25]	Mechanisms based on metadata	The percentage of false positives in this approach is higher than in any other
[2,10,18,28]	Trust in IoT deployments based on Blockchain	The delay of transactions communicated through Blockchain networks grows up exponentially
[14]	Hybrid approaches	Still very weak against manipulations

Therefore, in our proposal, we are combining most of these approaches into an innovative distributed architecture. The solution is service-oriented and it is supported by Blockchain, although not all transactions must go through this network in order to preserve the system performance. Besides, trust calculation

includes four different views (cognitive, computational, neurological, and game-theoretical), in order to guarantee the reactive and proactive character of the solution.

3 A New Trust Calculation Framework and Architecture

In this section, we propose a novel architecture for trust calculation in IoT deployments. This architecture (Sect. 3.1) includes a Blockchain network for global trust calculation using SmartContracts. Besides, nodes may perform four different trust calculations at local level: cognitive (Sect. 3.2), computational (Sect. 3.3), neurological (Sect. 3.4), and game-theoretical (Sect. 3.5).

3.1 Proposed Distributed Architecture for Trust Calculation

Figure 1 shows the proposed architecture for trust calculation.

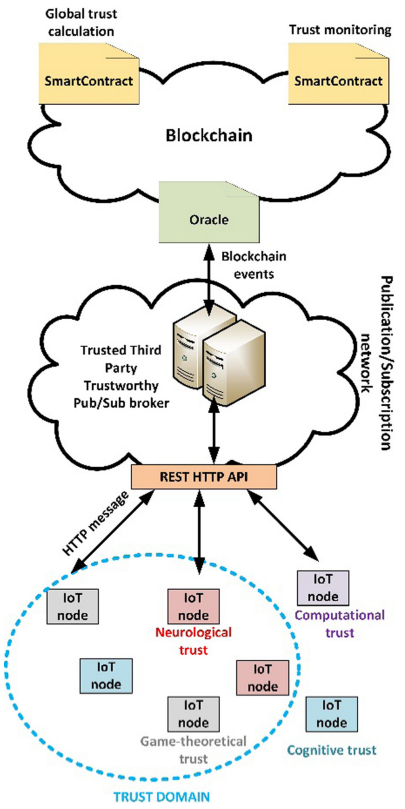

Fig. 1. Proposed architecture for trust and reputation calculation

In the proposed solution, each IoT node may execute locally one trust calculation algorithm, among the four existing ones: cognitive, computational, neurological, and game-theoretical. In general, and depending on the system configuration, nodes may select the trust calculation algorithm in an autonomous manner (according to their capabilities, knowledge, etc.) or the system administrator can do it. Any case, it is important to guarantee that all four calculation algorithms have a homogenous presence in the IoT deployment (in order to avoid biases in the global trust calculation function).

Nodes in the IoT deployment, on the other hand, are connected to the global trust calculation infrastructure through a publication/subscription network. This network offers a REST (representational state transfer) API (application programming interface) and service, so nodes can relate with the infrastructure using HTTP messages. HTTP messages are easier to parse, send, receive and process than bit-oriented protocols, although they show higher latencies. Besides, HTTP messages are nowadays, the standard communication medium for IoT nodes and deployments.

Using these messages, IoT nodes may subscribe to different trust services and the updates on the trust values from other nodes, other trust calculation algorithms and/or the global trust calculation infrastructure. At the same time, the global trust calculation infrastructure (i.e. the Blockchain network) is subscribed to all updates from the IoT nodes. On the other hand, when a relevant change on the locally calculated trust values is detected by an IoT node, it can publish the new results. All these message exchanges and pub/sub management is controlled by a trustworthy broker acting as TTP. In fact, this broker requires to IoT nodes and the Blockchain network to get authenticated and employ cryptographic mechanisms to preserve the privacy and security of communications. All nodes that cannot be authenticated by the TTP are automatically rejected.

