Exploring Challenge-Response Mechanism Designs for IoT Initial Trust Establishment

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*—More than ever, with the proliferation of IoT devices interconnected by 5G networks, it is crucial that IoT devices and subsystems are protected from being compromised and deployed for security attacks. Trust has been playing an essential role in admitting an IoT device into a 5G system. However, trust evaluation usually relies on historical interactions and recommendations which are often not available at the first encounter of the device and the system. As demonstrated in our previous studies, the challenge-response mechanism is an effective approach to learn the device's behavior and build the knowledge about its trustworthiness when prior knowledge is limited. It is essential to design the challenge-response mechanism with the intention of revealing the relevant and reliable information about the trustworthiness of IoT devices. The question is how to design the challenge and the common knowledge between the system (challenger) and the devices (respondents) so that the design engineers the devices to reveal their trustworthiness. This paper tackles this question by exploring challenge-response mechanism designs for the initial trust establishment in a mobile and dynamic environment called personal space IoT system. The paper develops principles for workable and consistent designs. Extensive simulations are conducted to consolidate the principles with numerous designs.**

I. Introduction

The personal space IoT system introduced in our earlier work [1], [2] refers to a group of user's devices, and other IoT devices that are within the wireless communication radius of the user's devices and likely to provide services to the user. A more powerful device acts as a controller for admitting devices and monitoring their activities. Admitted devices of the IoT subsystem, subsequently the supporting 5G networks and applications, usually capture, process and communicate personal data within the subsystem and with the external entities to provide services. Moreover, the personal space IoT system often deploys in a less secure environment. It is thus essential for the system to safeguard and manage the devices' behavior from their inception to the end of their lifecycle.

Trust has played a crucial role in enhancing the security of IoT systems such as minimizing the ricks of insider attacks by detecting and isolating misbehaving admitted devices. To guarantee the integrity of IoT systems, the devices' behavior must constantly be evaluated in the form of trust not only from their admission to the system but also entire their lifecycle. Specifically, the device must establish some level of trust before it is authenticated with the system for further interactions. Thus, an initial trust establishment procedure, conducting before the device is authenticated, is essential for IoT systems when making decision on admitting new devices.

Currently, proposed trust evaluation schemes primarily rely on the previous interactions and recommendations [3]–[6]. These methods work effectively on detecting misbehaving authenticated devices in the system based on the above resources. However, the prior resources for the initial trust evaluation are often not available. Therefore, a mechanism for building the knowledge about the trustees (new devices) for the initial trust establishment is essential.

In our earlier studies [1], [2], we proposed a challenge-response mechanism and a trust assessment scheme to evaluate initial trust level of a device. To make the trust assessment work, an implicit relationship between the information content of challenges and the knowledge of the devices conveyed in the responses is assumed. In this paper, we propose the mechanism design for the challenge-response and explore possible designs to develop guiding principles for workable designs so that there exists the relationship between the challenges and the devices' knowledge. The purpose of the mechanism design is to allow the initial trust assessment scheme to consistently determine the initial trust level of a device by conducting challenge-response operations with given workable designs.

Our challenge-response mechanism design consists of a set of challenges and a set of possible responses to each challenge. According to Shannon [7], the information content of a challenge in our design depends upon its probability of occurrence. To design the information content of the challenges, we focus on designing their probability distribution. In addition, the relationship between the challenge and the devices' knowledge is reflected by the probability of the responses conditioned on the given challenge. Therefore, we also design the conditional probability distribution of the responses given a challenge so that there always exists a correlation between the challenge and the response, or equivalently the target devices' knowledge. No useful outcome from the challenge-response operation is achieved if the devices are ignorant (uncorrelated) of the challenges making it meaningless for the initial trust assessment. The question is how to design these probability distributions that represent the consistent correlation between the challenge and the device's response.

In this paper, we propose a probabilistic design of the challenge-response mechanism. Next, we introduce our definition of the correlation between a challenge and a response and the desired characteristics of a workable design for the challenge-response mechanism. We then develop guiding principles and demonstrate their feasibility in identifying workable designs for the challenge-response mechanism. We also investigate the initial trust establishment procedure using our challenge-response mechanism design via simulation. Simulation results show that the challenge-response mechanism designs established with developed principles allow the

challenge-response-based initial trust establishment to consistently determine the initial trust level of new devices before making decision on admitting a device.

