Challenge-Response Trust Assessment Model for Personal Space IoT

Tham Nguyen, Doan Hoang
Centre for Innovation in IT Services and Applications
University of Technology Sydney
Australia

Aruna Seneviratne
Mobile System Research Group
NICTA, Sydney
Australia

***Abstract*—Internet of Things (IoT) embraces the interconnection of identifiable devices that are capable of providing services through their cooperation. The cooperation among devices in such an IoT environment often requires reliable and trusted participating members in order to provide useful services to the end user. Consequently, an IoT environment or space needs to evaluate the trust levels of all devices in contact before admitting them as members of the space. Existing trust evaluation models are based on resources such as historical observations or recommendations information to evaluate the trust level of a device. However, these methods fail if there is no existing trust resource. This paper introduces a specific IoT environment called personal space IoT and proposes a novel trust evaluation model that performs a challenge-response trust assessment to evaluate the trust level of a device before allowing it to participate in the space. This novel challenge-response trust assessment model does not require the historical observation or previous encounter with the device or any existing trusted recommendation. The proposed challenge-response trust assessment model provides a reliable trust resource that can be used along with other resources such as direct trust, recommendation trust to get a comprehensive trust opinion on a specific device. It can also be considered as a new method for evaluating the trust value on a device.**

I. Introduction

A broad definition of IoT entails a number of smart entities that are identifiable through unique addresses, have ability to sense their surroundings, connect to the Internet, and interact with one other to achieve the goals of a particular application [1]. Simply, we view IoT as the interconnection of identifiable and smart objects capable of providing services. These objects are known as devices with unique identifications.

The interconnection and communication ability of these objects enable IoT applications in numerous domains from industry, society to the environment [2]. The scope of an IoT space can be limited to a local sensing system or cover a global monitoring network. It is impossible to discuss an IoT application without defining the perimeter of the IoT space. This paper introduces a particular IoT space, $the\ personal\ space\ IoT$.

Definition of personal space IoT The personal space IoT centers on a person's space. It includes all objects implanted or wearable by the person such as implanted sensors, smart watches, Google glasses, ECG sensors, and smartphones. It also includes all fixed or mobile objects and devices that come into contact (or reachable) with wearable objects on the person. Devices are reachable when they are within the wireless transmission radius of one another. The radius is technology and energy dependent (Bluetooth, Zigbee, etc). In this personal space IoT, some devices work together and form their own IoT space so that the space can provide services to the owner. Some devices may belong to other personal space IoT and are able to exchange services with other personal spaces. Others may stand alone and may interfere maliciously with other reachable personal spaces.

This work focuses on the personal space IoT. The focus is on a group of devices associated with the personal space of a person and provides services to the owner. These devices are supposed to be carried or worn by the owner. Keeping in mind that all these wearable devices are small and powered by battery, optimized energy consumption is critical in their operation. In our focused personal space IoT, we designate one of the devices called the controller to manage activities within the personal space IoT on behalf of other devices within. The devices in the personal space IoT are able to interconnect with each other and connect to surrounding devices or the Internet all through the controller.

In practice, the personal space operates within a large environment with multiple surrounding devices. These surrounding devices are called as foreign devices. The foreign devices can also form other personal spaces IoT for their own purposes. In the focused personal space IoT's point of view, the foreign devices can be friends, strangers or even intruders. In addition, the focused personal space IoT can move around as the owner moves. Thereby, the focused personal space co-exists with other personal spaces which may contain the friends, strangers or intruders in a specific environment. In fact, we model a personal space IoT as a "smart software Personal Space IoT object" that has its own identity and characteristics, is dynamic and mobile, and interacts with other personal space IoT objects.

Due to the co-existence with other devices in a common environment, the focused personal space IoT may suffer from the harmful interactions of the foreign devices. Besides, the malicious devices may try to join the space and work to destroy our personal space. Also, the focused personal space may be tracked by the intruders and strangers. Therefore, the personal space IoT has to be able to protect itself from all harmful activities in the environment.