Moreover, through an SmartContract acting as oracle, the Blockchain network monitors and stores all updates about trust calculations done by IoT nodes in the deployment. In that way, in the Blockchain network (using a second SmartContract) there is an accountable tracking of reputation and trustworthiness of all IoT nodes, from different perspectives (cognitive, computational, neurological, and game-theoretical) and from different local analyses (as many as IoT nodes are observing an analyzing the behavior of the given node). Each time this not rejectable, transparent record is updated, a third SmartContract updates the global trust calculation (using stochastic functions). Each time the global trust values are updated, the Blockchain network generates an event, which is publish through the pub/sub network. Then, all nodes are informed about the global trustworthiness of all nodes in the IoT deployment.

With all this information (global trust and rejections caused by the TTP), IoT nodes may define their own "trust domain", selecting with which nodes they want to establish a connection (see Sect. 3.5). Hereinafter we assuming rejected nodes are not connected with any other nodes, and we are focusing on trust calculation (both, at local and global level).

3.2 Cognitive Trust Calculation

As said, each IoT node is locally executing one different trust calculation algorithm. Each one representing a different perspective and understanding of the idea of trust. In this section we are focusing of the cognitive trust T_{cog}.

Cognitive trust refers the reputation and trust supported by a priori beliefs, and it is typically a function of the degree of these beliefs. In a technological context, these beliefs refer the expectation of a node to have the necessary competence, benevolence, and integrity to be relied upon [24]. However, these qualities are not technical, but sociological. And then, they are inherited from the node's owner, location, etc. At them, they are inherited from the node's metadata.

Thus, given an IoT node n_i (or target node) with an associated collection of metadata $MD(n_i)$ (1), and a second node n_j (or observer node) and a set of a priori trustworthy metadata $MD^+(n_j)$ (2), it may be calculated the cognitive trust $T_{cog}(n_i; n_j)$ for this pair of nodes (3).

$$MD\left(n_i\right) = \left\{md_k\left(n_i\right) \quad k = 1, \ldots, K_T\right\} \tag{1}$$

$$\begin{aligned} MD^+(n_j) &= \left\{MD_k^+(n_j) \quad k = 1, \ldots, K_T\right\} \\ MD_k^+\left(n_j\right) &= \left\{md_{k,r}^+\left(n_j\right) \quad r = 1, \ldots, R_{k,j}\right\} \end{aligned} \tag{2}$$

$$T_{cog}(n_i; n_j) = P_{trust}(n_i; n_j) = \sum_{k=1}^{K_T} \sum_{r=1}^{R_{k,j}} (\alpha_{k,r}\ \delta[md_k(n_i) = md_{k,r}^+(n_j)] + \beta_{k,r}\ \delta[md_k(n_i) \neq md_{k,r}^+(n_j)]) \tag{3}$$

In this expression (3), the result refers the target node n_i according to the local observations of node n_j. The result $T_{cog}(n_i; n_j)$ must be understood as the probability $P_{trust}\left(n_i; n_j\right)$ of node n_i to be trustworthy, considering the observation of node n_j. Besides, $\delta\left[\cdot\right]$ is the Kronecker's delta function and $\alpha_{k,r}$ and $\beta_{k,r}$ are real parameters to represent the degree or weight of the node's beliefs.

Cognitive trust may be calculated before the system starts operating, but needs the definition of a protocol to share the nodes' metadata with the entire system.

3.3 Computational Trust Calculation

Computational trust T_{comp} is associated to the behaviors that follow the rules and requirements of authorities in the IoT deployment. Typically, in topics related to cyberprotection such as cryptography. Although, in most common proposals, this vision of trust is only employed to enable or disable the spontaneous collaboration among nodes, it is also possible to define a more elaborated metric for computational trust.