The rest of the paper is organized as follows. Section II gives an overview of our proposed challenge-response mechanism. Section III describes the challenge-response mechanism design. Section IV develops guiding principles for the mechanism design. Section V presents the evaluation of our proposed mechanism design. Section VI concludes the paper and outlines our future work.

II. Challenge-Response Mechanism

Previous trust-related research studies have been mainly investigated the trust of admitted entities during the system's ongoing operation. To the best of our knowledge, no related work has yet attempted to provide a solution for establishing the initial trust on an entity before it is admitted to the system without prior knowledge. This section provides an overview of our proposed challenge-response mechanism for establishing initial trust of IoT device before its admission to the system.

Our proposed challenge-response (C-R) mechanism [2] is a process of collecting evidence/knowledge for the initial trust assessment scheme. It is performed intentionally by the controller at the first encounter between the system and an unknown device to investigate the device's behavior and then use this knowledge for the trust evaluation before deciding on whether to admit it into the system. The C-R mechanism is accomplished by exploiting typical interactions between the controller and the devices at their first encounter such as in the pairing process in Bluetooth Low Energy protocol as indicated in our previous work [2].

In fact, the challenge-response scheme has been used in various existing authentication approaches [8], [9] where a party must provide a valid response to a challenge from another party to be authenticated. The valid response can only be generated by using an algorithm known by both parties. However, our C-R mechanism aims at generating the knowledge about unknown entities which have first encountered the system. It does not require a prior shared secret or a known algorithm between the challenger and the respondent which is usually not feasible at the first encounter.

Our proposed C-R mechanism purely provides the process of collecting the trust knowledge based on a set of challenges and a set of responses. However, the information content of the challenges and the relationship between the challenge and the response is implicitly assumed and never investigated.

III. Design of Challenge-Response Mechanism

A. The Probabilistic Design

In our challenge-response design, following the mechanism design in game theory [10], we design the challenge-response through which gets the respondent playing strategies that end up implementing exactly what the system intended. The purpose of designing the challenge-response mechanism is to maximize the knowledge about the truthfulness of respondents. For the desired knowledge, two design elements are necessary *i*) the information content of the challenges appropriate for the potential respondents and *ii*) the relationship between the challenge and the knowledge of respondents. The first element is related to intention of the challenge-response process and the second element is related to the assumed correlation between the targeted response space and the challenge space. The ultimate aim of the challenge-response mechanism is to lead the respondents providing relevant information about its trustworthiness. No useful outcome is achieved if the respondents are ignorant (uncorrelated) of the challenges.

We assume that the mechanism design consists of a set of n challenges and a set of m responses corresponding to each challenge. A challenge is considered as a random variable with a probability of occurrence which determines the information content of the challenge. Let C denote the random variable which can take on a value c_i ($i = 1..n$), referring to a challenge in the challenge set. To design the information content of the challenge which must be appropriate for potential respondents, we design a probability distribution $P(C)$. Also, let R denote the random variable which can take on a value r_j ($j = 1..m$) referring to a possible response in the response set. To reflect the relationship between the challenge and the knowledge of potential respondents, we design a conditional probability distribution $P(R|C)$ defining the probability of occurrence of a response conditioned on a given challenge.

The main focus of this work is designing the two probability distributions $P(C)$ and $P(R|C)$ of the challenge-response mechanism so that it is workable and consistent for the initial trust establishment. The design of probability distributions is meaningless if they do not reflect the desired relationship between the challenge and the knowledge of potential respondents. The question is to what extent the probabilistic-based challenge-response design is workable for the initial trust assessment. The following section introduces our definition of correlation measure and desired characteristics of a workable challenge-response mechanism design.

