Initial Trust Establishment for Personal Space IoT Systems

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

***Abstract*—Increasingly, trust has played a crucial role in the security of an IoT system from its inception to the end of its lifecycle. A device has to earn some level of trust even before it is authenticated for admission to the system. Furthermore, once the device is admitted to the system, it may behave maliciously over time; hence its behavior must be evaluated constantly in the form of trust to ensure the integrity of the system. Currently, no mechanism exists to establish an initial trust on a device, without prior knowledge, before its admission to an IoT system. Even when trust is applicable, trust evaluation models require direct/indirect observations over time, historical data on past encounters, or third party recommendations. However, this type of past data is not available in the first encounter between the system and the device. The question is how to establish whether a device can be trusted to a level that merits further evaluation for admission into a mobile and dynamic IoT system when it encounters the system for the first time? This paper addresses this challenge by proposing a challenge-response method and a trust assessment model to establish, without prior knowledge, the initial trust that a device places on another in a mobile and dynamic environment called personal space IoT. The initial trust is established before further interaction can take place and under the assumption that only a limited window of time is available for the trust assessment. The paper describes and evaluates the proposed model theoretically and by simulation. It also describes a practical scheme for realizing the proposed solution.**

I. Introduction

A personal space IoT system refers to a group of implanted and wearable devices providing services to a user, and other devices that are within the wireless communication radius of the users devices. In this system, a smartphone or a capability-comparable device acts as the centralized controller, managing of the space including admitting devices and monitoring their activities. As defined in [1], an IoT system can be modelled as a mobile entity whose constituents vary dynamically. Figure 1 illustrates the personal space IoTs where each circle represents one personal space IoT system.

The operation of an IoT system, particularly a personal space IoT system, mainly relies on the cooperation and interconnection among devices. In addition, the personal space IoT system often operates in a hostile environment where there is high density of malicious and intruders. Existing IoT systems rely on authentication approaches for establishing secure communications among devices [2]. However, during the operation phase, an authenticated device may behave maliciously over time by not cooperating with others, providing inaccurate data or poor services to gain its own benefits. Moreover, an authenticated device may deploy improper system teardown or decommission to cause damage afterward. In fact, trust has been used to monitor device's behavior and detect malicious device. In order to guarantee the integrity of the system, the device's behavior must be evaluated constantly in the form of trust not only from its admission to the system but also its entire lifecycle. Specifically, the device must establish some level of trust before it is authenticated for admission to the system. Furthermore, it also needs to keep on being a trustworthy member of the system. Relying on the initial trust level to admit devices is thus essential for creating a secure personal space IoT system and the trust assessment algorithm plays the crucial role in the process.

Currently, no existing work has yet attempted to provide a solution for establishing the initial trust on an entity, without prior knowledge and before its admission to the system. Several trust models proposed for IoT rely on trust evidences from direct/indirect observations over time, historical data in past encounters, or recommendations. However, such trust information is not available at the first encounter between the device and the IoT system. The proposed trust models only evaluate trust level of devices after they are admitted to the system. Therefore, a trust assessment model for establishing the initial trust on a device on its first encounter is needed.

The question is how to establish this initial trust on a device when the pre-knowledge about the device is not available at the first encounter? One view is that it is reasonable to place an initialized trust value equally to all devices. This assumption has been used in existing trust models which only assess trust degree of devices after a long operational period to detect the misbehaving devices [3]. However, the initialized value does not represent the real behavior of all devices. Another idea is that it is necessary to create the knowledge about

