Detecting Malicious Components in Large-Scale Internet-of-Things Systems and Architectures

Borja Bordel(✉), Ramón Alcarria, and Diego Sánchez-de-Rivera

Universidad Politécnica de Madrid, Madrid, Spain
{bbordel,diegosanchez}@dit.upm.es, ramon.alcarria@upm.es

Abstract. Current large-scale Internet-of-Things systems and architectures incorporate many components, such as devices or services, geographic and conceptually very sparse. Thus, for final applications, it is very complicated to deeply know, manage or control the underlying components, which, at the end, generate and process the data they employ. Therefore, new tools to avoid or remove malicious components based only on the available information at high level are required. In this paper we describe a statistical framework for knowledge discovery in order to estimate the uncertainty level associated with the received data by a certain application. Moreover, these results are used as input in a reputation model focused on locating the malicious components. Finally, an experimental validation is provided in order to evaluate the performance of the proposed solution.

Keywords: Internet-of-Things · Knowledge discovery · Security · Uncertainty · Information systems · Pervasive sensing · Grid computing

1 Introduction

Nowadays, Internet-of-Things (IoT) has matured from its origin as a research concept to commercial products and real deployments, such as the current smart cities [1]. In particular, large-scale IoT pilots are the most interesting and recent topic on IoT innovation [2]. These pilots include very complex systems and architectures which involve a great amount of components (such as devices, services, execution engines, etc.). This complexity facilitates the appearance (deliberate or not) of malicious components; those which provide uncertain data, services or information. In general, IoT architectures try to merge very different devices and other components, which may be (and used to be) geographically sparse and conceptually very distant [3]. Thus, low-level information must be collected, transformed, aggregated and translated various times (using, for example, semantic technologies) before being sent to the high-level final applications. However, none meta-information about the underlying hardware platform (such as sensor sensibility) or other low-level components is provided to the high-level layers.

Therefore, final applications have a very limited knowledge about the system and almost no control over the infrastructure which provides them with the operation data [4]. In this context, extremely important concepts such as the uncertainty level associated with the received data or the real quality associated with the offered services cannot be

Á. Rocha et al. (eds.), *Recent Advances in Information Systems and Technologies*,
Advances in Intelligent Systems and Computing 569, DOI 10.1007/978-3-319-56535-4_16

estimated using traditional configuration algorithms (as they require special control information in order to calculate the results) [5]. Instead of that, new solutions based only on the available information at high-level are necessary.

The objective of this paper is to describe a statistical framework for knowledge discovery in order to estimate the uncertainty level associated with the received operation data by a certain application. Additionally, these results are used as input in a reputation model focused on locating the malicious components. Thus, if possible, final applications may discard information from these components.

The rest of the paper is organized as follows: Sect. 2 describes the state of the art on uncertainty management and reputation models; Sect. 3 includes the mathematical formalization of the proposed framework and reputation model; Sect. 4 presents an experimental validation based on a simulated scenario in order to test the performance of the proposed solution; Sect. 5 contains the experimental results and Sect. 6 concludes the paper.

2 Related Works

Uncertainty management is one of the key problems in IoT scenarios; however, little work has treated this topic. Most papers, moreover, are focused on how uncertainties affect control loops and algorithms. In this case, they use to focus the research on Cyber-Physical Systems [6] (sometimes understood as a specific IoT scenario) which may be described using finite difference equations, which are influenced by unknown discrete functions representing the uncertainties [7]. Additionally, some works [8] propose a mathematical framework in order to calculate the optimal reaction in order to cancel the effect of uncertainties in control loops.

On the other hand, typical works on uncertainty management in IoT scenarios try to measure the influence of factors that designers know they do not know (noise, packet losses, etc.). Thus, uncertainty taxonomies [9], modeling [10] and processing [11] are really typical. Nevertheless, factors that designers do not know they do not know are never addressed; and this kind of factors is the most important in large-scale IoT systems. Thus, a more general framework is required.