B. Workable Challenge-Response Design

Correlation definition In our design, the measure of information content of a challenge c_i is defined by following Shannon's definition [7].

$$I(c_i) = -\log_2(p(c_i)) \tag{1}$$

In a challenge-response operation, given that the response r_j occurs, to determine the correlation between the given challenge and the received response, we work out the probability that the challenge was c_i. It is given by Bayes' formula.

$$p(c_i|r_j) = \frac{p(r_j|c_i)p(c_i)}{\sum_{k=1}^{n} p(r_j|c_k)p(c_k)} \tag{2}$$

Thus, given that a response r_j occurred in a challenge-response operation, the information content of the event that the challenge was c_i, can be derived as in (3).

$$I(c_i|r_j) = -\log_2(p(c_i|r_j)) \tag{3}$$

We define the correlation between a challenge c_i and a response r_j as the difference between the information content of c_i and the information content one learns that the challenge was c_i when he knows the response occurred in the challenge-response operation is r_j. It is denoted by Δ_{ij} in (4).

$$\Delta_{ij} = I(c_i) - I(c_i|r_j) \tag{4}$$

As defined in (4), the correlation value between a challenge and a response can be a positive value representing the occurrence of a related response, a negative or zero value referring the occurrence of an uncorrelated response. The scale of the correlation depends on the difference between the two information content values. Note that the information content of an event is equivalent to the surprise that one has when he learns about the occurrence of the event [7]. In our design, a positive correlation is expected when the response r_j is favorable/relevant to the challenge c_i so that the occurrence of this response brings additional knowledge about the challenge c_i. Thus, knowing r_j will reduce the information content (surprise) one learns that the challenge was c_i. On the contrary, a non-positive correlation value is desired when knowing the occurrence of the response r_j, the surprise one has when he learns that the challenge was c_i is not changed or even increased compared to that before knowing r_j.

By replacing (1), (2) and (3) to (4), we can determine the conditions for a positive correlation as in (5).

$$\begin{aligned} \Delta_{ij} &= -\log_2(p(c_i)) + \log_2(p(c_i|r_j)) > 0 \\ &\Leftrightarrow p(r_j|c_i)(1-p(c_i)) > \sum_{k=1,k\neq i}^{n} p(r_j|c_k)p(c_k) \end{aligned} \quad (5)$$

Characteristics of a workable design Our probabilistic design of the challenge-response mechanism defines the relationship between the challenge set and the response set. A workable design needs to reflect the relationship between the challenge and the knowledge of the respondents so that there is a consistent correlation between each challenge and its responses. Specifically, the workable design must allow the challenger to distinguish the favorable response from other responses via their correlation measures. It is expected that a positive correlation is given between each challenge and its favorable response. Other responses are unintended and given a non-positive correlation with the challenge. As a result, the probabilistic design of the workable challenge-response mechanism must maintain a *consistent correlation measure* to all possible pairs of a challenge and a response.

According to information theory, learning about an unlikely event's occurrence is more informative than learning about the occurrence of a more likely event. For a challenge-response operation, when a highly unpredictable challenge is used to judge the respondent, it is expected that the knowledge learned from the response towards this challenge is more informative than that from the response towards other more predictable challenges. Therefore, in the C-R mechanism design, the relationship between the challenge and the response must also weight higher *priority of the correlation* associated with the highly unpredictable challenge over the more likely challenges when placing a trust level to the respondent.

In summary, a design of challenge-response mechanism is workable for the initial trust establishment only when it has such desired characteristics. Next section explores the conditions and establishes the principles for workable designs.

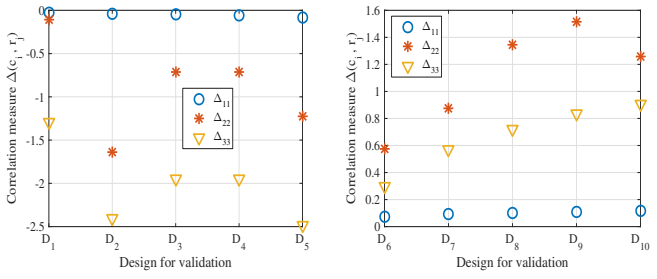
IV. Principles of the Challenge-Response Mechanism Design

In this section, we first demonstrate that without any principle, a challenge-response design is just an ad hoc process and is unlikely to achieve its goal of creating meaningful knowledge for an initial trust assessment scheme. We then develop guiding principles of our mechanism design and validate the feasibility of the defined principles.