In order to protect its personal space IoT, the controller

plays a central role looking after its elements just like a person's brain which acts as a commanding centre managing and protecting all parts of a person. In particular, the controller needs to be able to recognize and classify all the devices within reach into separate categories: its own devices, admissible and inadmissible devices. The controller only allows the trusted devices to be the member of the personal space. However, it permits other nearby devices to exchange useful information and services with the personal space if they are trusted. Otherwise, the devices are untrusted intruders and do not have the permission to join the personal space IoT. In order to do so, a trust evaluation scheme is needed.

Existing trust models are based on some trust resources such as the experience of a previous encounter between two entities (subject and agent), the direct observations between them in the past, and the recommendations from nearby third parties. Some trust models used the combination of these resources. The disadvantage of these existing methods is that they require the experience of a node on another (a subject on its agent) and/or the presence of the third parties for recommendations. However, in most realistic situations, the subject has no experience on the agent or in situations where nearby third parties are not able to make the recommendation due to the lack of information about the agent or dynamic changes in the environment. In these situations, alternative trust models are needed. In this paper, we propose a novel trust evaluation method - the challenge-response trust assessment model for personal space IoT.

Our trust evaluation scheme uses a trust assessment whereby the controller tests all the discovered devices and evaluates the trust degree on each device before making a decision whether to accept it to its personal space. The trust evaluation method is numerical - based trust which uses the conditional probability throughout the trust assessment and the associated entropy to measure the uncertainty about the device. Finally, the entropy is translated to the trust degree that the controller places on the device.

The proposed trust evaluation scheme can be used together with existing methods to provide additional trust evidence for the decision making. It can also be used as a separate trust evaluation component of the trust management models to evaluate the trust value on a specific device. The main benefit of our proposed trust evaluation model is that it can be used for all situations without relying on the historical experience or the recommendations.

The remaining of the paper is organized as follows. Section II discusses the related work. Section III describes our challenge-response trust assessment model. The calculation of trust value is presented in section IV. Section V presents the experimental results on the consistency of the trust value. Finally, section VI gives the conclusion remarks along with directions for future research.

II. Related work

In [3], the authors proposed a trust evaluation model as a path problem on a directed graph where nodes represent entities and edges represent trust relations. The indirect trust relation between two users is established by using the second-hand information from a third party. Thus, their trust model needs direct trust relations between the third entity and one of the two users. Also, there is no mechanism to guarantee that the third entity is a trusted recommender.

The authors of [4] proposed a distributed-based framework whereby the trust parameters are observed via the information transmission. A node can compute the trust level of its neighbors based on observation of their past behavior. This approach requires the historical experience of the subject on the agent before evaluating the trust level on this agent.

Varadharajan et al., in [5] presented a trust evaluation model in a peer-to-peer environment whereby the trust value of an unknown peer is determined by investigating its historical interaction with other peers. A requesting peer relies on both its historical interactions and its friend's recommendations to collect the trust opinion on a target peer. The limitation is that the requesting peer highly depends on its neighbor peers' recommendation if it has no historical interactions with its target peer. Therefore, the number of neighbors and their interactions with the target peers, and the quality of recommendations affects the accuracy of the achieved trust value.

The authors of [6] suggested a new method of measuring trust value through measuring uncertainty. This work demonstrated that trust can be measured by determining the degree of uncertainty in the future action of an agent. The trust value can then be obtained from the amount of uncertainty which is measured by its information entropy. However, this approach depends solely on third party's recommendations. Moreover, applying the trust propagation in this concatenation of recommendation fashion results in a degradation of the trust value when a series of recommenders are deployed in tandem away from the target object. The reason is that the concatenation propagation of trust does not increase trust [6].

Existing trust models rely either on the direct experiences in the past or the interaction of recommenders to evaluate the trust value an entity places on another. Our challenge-response trust assessment scheme adopts a $push$ model whereby a challenge is initiated and a trust assessment procedure is performed to obtain the trust value without the need for historical interactions or recommendations. Therefore, the dependency on the third entities is eliminated and the trusting subject can control the trust assessment adaptively to specific situations.

III. Challenge-Response Trust Assessment Model

This section describes our challenge-response trust assessment model. The proposed model is accomplished by a trust assessment with a challenge-response process. The purpose of the assessment is to learn how much uncertainty is in the device's response. The uncertainty is measured with the associated information entropy and then interpreted to the trust value.