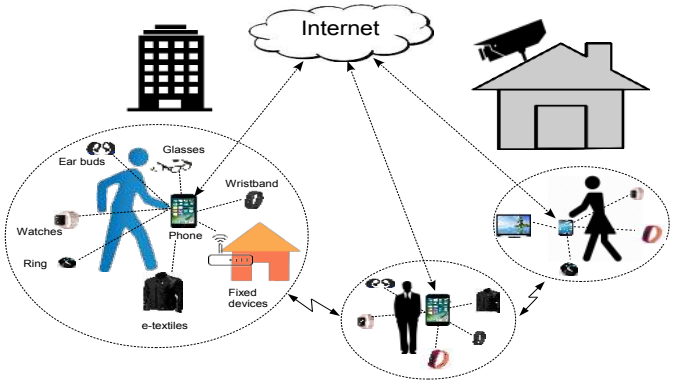

Fig. 1: The real world personal space IoTs

the device by assessing its behavior. A possible approach is to aggregate a committee to judge the trustworthiness of the device at the instance of its encounter with the system [4]. In the personal space IoT scenario, collective community judgment is not feasible and only a limited amount of time is available for establishing the initial trust. To overcome this obstacle, we propose a challenge-response method whereby the initial trust on a device is to be established by the controller through the uncertainty level of the device's behavior captured from challenge-response rounds. Although the challenge-response technique has been used in authentication methods [5], [6], their purposes are different from our challenge-response mechanism as they only verify the device's identity without concerning on trustworthiness of the device. To the best of our knowledge, we are the first to establish initial trust value on a device by utilizing the challenge-response mechanism during the first encounter of the device and the system.

In this paper, we propose a challenge-response-based initial trust assessment model to establish the initial trust level that a device places on another at their first encounter. The challenge-response mechanism is used to create the knowledge about the device by learning the uncertainty level in its behavior. The initial trust assessment model then relies on the results of the challenge-response process to assess if a device can be trusted to a level that can be used for its admission to the personal space IoT system. We extensively evaluate our proposed model theoretically and via simulation. Results show that the challenge-response mechanism can capture the behavior of the device properly. The initial trust assessment model allows a mobile and dynamic system to establish initial trust level on devices within a limited time period at the beginning of their first encounter. We also describe a realistic scheme for realizing the proposed solution.

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

II. Related work

Trust has increasingly played an important role in the security of an IoT system from its inception to the end of its lifecycle. In the literature, a number of trust management systems investigating computational trust models have been introduced in wireless networks and in the context of IoT [7]. In computational trust models, Bayesian approaches have been widely used in reputation systems to evaluate trust [8]–[11].

Ganeriwal et al. [9] introduced a classical beta reputation-based framework for sensor networks where nodes use reputation to evaluate other's trust level. In this work, a node estimates the reputation of other nodes based on their transactions over a period and reputation information recommended by its neighbors. By fitting the distribution of the node's reputation to Beta distribution, the authors define the trust level of a node as the statistic expectation value of the Beta probability density function (pdf) associated with its reputation.

In [11], a probabilistic trust management model is proposed based on the experience of previous interactions and recommendations. The trust value is influenced by the expectation value of the Beta distributed probability of a satisfactory interaction where the pre-knowledge about the number of previous satisfied and unsatisfied interactions from direct observations and recommendations are recorded. However, in this approach devices must keep lists of all historical interactions with others. Similarly, Chen et al. [8] proposed a trust management for service oriented architecture based IoT by adopting Bayesian framework as the underlying model for evaluating direct trust towards a service from user's experience. The trust value is the weighted combination of his satisfactory direct experience and recommendations from his friends. This work requires entities to maintain their past observations of all other entities in the system.

In [10], Sun et al. argued differently that uncertainty can be used as a measure of trust. The trust value can be calculated by determining the degree of uncertainty in the future action of an agent. When the direct observation is not available, the uncertainty is measured through concatenation and multipath propagation of recommendations. However, these techniques result in a degradation of trust value when it is propagated via a series of recommenders.

Our work differs from previous work as we introduce an initial trust assessment model which conducts a challenge-response process to establish initial trust on a device before it is admitted into a mobile and dynamic IoT system. We propose the challenge-response mechanism that allows device to generate the evidence for trust computation instead of waiting for the recommendations or actual interactions for a long period.

III. Challenge-Response-based Initial Trust Assessment Model

This section describes our proposed challenge-response-based initial trust assessment model. We first describe the challenge-response mechanism for evaluating the uncertainty level in a device's behavior that encounters the system for the first time. Then, we explain how the uncertainty level is measured from the results of the challenge-response process through information entropy. Finally, we present the translation of the uncertainty level to the initial trust value.