A. Mechanism Design without Principles

The challenge-response mechanism design to be validated consists of a set of three challenges, c_1, c_2, and c_3 and a set of four responses, r_1, r_2, r_3, and r_4. We investigated designs without any principles with a given $P(C) = \{0.7, 0.2, 0.1\}$. By challenging the potential respondents with each challenge c_1, c_2, c_3, the challenger expects to receive favorable response r_1, r_2, and r_3, respectively. Specifically, given challenge c_1, if the respondent returns response r_1, a positive correlation is reasonable and desired. Otherwise, a non-positive correlation is expected. The similar expectation is for challenges c_2 and c_3. We assess if there are combinations of $P(C)$ and $P(R|C)$ designed without any principles, that do not provide characteristics of a workable design.

Without any principles, many designs do not provide consistent correlation measure. For example, Fig. 1a presents the inconsistent correlation measures between each challenge and its favorable response in designs D_1 to D_5. In all presented designs, the correlation measures between each challenge and its favorable response $(\Delta_{11}, \Delta_{22}, \Delta_{33})$ are negative which violate the first characteristic of a workable design.

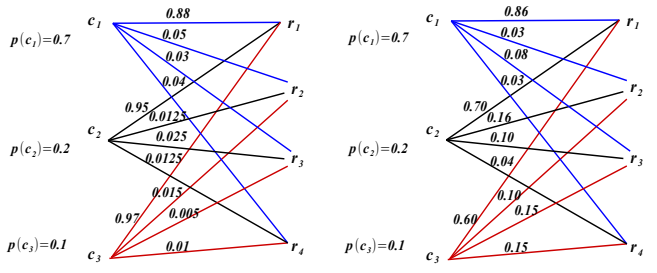


(a) (b)

Fig. 1: Designs without principles provide (a) negative correlation between each challenge and its favorable response (b) no prioritization of correlation

The reason for this violation can be explained as follows. As designed, response r_i is related to all challenges with different conditional probabilities. Therefore, when r_i is designed as the favorable response to challenge c_i, the design of $p(r_i|c_i)$ and other $p(r_i|c_k)$ decides the direction of the correlation. It can be seen that when the relation of $r_i j$ with challenge c_i is weaker than that of r_i with other c_k, i.e., $(p(r_i|c_i) < p(r_i|c_k), \forall k \neq i)$, the condition in (5) is violated leading to a non-positive correlation. For instance, with the design D_2 described in Fig. 2a, for any pair of each challenge and its favorable response, $p(r_i|c_i)$ is always smaller than other $p(r_i|c_k)$. This implies that the response r_i has a weak relation with the challenge c_i. Moreover, it has stronger relations with other challenges with higher probabilities. Such designs do not meet the condition in (5) which results in a negative correlation between each challenge and its favorable response.

Although many other designs (without principles) built with consistent correlation for a workable design, they are not built with the desired priority of correlation. Specifically, the size



(a) Design D_2 (b) Design D_8

Fig. 2: Example of probabilistic design of validated designs

of correlation between challenge c_3 and its favorable response is expected to be the largest since c_3 is the most unpredictable challenge. However, as represented in Fig. 1b, with validated designs (D_6 to D_{10}), the correlation between challenge c_3 and its favorable response is less than the correlation between challenge c_2 and its favorable response.

This violation can also be explained as follows. Each challenge is spread out to all possible responses with different conditional probabilities. The distribution of those conditional probabilities and the unpredictability of a challenge directly affect the size of the correlation. It implies the importance of designing the ratio among conditional probability distributions and the ratio among the unpredictability of challenges so that the correlation measure is inversely proportional to the unpredictability of the challenge. Figure 2b describes D_8 in which the ratio between conditional probability distribution $p(r_j|c_2)$ and $p(r_j|c_3)$ $(\forall j = 1..4)$, and the ratio between $p(c_2)$ and $p(c_3)$ are not designed carefully. Hence, the size of correlation associated with c_3 and its favorable response is less than that of c_2 while c_3 is more unpredictable than c_2.

Many designs established without any principles do not have desired characteristics for a workable challenge-response mechanism for the initial trust assessment. Therefore, it is essential to establish principles of the challenge-response mechanism design towards a consistent trust assessment model.