Thus, given an IoT node n_i (or target node) communicating with a node n_j (or observer node), it may be calculated the computational trust $T_{comp}(n_i; n_j)$ for this pair of nodes (4).

$$T_{comp}(n_i;n_j) \ = P_{trust}(n_i;n_j) = \begin{cases} 1; & k < K_{th} \\ \sqrt{2}\frac{h_{i,j}}{\sqrt{1+{h_{i,j}}^2}}; & k > K_{th} \end{cases} \tag{4}$$

The proposed function for computational trust is a sigmoid, so it varies in the interval $[0, 1]$ as probabilities do. In this case, the result has also to be understood as the probability of node n_i to be computationally trustworthy according to the local calculation performed by node n_j.

In this case, k represents the time slots elapsed since the IoT deployment started operating, and $h_{i,j}$ is a parameter representing the percentage of times the node n_i employed the correct cryptographic configuration (as indicated by the TTP) when communicating with node n_j (5). As this kind of behavior-based trust calculation algorithms may need a period to converge, for all time instants before K_{th}, node n_i is considered trustworthy (so the capabilities of the IoT deployment are not reduced by default).

$$\begin{aligned} h_{i,j} &= \sum_{m=0}^{k} u_{i,j}[-m] \cdot r_{i,j}^{m+1} \\ u_{i,j}[m] &= \frac{c_{i,j}[m]}{t_{i,j}[m]} \end{aligned} \tag{5}$$

On the other hand, in order to introduce a temporal decreasing effect (past events are less relevant than the recent ones), parameter $h_{i,j}$ is obtained through a geometric sum, with a ratio $r_{i,j}$. Then, the ratio $u_{i,j}[m]$ between transactions with the correction configuration $c_{i,j}[m]$ and the total number of transactions $t_{i,j}[m]$ in the m-th time slot is weighted according to its antiquity.

3.4 Neurological Trust Calculation

Neurological trust T_{neu} is the most traditional behavior-based approach for trust. In general, nodes analyze the honesty of other IoT nodes in the deployment and obtain a trust value according to the observed and past experiences.

In neurological trust, the observer node n_j monitor the number of successful transactions $s_{i,j}\,[m]$ with the target node $n_i in$ each time slot m. This quantity is employed to generate a ratio $w_{i,j}\,[m]$ by considering the total number of transactions between both nodes $t_{i,j}\,[m]$ (6).

$$w_{i,j}\,[m] = \frac{s_{i,j}\,[m]}{t_{i,j}\,[m]} \tag{6}$$

However, as said in Sect. 3.3, the impact of past measurements must be lower than recent evaluations, so all the partial results for every time slot are combined in a geometric sum (7).

$$h_{i,j} = \sum_{m=0}^{k} w_{i,j}\,[-m] \cdot r_{i,j}^{m+1} \tag{7}$$

The resulting parameter, $h_{i,j}$, depends on the selected ratio for this sum $r_{i,j}$, which control the evanescence of the impact of past measurements. Finally, in order to calculate the neurological trust, a sigmoid function is employed, where k represents the time slots elapsed since the IoT deployment started operating (8).

$$T_{neu}(n_i; n_j) = P_{trust}(n_i; n_j) = \begin{cases} 1; & k < K_{th} \\ \sqrt{2}\frac{h_{i,j}}{\sqrt{1+{h_{i,j}}^2}}; & k > K_{th} \end{cases} \tag{8}$$

As in other previous calculations, this result must be understood as the probability of node n_i to be neurologically trustworthy according to the local calculation performed by node n_j.

3.5 Game-Theoretical Trust Calculation

Contrary to computational or neurological trust, game-theoretical trust T_{game} is a proactive approach. In this case, trust is obtained as the most rational and probable value in the future, considering the past evidence, behaviors and evolution of trust. In conclusion, game-theoretical trust employs a historical data repository to predict the future values of trust.