A. Challenge-response mechanism

The challenge-response mechanism is a process of creating knowledge about a device by investigating its behavior towards challenges. It is performed intentionally by the controller at the creation phase of a personal space IoT system to investigate the uncertainty level about a device's behavior. The process contains several challenges that the controller requests responses from a mobile/non-mobile device before its admission to the system. A challenge can be a request for the knowledge about the surrounding environment. It can be an action that the device must perform properly. The type

of challenges varies depending on the applications that the personal space IoT system supports or the environment where the system is operating.

Each challenge followed by a response can be considered as a challenge-response round. The result of a challenge-response round is either an expected response or an unexpected response provided by the device under testing. Once a round completed, the obtained result will be combined with previous results to form the knowledge about the device that is utilized to measure the uncertainty level in its behavior.

During the challenge-response process, the uncertainty level in a device's behavior is measured via information entropy. Then, the initial trust value that the controller places on the tested device will be computed from the uncertainty level. Now, the question is that given the results from the conducted challenge-response rounds, how to measure the uncertainty level in the device's behavior?

B. Uncertainty measurement

The base of uncertainty measurement is the probability. In our initial trust assessment model, the probability associated with the uncertainty level in a device's behavior refers to the probability that the device will behave as expected to a challenge, or equivalently the probability that the device provides an expected response to a challenge.

In [1] we proposed an approach to measure the uncertainty level through a conditional probability associated with the trust relationship between the controller and a device. The calculation of this conditional probability relies on the probability that a device is considered as an expected device given its response to a challenge and the probability that the controller trusts a response from this device. For a more feasible solution, in this paper we measure the uncertainty amount in a device's behavior through Bayesian analysis where the posterior model describes the distribution of the probability associated to the uncertainty measurement conditional on the results from the challenge-response mechanism.

Prior to any challenge-response rounds, the probability associated with the uncertainty level of a device's behavior is a random variable which is uniformly distributed over $[0, 1]$ as there is no pre-knowledge about the device's behavior. When the result from each challenge-response round occurs, this probability value could reasonably be distributed over a smaller scope as there is more evidence on how the device behaves to the challenge. The posterior distribution of this probability will be derived from the prior distribution and the results of the challenge-response process to reflect our new information about the device's behavior.

Let θ denote the probability associated with the uncertainty level in a device's behavior. To estimate the value of θ, we first assign a prior distribution to θ, $p(\theta)$, that is associated with the uncertainty in device's behavior before any challenge-response rounds. Initially, θ is an unknown parameter and equally likely to take all values between 0 and 1 inclusive. It is reasonable to take $p(\theta)$ from the Beta family which is defined as follows [8], [9], [12].

$$p(\theta) = \frac{1}{B(\alpha, \beta)} \theta^{(\alpha-1)} (1-\theta)^{(\beta-1)} \tag{1}$$

To represent the non-informative prior distribution of θ before any challenge-response rounds, we can choose parameters $\alpha = \beta = 1$.

The challenge-response rounds in our initial trust assessment model are considered as binary events with two possible outcomes. Let R denote the outcome from one round. Thus, R can take a value in $\{0, 1\}$ that reflects the unexpected response or expected response, respectively. In this paper, we design independent challenge-response rounds for estimating the value of θ. The probability that the outcome R will occur in each challenge-response round given the unknown probability θ can be expressed as follows.

$$p(R \mid \theta) = \theta^R (1-\theta)^{1-R} \tag{2}$$

Once a challenge-response round completed, the posterior distribution of θ can be updated by applying Bayes' theorem.

$$p(\theta \mid R) = \frac{p(R \mid \theta) p(\theta)}{\int_0^1 p(R \mid \theta) p(\theta) d\theta} \tag{3}$$

Replacing (1) and (2) to (3), the expression of the posterior distribution of θ becomes as below.

$$\begin{aligned} p(\theta \mid R) &= \frac{\theta^{\alpha+R-1}(1-\theta)^{\beta+1-R-1}}{\int_0^1 \theta^{\alpha+R-1}(1-\theta)^{\beta+1-R-1} d\theta} \\ &= \frac{\theta^{\alpha+R-1}(1-\theta)^{\beta+1-R-1}}{B(\alpha+R, \beta+1-R)} \end{aligned} \tag{4}$$

The expression in (4) shows that the posterior probability of θ has a $Beta$ distribution with parameters $(\alpha + R)$ and $(\beta + 1 - R)$ where α and β are parameters of the prior distribution before the current round takes place. It can be seen that, when the outcome from the first round occurs, the posterior distribution of θ has $Beta$ distribution with parameters $(1 + R)$ and $(1 + 1 - R)$ as its prior distribution is non-informative.

