Dirichlet-based Initial Trust Establishment for Personal Space IoT Systems

Tham Nguyen[†§], Doan Hoang[†], Aruna Seneviratne[‡§]
[†]University of Technology Sydney, [‡]University of New South Wales, [§]Data61-CSIRO, Australia
Emails: *thitham.nguyen@student.uts.edu.au*, *doan.hoang@uts.edu.au*, *aruna.seneviratne@data61.csiro.au*

***Abstract*—Trust has played a crucial role in enhancing the security of IoT systems over their lifecycles from creation to retirement. Particularly, in a personal space IoT system where devices join and leave the system dynamically, it is important to evaluate the device's behavior in the form of trust on its admission to the system to reduce the risk and uncertainty of the overall system. Currently, proposed trust evaluation models primarily rely on the historical knowledge or trusted recommendations. However, in many situations, such information is not available at the first encounter between the system and the device. The challenge tackled by this paper is how to establish whether a device can be trusted to a level that merits further evaluation for admission into an IoT system when it encounters the system for the first time. We propose a Dirichlet-based trust assessment model to establish the initial trust that the system places on a device in a mobile and dynamic environment called personal space IoT. The proposed scheme can also be used to affirm the trust of a device during its operation or when it is being re-admitted to the system after an interruption. We describe and evaluate our proposed model theoretically and by simulation.**

I. Introduction

The personal space IoT system introduced in our previous work [1], [2] refers to a group of user's device, and other devices that are within the wireless communication radius of the user's devices and likely to provide services to the user. A smartphone or a capability-comparable device acts as the centralized controller, managing of the space including admitting entities and monitoring their activities. In the personal space IoT system, its membership varies dynamically over it lifecycle due to the joining or leaving of devices and their services while interacting with others.

Authentication is mainly used in information systems for granting access to a new device and establishing secure communication among devices. However, authenticated devices may behave maliciously over time by not cooperating with others or providing poor services for its benefits [3]. Therefore, it is necessary to protect the system from insider security attacks deployed by its admitted entities. Trust is recognized as an essential factor for monitoring entities activities and detecting malicious behavior. It has increasingly played a crucial role in establishing a secure IoT system over its entire lifecycle. It is important that the new device or the rejoining device is established with a certain degree of trust before it is granted access or admitted to the personal space IoT system. Existing proposed trust models primarily solve the issues of monitoring the malicious behavior and managing the trust level of authenticated devices. However, none of them attempts to provide a solution for assessing the trustworthiness of unknown devices at their first encounter with the system as well as devices that rejoin the system after an interruption. Instead, most of them rely on the belief that all devices are trusted at their admission phase. In addition, the existing trust assessment scheme does not suit for the initial trust assessment as they require experience from past interactions or trusted recommendations. In many situations, such information is not available. The challenging problem is that how to capture the trust knowledge about a device within a narrow window of time at its first encounter with the system.

Our earlier work [2] proposed a challenge-response mechanism and a trust evaluation scheme to solve this problem. Specifically, we proposed a Bayesian approach for initial trust assessment scheme where the challenge-response operation is utilized for collecting the evidence about the device's behavior, and the Beta distribution is used to derive the trust knowledge during the challenge-response process. We developed a binary trust evaluation scheme where the challenger assesses the devices response to evaluate whether it is an expected or an unexpected response. However, the outcomes from a challenge-response operation at the first encounter are often not binary but multiple levels indicating various degrees of satisfaction. This is the motivation for proposing a trust evaluation algorithm for multi-valued satisfaction level.

In this paper, we present a Dirichlet-based trust assessment model considering the multi-valued satisfaction level of the response to a challenge. With this setting, the evaluation of a device's response leads to multiple outcomes, i.e., multiple levels associated with various degrees of satisfaction of the challenger from a device's response. We propose a Bayesian approach that adopts the Dirichlet distribution as the theoretical foundation for measuring the uncertainty level in the device's behavior considering multi-valued satisfaction level. A trust evaluation method is proposed to interpret the uncertainty level to the degree of trust.

Specifically, we model the posterior distribution of the probabilities associated with multi-valued satisfaction level by a Dirichlet distribution. In other words, we can estimate the Dirichlet probability density function (pdf) of these probabilities and their posterior expected values. Finally, the uncertainty level in the device behavior measured through posterior expected values is then interpreted to the degree of trust given on a device after conducting the challenge-response process. Our challenge-response process continuously updates and aggregates the initial trust from evidence within a short period at the first encounter of the device with the system.