Papers on uncertainty level estimation in IoT scenarios are strange, and usually research works on this topic talk about trust levels. Any case, there is also little work on trust management for IoT environments. Furthermore, most of these works are based on the concept of reputation.

Some works try to stablish the definition of reputation [12] in IoT systems, and apply the model in a horizontal way (inside the underlying sensor network, in order to calculate the reputation of nodes) [13]. These models, however, only consider Quality-of-Service (QoS) trust metrics like packet forwarding/delivery ratio and energy consumption. More general models have been also proposed [14], including philosophical concepts such as honesty, cooperativeness, or community-interest.

If vertical solutions are considered, works on service reputation are also found [15]. In particular, models based on the evaluation of user's trust in a service and service classification [16]; and models considering authentication history and penalty [17] can be found. However, none of these models consider the previously described theoretical formalization, and concepts such as the service honesty are not defined.

In comparison with all the cited works our proposal formalizes the concept of uncertainty level in IoT scenarios using statistical tools. Additionally, definitions initially proposed for sensor networks are extended to services and other IoT components. As a result, malicious components are efficiently located and policies in order to remove or avoid them are enabled.

3 Formalization of the Proposed Solution

Malicious components are those which provide uncertain data, service or information. This behavior may be due to a cyber-attract, a bad programming or a malfunction in hardware (among other reasons). In order to avoid sever damage to entire system, these components must be isolated. With this objective, the concept of "reputation of a IoT entity" is defined.

The reputation of an IoT component Σ, $\mathcal{R}_\Sigma$, is defined as the global perception of its behavior in the system, in particular, whether transactions including this component present in general positive outcomes. As can be seen, reputation is a global concept, so all components in the system should be involved in its estimation. However, a global definition of reputation may be impractical, thus we also define the concept of local reputation.

The $\Lambda-$local reputation of an IoT component Σ, $\mathcal{R}_\Sigma|_\Lambda$, is the local perception of the behavior of the component Σ in a certain system's component Λ, in particular whether transactions including both components present in general positive outcomes.

Then, it is trivial to deduct that the relation between $\mathcal{R}_\Sigma$ and $\mathcal{R}_\Sigma|_{\mathit{\Lambda}}$ is which indicated in (1), where $\mathfrak{C}$ is the set of all components in the system and λ_Λ the relative weight of $\mathcal{R}_\Sigma|_\Lambda$.

$$\mathcal{R}_\Sigma = \sum_{\Lambda \in \mathfrak{C}} \lambda_\Lambda \cdot \mathcal{R}_\Sigma|_\Lambda \tag{1}$$

The $\Lambda-$local reputation of an IoT component Σ it is calculated as the weighted sum of three values: the nobleness $\mathcal{N}$, the solidarity $\mathcal{S}$, and the relevance $\mathcal{R}e$ of the component Σ perceived by the component Λ (2).

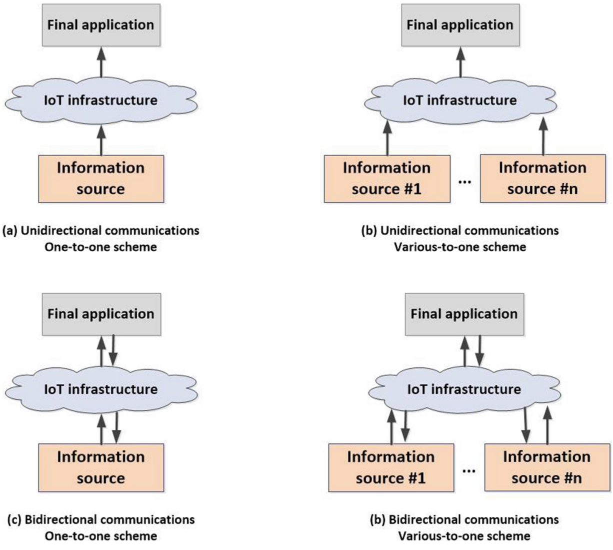
$$\mathcal{R}_\Sigma|_\Lambda = \begin{bmatrix} \alpha & \beta & \gamma \end{bmatrix} \cdot \begin{bmatrix} \mathcal{N} \\ \mathcal{S} \\ \mathcal{R}e \end{bmatrix} \tag{2}$$