Generally, the trust relationship between two entities can be expressed as $\{$Subject: Agent, Action$\}$ whereby Subject

is the entity that performs trust evaluation, and Agent is the entity that trust is evaluated on its action. Information entropy has been used as the measurement of uncertainty in a signal or a random event [7]. Trust opinion can be interpreted from the level of uncertainty about a specific person or thing. A subject can decide to trust or distrust an agent by assessing the uncertainty in the action of the agent. The full trust degree and complete distrust degree are only interpreted from the fact that there is no longer uncertainty in the action of the agent. Otherwise, the trust degree is transferred to a neutral, a more trust or more distrust value depending on how much uncertainty still remains in the action.

Due to the relation of the trust definition and information entropy with the uncertainty concept, the trust value can be measured via entropy. Our challenge-response trust assessment model is a probability-based model based on the one-to-one relationship between the probability of an event and the trust on it. The information entropy is computed based on the event probability and then translated to a trust value.

In our proposed model, the controller plays the role of the subject while the device under assessment is the agent. The device will be tested by the controller with challenges. Thus, the action expected from a device is to respond to the challenge correctly in the controller's point of view. The trust value is depicted as a real number in the [-1, 1] interval whereby the trust values range from a complete distrust over neutral trust measure to a full trust as shown in Fig. 1.

The trust assessment contains a number of challenges that the controller requests responses from the device. The challenge can be a question that requires the devices provide correct answer. It can also be the command that the controller needs the devices to perform. The type of challenge depends on the application that the personal space IoT supports. Each challenge followed by a response can be considered as a stage of the assessment. In each stage, the response of the device may or may not be accepted by the controller depending on whether it satisfies the controller. After each stage, the controller can measure how much uncertain is in device's behavior by assessing the response. The uncertainty is measured via entropy which is computed based on conditional probabilities. During the trust assessment, the controller gradually learns the behavior of the device.

The base of uncertainty measurement is the probability. The associated probability for measuring the uncertainty of a device in our trust assessment refers to the probability that an expected device provides expected responses to the challenge. In fact, the controller may trust on the context of a given response at a certain degree. Meanwhile, the device provided a given response may or may not be the expected device. Consequently, the associated probability with the uncertainty of a device relies on the probability the controller trusts on a given response and the probability that the device provided this response is the expected device.

The mapping between the probability and the trust value is one-to-one. If there is a high probability that an expected response comes to the controller from a device, it is more likely that the device will be trusted. Likewise, when this probability is very low, it is more likely that the device will be distrusted. The higher the probability, the more trust the controller places on the device.

In order to calculate the associated probability with which the uncertainty can be measured, we design two conditional probabilities. Firstly, we take into account the probability that the controller trust on the context of a given response. If the response is an expected response to the controller, it is more likely that the device which provided this response is the expected device. Otherwise, if the response does not satisfy the requirement of the controller for a specific challenge, it is more likely that the device is not the expected device. Therefore, the second conditional probability is the probability that the device is the expected device given that it provided an expected or an unexpected response.

The associated probability expressed how much the controller trust on a specific device is computed based on two conditional probability components. The calculation of this probability is presented in section IV. The uncertainty will be measured from this probability via entropy function and then interpreted to trust value. The measurement and interpretation process is performed after each stage and the overall trust value is derived from the trust values of the stages.

In practice, the device which provides an expected response may not be the expected device. On the other hand, the device which provides an unexpected response may not be a malicious intruder as the device may make a mistake during the trust assessment procedure. Our trust assessment provides chances for a device to recover and improve its trust value. Likewise, the trust assessment stops when a device presents a response indicates that the trust is unlikely to recover in future stages. In addition, the trust assessment will be stopped whenever the trust value reaches a given acceptable threshold.

IV. Trust Value Calculation

In this section, we discuss the uncertainty measurement and its interpretation to the trust value.