The estimation of θ in subsequent challenge-response rounds will take the previous updated posterior distribution of θ as the prior distribution. Updating from the prior distribution and the outcomes of the challenge-response rounds by the same way, the posterior distribution of θ after n rounds $p(\theta \mid R_1 R_2 \dots R_n)$ is again $Beta$ distribution with parameters $(1 + n\bar{R})$ and $(1 + n - n\bar{R})$ where $\bar{R} = \frac{1}{n}\sum_{i=1}^{n} R_i$ and $R_i \in \{0, 1\}$.

As θ is a probability variable, for a given θ the probability density $p(\theta \mid \bar{R})$ represents the probability that θ has a specific value. Since the variable θ is continuous, the second-order probability $p(\theta \mid \bar{R})$ for any given value of θ in $[0, 1]$ is very small and hence meaningless [12]. It is only meaningful to compute the posterior expectation value of θ:

$$E[\theta \mid \bar{R}] = \frac{n\bar{R} + 1}{n + 2} = \frac{1}{n+2} + \bar{R} \times (1 - \frac{2}{n+2}) \tag{5}$$

The form of posterior expectation value calculation in (5) shows that when we conduct a large number of challenge-response rounds, i.e., n grows very large, the posterior expectation value of θ mainly relies on the mean of observation results.

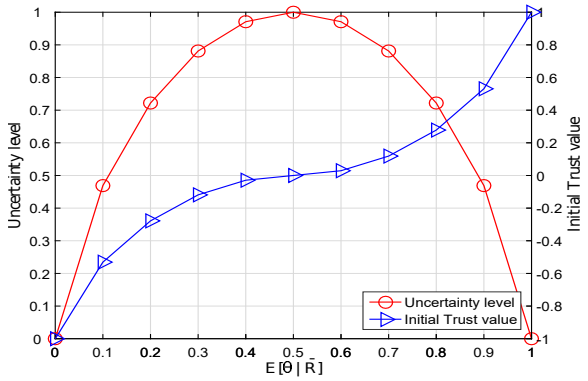

Fig. 2: Uncertainty measurement with associated probability

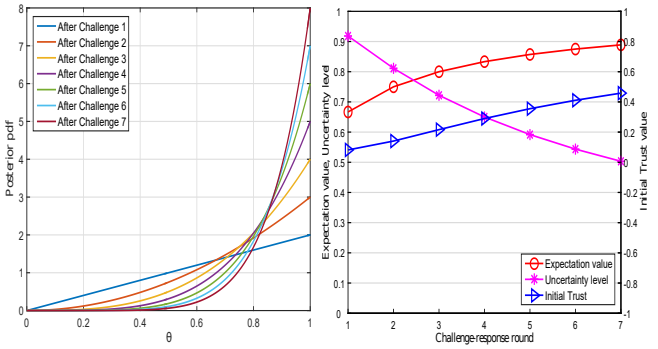

Fig. 3: Investigated values changing over 7 C-R rounds with all expected responses

Information theory states that entropy is a nature measure of uncertainty. We measure the uncertainty level in the device's behavior by using the Shannon entropy [13].

$$H(x) = -xlog_2(x) - (1-x)log_2(1-x) \tag{6}$$

where $x = E[\theta \mid \bar{R}]$ is the posterior expectation value of θ that represents the probability associated to the uncertainty level in device's behavior after a number of challenge-response rounds.

C. Initial trust computation

Figure 2 shows the uncertainty level in the device's behavior measured from the associated probability that refers to the posterior expectation value of θ, i.e., $E[\theta \mid \bar{R}]$, taking a value from $[0, 1]$. In fact, trust is an increasing function of the probability. Trust value should be increased when the probability that the device behaves as expected increases from 0 to 1.