Thus, a component Σ is categorized as malicious by a certain component Λ if its $\Lambda-$local reputation falls below a certain threshold μ_Λ (a solution which in practical applications should be complemented with, for example, a token-based danger detection technology see Sects. 5 and 6). On the contrary, it is classified as a regular component. Malicious components should be avoided and, in that way, they would tend to be isolated as time passes.

Although these concepts may be applied to any couple of IoT components in a system or architecture, in this work we are focused on the reputation that final applications perceive about their primary data sources (i.e. mainly, services and hardware devices).

In order to evaluate the local reputation, the three parameters which compose it must be defined. For that, four different scenarios may be defined (see Fig. 1), depending on two independent criteria.

– Transmission mode: Bidirectional communications generate a more complex model as two data flows have to be considered. In the simplest case, data only flows from the information source to the final application (unidirectional communications).
– Data aggregation: In some occasions, data received by a certain application are obtained by aggregating the flows from various components (various-to-one scheme). In that case, measurements refer a global vision, and estimating the individual reputation is more complicated than in one-to-one schemes (where data are generated only in one component).



(a) Unidirectional communications One-to-one scheme

(b) Unidirectional communications Various-to-one scheme

(c) Bidirectional communications One-to-one scheme

(b) Bidirectional communications Various-to-one scheme

Fig. 1. Possible scenarios for the local reputation calculation

For this first work a reduced model is considered. Thus, only unidirectional communications based on a one-to-one scheme are considered. Additionally, in this first study, it is considered that $\beta = \gamma = 0$ and $\alpha = 1$, so the value of the local reputation matches the nobleness value. Next subsection describes the calculation of this parameter.

3.1 Uncertainty Level Estimation: Nobleness Calculation

The nobleness $\mathcal{N}$ of an IoT component Σ, according to a second component Λ, is defined as the expectance of Λ to obtain correct information from Σ. This information may be production data or meta-information (such as the offered QoS for a certain service).

Nobleness calculation is based on previous experiences, which are weighted in order to limit the effect of events very distant in time. Moreover, it is difficult to stablish the nobleness of a component based on a few interactions. Thus a threshold N_{th} must be defined in order accumulate the required measurements to start estimating the nobleness value.

Equation (3) represents the mathematical model for nobleness calculation; where n is the number of accumulated nobleness measurements and h is the weighted ratio of the number of times the component behaved nobly (i.e. it sent correct information).

$$\mathcal{N} = \begin{cases} 1\,; n < N_{th} \\ \sqrt{2}\dfrac{h}{\sqrt{1+h^2}}; n > N_{th} \end{cases} \tag{3}$$

As can be seen, nobleness follows an algebraic function belonging to the sigmoid class. Thus, $\mathcal{N} \in [0,1] \forall h \in [0,1]$. Moreover, the model includes the presumption of nobleness, as every component is sincere ($\mathcal{N} = 1$) until enough measurements are collected. In order to calculate the weighted ratio h, we are considering a geometric sum (4); where the common ratio r can be freely fixed (in order to limit the influence of the past behaviors, as $|r| \rightarrow 0$).

$$h = \sum_{j=0}^{n} u[-j] \cdot r^{j+1} \tag{4}$$

The sequence $u[\cdot]$ represents the natural ratio of the number of times the component behaved honestly in every time slot. $u[j]$ is defined (5) as the quotient between the times the component provided correct information in the j-th time slot p_j and the total number of transactions in that time slot t_j.

$$u[j] = \frac{p_j}{t_j} \tag{5}$$

In order to calculate whether an IoT component has provided correct information in a certain transaction, we are evaluating the uncertainty level θ associated with the provided information. If this level remains below a certain threshold μ_h it is considered the component has been honest. In some cases, the detected uncertainty may not be caused by the analyzed component. However, from the final applications' point of view the provided information is uncertain and, in an aggregated vision, the component is not honest.