Given an IoT node n_i with a sequence of global trust values $tr\,[k]$ (9), the game-theoretical trust is calculated by node n_j using the Lagrange polynomial (10). After calculated this polynomial, the observer node n_j can obtain the game-theoretical trust in any future time slot k_{next} using function $L\,(k)$.

$$tr\,[k] = \{tr\,[k] \quad k = 1, \ldots, K_j\} \tag{9}$$

$$\begin{aligned} L\,(k) &= \sum_{m=1}^{K_j} tr\,[m] \cdot \ell_m\,(k) \\ \ell_m\,(k) &= \prod_{r=1,\ r\neq m}^{K_j} \frac{k-r}{m-r} \end{aligned} \tag{10}$$

Each observer node n_j may develop this extrapolation using a different number of previous trust measures K_j. The final result for game-theoretical trust $T_{game}\,(n_i; n_j)$ will depend on the local values of K_j and k_{next} (11). As global trust values are points from an stochastic function, as in all previous calculations, the result $T_{game}\,(n_i; n_j)$ is understood as the probability of node n_i to be game-theoretical trustworthy according to the local calculation performed by node n_j.

$$T_{game}\,(n_i; n_j) = P_{trust}\,(n_i; n_j) = L\,(k_{next}) \tag{11}$$

3.6 Global Trust Calculation

Finally, all IoT nodes in the system send their local evaluations for the target node n_i to the global trust calculation infrastructure (Blockchain network), to be combined in a global trust value.

Given the IoT deployment has M_T nodes, at this point M_T different trust values $trust_j^i$ will be collected for each target node n_i. Each one obtained through a different mechanism and from a different local perspective. Then, in the global trust calculation system, all these values are employed to create a unique probability distribution for each target node n_i. Using the Laplace's notion of probability, all values are grouped to define a discrete probability density function T_{global} with Y_T points (12).

$$T_{global}[y] = \frac{1}{M_T}\ card\left\{ trust_j^i \quad j = 1, \ldots M_T \ \vdots \ th_y \leq trust_j^i < th_{y+1} \right\} \\ with \quad y = 1, \ldots, Y_T, \ with\ th_y \ \in [0,1] \ and \quad th_1 = 0 \ \ and\ th_{Y_T} = 1 \tag{12}$$

To do that, the cardinality $card\{\cdot\}$ function is employed to determine the number of elements in each set meting a given condition, and limits th_y are employed to define the intervals for grouping the local trust values.

Finally, in order to inform the nodes about the global results using only one real number (matching, for example, the requirement of game-theoretical trust calculation algorithm), the non-central moments λ_z (13) or central moments μ_z (14) may be employed, depending on the implementation.

$$\lambda_z = \frac{\sum_{y=1}^{Y_T} \left(T_{global} \ \ [y]\right)^z}{Y_T} z \in [0, \infty] \tag{13}$$

$$\mu_z = \frac{\sum_{y=1}^{Y_T} \left(T_{global} \ \ [y] - \lambda_1\right)^z}{Y_T} z \in [0, \infty] \tag{14}$$

4 Experimental Validation: Simulations and Results

In order to evaluate the performance of the proposed solution, an experimental validation was planned and carried out. During this validation, two different experiments were performed, in order to analyze the convergence time of the proposed security mechanism, and the success rate when detecting the malicious nodes in an IoT deployment.

Both experiments were performed using simulation methodologies and the MATLAB 2020.B and Simulink suite. Using this numerical tool, one hundred and twenty (120) devices were represented, each one executing a different application and trust calculation algorithm. Besides, different amounts of malicious nodes were considered for different evaluations. All simulation were performed in a Linux architecture.

Simulated IoT nodes represented a common architecture based on the ESP-32 microcontroller, WiFi communications and simple sensors such as temperature or humidity. Trust calculation algorithms were distributed among nodes in a homogeneous but random manner. Nodes also could behave in a malicious manner randomly, but according to the configured percentages.

All simulation were repeated twelve times to remove all possible exogenous effects. Presented results are obtained as the average of all these partial simulations. Simulations represented twenty-four hours of real-time operation in the IoT deployment.

The first experiment was focused on the success rate of the proposed solution. For different amounts of malicious nodes in the IoT deployment, it is analyzed the percentage of them that are correctly detected and isolated.