In our trust model, the proportion of $(n\bar{R}+1)$ to $n+2$ decides the uncertainty level in the device's behavior. The maximum value of the uncertainty level about the device's behavior is at 1 when the device provides the expected responses and the unexpected responses equally. In this case, trust should be a neutral value to indicate that there is no trust or distrust places on this device. In addition, the uncertainty level reduces from 1 to 0 when the associated probability spreads far away from 0.5 towards 0 or 1. As the uncertainty level is a symmetric function of the probability, it reaches nearly 0 when either $n\bar{R}+1 \ll n+2$ or $n\bar{R}+1 \sim n+2$. The corresponding trust value should be interpreted to -1 which refers to a full distrust opinion places on the device that provided unexpected responses to all the challenges. In contrast, the trust value should be interpreted to 1 which indicates a complete trust opinion places on the device that behaved as expected in all the challenges.

To interpret the uncertainty level of the device's behavior to the trust value, (7) is used [10], where $x = E[\theta \mid \bar{R}]$.

$$T = \begin{cases} 1 - H(x), & \text{if } 0.5 \leq x \leq 1 \\ H(x) - 1, & \text{if } 0 \leq x < 0.5 \end{cases} \tag{7}$$

The mapping in (7) satisfies the requirements for the trust metric as discussed above. Figure 2 also illustrates our interpretation of uncertainty level to initial trust value with associated probabilities. The trust level depicts a value from the range of $[-1, 1]$ which can represent a full distrust, a less distrust, a neutral trust, a more trust or a complete trust opinion when the associated probability increases from 0 to 1.

It is important to end the initial trust assessment process within the creation phase of the personal space IoT system. We 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 Results

This section presents the evaluation of our proposed model via simulation and discusses the obtained results. To study fully the behavior of the proposed model and the impact of salient parameters under various circumstances, we will not impose the time limit or the number of iterations in the challenge-response (C-R) process in our investigation below.

In the experiment, we conduct a challenge-response process with seven C-R rounds where each new device will be tested with seven challenges by the controller. We investigate how the posterior pdf, expectation value of the associated probability, the corresponding uncertainty level and initial trust value change during the challenge-response process with various cases of device's responses.

Figures 3 shows the change of investigated values when a device provides expected responses to all challenges. The curve representing the posterior pdf has gradually shifted to the right side when more expected responses received from the device. The expectation value of the probability associated with device's behavior increases from 0.68 to 0.88 that leads to a reduction in the uncertainty level. The initial trust value increases from 0.1 to around 0.48 which refers to a trust opinion placed on the device because it provided good behavior consistently through challenge-response rounds. After the challenge-response process, the controller gains more knowledge concerning the device and places an initial trust value of 0.48 on the device.

Figure 4 presents the change of investigated values during the challenge-response process when a device provides unexpected responses to all challenges. Since the device behaved badly in all rounds, the posterior pdf has gradually shifted to the left side. Consequently, the expectation value of associated probability continuously reduces from 0.34 to 0.11. Thus, the

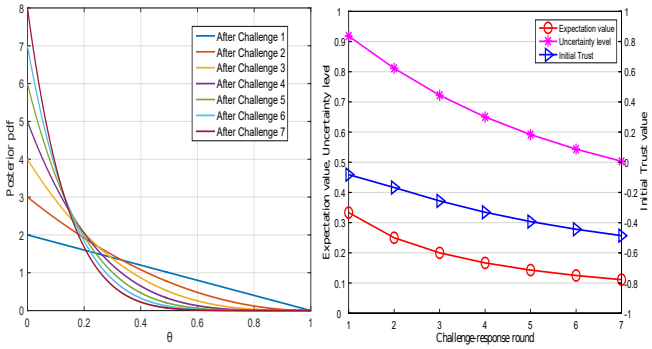

Fig. 4: Investigated values changing over 7 C-R rounds with all un-expected responses