In order to evaluate the uncertainty level θ we use the following statistical model. Figure 2 represents the scenario under study. A final application received from an information source (IoT component) a certain information $\bar{\bar{x}}$. In large-scale IoT systems, the uncertainty level associated with $\bar{\bar{x}}$ is the addition of two amounts.

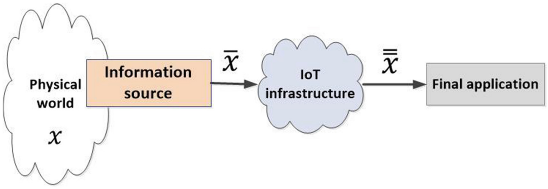


Fig. 2. Scenario under study

First, the uncertainties $\mathfrak{T}_{IT}$ about the equivalence between the received information $\bar{\bar{x}}$ and the information generated by the information source $\bar{x}$. In this first case, the relation between both data may be described as a surjective stochastic application $T[\cdot]$, as every information $\bar{\bar{x}}$ must be the image of a certain information $\bar{x}$. These uncertainties are caused by the IoT infrastructure, so they are IT uncertainties.

And, second, the uncertainties $\mathfrak{T}_{PHY}$ about the equivalence between the information generated by the information source $\bar{x}$ and the real information existing in the physical world x. These uncertainties are caused by physical limitations in the information capture. Therefore, they are physical uncertainties.

Thus, associated with a received information $\bar{\bar{x}}$ there exists an enumerable set of uncertainty sources $\mathfrak{T} = \left\{ \mathfrak{T}_{PHY}, \mathfrak{T}_{IT} \right\} = \{ i_k, k = 1, \ldots, K \}$ whose cardinality K may reach the cardinality of the natural numbers $\aleph_0$. This uncertainty sources transform the process of acquiring a certain information $\bar{\bar{x}}$ in a random experiment ε, which takes values from the discrete sample space Ω.

Each uncertainty source is described as a bi-varied stochastic process (6), being Ψ the sample space of all possible values for the uncertain event.

$$i_k \asymp \mathrm{X}_k[m;\omega, \psi)/\omega \in \Omega, \psi \in \Psi \tag{6}$$

Stochastic processes are discrete in time as final applications are a cyber component, but the sample space Ψ may be continuous or discrete, depending on the nature of the uncertainty source. For example, the measurement error has a continuous nature; however, the possibility of suffering a cyber-attack is described by a discrete variable. Furthermore, in general, uncertainties' value change pretty slow, so these stochastic processes may be considered stationary during a time slot.

As they are unknown effects, stochastic processes are expressed in a parametric way, depending, each one, on a certain parameter ϑ_k. Three basic probability density functions or probability distributions may be used to describe uncertainty sources: uniform distributions, triangular distributions and Gaussian distributions (see Fig. 3).

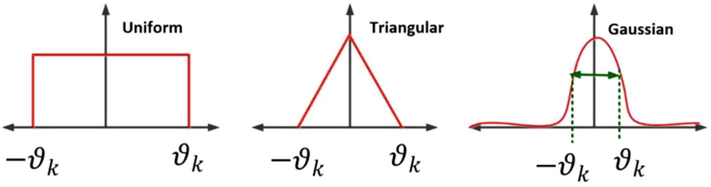


Fig. 3. Basic probability density functions

Uniform distributions are employed to describe unknown effects whose effect is limited to the range $[-\vartheta_k, \vartheta_k]$. In data acquisition processes this is most general distribution, as the sample space is bounded. Triangular distributions are employed when, besides the variation range, it is known that the error probability goes down as its value goes up. Finally, if more information is available (for example, if noise is considered) a Gaussian distribution with typical deviation ϑ_k can be employed.