Firstly, the calculation of the probability associated with the trust relationship between the controller and a device is presented. Let p_{CR_i} denote the probability that the controller trusts a given response i^{th}, p_{DR_i} denote the probability that the device is considered as the expected device at the i^{th} response. We also define p_{R_i} as the probability that the response is expected, $p_{D|R_i=1}$ as the probability that the device is an expected device given its response is an expected response, and $p_{D|R_i=0}$ as the probability that the device is an expected device given its response is an unexpected response. Then, the probability associated with the trust relationship between the controller and a specific device after stage i^{th}, p_{CD}, can be calculated as:

$$p_{CD} = p_{R_i} \cdot p_{D|R_i=1} + (1 - p_{R_i}) \cdot p_{D|R_i=0} \qquad (1)$$

As the controller can evaluate the response, it is reasonable for the controller to assume that $p_{R_i} = p_{CR_i}$ and $p_{D|R_i=1} = p_{DR_i}$. In addition, if a device provides an unexpected response

then there is a low probability that it can be considered as expected device. Thus, we can calculate $p_{D|R_i=0}$ by subtracting $p_{D|R_i=1}$ from 1. Consequently, (1) becomes

$$p_{CD} = p_{CR_i} \cdot p_{DR_i} + (1 - p_{CR_i}) \cdot (1 - p_{DR_i}) \quad (2)$$

The associated probability is then used to measure the uncertainty about the device's behavior. Information entropy is the measurement of the uncertainty. By interpreting the amount of uncertainty to the trust value through entropy, the controller will be able to decide to trust or distrust the device to a specific trust degree. We measure the uncertainty about the device's behavior by using the Shannon entropy [7]:

$$H(p) = -p \cdot log(p) - (1 - p) \cdot log(1 - p) \quad (3)$$

where, p is the associated probability of the trust relationship between the controller and the device.

The purpose behind our trust assessment is to reduce the uncertainty about a device of which the controller has no knowledge at the initial of the assessment. After the trust assessment, the controller learns more about the device and it is able to place the trust value on the device by transferring the uncertainty level to the trust value.

In fact, the trust is an increasing function of the probability. Specifically, the trust value is increased when the associated probability is increasing from 0 to 1. However, the entropy is a symmetric function of probability. It is a non-negative quantity and it reaches maximum value at 1 when the probability is 0.5, minimum value at 0 when the probability is at 0 or 1 as indicated in Fig. 1.

Specifically, the maximal entropy implies the highest uncertainty about the device so that the controller cannot make a decision to trust or distrust the device. Therefore, the trust value is a neutral trust measure and is interpreted to 0. On the side with probabilities lower than 0.5, the uncertainty about the device reduces when the probability decreases. It reaches 0 at the probability of 0, and obviously, there is certain that the device will not provide an expected response. Thus, the trust value should be translated to -1 which refers to a complete distrust opinion of the controller. Likewise, on the opposite side, the uncertainty reduces when the probability increasing from 0.5 to 1. It reaches 0 at the probability of 1. This implies that there is certain that the device will provide an expected response. Therefore, the trust value should be interpreted to 1 which refers to a full trust opinion of the controller on the device. Fig. 1 shows the entropy and the trust value as functions of the probability.

In order to interpret the entropy of the device at each stage to the trust value, (4) is used as it satisfies all the requirements of the trust value translation.

$$T = \begin{cases} 1 - H(p), & \text{if } 0.5 \leq p \leq 1 \\ H(p) - 1, & \text{if } 0 \leq p < 0.5 \end{cases} \quad (4)$$

During the trust assessment, the trust value is measured after each challenge-response stage. The overall trust value

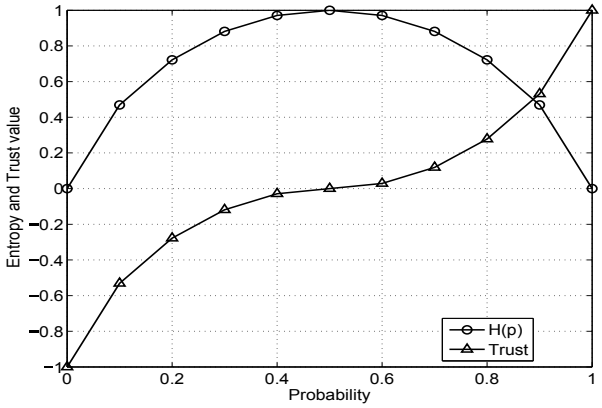

Fig. 1. Entropy and Trust value with associated probability

is aggregated up to the last stage by combining the previous trust values with the latest trust value.

$$T_j^{ovr} = \omega_i \cdot T_i^{ovr} + \omega_j \cdot T_j^{ind} \quad (5)$$

where, T_i^{ovr} and T_j^{ovr} are the overall trust after stage i^{th} and stage j^{th}, respectively; T_j^{ind} is the individual trust after stage j^{th}; ω_i and ω_j are the weights for the overall trust value after i stages (from first stage to i^{th} stage) and for the individual trust value at j^{th} stage, respectively, and $\omega_i + \omega_j = 1$.

