Trust-Based Decision Making for Health IoT Systems

Hamid Al-Hamadi[†] and Ing-Ray Chen[*]

[†]Department of Computer Science
Kuwait University
hamid@cs.ku.edu.kw

[*]Department of Computer Science
Virginia Tech
irchen@vt.edu

***Abstract*—With the onset of the Internet of Things (IoT) era, the number of IoT devices and sensors is increasing tremendously. This paper is concerned with a health IoT system consisting of various IoT devices carried by members of an environmental health community. We propose a novel trust-based decision making protocol that uses trust-based information sharing among the health IoT devices, so that a collective knowledge base can be built to rate the environment at a particular location and time. This knowledge would enable an IoT device acting on behalf of its user to decide whether or not it should visit this place/environment for health reasons. Unlike existing trust management protocols, our trust-based health IoT protocol considers risk classification, reliability trust, and loss of health probability as three design dimensions for decision making, resulting in a protocol suitable for decision making in health IoT systems. Our protocol is resilient to noisy sensing data provided by IoT devices either unintentionally or intentionally. We present performance data of our trust-based health IoT protocol and conduct a comparative performance analysis of our protocol with two baseline protocols to demonstrate the feasibility.**

***Keywords* —Internet of things (IoT), trust management, decision trust, health IoT, trust-based decision making.**

I. Introduction

In this paper, we propose a trust-based approach for information sharing in a health Internet of Things (IoT) system comprising IoT devices carried by members of an environmental health community. Smart IoT devices in this health IoT system share location-based information obtained through their personal area networks (PANs) with the goal of maximizing the safety of their human owners. We are interested in building a reliable and effective trust management system that can guide IoT devices to use the most trustworthy environmental health information for decision making. A possible use scenario is that a pollutant sensitive user must determine whether or not he/she should enter a location at a particular time to avoid health related issues. Without loss of generality, we shall illustrate the utility of our proposed health IoT system with this use scenario.

Through the adaptation of IoT technology, it is expected that the number of connected IoT devices will reach 50 billion by 2020 [1]. With this kind of tremendous growth, IoT devices would find their way into our everyday life from environmental monitoring to general public healthcare monitoring. Communication technologies for low-power resource-constrained devices, such as Low-Power 802.15.4 and Bluetooth Low Energy (BLE) [2], will play a major role in enabling the integration of such devices with the Internet and increasing the footprint of health IoT.

There is a great potential for applying IoT technology across all sectors including both industrial and public to improve operation efficiency, reduce cost, and provide better service. Healthcare and public safety domains have a clear opportunity today to seize the benefits of IoT technology. Remote monitoring of medical parameters, smart hospital services, individual well-being, and emergency site and rescue are a few examples of applications that fall under these domains [3]. Environmental health IoT devices [4, 5] are available at a very affordable price, and when combined with a mobile application running on smart phones, can provide high quality readings for various environmental parameters, like CO levels, humidity, hydrocarbons, dust, noise, chemical fumes, fragrances, and so on. Since the measurement of the environment has a direct relation with healthcare of certain ailments and health in general, health IoT devices are expected to play a major role in providing excellent support in day-to-day healthcare. For example, an elderly person suffering with high blood pressure might not want to go to a place where noise levels are very high. Prior knowledge of the environment can safeguard decision making.

We note that it is difficult for health professionals to personally attend to all patients at all times. It is even more difficult to give personalized assessments regarding the health risk for patients entering into different physical locations due to the absence of monitoring tools providing detailed location-aware information that may span large geographic areas. More importantly, a health decision must take into account the current health status of a patient.

Our paper has the following unique contributions:

1. To the best of our knowledge we are the first to design and analyze a trust-based decision making protocol for a health IoT system consisting of IoT devices carried by members of an environmental health community. In our

protocol design, an IoT device will collect and aggregate environmental health related data on behalf of its owner through collaboration with other IoT devices. Our trust protocol running on an IoT device will accurately assess both data and source trustworthiness for trustworthy decision making for its owner.