Considering $\mathcal{F}$ the set of parts of Ω, and a function $P(A)A\varepsilon\mathcal{F}$ which fulfills the three Kolmogorov's probability axioms, the experiment ε is completely characterized with the event algebra $E = \langle \Omega, \mathcal{F}, \ P(\cdot) \rangle$, which (additionally) is a $\sigma-$algebra.

In this context, it is possible to create a partition $\Pi = \{\pi_1, \ldots, \pi_p\}$ of Ω, and select a main value $\delta_i \in \pi_i$ representing every cluster. Then, the process to estimate the uncertainty level $\theta[j]$ in the j-th time slot is as follows.

When certain information $\bar{\bar{x}}$ is received, it is included in the observations vector v_j of the current time slot (7).

$$v_j = \left(\bar{\bar{x}}_1, \ldots, \bar{\bar{x}}_m \right) \tag{7}$$

As these observations are independent, it is possible to calculate the value of the ϑ_k parameter for each uncertainty source using the maximum likelihood estimation (MLE) [18] algorithm and the vector v_j. This method is the most adequate as prior probability distributions are unknown. Then, the event π_i to which belongs the received information it is located. For each uncertainty source, the probability ρ_i^j of the received information to really belong to the event π_i in that time slot is calculated (8).

$$\rho_i^j = \int_{\pi_i} \mathrm{X}_k[j\,; \bar{\bar{x}}, \psi) d\psi \text{ or } \rho_i^j = \sum\nolimits_{\psi \in \pi_i} \mathrm{X}_k[j\,; \bar{\bar{x}}, \psi] \tag{8}$$

In that way, as uncertainty sources are also independent, the global probability ρ^j of $\bar{\bar{x}}$ to belong to π_i is calculated as a probability multiplication (9).

$$\rho^j = \prod_{k=1}^{K} \rho_k^j \tag{9}$$

Finally, the information δ_i is considered to be received with an uncertainty level $\theta[j]$ calculated as indicated in (10).

$$\theta[j] = 1 - \rho^{j} \tag{10}$$

In this transaction, the information source is considered to be honest if meets the condition explained above ($\theta[j] > \mu_h$).

4 Experimental Validation

In order to evaluate the proposed solution, an experimental validation was designed. The proposed experiment consisted of a simulation scenario, where a large-scale IoT system was deployed (Fig. 4).

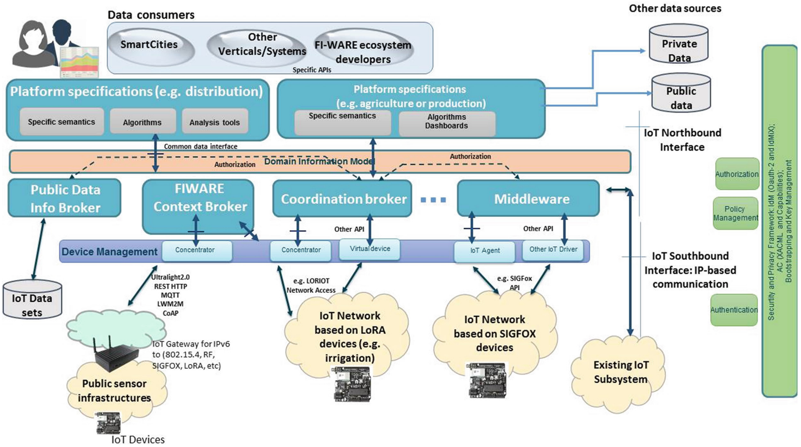


Fig. 4. Simulation scenario

The simulated scenario (based on a real European deployment) included four different networks of information sources (public sensors, LoRA devices, etc.) geographically sparse. Each network was composed by one hundred and fifty (150) components. Randomly, the configuration of ten (10) components was created to force them to provide uncertain information (and being considered as malicious). Basically, the precision of the instruments was reduced, the electromagnetic interferences and the packet losses were strengthened and, in one case, it was supposed an intruder controls the component (causing this component to provide erroneous information). One final application was hosted in the FI-WARE ecosystem.