The weights allow us to take into account various considerations such as the environment in which the personal space IoT operates and the emphasis of different stages of the challenge-response process. For example, the trust value of a stage may weight more than that of the previous stage to reflect the degree of knowledge gained through the assessment process.

V. Experimental Results

In this section, we present the experiment setup and discuss the obtained results with our proposed scheme.

In the experiments, it is assumed that the controller places trust on the context of the response. The device provides an expected response is likely to be trusted as an expected device with a high probability value. Likewise, the device provides an unexpected response is likely to be trusted as an expected device with a very low probability value. The assigned probability is assumed to increase if an expected response follows another expected response and to decrease if an unexpected response follows another unexpected response. The weight assigning for the trust value at each stage can be flexibly assigned. Our experiments focus mainly on the feasibility and consistency of the proposed scheme.

In the following experiments, we assume 0.98 as the probability that the controller trusts the response, 0.9 or greater is the probability that the device is the expected device conditioned on an expected response. The weight assigned to the trust of the latest challenge is 0.6 and for the previous challenge is 0.4. The distrust and trust threshold values with which the trust assessment stops are -0.8 and 0.8, respectively.

In the first experiment, we conduct a trust assessment with two challenges. There are four cases in this experiment. In the

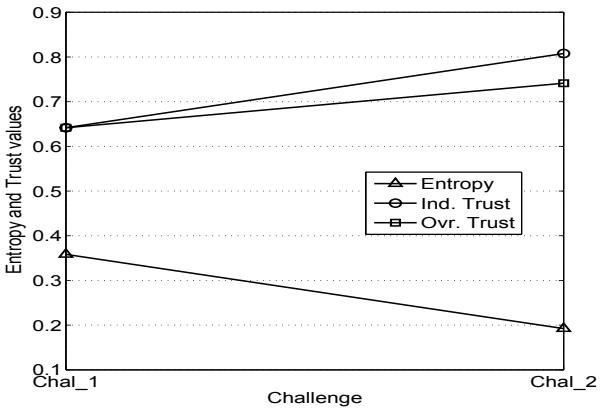

Fig. 2. Experiment 1: Entropy and Trust values with two expected responses

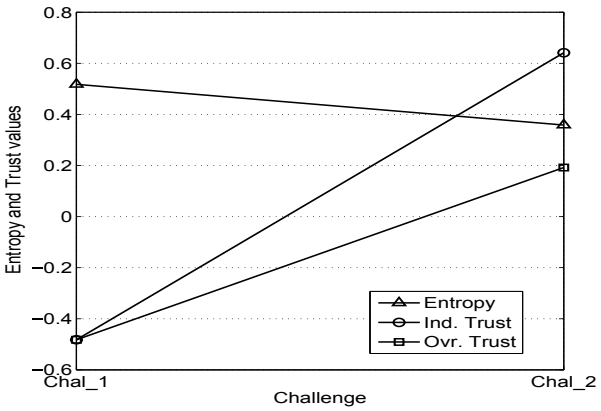

Fig. 4. Experiment 1: Entropy and Trust values with the first unexpected response followed by an expected response

first case, a device under the trust assessment provides both expected responses. In the second case, a device provides an expected response at the first challenge and an unexpected response at the second challenge. The third case considers a device which provides an unexpected response at the first challenge and an expected response at the second challenge. In the last case, a device provides both unexpected responses in the trust assessment.