B. Principles of the Challenge-Response Mechanism Design

As demonstrated earlier, the challenge-response mechanism should be designed with guiding principles so that it is built with desired characteristics of a workable design. From the desired features of a workable challenge-response design, we develop principles of our mechanism design as below.

Consistent correlation: Correlation measure associated with each challenge and its favorable response is positive; otherwise, it is non-positive.

The condition entailed in this principle is as below.

$$\begin{cases} \Delta_{ij} > 0, & \text{if } r_j \text{ is favorable response of } c_i, \forall i, j \\ \Delta_{ij} \leq 0, & \text{otherwise} \end{cases} \quad (6)$$

Prioritization of correlation of highly unpredictable challenge over other challenges: Correlation between a challenge and its favorable response is inversely proportional to the challenge's unpredictability.

The condition entailed in this principle is given by (3) where r_k, r_t are favorable responses of c_i, c_j, respectively.

$$\Delta_{ik} > \Delta_{jt}, \qquad \forall i, j \ \& \ p(c_i) < p(c_j) \quad (7)$$

C. Validation of Established Principles

This section validates the feasibility of the defined principles of our mechanism design. We show that for a design of $P(C)$, by establishing our defined principles, there always exist a number of configurations of $P(R|C)$ so that the combinations of $P(C)$ and $P(R|C)$ are workable for the challenge-response operation. Given a found workable design, we determine the boundary of its parameters (probabilities) so that modifying the parameters within their boundaries, designs with new parameters are still workable. On the other hand, when any modified parameters are exceeded identified boundaries, designs with these parameters are unworkable.

We follow the defined principles to find workable designs. Specifically, we generate the conditions entailed with the principles and use them as the constraints to search for the workable designs. With a found workable design, we determine the boundaries for its parameters by simultaneously increasing or decreasing parameters by a predefined value.

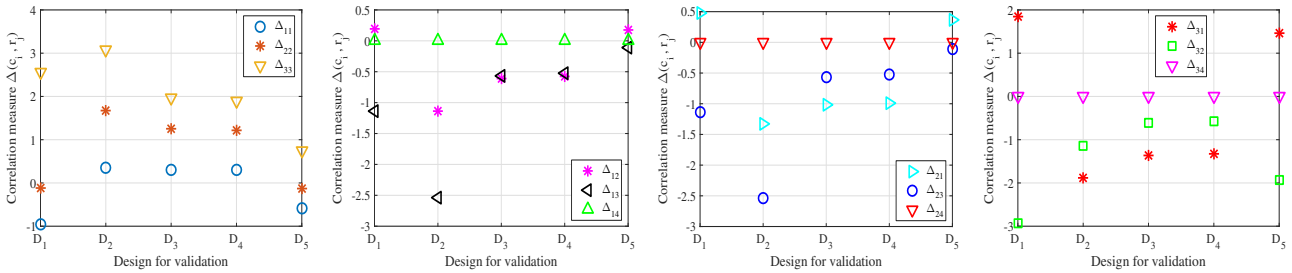
TABLE I: Workable designs (D_2, D_3, D_4) and unworkable designs (D_1, D_5) with $P(C)$ of $\{0.7; 0.2; 0.1\}$

$Design$	$p(r_j\|c_1)(\forall j = 1..4)$	$p(r_j\|c_2)(\forall j = 1..4)$	$p(r_j\|c_3)(\forall j = 1..4)$
D_1	$0.07; 0.61; 0.01; 0.31$	$0.19; 0.49; 0.01; 0.31$	$0.49; 0.07; 0.13; 0.31$
D_2	$0.61; 0.07; 0.01; 0.31$	$0.19; 0.49; 0.01; 0.31$	$0.13; 0.07; 0.49; 0.31$
D_3	$0.70; 0.16; 0.10; 0.04$	$0.28; 0.58; 0.10; 0.04$	$0.22; 0.16; 0.58; 0.04$
D_4	$0.71; 0.17; 0.11; 0.01$	$0.29; 0.59; 0.11; 0.01$	$0.23; 0.17; 0.59; 0.01$
D_5	$0.15; 0.73; 0.11; 0.01$	$0.29; 0.59; 0.11; 0.01$	$0.62; 0.17; 0.20; 0.01$

To show the feasibility of our defined principles, we present designs for several configurations of $P(C)$ with three challenges. We assume that there are four possible responses to each challenge. Moreover, it is supposed that the favorable response to each challenge is given with the same label with the respective challenge.