The simulated final application included the proposed uncertainty level calculation algorithm and the described reputation model (expressions from (1) to (10)). The other entities could be measured, but they were not provided with the reputation calculation module.

In order to perform the proposed simulation, the NS3 simulator was employed. NS3 is a network simulator whose scenarios and behavior are controlled and described by means of C++ programs, and which is extensively used in research due to its flexibility.

Data about the number of transactions performed by the malicious nodes were collected. Moreover, the evolution of the local reputation of the malicious nodes was monitored.

5 Results

Figure 5(a) presents the evolution of the number of transactions performed by the malicious components as times passes. As can be seen, firstly the number of transaction remains constant, but from a time between $t = 80$ and $t = 200$ min, the number of transaction in every malicious node descends slowly but continuously, following an exponential-like law. This exponential tendency is explained by the fact that, once the reputation goes below the stablished threshold, final applications look for other information sources to obtain their data immediately. Depending on the uncertainty of the received data (see Expression 9 and Fig. 3), the descent phase can start later or be very abrupt from the beginning. Moreover, components performing a low number of transactions require more time to be isolated, as more time is required to acquire the necessary information about their behavior. Any case, each of the ten malicious components, at the end, got isolated, so the objective of the proposed solution is met.

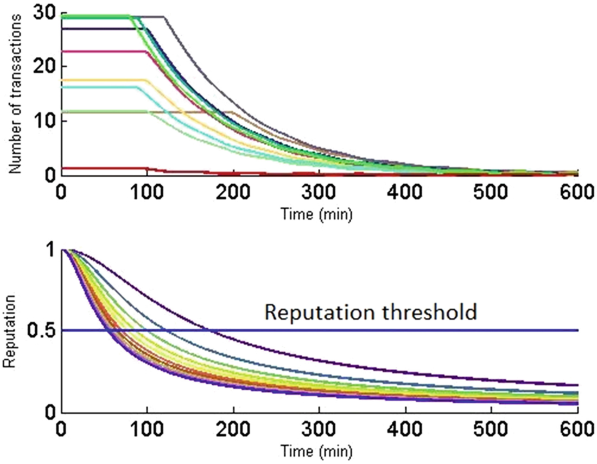


Fig. 5. Simulation results

On the other hand, the correspondence between the amount of performed transactions and the calculated reputation can be seen in Fig. 5(b). In this figure a group of sigmoid functions is showed, as the nobleness calculation model is described using these functions. In this case, the reputation level descends constantly since the initial instant, as malicious components behave in a disingenuous way from the beginning. In comparison, the number of performed transaction remains constant for every component, until its reputation goes below the fixed threshold. This fact must be taken into account, as there is a convergence time during which malicious components may affect the entire system. The descent stops when no transactions are performed by the component (see Fig. 5(a)) and measurements are not updated.

6 Conclusions and Future Works

In this paper we have described a mathematical framework for the data uncertainty level calculation, which allows final application to estimate the nobleness and the reputation of the information sources and other IoT components in large-scale systems and architectures. Results showed that malicious components get isolated as time passes if implanted the proposed technology.

On the other hand, the proposed reputation model may be enriched with additional measurements (such as the component solidarity) in order to accelerate the isolation process. Future works should consider these ideas (exposed also in Sect. 3), as well the possibility of including a token-based rapid hazard detection system (in order to avoid severe damage during the convergence time). Finally, both, the formalization of the solution and the simulation scenario, describe the basic problem, so future works should extend the proposed framework to scenarios where bidirectional communications and data aggregation are presented.

Acknowledgments. Borja Bordel has received funding from the Ministry of Education through the FPU program (grant number FPU15/03977). Additionally, the research leading to these results has received funding from the Ministry of Economy and Competitiveness through SEMOLA project (TEC2015-68284-R) and from the Autonomous Region of Madrid through MOSI-AGIL-CM project (grant P2013/ICE-3019, co-funded by EU Structural Funds FSE and FEDER).