The experimental evaluation shows that our challenge-response-based trust assessment scheme can capture the device's behavior effectively by conducting the challenge-response process and estimating the distribution of the probability that the device's response satisfies one of the satisfaction levels. The initial trust value computed during the challenge-response process is consistent and matches the device's response patterns.

The rest of the paper is organized as follows. Section II provides related work. Section III describes our challenge-response mechanism and Dirichlet-based initial trust assessment model. Section IV presents the evaluation of our proposed model via simulation. Finally, section V concludes the paper and suggests directions for future research.

II. Related work

In the literature, a number of trust management systems investigating computational trust models have been introduced in wireless networks as well as IoT [3], [4]. In computational trust models, Bayesian approaches have been widely used to evaluate trust where Beta distribution is adopted for binary trust assessment [5], [6] and Dirichlet distribution is utilized for multi-level trust assessment [6]–[10]. In addition, information theory is also used as the basis for trust evaluation [11].

Josang et al., use the Dirichlet distribution as the basis for a multi-level reputation system in e-commerce where parties can rate each other with graded levels from a set of predefined values [10]. The posterior Dirichlet model combines the prior reputation score with a new rating to find the updated reputation score of an agent. This work provides the process for aggregating the reputation of agents that mainly relies on the rating recommended by other agents in the community. The drawback is that it requires massive transactions and long-term rating process to build the reputation.

The work in [7] adapted Dirichlet-based trust management to collaborate host-based intrusion detection networks (HIDS) to detect intrusions and malicious nodes. This model determines the trustworthiness of a HIDS node by collecting both intrusion consultations and its feedbacks to *test* messages during the operational stage. The trust level of a HIDS node is derived from the posterior distribution model updating the prior information with the collected consultations and feedbacks. This approach mainly focuses on detecting the malicious and intrusions once the HIDS is in operational stage and requires long-term collaboration.

In [9], the authors proposed a Dirichlet-based trust management for an inter-provider cooperation network where the entities in different domains cooperate with each other using client-server interactions. The Dirichlet distribution combines the prior beliefs about a client with the collected data from its request sequence to predict the quality of interaction level of those requests for evaluating its trust ranking. This work relies on the sequence of requests of clients from different domains to the server. The server implicitly evaluates the trustworthiness of the requested client and decides the degree of quality of service should provide to the client.

Sun et al., introduced the utilization of uncertainty as a measure of trust [11]. The trust can be measured by determining uncertainty level in the future actions of an agent. When the direct observation is not available, the uncertainty is measured through concatenation and multi-path propagation of recommendations. This approach fails to measure the initial trust of unknown entities due to the lack of third parties' recommendations at their first encounter with the system.

In this paper, we adopt Dirichlet distribution as the theoretical foundation for evaluating the initial trust value of a device. The system defines the multi-valued satisfaction level including multiple degrees of satisfaction of the challenger from a response. Each satisfaction level acts as the base for measuring the trust value. Our work differs from previous Dirichlet-based trust models as we conduct the challenge-response mechanism for capturing the initial trust knowledge without requiring long-term interaction, recommendations, or prior knowledge. Also, we model our trust assessment by the posterior Dirichlet distribution for evaluating uncertainty level of the device's behavior and introduce a new trust interpretation method.

III. Dirichlet-based initial trust assessment model

This section describes our proposed initial trust assessment model which utilizes a challenge-response mechanism for judging a device that encounters the system for the first time, and the posterior Dirichlet-based probability distribution to evaluate the uncertainty level in the device's behavior and estimate its trustworthiness based on the evidence collected from the challenge-response process.

A. Challenge-response mechanism

We first provide an overview of our proposed challenge-response mechanism. This is a process of collecting evidence for the trust assessment scheme where a device's trustworthiness is investigated via its responses towards challenges. It is performed intentionally by the controller during a short time window at the first encounter between the system and an unknown device to investigate the uncertainty level about the device's behavior and then use this knowledge for the trust evaluation. The process contains several challenges that the controller requests responses from the IoT device before deciding on whether to admit it into the system. The challenge-response mechanism is accomplished by exploiting typical interactions between the system and the devices at their first encounter such as in the pairing process in Bluetooth protocol as indicated in our previous work [2].