2. Unlike existing trust management protocols for trust-based service management of IoT systems [6, 7] which consider only service providers' trust scores for decision making, we additionally consider a patient's risk classification and loss of health probability for decision making. Different from a general service-oriented IoT system, a health IoT system must take a patient's health status (cost) and tolerance toward loss of health (payoff) into consideration for decision making since the consequence of an incorrect decision can be catastrophic.
3. Our trust protocol is resilient to noisy sensing data provided by IoT devices either unintentionally or intentionally. This is achieved by our trust score computation method which considers not only the location rating trust score, but also the rater trust score and witness trust score.

The rest of the paper is organized as follows. In Section II we provide a literature survey of related work and compare/contrast our work with existing work. In Section III we discuss the system model, trust-based decision making model, and threat model for health IoT systems. In Section IV we describe our trust-based decision-making protocol for health IoT systems. In Section V we perform a performance analysis and conduct a comparative analysis with two baseline protocols. Finally, in Section VI we conclude the paper and outline future work.

II. RELATED WORK

We survey related work in three areas: (a) security of health IoT systems, (b) trust-based service management of IoT systems, and (c) health IoT applications needing runtime decision making. We provide an analysis for each area, as well as compare and contrast existing approaches with our approach whenever appropriate.

Security of Health IoT Systems: Many research papers have focused on the security aspect of health IoT systems because of the dire consequence of security and privacy failure. Habib et al. [8] provided an integrated security analysis of an E-health IoT based patient monitoring system by addressing the security requirements of the wireless body area network, communication infrastructure, and the hospital network. The vulnerabilities, threats, and attacks such as data counterfeit, eavesdropping, spoofing, and man-in-the-middle are analyzed for each of these segments. They suggested securing patients IoT devices by encrypting the patient data and incorporating security mechanisms to guard against software attacks. In [9] and [10] the authors discussed security challenges in health IoT and various medical services including Internet of m-health Things (m-IoT) and Ambient Assisted Living (AAL). They compared various cryptographic algorithms such as Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Rivest-Shamir-Adleman (RSA), and concluded that RSA provides the best cost-effective security for IoT devices. The emphasis was on the use of 6LoWPAN technology in IoT devices to build a practical m-IoT system. Unlike [8-10] cited above which focus on cryptography based security of health IoT, our work considers trust-based security. The security protection is not about encrypting/decrypting user data, but about how a user in a heath community can use trust information to filter out untrustworthy input when gathering health information to enhance IoT health security.

Trust-based Service Management of IoT Systems: Trust management of IoT systems is still in its infancy stage. Yan et al. [11] provided a survey of contemporary trust management techniques for IoT. However, no specific goals for health IoT were discussed. Our paper on the other hand has a specific goal. That is, we aim to help environment health conscious users carrying IoT devices become situation aware of surrounding environments. The novelty is in the use of trust management to effectively collect various geo-based health related data and to use this data for reliable decision making. Very recently [6, 7, 12, 13] discussed trust management for distributed IoT systems, where social relationships are established between things based on interactions. Both direct observations and indirect recommendations are factored into trust assessment of nodes. Unlike our work, their emphasis is how the social relationship of distributed IoT entities would affect the trust relationships and thus the service dispositions between IoT devices which provide services toward each other. While the trust management mechanisms proposed are valid for service composition and binding IoT applications, they cannot be applied to health IoT applications since the main characteristics of health IoT are not taken into consideration. Unlike [6, 7, 12, 13] cited above which consider only service providers' trust scores for decision making, we specifically consider a patient's risk classification and loss of health probability for trust-based decision making. Saied et al. [14] proposed a centralized IoT trust management system where a service requesting node is provided with the best assisting nodes to best answer the service request. This is achieved by computing "service context similarity" between reports stored centrally in the cloud and the target service where the weight of a report is based on the trustworthiness of the reporting node. Requesting nodes evaluate assisting nodes after the service is rendered by sending a report to the centralized trust management system in which it either rewards or punishes the assisting nodes. A recommender's trust is based on the deviation between its reports with the majority of other reports with similar service context. Similar to [14], our work also recognizes the benefit of a centralized trust management system to offload the overhead from resource constrained devices and avoid communication overheads. However, in our model, the reporting information includes necessary context information such as time, location, and phenomenon which are necessary for both accurate answering of queries and assessment of location raters. Furthermore, our work is based on the collaboration of mobile members within a health IoT system where the decision making is based on the member's health attributes and the gathered spatiotemporal environmental data. In our work the centralized trust management system not only compares a reporting member's location rating with similar ratings from other members, but also tries to build evidence of the validity of reports by verifying the location and comparing with self-observations.