Tables I and II present the probabilistic designs of a found workable design D_3, two workable designs at the boundaries (D_2 and D_4) and two unworkable designs (D_1 and D_5), with the $P(C)$ of $\{0.7, 0.2, 0.1\}$ and $\{0.05, 015, 0.8\}$, respectively. In Table I, for a workable design described in D_3, we determine the boundaries of $p(r_j|c_i)$, $(j = 1..3)$, by simultaneously increasing or decreasing them by 0.01 until the principles are violated. The value of $p(r_4|c_i)$ is the subtraction of 1 and other $p(r_j|c_i)$. The results show that there are 11 workable designs within the boundaries. The boundaries are the parameters described in designs D_2 and D_4. For example, the boundaries for $p(r_1|c_1)$ is from 0.61 to 0.71, $p(r_1|c_2)$ is from 0.19 to 0.29, etc. If any parameter in a design is beyond its boundary found at D_2 and D_4, it becomes unworkable as the principles are no longer satisfied. For instance, in D_1 and D_5, $p(r_1|c_1)$ is 0.07 and 0.15, respectively, which exceeds the boundary. Hence, the first principle is not guaranteed.

Figure 3 presents the correlation measures from designs whose parameters are described in Table I. As shown in Fig. 3a, with designs D_2, D_3 and D_4 the correlation between any challenge and its favorable response is always positive, whereas with designs D_1 and D_5, only correlation measure between challenge c_3 and its favorable response is positive. In addition, with designs D_2, D_3, D_4, the size of correlation between challenge c_3 and its favorable response is always



(a) (b) (c) (d)

Fig. 3: Correlation measures from designs within the boundaries and beyond the boundaries with given P(C) of $\{0.7, 0.2, 0.1\}$

the largest which satisfies the prioritization of correlation of the most unpredictable challenge. As indicated in the Figs. 3b - 3d correlation measures between challenge c_1, c_2, c_3 and the responses other than their favorable response are always non-positive with designs D_2, D_3, and D_4. In contrast, with designs D_1 and D_5, there always exist some positive correlation measures where the non-positive is expected.

TABLE II: Workable designs (D_2, D_3, D_4) and unworkable designs (D_1, D_5) with $P(C)$ of $\{0.05; 0.15; 0.8\}$

$Design$	$p(r_j\|c_1)(\forall j = 1..4)$	$p(r_j\|c_2)(\forall j = 1..4)$	$p(r_j\|c_3)(\forall j = 1..4)$
D_1	$0.01; 0.57; 0.01; 0.41$	$0.01; 0.51; 0.01; 0.47$	$0.49; 0.09; 0.01; 0.41$
D_2	$0.57; 0.01; 0.01; 0.41$	$0.03; 0.53; 0.03; 0.41$	$0.01; 0.09; 0.49; 0.41$
D_3	$0.66; 0.10; 0.10; 0.14$	$0.12; 0.62; 0.12; 0.14$	$0.10; 0.18; 0.58; 0.14$
D_4	$0.70; 0.14; 0.14; 0.02$	$0.16; 0.66; 0.16; 0.02$	$0.14; 0.22; 0.62; 0.02$
D_5	$0.14; 0.70; 0.14; 0.02$	$0.16; 0.66; 0.16; 0.02$	$0.62; 0.22; 0.14; 0.02$

Similarly, given a found workable design as described in D_3 in Table II, we can find the boundaries for parameters of the workable designs. There are 14 workable designs whose parameters are within the identified boundaries. For example, the boundaries for $p(r_2|c_2)$ is from 0.53 to 0.66.