A challenge can be a request for the knowledge about the surrounding environment or a task that the device must perform successfully and honestly. It can be generated artificially by using a knowledge database built from surveys or the learning process, etc. The semantics of the challenge varies depending on the type of the device, the population in the environment, and the knowledge of the population, etc. A response is distinguished from others via predefined satisfaction levels to the challenger.

B. Dirichlet-based initial trust model

Our initial trust assessment model relies on the evidence captured from the evaluation of the device's response during the challenge-response (C-R) process. In the evaluation, the device's response is evaluated carefully and assigned with one of the levels from a predefined multi-valued satisfaction. The more likely that the device's response is assigned a high satisfaction level, the more likely the device is trusted by the system and vice versa. In addition, the more satisfaction levels are considered in the evaluation process, the more precise of the response evaluation is. Thus, the evaluation of the device's response based on the multi-valued satisfaction level allows the system to capture the device's behavior providing meaningful knowledge for the trust evaluation.

According to Bayesian statistic, the posterior distribution presents the updating in the prior distribution of an unknown event once the prior belief is updated with more evidence. In fact, the posterior Dirichlet distribution of a multi-component random variable is based on its prior distribution and the observations on the distribution of its components. In our trust assessment model, the evidence is evaluated and collected based on a multi-valued satisfaction level of the device's response to the challenger. Therefore, the posterior Dirichlet distribution allows us to refine and provide a better estimate of the distribution of the satisfaction level of observed responses.

Let X be the discrete random variable representing the discrete satisfaction level of a response to a challenge. The system defines k values for the satisfaction level to evaluate the response. Therefore, X can take on one of k values $x_1, x_2, .., x_k$, where x_i denotes one of the satisfaction levels. Each satisfaction level x_i is assigned a weight value w_i in a way that for $x_{i+1} > x_i, w_{i+1} > w_i$ and $\sum_{i=1}^{k} w_i = 1$.

Let Θ denote the random variable representing the probability that a device will return a response with a certain satisfaction level. Note that, Θ is a k-component random variable, $\Theta = \theta_1, \theta_2, \cdots, \theta_k$. Let θ_i denote the probability that a device will return a response with a satisfaction level x_i. In other words, the probability that X takes value x_i is θ_i.

$$\theta_i = P(X = x_i) \quad s.t \quad \sum_{i=1}^{k} \theta_i = 1 \tag{1}$$

Before any C-R round, the pre-knowledge on the probability distribution Θ is not available. It is reasonable to consider that the prior distribution of Θ is uniform, i.e., the probability that the device will provide a response with one of the satisfaction levels is equally likely. In fact, the uniform distribution captures initial ignorance and is a special case of the Dirichlet distribution. Therefore, it is reasonable to choose Dirichlet as the prior distribution Θ as in (2).

$$p(\theta_1, .., \theta_k; \alpha_1, .., \alpha_k) = \frac{\Gamma(\sum_{i=1}^{k} \alpha_i)}{\prod_{i=1}^{k} \Gamma(\alpha_i)} \prod_{i=1}^{k} \theta_i^{\alpha_i - 1} \tag{2}$$

To represent the non-informative prior distribution of Θ we choose parameters $\alpha_i = 1, \forall i = 1..k$.

The outcome from the evaluation of the device's response conducted after a single C-R round is one of satisfaction levels assigned by the system to the received response. Let Y^j denote the outcome vector from round j^{th}. Let y_i represent the i^{th} element in vector $Y^j = y_1, ..., y_k$. Note that each y_i can take a value in $\{1, 0\}$ which indicates that the device's response satisfies level x_i or not, i.e., $y_i = 1$ means the device's response satisfies level x_i whereas $y_i = 0$ refers to the fact that it satisfies other levels.

After each challenge-response round, we accumulate the number of rounds in which the device returns a response with a given satisfaction level. Let s_i denote the number of rounds that the response satisfies level x_i after n challenge-response rounds and $\sum_{i=1}^{k} s_i = n$. We accumulate s_i as below

$$s_i = \sum_{j=1}^{n} Y^j\{y_i\} \tag{3}$$

where $Y^j\{yi\}$ is the i^{th} element in vector Y^j which indicates whether the device's response satisfies level x_i at round j^{th}.