Health IoT Applications Needing Runtime Decision Making: Many health IoT applications require runtime decision making. In the area of environmental monitoring, [15] presents an architecture that uses web-enabled environmental IoT sensors to provide real-time monitoring of events and decision making. It makes decisions on adaptively sampling dynamic water quality parameters during the most relevant interval, thus improving resource usage and quality of real-time monitoring. [16] presents a decision support tool for energy-efficient urban storm water management where energetic and environmental criteria are factored into the decision making process. The tool quantifies the economic cost, savings, energy consumption, and CO_2 emissions of different drainage scenarios and displays the results for decision making. In our work, we also collect spatiotemporal environmental data for decision-making but our work differs from [15, 16] cited above in that we consider health IoT where members with different trust levels share their environmental readings and provide health related recommendations to aid decision making. In the area of patient health monitoring, [17] discusses how web-based tools can be used for dissemination of health related information and for providing a better quality of care to patients. It concludes that patients are more probable to follow advice from peers and patients with similar diseases. Our work also builds on the idea that individuals are willing to join a health community for their own health and safety. [18] considers a distributed health platform using IoT devices. User health goals are specified and home smart appliances (e.g. microwave oven, smart TV, etc.) are all involved in monitoring the user health goals. However, their model does not consider data sharing between individuals and no trust information is used in decision making. [19] proposes a context-aware, interactive m-IoT system for diabetics based on an IoT cloud. A cloud server stores patient data which is accessible by patients and health professionals. The system detects abnormal blood-glucose levels relying on a rule-based system. Each patient has a profile with individual blood-glucose grade ranges set based on their doctor's suggestion. The ranges will determine which alerts and actions to be taken. In case of critical health status, a patient's caregiver is notified automatically regarding the health status. Our work differs from [19] in that we consider information sharing between patients as well as location-based recommendations regarding health of patients.

Summarizing above, our work differs from [6-19] cited above in that we aim to achieve effective and scalable trust-based decision making to health IoT members. We propose to leverage ubiquitous cloud service to serve a large number of mobile IoT devices for scalability and to derive trust ratings from various sources to produce a system that is inherently reliable. The system must be built in a way so that it promotes sharing of trustable data among members. The goal of the health IoT system is to provide its members the most trustworthy information to make decisions resulting in the most reliable outcome with regards to their health. Members of the health IoT system share their location-based information obtained from sensing. Thus, the health IoT system is dependent on the collaboration of members. We consider the use of trust management to determine the most trustworthy data to be used for decision making.

III. System Design of Health IoT Systems

A. System Model

Each member of a health IoT system is equipped with a PAN consisting of a gateway device, and several sensors. For example, a smart phone can act as a gateway, and the sensors can be small devices possibly attached to a member's body or vehicle (e.g. wheelchair). For our system model, we can simply consider a member as a health IoT device (acting on behalf of a user) capable of sensing and reporting. A health IoT member can be categorized in two classes:

1) Measuring environment factors: A health IoT device would monitor the surrounding environment (e.g. Air Quality Index, noise, NO_2, CO, hydrocarbons, electromagnetic radiation and so on).

2) Measuring personal health statistics: A health IoT device would measure the user's current health statistics. The measurements from this would be used primarily to derive the risk that the user can take at a particular point in time, e.g., body temperature, rate of breathing, blood pressure and so on.

Environment data is shared among all members of the health IoT system while personal data related to the member is not shared and is used as input into the decision making process. By contributing to the health IoT and sharing correct environment data, members make sure that they maximize their probability of correct decision making. Furthermore, members that misbehave by sending incorrect data increase their probability of being evicted from the health IoT system.