The figures show the entropy, the individual trust value computed after each challenge, and the overall trust value which is aggregated from challenges including the previous challenges and the considering challenge. Fig. 2 shows the obtained results of the first case. The entropy is reduced during the trust assessment. Specifically, the entropy is about 0.37 after the first challenge. It reduced to 0.2 after the second challenge. Due to the reducing of the entropy and the responses are expected, the associated trust value after each challenge is increased from 0.64 to 0.80. However, the overall trust value after the trust assessment is only 0.74 because it takes into account the uncertainty of the device from both challenges.

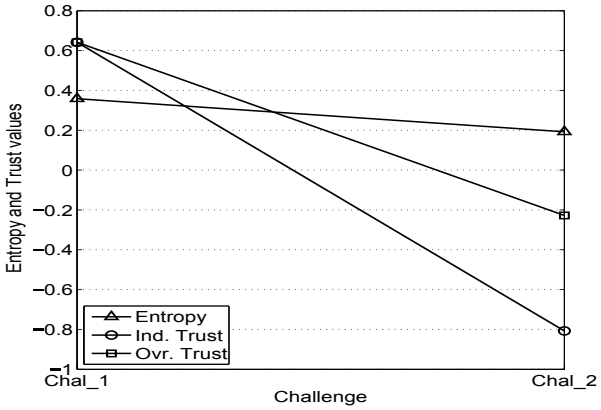

Fig. 3. Experiment 1: Entropy and Trust values with first expected response followed by an unexpected response

As shown in Fig. 3, the trust value from the second case is degraded because the unexpected response at the second challenge takes more weight. The overall trust value is higher than the trust value at the second challenge but it still indicates the distrust opinion of the controller. On the contrary, Fig. 4 shows that the trust value is recovered as the device provides an expected response at the second challenge after an unexpected response at the first challenge. The overall trust value is lower than the trust value at the second challenge but it also indicates the trust opinion.

Fig. 5 shows the consistency of the entropy values with the trust values in the fourth case. The entropy is reduced over the assessment and the trust value is degraded as the device provides both unexpected responses.

It is interesting to discuss the characteristic of the overall trust value. The overall trust value combines individual trust values according to the weights assigned to them. By using the weights, the overall trust value takes into account the trust values from all challenges. Specifically, the overall trust value of a device is improved if it provides expected responses to the challenge. Otherwise, the overall trust value is reduced if the device provides unexpected responses to the challenge.

In order to see how the threshold affects the trust assessment procedure, the second experiment is performed. This experiment conducts a trust assessment with no fixed number of challenges. We present two cases: the device provides all expected responses in the first case, and the device provides all unexpected responses in the second case.

In the first case, all the responses are expected responses. Thus, the probability that the device is an expected device increases after each challenge. The overall trust value reaches the trust threshold after four challenges as shown in Fig. 6. Therefore, the trust assessment stops without performing further challenges.

Fig. 7 shows the obtained results from the second case of experiment 2. As the responses are unexpected from the initial of the assessment, the overall trust value is degraded to a distrust threshold after the third challenge. Then, the trust assessment stops after three first challenges. According to the two cases in experiment 2, the trust assessment can converge after a specific amount of time.