For vector $\Theta = \theta_1, .., \theta_k$, we can treat $\theta_1, .., \theta_k$ each as an independent variable. The challenge-response observation conforms to multinomial distribution as each round is independent and its outcome is one of k possible satisfaction levels. Each θ_i is converged on an unknown value $(0 < \theta_i < 1)$. Therefore, the probability that a device's response satisfies a satisfaction level x_i in s_i rounds given the unknown probabilities θ_i is given as below.

$$p(s_1, .., s_k \mid \theta_1, .., \theta_k) = \frac{n!}{\prod_{i=1}^{k} s_i!} \prod_{i=1}^{k} \theta_i^{s_i} \tag{4}$$

Then, the posterior distribution of θ_i can be updated from the prior Dirichlet distribution in (2) and the likelihood in (4) according to Bayes' formula as below.

$$\begin{aligned} p(\theta_i \mid s_i) &= \frac{\frac{n!}{\prod_{i=1}^{k} s_i!} \prod_{i=1}^{k} \theta_i^{s_i} \frac{\Gamma(\sum_{i=1}^{k} \alpha_i)}{\prod_{i=1}^{k} \Gamma(\alpha_i)} \prod_{i=1}^{k} \theta_i^{\alpha_i - 1}}{\prod_{i=1}^{k} \int_0^1 \frac{n!}{\prod_{i=1}^{k} s_i!} \prod_{i=1}^{k} \theta_i^{s_i} \frac{\Gamma(\sum_{i=1}^{k} \alpha_i)}{\prod_{i=1}^{k} \Gamma(\alpha_i)} \prod_{i=1}^{k} \theta_i^{\alpha_i - 1} d\theta_i} \\ &= \frac{1}{\prod_{i=1}^{k} \int_0^1 \theta_i^{s_i + \alpha_i - 1} d\theta_i} \prod_{i=1}^{k} \theta_i^{s_i + \alpha_i - 1} \\ &= \frac{1}{B(s_i + \alpha_i)} \sum_{i=1}^{k} \theta_i^{s_i + \alpha_i - 1} \end{aligned} \tag{5}$$

The expression in (5) shows that the posterior distribution of θ_i has Dirichlet distribution with parameters $s_i + \alpha_i$. It can be seen that, when the outcome from the first C-R round occurs, the posterior distribution of θ_i has Dirichlet distribution with parameter $y_i + 1$ as its prior distribution is non-informative $\alpha_i = 1$, where y_i takes a value in $\{1, 0\}$. The estimation of θ_i in subsequent C-R rounds will take the previous posterior distribution of θ_i as the prior distribution. Updating from the prior distribution and the accumulated likelihood, the posterior distribution of θ_i after n rounds also has Dirichlet distribution with parameter $s_i + 1$ where s_i is given in (3).

As each θ_i is a probability variable, the posterior probability distribution density $p(\theta_i \mid s_i)$ represents the probability that θ_i has a specific value. Since the variable θ_i is continuous, the second order probability $p(\theta_i \mid s_i)$ for any given value of θ_i in $[0, 1]$ is very small and hence meaningless [12]. It is only meaningful to compute the posterior expected value of θ_i from its Dirichlet posterior distributionas below.

$$E(\theta_i \mid s_1, .., s_k) = \frac{1 + s_i}{k + \sum_{i=1}^{k} s_i} \tag{6}$$

In our model, we derive the uncertainty level in the device's behavior from posterior distribution of the probability vector Θ for capturing the trust degree of the device. We measure the uncertainty level based on the posterior expected value of θ_i and the weight value of each satisfaction level by using Shannon entropy [13]. Note that the purpose of using weight value is to prioritize the responses with high satisfaction levels in measuring trust value.

$$H = \sum_{i=1}^{k} -w_i E[\theta_i \mid s_1, .., s_k] \log_2 \left(w_i E[\theta_i \mid s_1, .., s_k]\right) \tag{7}$$

We also determine the *average value* of the posterior expected values of elements in vector Θ, called $\overline{\theta}$, as given in (8). This will be used as a factor to determine whether the trust level should be interpreted, from uncertainty level, to a trust or a distrust value.

$$\overline{\theta} = \sum_{i=1}^{k} w_i E[\theta_i \mid s_1, .., s_k] \tag{8}$$

C. Initial trust evaluation

Figure 1 shows the uncertainty level in the device's behavior in 3-dimensional space where the system defines three satisfaction levels with weight values of 0.3, 0.3 and 0.4, respectively. In fact, trust is an increasing function of the probability. Thus, it should be increased when the average value of posterior expected values of elements in vector Θ, $\overline{\theta}$, increases from 0 to 1. It is clear that the minimum uncertainty level is at 0 when one of the elements $E[\theta_i]$ is 1, i.e., there is certain that the device will provide a response with a given satisfaction level. For all other combinations of posterior expected values $E[\theta_i]$, the uncertainty level is spanned across the 3-dimensional space with values from 0 to a maximum value computed depending on the contribution of each $E[\theta_i]$.