The second experiment was focused on the convergence time. For different amounts of malicious nodes, the maximum convergence time required to evaluate all nodes and configure the final IoT deployment was evaluated.

Figure 2 shows the results of the first experiment. As can be seen, the success rate is above 85% in all cases. As the number of malicious nodes goes up, the success rate also grows up, although this effect is common to most technologies. The most interesting result in Fig. 2 is the lack of any asymptote. As can be seen, even if 50% of nodes in the IoT deployment are malicious, the proposed solution does not get saturated and it is able to operate normally, detecting up to 98% of malicious nodes.

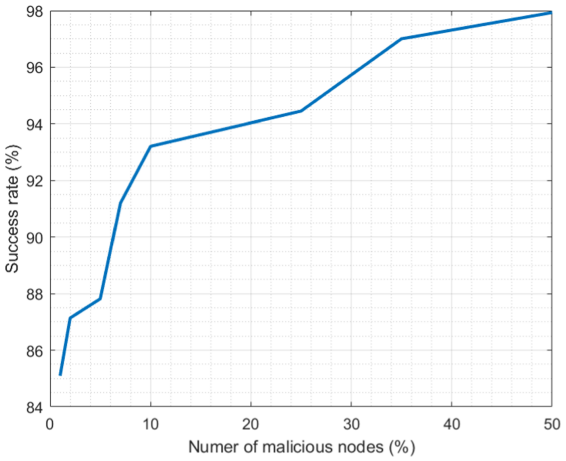

Fig. 2. Results of the first experiment

Figure 3 shows the results of the second experiment. As can be seen, for malicious nodes up to 10%, the convergence time is below one hour (3600 s). However, from this point, the convergence time starts growing up exponentially. For 25% of malicious nodes, the convergence time reaches two hours, and for any number of malicious nodes above this limit, Fig. 3 does not show a clear convergence. Any case, these results are acceptable, considering the convergence time of other IoT components such as CO_2 sensors.

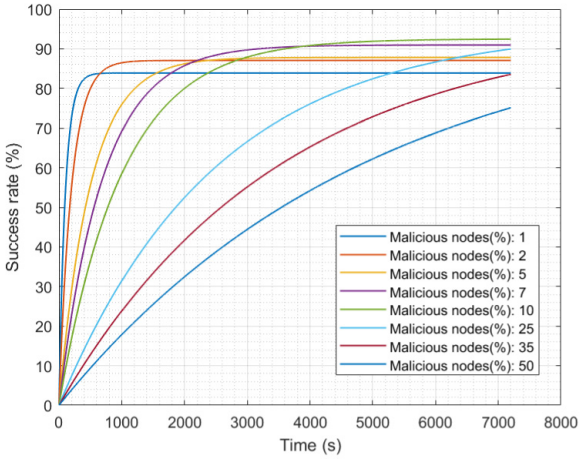

Fig. 3. Results of the second experiment

5 Conclusions and Future Works

In this paper we propose a new distributed architecture for the provision of trust and reputation services in IoT systems. The architecture is based on Blockchain technologies and the composition of different conceptual models (cognitive, computational, neurological, and game-theoretical) using stochastic functions. Results shows the proposed technology presents a good detection rate and convergence time. Specifically, success rate is above 85% in very situation and for malicious nodes up to 10%, the convergence time is below one hour. These values are acceptable for most IoT deployments, as they typically operate with a limited number of nodes and generate information in a quite low speed.

Future works will evaluate the proposed solution in real IoT deployment with commercial hardware devices. Although the proposed simulation scenario shows a high precision, real deployments are affected by exogenous and unexpected phenomena which may modify the results introduced in this paper. These impacts will be evaluated in future works.

Acknowledgments. The research leading to these results has received funding from the Ministry of Science, Innovation and Universities through the COGNOS project (PID2019-105484RB-I00).