Figure 4 shows the correlation measures from five different designs described in Table II. As seen in Fig. 4a, with workable designs D_2, D_3, and D_4, as c_1 is the most unpredictable challenge, the correlation associated with c_1 and its favorable response is positive and has the largest size compared to that of other challenges. Moreover, other correlation measures between challenges and the responses other than the favorable response are non-positive as represented in Figs. 4b - 4d. On the contrary, with designs D_1 and D_5, since their parameters are beyond the boundaries of the workable design, the correlation between challenges c_1 and its favorable response are negative as shown in Fig. 4a. Furthermore, the correlation between each challenge and an un-intended response is sometimes positive as shown in Figs. 4b - 4d.

In summary, by establishing our defined principles, for any given configuration of $P(C)$, we are always able to find workable designs and the boundaries for their parameters so that they are appropriate challenge-response designs for the initial trust establishment in certain environments.

V. Experiment Evaluation

In this paper, the correlation between the challenge and the response occurred in a single C-R round is interpreted to an instant trust value. The initial trust level of a respondent is updated once a round completed and it is a weighted aggregation of instant trust values from all C-R rounds. The computation of the instant trust value from round k^{th}, τ_k, and the initial trust value after k rounds, $T^{(k)}$, are given in (8) and (9). Note that, α is the translating parameter to scale up the trust value to [-1, 1], ω_k is the weight value assigned to the instant trust value from round k^{th}, and Δ_{ij} is the correlation between c_i and r_j occurred in round k^{th}.

$$\tau_k = \alpha \Delta_{ij} \tag{8}$$

$$T^{(k)} = (1 - \omega_k) T^{(k-1)} + \omega_k \tau_k \tag{9}$$

Evaluation setup We evaluate our proposed design with a C-R mechanism that consists of three challenges with a given $P(C)$ of $\{0.05, 0.15, 0.8\}$. Assuming that there are four possible responses to each challenge and one of them is the favorable response to the challenge. We assume that each challenge c_i has its favorable response r_i, (i = 1,2,3). We select the design D_3 described in Table II for our evaluation. The challenge at each round and corresponding response to the selected challenge are chosen based on their corresponding probability described in D_3 in Table II.

We first conduct 90 tests of the single-round C-R process and determine the obtained instant trust value from each test. Parameter α is set to $1/(2x)$, where x is the size of the largest correlation that can be obtained from the design to scale up the instant trust value to [-1, 1].

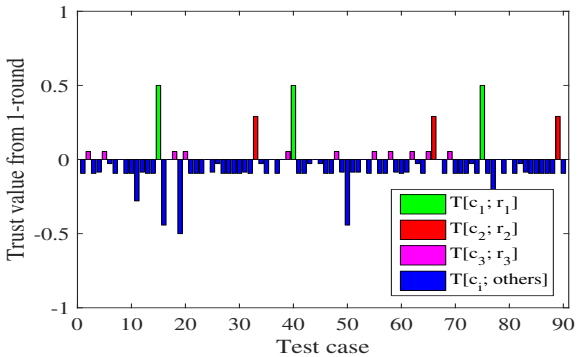
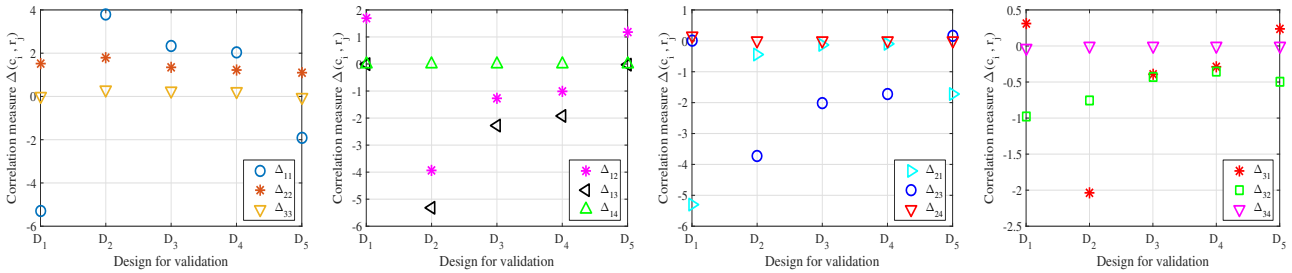


Fig. 5: Instant trust value from 1-round challenge-response operation

As shown in Fig. 5, when the respondent provides a favorable response to the respective challenge, a trust level



(a) (b) (c) (d)