We analyze the requirements for our initial trust evaluation from the uncertainty level. Firstly, at the maximum value of the uncertainty level, the trust value should be a neutral value indicating there is no trust or distrust can be decided. At the minimum uncertainty level, the trust value should be translated to a lowest or highest value in the trust scale. At any other values of the uncertainty level, depending on the average value $\overline{\theta}$, the trustworthiness of the device should be interpreted to some degree of trust or distrust considering the fact that trust is an increasing function of probability. If $\overline{\theta}$ is less than $1/k$, at which the distribution of θ_i is uniform leading to a neutral belief on the trustworthiness, the uncertainty level is translated to a distrust value. Otherwise, it is interpreted to a trust value.

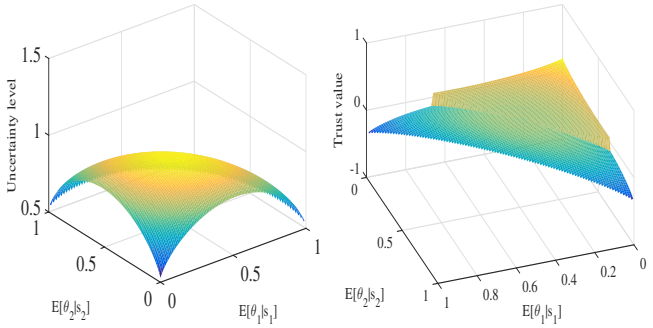

Fig. 1: Uncertainty level and Trust value with expected values $E[\theta_i]$ for 3 satisfaction levels

As $\overline{\theta}$ can be identical for many permutations of $E[\theta_i]$, we embed $(1 - \overline{\theta})$ and $\overline{\theta}$ to the trust interpretation in order to distinguish different response patterns. The using of factors $(1 - \overline{\theta}\ )$ and $\overline{\theta}$ is to ensure the consistent interpretation of the uncertainty level to the trust scale of $(-1, 1)$.

We use (9) to interpret trust value from the uncertainty level, where H_{max} is the maximum uncertainty value considering the number of satisfaction levels and their weight values. For instance, in a trust assessment model with three satisfaction levels, the maximum value H_{max} places at the peak area of the uncertainty level visualized in Fig. 1.

$$T = \begin{cases} (1 - \overline{\theta})(H - H_{max})\frac{1}{H_{max}}, & \text{if } 0 \leq \overline{\theta} \leq 1/k \\ \overline{\theta}(H_{max} - H)\frac{1}{H_{max}}, & \text{otherwise} \end{cases} \tag{9}$$

The mapping in (9) meets the discussed requirements. Figure 1 also illustrates the trust value in 3-dimensional space with a trust plane and a distrust plane. The trust level depicts a value representing a distrust value, a neutral value, or a trust value when the probability elements $(E[\theta_i])$ increase from 0 to 1. It should be noted that the trust values can be scaled up within the range $(-1, 1)$. It is important to set thresholds for the initial trust to ensure that the trust assessment process ends upon the established initial trust value reach a given threshold.

IV. Experimental evaluation

In this section, we present the evaluation of our proposed trust assessment model via simulation.

Experiment 1 In order to visualize the the posterior Dirichlet pdf, we first conduct an experiment that simulates the initial trust assessment with three satisfaction levels $(k = 3)$ in eight rounds $(n = 8)$. Three satisfaction levels can be mapped to unsatisfied, neutral, and satisfied opinion of the system about the devices response. We show how the Dirichlet pdf refines the investigated probability distribution when more observed responses are available. We also investigate how the average value of posterior expected values $E[\theta_i]$, the uncertainty level and the initial trust value change during the challenge-response process. The weight values for satisfaction levels are set at 0.05, 0.2 and 0.75, respectively. This experiment simulates a case that the device satisfies the challenger with level 1 in two first rounds, level 2 in two subsequent rounds and level 3 in the last four rounds.