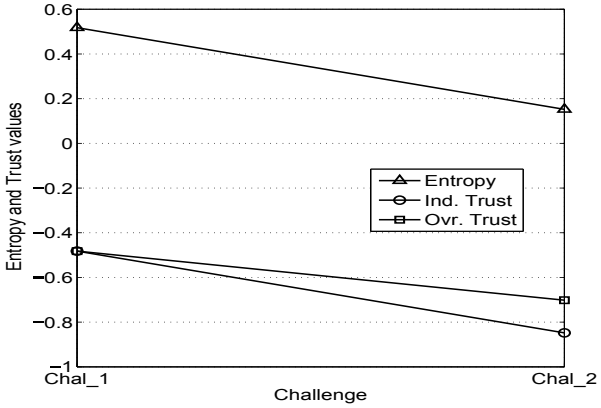

Fig. 5. Experiment 1: Entropy and Trust values with two unexpected responses

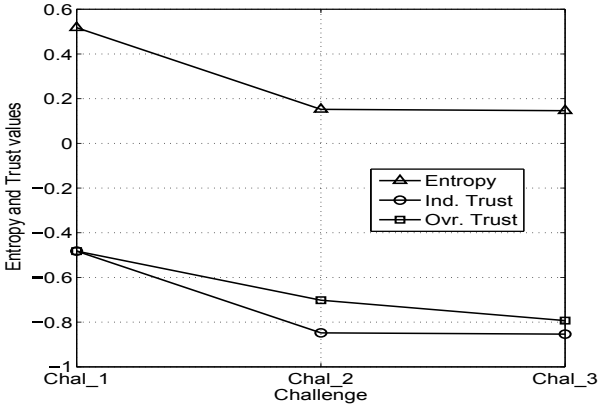

Fig. 7. Experiment 2: Entropy and Trust values with all unexpected responses

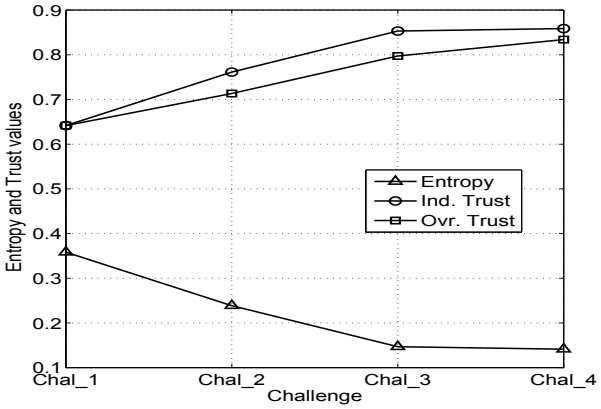

Fig. 6. Experiment 2: Entropy and Trust values with all expected responses

The main emphasis of the experiments is to show that the proposed scheme is feasible as an alternative/supplementary scheme for trust evaluation and to demonstrate that it is consistent in the way we evaluate trust. Clearly, without direct observations or the presence of a recommender, the proposed scheme can initiate a challenge and then evaluate the response to obtain an informed trust assessment as shown by the results. While, in the recommendation scheme, the trust value does not increase with the concatenation of recommendation and this is consistent and expected since the overall entropy of the system increases with the additional recommendation. For our scheme, trust level should increase with additional expected responses and decrease with unexpected responses. The consistency of the proposed scheme has been demonstrated. There are many interesting factors to be explored in the design of the proposed scheme as they are pertinent to and dependent on the specific environment and objective of the application.

VI. Conclusion

This paper introduced the concept of a personal space IoT and described the proposed challenge-response trust assessment model for this personal space IoT. In the trust assessment, the device is tested with challenges from the controller. This model does not require the historical interaction between two entities or the recommendations of third parties. The trust assessment measures the uncertainty about the device's behavior via entropy and then translates the associated entropy to trust value. The experimental results demonstrated the consistency of the model in that the achieved trust values can be gained or degraded during the trust assessment depending on the device's response. The challenge-response process allows the controller to assess the uncertainty or entropy of a device's behavior and allows it to make an informed trust/distrust decision on the device.

For future research, we plan to explore comprehensively various parameters of the proposed model and to develop a trust management framework that combines our trust assessment scheme with existing models. The comprehensive trust management framework will be robust and able to adapt to various operational environments as the direct trust, the indirect trust and the challenge-response trust assessment schemes can be used simultaneously to improve the accuracy of the evaluation.

Acknowledgment

This work was supported by NICTA (National ICT Australia).

References

[1] A. Serbanati *et al.*, *Building Blocks of the Internet of Things: State of the Art and Beyond*. InTech, 2011, ch. Deploying RFID - Challenges, Solutions, and Open Issues.

[2] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[3] G. Theodorakopoulos and J. Baras, "On trust models and trust evaluation metrics for ad hoc networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 318–328, 2006.

[4] G. Crosby *et al.*, "A framework for trust-based cluster head election in wireless sensor networks," in *Second IEEE Workshop on Dependability and Security in Sensor Networks and Systems*, April 2006, pp. 10 pp.–22.

[5] Y. Wang and V. Varadharajan, "Trust2: developing trust in peer-to-peer environments," in *IEEE International Conference on Services Computing*, vol. 1, July 2005, pp. 24–31.

[6] Y. Sun *et al.*, "Information theoretic framework of trust modeling and evaluation for ad hoc networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 305–317, 2006.

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