Fig. 4: Correlation measures from designs within the boundaries and beyond the boundaries with given P(C) of $\{0.05, 0.15, 0.8\}$

$(0 < T_k \leq 1)$ is placed on the device. Otherwise, a distrust or neutral value $(-1 \leq T_k \leq 0)$ is placed on the respondent depending on the size of the correlation measure and the used translating parameter. For example, at many tests, the instant trust value is at a neutral position $(T_k = 0)$ since the respondent fails to provide a favorable response to the challenge. At the test 15^{th}, 40^{th} and 75^{th} the challenge was the most unpredictable challenge c_1, and the device returns a favorable response r_1. Thus, a high trust value $(T_k = 0.5)$ is placed on the device. In many other tests, the device provides unintended responses, it is given some distrust levels $(T_k < 0)$. This investigation demonstrates that the tested design provides desired characteristics of a workable design.

We further conduct a five-round C-R process repeated in 100 times using design D_3 presented in Table II to validate if the obtained initial trust value is reliable with various device's behaviors to different challenge patterns. For the initial trust computation, the weight for the instant trust value from the current round is set to 0.3 if the response is the favorable response. Otherwise, it is set to 0.7. With this setup, the speed for a device to gain its trust is slower than to lose its trust.

Figure 6 shows typical trends of the updating of initial trust value over the experiment from selected simulations. It can be seen that the device gains its trustworthiness if it keeps responding favorable responses to the respective challenges. The more trust is placed on the device if the selected challenge is highly unpredictable. For example, in simulation 40^{th}, the device gains its trust when it consistently returns a favorable response to the highly unpredictable challenges c_1 and c_2.

Moreover, these trends show that the device loses its trust when it does not consistently provide the relevant information to the challenge. The trend from simulation 15^{th} shows that when a device first returns a favorable response to challenge c_1 and then fails to do so in all other rounds, it quickly loses its trust. The device will not recover its distrust level if it cannot provide a favorable response to the respective challenge as presented in the trend of simulation 35^{th}. These trends show that the initial trust establishment consistently measures reasonable initial trust value per various device's behaviors.

VI. Conclusion

This paper explores the principles for guiding mechanism designs for our proposed challenge-response-based initial trust assessment scheme. The information content of the challenges and their relationship with the respondents' knowledge are designed in the form of probability distributions. Our established principles ensure that the design will be workable for the required environment. Extensive simulations are conducted to consolidate the principles with numerous designs. The next plans are to propose a mapping algorithm to map the probabilistic design of the challenge-response mechanism to practice and implement the challenge-response mechanism-based initial trust establishment for practical 5G environments.

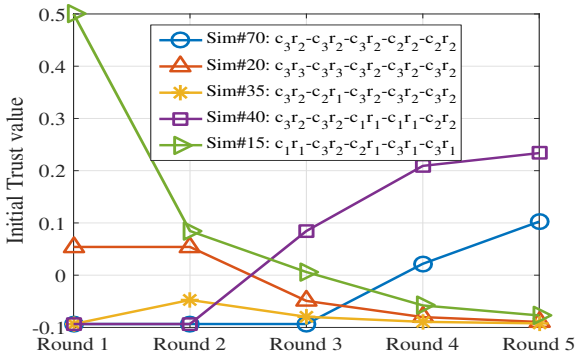


Fig. 6: Initial trust value from a 5-round challenge-response process

References

[1] T. Nguyen, D. Hoang, and A. Seneviratne, "Challenge-response trust assessment model for personal space iot," in *Proc. of IEEE 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 *Proc. of IEEE INFOCOM 2017*, May 2017, pp. 784–789.

[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] Y. L. Sun, Z. Han, W. Yu, and K. J. R. Liu, "A trust evaluation framework in distributed networks: Vulnerability analysis and defense against attacks," in *IEEE INFOCOM*, 2006, pp. 230–236.

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

[8] K. Rhee, J. Kwak, S. Kim, and D. Won, *Challenge-Response Based RFID Authentication Protocol for Distributed Database Environment*. Springer Berlin Heidelberg, 2005, pp. 70–84.

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

[10] S. Tadelis, *Game Theory: An Introduction*. Princeton University Press, 2013.