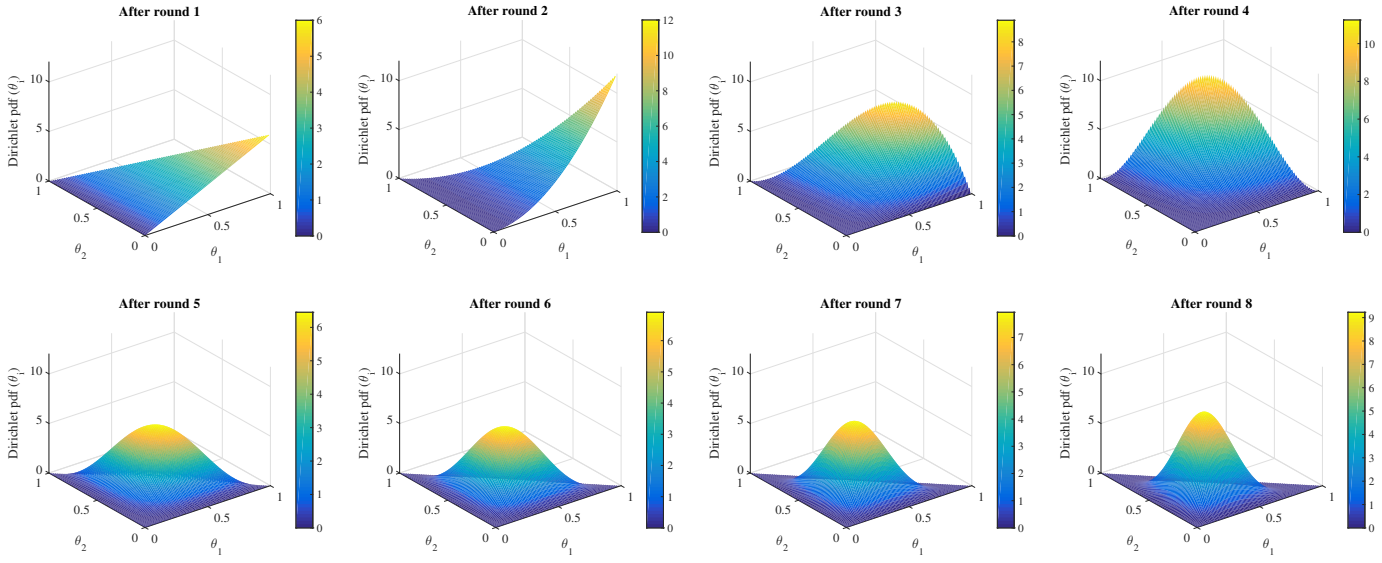

Fig. 2: The posterior Dirichlet pdf over 8 C-R rounds with pattern of satisfaction level in experiment 1

Figure 2 illustrates the changing in the shape of the posterior pdf with the probability vector $\{\theta_1, .., \theta_k\}$ and the parameter vector $\{s_1, .., s_k\}$ updated over the challenge-response process. It also shows how the maximum value of the pdf moves within the 3-dimensional space over eight rounds. After two first rounds, the shape of the pdf in 3-dimensional space is flat. It achieves the maximum value when θ_1 grows to 1 as the device provides a response with satisfaction level 1 in both rounds. The flat shape is narrower and gets higher maximum value after round 2 due to the more contribution of θ_1 to the density. Then, after rounds 3 and 4, the curve representing the posterior pdf has bell shape and moves towards the center of the space since θ_2 also contributes to the pdf and changes the parameters of the posterior Dirichlet distribution. When the device continuously provides response with the highest satisfaction level from round 5 to round 8, the curve is narrower due to the contribution of θ_3.

Figure 3 shows the changing of investigated metrics over eight rounds. As shown in Fig. 2, the posterior pdf curve is narrower when more responses are observed. It can be seen that the expected values of θ_i will be updated to new value according to the moving of the maximum area of the pdf curve. According to the setting of the weight values, the expected value associated with satisfaction level 3 (i.e., $E[\theta_3]$) contributes the most to the average value $\overline{\theta}$. During eight rounds, the average value is lower than 1/3, at which the distribution of θ_i is uniform indicating neutral belief, in the four first rounds and then getting higher than 1/3 in the four last rounds. The reason is during four last rounds there is contribution of the responses with satisfaction level 3 and its highest weight value to the computation of $\overline{\theta}$.