References

1. Abhishta, A., van Heeswijk, W., Junger, M., Nieuwenhuis, L.J.M., Joosten, R.: Why would we get attacked? An analysis of attacker's aims behind DDoS attacks. J. Wirel. Mob. Netw. Ubiquit. Comput. Dependable Appl. (JoWUA) **11**(2), 3–22 (2020)

2. Alcarria, R., Bordel, B., Robles, T., Martín, D., Manso-Callejo, M.Á.: A blockchain-based authorization system for trustworthy resource monitoring and trading in smart communities. Sensors **18**(10), 3561 (2018)
3. Alizadeh, M., Andersson, K., Schelen, O.: A survey of secure internet of things in relation to blockchain. J. Internet Serv. Inf. Secur. (JISIS) **10**(3), 47–75 (2020)
4. Anada, H.: Decentralized multi-authority anonymous authentication for global identities with non-interactive proofs. J. Internet Serv. Inf. Secur. (JISIS) **10**(4), 23–37 (2020)
5. Bordel, B., Alcarria, R.: Assessment of human motivation through analysis of physiological and emotional signals in industry 4.0 scenarios. J. Ambient Intell. Hum. Comput. 1–21 (2017)
6. Bordel, B., Alcarria, R., De Andres, D.M., You, I.: Securing internet-of-things systems through implicit and explicit reputation models. IEEE Access **6**, 47472–47488 (2018)
7. Bordel, B., Alcarria, R., de Rivera, D.S., Robles, T.: Process execution in cyber-physical systems using cloud and cyber-physical internet services. J. Supercomput. **74**(8), 4127–4169 (2018)
8. Bordel, B., Alcarria, R., Martín, D., Sánchez-de Rivera, D.: An agent-based method for trust graph calculation in resource constrained environments. Integr. Comput.-Aided Eng. **27**(1), 37–56 (2020)
9. Bordel, B., Alcarria, R., Martín, D., Sánchez-Picot, Á.: Trust provision in the internet of things using transversal blockchain networks. Intell. Autom. Soft Comput. **25**(1), 155–170 (2019)
10. Bordel, B., Alcarria, R., Robles, T.: Denial of chain: evaluation and prediction of a novel cyberattack in blockchain-supported systems. Futur. Gener. Comput. Syst. **116**, 426–439 (2021)
11. Bordel, B., Alcarria, R., Robles, T., González, D.: An industry 4.0 solution for the detection of dangerous situations in civil work scenarios. In: Rocha, Á., Ferrás, C., Paredes, M. (eds.) ICITS 2019. AISC, vol. 918, pp. 494–504. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-11890-7_48
12. Bordel, B., Alcarria, R., Robles, T., Iglesias, M.S.: Data authentication and anonymization in IoT scenarios and future 5G networks using chaotic digital watermarking. IEEE Access **9**, 22378–22398 (2021)
13. Bordel, B., Alcarria, R., Robles, T., Sanchez-Picot, A.: Stochastic and information theory techniques to reduce large datasets and detect cyberattacks in ambient intelligence environments. IEEE Access **6**, 34896–34910 (2018)
14. Bordel, B., Alcarria, R., Sánchez-de-Rivera, D.: Detecting malicious components in large-scale internet-of-things systems and architectures. In: Rocha, Á., Correia, A.M., Adeli, H., Reis, L.P., Costanzo, S. (eds.) WorldCIST 2017. AISC, vol. 569, pp. 155–165. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-56535-4_16
15. Bordel, B., Alcarria, R., Sánchez de Rivera, D., Martín, D., Robles, T.: Fast self-configuration in service-oriented smart environments for real-time applications. J. Ambient Intell. Smart Environ. **10**(2), 143–167 (2018)
16. Bordel, B., Alcarria, R., Sánchez-de-Rivera, D., Robles, T.: Protecting industry 4.0 systems against the malicious effects of cyber-physical attacks. In: Ochoa, S.F., Singh, P., Bravo, J. (eds.) UCAmI 2017. LNCS, vol. 10586, pp. 161–171. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-67585-5_17
17. Haroon, A., Akram, S., Shah, M.A., Wahid, A.: E-lithe: a lightweight secure DTLS for IoT. In: IEEE Vehicular Technology Conference, vol. 2017-September, pp. 1–5, February 2018