References

1. Sarkar, A.N.: Significance of smart cities in 21st century: an international business perspective. FOCUS: J. Int. Bus. **2**(2), 53–82 (2016). doi:10.17492/focus.v2i2.8623
2. Hong, K., Lillethun, D., Ramachandran, U.: Mobile fog: a programming model for large-scale applications on the internet of things. In: Proceedings of the Second ACM SIGCOMM Workshop on Mobile Cloud Computing, pp. 15–20. ACM (2013)
3. Lee, H., Jo, S.K., Lee, N., Lee, H.W.: A method for co-existing heterogeneous IoT environments based on compressive sensing. In: 18th International Conference on Advanced Communication Technology (ICACT), pp. 206–209. IEEE (2016)
4. Robles, T., Alcarria, R., Martın, D., Navarro, M.: An IoT based reference architecture for smart water management processes. J. Wirel. Mob. Netw. Ubiquit. Comput. Dependable Appl. **6**(1), 4–23 (2015)
5. Bordel, B., Alcarria, R., Martín, D., Robles, T.: Self-configuration in humanized cyber-physical systems. J. Ambient Intell. Human. Comput. 1–12 (2016). doi:10.1007/s12652-016-0410-3
6. Stankovic, J.: A research directions for the internet of things. IEEE Internet Things J. **1**(1), 3–9 (2014)
7. Cardenas, A.A., Amin, S., Sastry, S.: Secure control: towards survivable cyber-physical systems. In: System (2008)

8. Zhu, Q., Başar, T.: Robust and resilient control design for cyber-physical systems with an application to power systems. In: 2011 50th IEEE Conference on Decision and Control and European Control Conference, pp. 4066–4071. IEEE (2011)
9. Zhang, M., Selic, B., Ali, S., Yue, T., Okariz, O., Norgren, R.: Understanding uncertainty in cyber-physical systems: a conceptual model. In: Wąsowski, A., Lönn, H. (eds.) ECMFA 2016. LNCS, vol. 9764, pp. 247–264. Springer, Cham (2016). doi:10.1007/978-3-319-42061-5_16
10. Aggarwal, C.C., Ashish, N., Sheth, A.: The internet of things: a survey from the data-centric perspective. In: Aggarwal, C.C. (ed.) Managing and Mining Sensor Data, pp. 383–428. Springer, New York (2013)
11. Hasan, S., Curry, E.: Approximate semantic matching of events for the internet of things. ACM Trans. Internet Technol. (TOIT) **14**(1), 2 (2014)
12. Chen, D., Chang, G., Sun, D.: TRM-IoT: a trust management model based on fuzzy reputation for internet of things. Comput. Sci. Inf. Syst. **8**(4), 1207–1228 (2011)
13. Boukercha, A., Xua, L., EL-Khatibb, K.: Trust-based security for wireless ad hoc and sensor networks. Comput. Commun. **30**(11–12), 2413–2427 (2007)
14. Bao, F., Chen, R.: Trust management for the internet of things and its application to service composition. In: World of Wireless, Mobile and Multimedia Networks (WoWMoM), pp. 1–6. IEEE (2012)
15. Chen, L., Yan, Z., Zhang, W.: TruSMS: A trustworthy SMS spam control system based on trust management. Future Gener. Comput. Syst. **49**, 77–93 (2015)
16. Liu, Y., Chen, Z., Xia, F., Lv, X., Bu, F.: A trust model based on service classification in mobile services. In: Green Computing and Communications (GreenCom), pp. 572–577. IEEE (2010)
17. Liu, Y., Wang, K.: Trust control in heterogeneous networks for internet of things. In: International Conference on Computer Application and System Modeling (2010)
18. Scholz, F.W.: Maximum likelihood estimation. In: Encyclopedia of Statistical Sciences (1985)