According to interpretation approach considering the average value of $E[\theta_i]$, the trust value in the four first rounds is interpreted to distrust value due to the unsatisfied responses. This trend is kept over round 5 and round 6 even though the device satisfies the system to highest level in these rounds due to the increasing in uncertainty level. Only after round 7, the trust value is recovered and slowly gets to the trust plane with a small value after four rounds of being satisfied the highest level and the reduction in uncertainty level. In particular, the trust value that the system places on the device first grows down to a distrust value at -0.09 and continuously decreases to -0.13 after two first rounds as the responses satisfy the lowest satisfaction level. The device gradually recovers its trustworthiness by providing more responses with highest satisfaction level and gets a small trust value of 0.04.

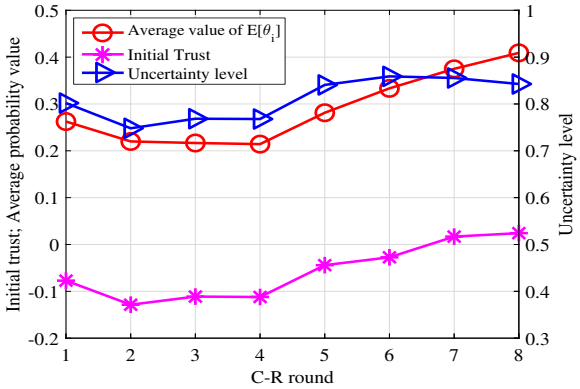

Fig. 3: Investigated values over 8 C-R rounds in experiment 1

Experiment 2 We then simulate a 5-round challenge-response-based trust assessment with five satisfaction levels. In practice, those levels can be mapped to extremely unsatisfied, unsatisfied, neutral, satisfied and extremely unsatisfied [10]. We present how investigated metrics change with various devices' response patterns. The weight values for satisfaction levels are 0.03, 0.07, 0.15, 0.25 and 0.5. It is worth noting that the optimal weight values vary with various applications.

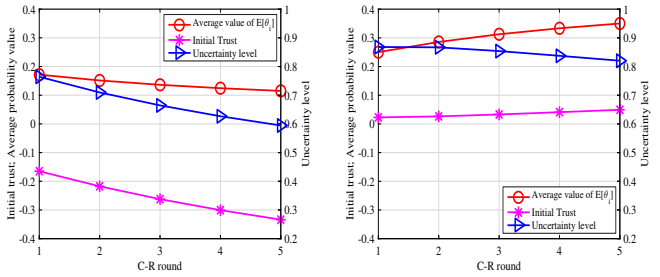

Fig. 4: Investigated values over 5 C-R rounds with (a) pattern of all satisfaction levels 1 (b) pattern of all satisfaction levels 5

Figure 4a the simulation results when the device's response is assigned satisfaction level 1 in all rounds. The average value of $E[\theta_i]$ continuously decreases and being below the value of 0.2 which indicates a neutral belief. The uncertainty level is continuously decreased over the simulation. The trust value is on the distrust plane and grows down from -0.14 to -0.32. This shows the consistency of our trust interpretation approach as it agrees with the trends of the changing of uncertainty level and the average probability value over the assessment.

Similarly, Fig. 4b presents the simulation results when the device responds with satisfaction level 5 in all rounds. The uncertainty level is reduced over five rounds. Since the average probability value is beyond 0.2 indicating the trust value should stay on the trust plane (as shown in Fig. 1). However, the trust is slowly gaining as we interpret trust in a way that the speed of gaining trust is less than the speed of losing trust. The trust value is increased from the neutral value to 0.05.