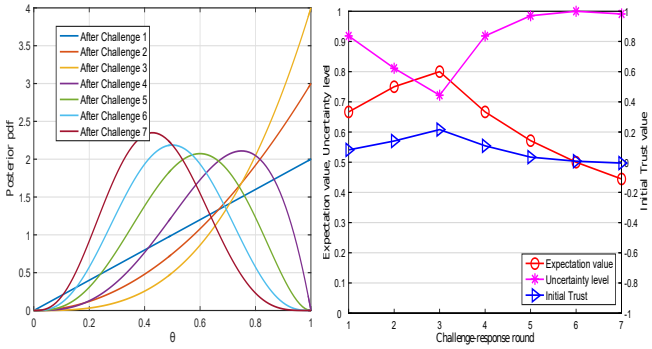

Fig. 5: Investigated values changing over 7 C-R rounds with three first expected responses followed by unexpected responses

corresponding measured uncertainty level reduces to around 0.5. Although the uncertainty level measured in this case is similar to that in the first case, the initial trust value is interpreted to -0.48 which refers to a distrust opinion placed on the device because it continuously provided bad behavior.

Figure 5 summarizes the change of investigated values during the experiment when a device provides expected responses at three first challenges and unexpected responses at subsequent challenges. The uncertainty level reduces over three first rounds and increases again to a very high value when the device provides bad behavior at the subsequent rounds. The corresponding initial trust value increases from a neutral value to 0.2 in three first rounds and drops to a neutral value as the device does not provide good behavior consistently.

Figure 6 illustrates the change of investigated values in case a device provides unexpected responses to two first challenges and expected responses to subsequent challenges. It can be seen that the curve of the posterior pdf is narrower and shifted to the right side and the expectation value reduces in two first rounds and increases over five subsequent rounds. The initial trust value drops to -0.5 which refers to a distrust opinion over two first rounds as the device provided unexpected responses. Although the device provides expected responses in the five subsequent challenges, the initial trust value increases to a small trust value at 0.07. This indicates that the controller only establishes a low trust level on this device.

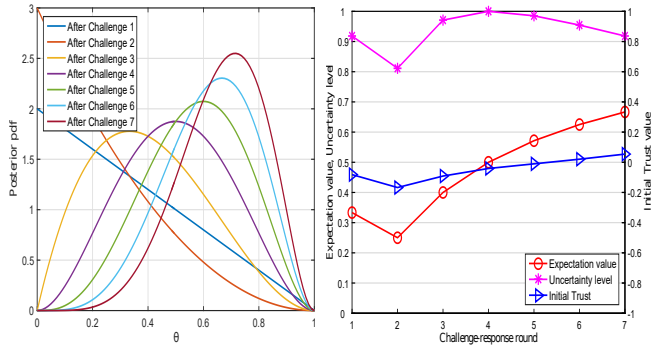

Fig. 6: Investigated values changing over 7 C-R rounds with two first unexpected response followed by expected responses

In summary, the results show that our challenge-response mechanism learns the device's behavior effectively. Based on this knowledge, the controller places an initial *trust opinion* on devices that behaved as expected consistently to the challenges.

V. Practical Realization

In this section, we describe a practical realization of our proposed solution to a personal space IoT system. Note that our initial trust assessment model relies on the results from the challenge-response process at the creation phase of the personal space IoT system where devices encounter the system for the first time. The challenge-response process is conducted during the first encounter of devices and the system by deploying interactions between devices and the controller.

In a practical personal space IoT system, the controller discovers nearby devices and admits devices that are suited to the system's requirements by establishing secure connections with them during the initial phase. The number of interactions between a device and the controller during their first encounter depends on the underlying communication technology used by the devices. The devices in personal space IoT system generally use Bluetooth Low Energy (BLE) or other short-range communication technologies for its communication with each other. Without loss of generality, we analyze the device's interactions during the creation phase of a personal space IoT system, where devices are connected and communicated with one another via BLE, to realize the practical implementation of our proposed solution.

Generally, BLE devices discover others during a discovery phase and establish secure connection with others through a pairing process. Figure 7 illustrates typical interactions between a controller and a device via BLE during their connection establishment at their first encounter. During the discovery phase, there are several interactions between devices for exchanging their identities and additional information such as the device type, service, manufacturer information, etc., through advertising, scan request and scan response packets. The devices participate in a pairing process when one of them initiates a connection request packet. During the pairing process, two devices exchange information of their input/output capabilities, random numbers and confirmation values for the authentication purpose. Note that, in BLE the "LE legacy