18. Huang, Z., Su, X., Zhang, Y., Shi, C., Zhang, H., Xie, L.: A decentralized solution for IoT data trusted exchange based-on blockchain. In: 2017 3rd IEEE International Conference on Computer and Communications, ICCC 2017, vol. 2018-January, pp. 1180–1184, March 2018
19. Ju, C., Wang, J., Xu, C.: A novel application recommendation method combining social relationship and trust relationship for future internet of things. Multimed. Tools Appl. **78**(21), 29867–29880 (2018)
20. Kasturi, G., Jain, A., Singh, J.: Detection and classification of radio frequency jamming attacks using machine learning. J. Wirel. Mob. Netw. Ubiquit. Comput. Dependable Appl. (JoWUA) **11**(4), 49–62 (2020)
21. Kim, E., Keum, C.: Trustworthy gateway system providing IoT trust domain of smart home. In: International Conference on Ubiquitous and Future Networks, ICUFN, pp. 551–553, July 2017
22. König, L., Unger, S., Kieseberg, P., Tjoa, S.: The risks of the blockchain a review on current vulnerabilities and attacks. J. Internet Serv. Inf. Secur. (JISIS) **10**(3), 110–127 (2020)
23. Liu, N., Yu, M., Zang, W., Sandhu, R.: Cost and effectiveness of TrustZone defense and side-channel attack on arm platform. J. Wirel. Mob. Netw. Ubiquit. Comput. Dependable Appl. (JoWUA) **11**(4), 1–15 (2020)
24. Murayama, Y., Hauser, C., Hikage, N., Chakraborty, B.: The sense of security and trust. In: Handbook of Research on Social and Organizational Liabilities in Information Security, pp. 493–502 (2008)
25. U. S. Premarathne: MAG-SIoT: a multiplicative attributes graph model based trust computation method for social Internet of Things. In: 2017 IEEE International Conference on Industrial and Information Systems, ICIIS 2017 - Proceedings, vol. 2018-January, pp. 1–6, February 2018
26. Raza, S., Shafagh, H., Hewage, K., Hummen, R., Voigt, T.: Lithe: lightweight secure CoAP for the internet of things. IEEE Sens. J. **13**(10), 3711–3720 (2013)
27. Robles, T., Bordel, B., Alcarria, R., Martín, D.: Mobile wireless sensor networks: modeling and analysis of three-dimensional scenarios and neighbor discovery in mobile data collection. Ad-Hoc Sens. Wirel. Netw. **35**(1–2), 67–104 (2017)
28. Robles, T., Bordel, B., Alcarria, R., Sánchez-de Rivera, D.: Enabling trustworthy personal data protection in eHealth and well-being services through privacy-by-design. **16**(5) (2020). https://doi.org/10.1177/1550147720912110
29. Sánchez, B.B., Sánchez-Picot, Á., De Rivera, D.S.: Using 5G technologies in the internet of things handovers, problems and challenges. In: Proceedings - 2015 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, IMIS 2015, pp. 364–369, September 2015
30. Son, J., Choi, W., Choi, S.-M.: Trust information network in social internet of things using trust-aware recommender systems. **16**(4) (2020). https://doi.org/10.1177/1550147720908773
31. Talreja, R., Sathish, S., Nenwani, K., Saxena, K.: Trust and behavior based system to prevent collision in IoT enabled VANET. In: International Conference on Signal Processing, Communication, Power and Embedded System, SCOPES 2016 - Proceedings, pp. 1588–1591, June 2017
32. Ud Din, I., Guizani, M., Kim, B.S., Hassan, S., Khan, M.K.: Trust management techniques for the internet of things: a survey. IEEE Access **7**, 29763–29787 (2019)
33. Wortmann, F., Flüchter, K.: Internet of things. Bus. Inf. Syst. Eng. **57**(3), 221–224 (2015)