Figure 5a shows the simulation results of a case where two very unsatisfied responses in two first rounds are followed by a neutral response and two very satisfied responses in the two last rounds. Firstly, the trust level is on the distrust plane as the device's response does not satisfy the system over three first rounds. Then, the device recovers its trustworthiness to a small degree of trust (around 0.035) since its responses are assigned satisfaction level 5 in the two last rounds. Figure 5b shows the changing of investigated metrics for the case where the device's response only satisfies the system with level 4 at the first round and then be assigned low satisfaction levels for the rest of the assessment. The uncertainty level is consistently decreased indicating the more knowledge on the

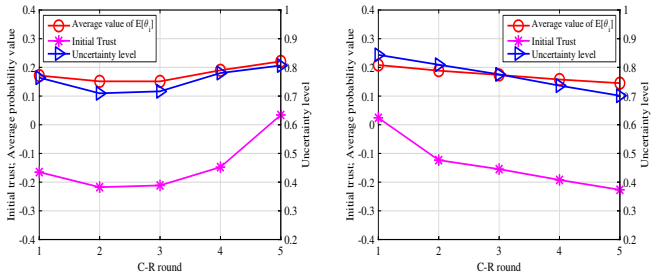

Fig. 5: Investigated values over 5 C-R rounds with (a) pattern of satisfaction levels 1-1-3-5-5 (b) pattern of satisfaction levels 4-2-2-1-1

trustworthiness of the device. As shown in Fig. 5b, the device is given a distrust value at -0.2 after five rounds of assessment due to its unsatisfactory behavior.

In summary, the trust value is aggregated over the challenge-response process, and it is considered as the initial trust value one the system stops the assessment, or the initial trust value reaches one of the predefined thresholds. Our estimation of the device's behavior through its uncertainty level and interpretation approach predicts the trust values consistently with respect to the response patterns with multi-level satisfaction.

V. Conclusion

This paper proposed a Dirichlet-based initial trust assessment model for personal space IoT systems. The system relies on the predefined multi-valued satisfaction level to judge the device's responses via a challenge-response process to collect the evidence for the trust evaluation. The posterior Dirichlet distribution is exploited as the mathematical foundation for measuring the uncertainty level in the device's behavior. Then, a trust interpretation approach is proposed to evaluate the initial trust value. The experimental results show that our proposed trust assessment model can consistently measure the trust degree of the device with various responses' patterns. For future work, we plan to investigate the challenge-response mechanism design considering multi-level of the system's satisfaction for a comprehensive initial trust assessment model.

References

[1] T. Nguyen, D. Hoang, and A. Seneviratne, "Challenge-response trust assessment model for personal space iot," in *2016 IEEE International Conference on Pervasive Computing and Communication (PerCom) Workshops*, 2016, pp. 1–6.

[2] T. Nguyen, D. Hoang, D. Nguyen, and A. Seneviratne, "Initial trust establishment for personal space iot systems," in *IEEE INFOCOM Workshops*, May 2017, pp. 1–6.

[3] H. Yu *et al.*, "A survey of trust and reputation management systems in wireless communications," *Proceedings of the IEEE*, vol. 98, no. 10, pp. 1755–1772, 2010.

[4] Y. Ben Saied *et al.*, "Trust management system design for the internet of things: A context-aware and multi-service approach," *Comput. Secur.*, vol. 39, pp. 351–365, 2013.

[5] I. R. Chen, J. Guo, and F. Bao, "Trust management for soa-based iot and its application to service composition," *IEEE Transactions on Services Computing*, vol. 9, no. 3, pp. 482–495, 2016.

[6] S. Ganeriwal *et al.*, "Reputation-based framework for high integrity sensor networks," *ACM Trans. Sen. Netw.*, vol. 4, no. 3, pp. 15:1–15:37, 2008.

[7] C. J. Fung *et al.*, "Dirichlet-based trust management for effective collaborative intrusion detection networks," *IEEE Transactions on Network and Service Management*, vol. 8, no. 2, pp. 79–91, 2011.

[8] K. Thirunarayan *et al.*, "Comparative trust management with applications: Bayesian approaches emphasis," *Future Gener. Comput. Syst.*, vol. 31, pp. 182–199, 2014.

[9] C. J. Fung *et al.*, "Quality of interaction among path computation elements for trust-aware inter-provider cooperation," in *IEEE ICC*, June 2014, pp. 677–682.

[10] A. Josang and J. Haller, "Dirichlet reputation systems," in *Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference on*, April 2007, pp. 112–119.

[11] Y. L. Sun *et al.*, "A trust evaluation framework in distributed networks: Vulnerability analysis and defense against attacks," in *Proceedings IEEE INFOCOM 2006. 25TH IEEE International Conference on Computer Communications*, 2006, pp. 1–13.

[12] A. Josang and R. Ismail, "The beta reputation system," in *In Proceedings of the 15th Bled Electronic Commerce Conference*, 2002.

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