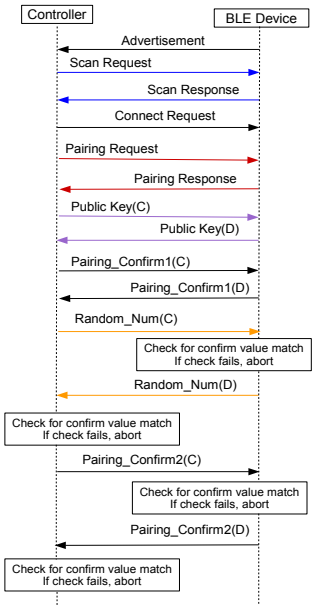

Fig. 7: BLE device's interactions during connection establishment

pairing" or "LE secure connection pairing" model can be used. In Figure 7, the *LE secure connection pairing* model is used. There are six pairs of interactions between two devices during their first encounter before they confirm whether the peer device is authenticated.

In BLE, the information exchanging over the pairing process is transferred in plain-text, except for the confirmation values which are outputs of AES-based functions. It is reasonable to add challenge and response information into packets that carry the plain-text information exchanging over the discovery and pairing processes. In fact, custom information can be included to advertising packets in BLE before establishing a connection. Beacons are implementation of using advertisements with BLE for simple information broadcast [14], [15]

For the example shown in Figure 7, our challenge-response process utilizes at least four pairs of interactions that exchange information in plain-text to conduct four challenge-response rounds (all arrows except for black ones represents the interactions will be used for challenge-response rounds). The number of rounds may increase if more than one pair of scan request and scan response packets are exchanged. It is clear that our challenge-response method can be conducted during the discovery and connection establishment phase, where devices encounter the system and establish a connection with each other, and before device is authenticated. Beacons are deployed for exchanging challenge-response information. Before authentication, the controller establishes the initial trust level on the testing device and decides if it is trusted to a certain level that can be used to support its admission to the system.

In fact, the possible interactions between two devices during the creation phase of the system might be insufficient for the challenge-response process to establish an initial trust on a device. To deal with the limited number of interactions, we design an efficient compression or encoding approach whereby multiple binary responses can be derived from a single challenge-response result. Investigating efficient encoding techniques for this purpose is underway.

VI. Conclusion

This paper proposed a challenge-response-based initial trust assessment model for personal space IoT systems. The proposed trust assessment model relies on the results from a challenge-response mechanism conducted at the initial stage of the system to measure uncertainty level in the device's behavior and then interpret it to initial trust value. The experimental results show that our proposed challenge-response mechanism can estimate effectively the uncertainty of a device's behavior. Realization shows that the challenge-response method fits nicely to possible interactions between devices during their first encounter. For future research, we are investigating the multi-level trust for establishing initial trust on a device. We plan to develop a trust assessment framework that combines the proposed initial trust model with existing models to investigate trust level of entities throughout the system's lifecycle.

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] J. L. Hernndez-Ramos *et al.*, "Toward a lightweight authentication and authorization framework for smart objects," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 4, pp. 690–702, 2015.

[3] 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.

[4] W. Sherchan, S. Nepal, and C. Paris, "A survey of trust in social networks," *ACM Comput. Surv.*, vol. 45, no. 4, pp. 47:1–47:33, Aug. 2013.

[5] Y. Gao *et al.*, "Obfuscated challenge-response: A secure lightweight authentication mechanism for puf-based pervasive devices," in *2016 IEEE International Conference on Pervasive Computing and Communication (PerCom) Workshops*, 2016, pp. 1–6.

[6] X. Du *et al.*, "Physical layer challenge-response authentication in wireless networks with relay," in *IEEE INFOCOM*, 2014, pp. 1276–1284.

[7] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for internet of things," *Journal of Network and Computer Applications*, vol. 42, pp. 120 – 134, 2014.

[8] 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.

[9] 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.

[10] 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.

[11] M. K. Denko and T. Sun, "Probabilistic trust management in pervasive computing," in *2008 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing*, vol. 2, 2008, pp. 610–615.

[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.

[14] Apple-Inc. ibeacon for developers. [Online]. Available: https://developer.apple.com/ibeacon/

[15] Texas-Instruments-Incorporated. Bluetooth low energy beacons. [Online]. Available: www.ti.com/lit/pdf/swra475