B. Trust-based Decision MakingModel

Figure 1 shows the system design space of a health IoT system. The health IoT cloud contains three main subsystems (or modules). The health expert subsystem is responsible for maintaining the thresholds data and is what health experts use to interact with the system. A trust management subsystem is responsible for trust and risk calculations and management. It further stores all member sensor readings for future decision making. A communication subsystem is responsible for handling incoming queries and incoming data. The subsystems interact to carry out the functions of the health IoT system. Since the IoT cloud can be accessed by all IoT devices ubiquitously wherever they are, we will interchangeably refer it as the Central Authority (CA). By using a centralized IoT cloud, the trust-based computation and information storage overhead is offloaded to the cloud, allowing resource-constrained IoT devices to be able to use the service with low computation and storage overhead.

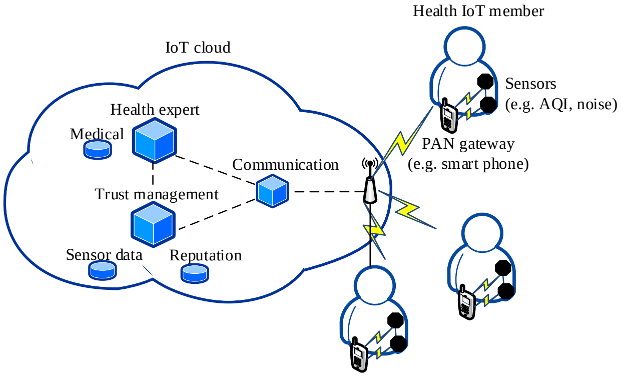


Figure 1: System design space of a health IoT system.

When a patient intends to change his location, he sends a query to the CA asking about the safety of entering this location. The CA performs the risk calculation utilizing the trust management and the health expert subsystems and responds to the query.

A doctor can evaluate the health of each member using the health IoT system based on the notion of decision trust [20] as follows: Based on the health assessment evaluation, the healthiness level or fitness level, denoted by *H*, is assigned to each user of the system. A set of thresholds are defined by an expert medical system. This could be as simple as given a level of dust, a level of hydrocarbons in air or a temperature reading, which maps to a probability that the user suffering from particular disease might face worsening of health.

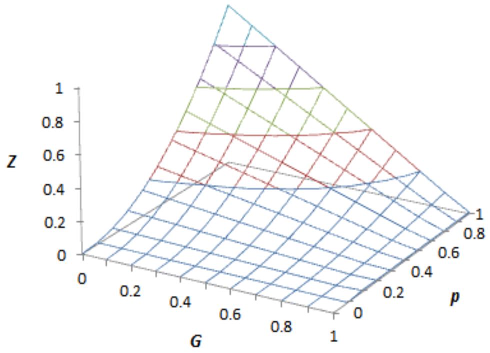


Figure 2: Parameter *Z* is a member's health classification by the doctor/medical center. Parameter *p* is the reliability trust of the source of the sensing data. Parameter *G* is the possibility of health loss as derived from the sensing data.

Figure 2 depicts the decision plane concept [20] as would be used by a doctor to assess the probability of health loss. In the following, we provide a detailed description of each of the three parameters in the graph:

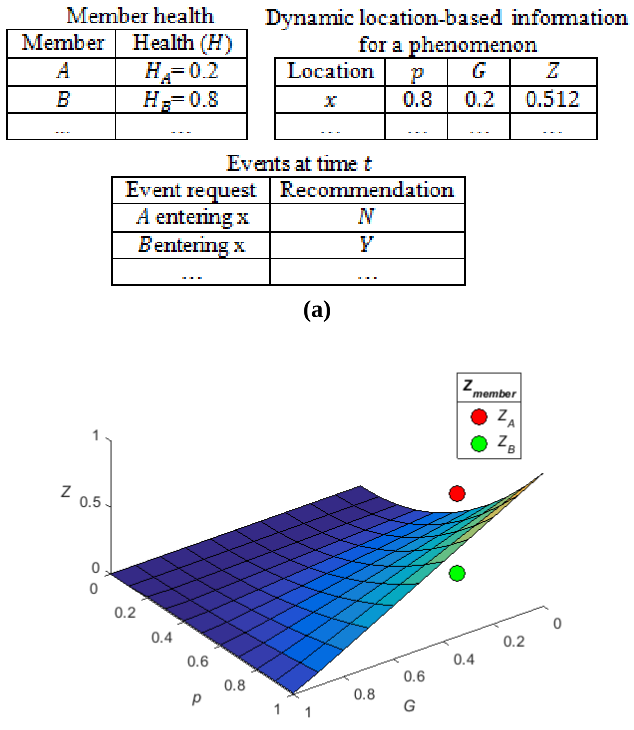
- A member's health classification (*Z*) – Each member is assigned a health level or fitness level parameter *H*. This health level or health index [21] can be derived by sensor data obtained from a user's personal area network or home environment. For example, blood pressure (BP) data can be automatically populated by BP sensors (carried by the user in a body network or in the user's home environment) which can communicate with the member's mobile application. This data can then be shared with the health IoT cloud to derive the member's health index automatically [21]. A doctor or medical expert, if necessary, can be consulted just once initially to map a patient's data to *H* and do not need to provide consultation afterwards making the system scalable as it does not require a doctor's attention once the system is up and running. After *H* is assigned, we calculate *Z* = *1*–*H* and plot this parameter Z. The scale of *Z* varies from 0 at the bottom to 1 at the top. In a way, we can define *Z* as the vulnerability index. An elderly person with multiple health conditions might be highly vulnerable to external factors, and will have a high *Z* value of 0.8 or more. A football player might not be very vulnerable to external environmental factors like dust and pollution, and will have a low *Z* value of 0.2 or less.
- Reliability trust of the source (*p*) – This parameter measures the trustworthiness of an agent who is (or agents who are) providing sensing data. Our trust computation method will assess this parameter.
- Probability of health loss (*G*) – This represents the possibility that the user might suffer worsening of his/her health as determined by the sensing data sent by the agent. Suppose due to a very high noise level, a high blood pressure patient may or may not suffer from high blood pressure. This parameter represents the possibility that the person would have adverse effects in a particular location. The probability of health loss is derived from the sensing data. Our trust-based decision making protocol will assess this parameter.

All the decision points below this graph are considered logically good decisions. Any of the decision points above this decision plane are considered risky decisions. For a healthy person, *H* will be high, say *H* = 0.9; thus, *Z* = 1 – 0.9 = 0.1. Now suppose that the trust on the agent/participant sending the sensing data is high, say *p* = 0.8. Also, the data sent by the agent could be mapped to a certain probability of worsening of user's health. Let this probability of loss of health (*G*) be 0.9. In this case this person can take this decision since the point (*Z*, *p*, *G*)=(0.1, 0.8, 0.9) would lie below the decision plane. But a person with *Z*=0.6 (not so healthy) cannot take this decision, because the point would lie above the decision plane.

The relationships between *p*, *Z*, and *G* are as follows: The higher the trust in the agent (who sends the data), the higher the *Z* value would be allowed. This is because the more one trusts the source of data and thereby the data itself, the more one can act on information even though one has a weaker health. The situation is opposite for *G*. The less the probability of harm to health, the more one can act on information. Given the above relationships, we adopt the following equation to relate p with Z and G, thus providing the decision plane for the decision trust [20].

$$Z = p^{\gamma} * (1 - G)^{\omega} \tag{1}$$

Here γ and ω are tuning parameters, whose values are application-specific. For our running scenario, we set γ =2 and ω =1.



Member health

Member	Health (H)
A	H_A= 0.2
B	H_B= 0.8
...	...

Dynamic location-based information for a phenomenon

Location	p	G	Z
x	0.8	0.2	0.512
...	...	...	...

Events at time t

Event request	Recommendation
A entering x	N
Bentering x	Y
...	...

(a)

(b)

Figure 3: Example of using the decision graph: (a) data used for decision making; (b) the action for member A is disapproval because $\boldsymbol{Z_A} > \boldsymbol{Z}$ and the action for member B is approval because $\boldsymbol{Z_B} \leq \boldsymbol{Z}$.

The calculated risk for performing the action (entering into a location in our running scenario) results in a decision point on the threshold decision plane dictating the health threshold required to perform this action. If member i's Z_i value ($Z_i = 1 - H_i$) is above this decision point ($Z_i > Z$) then the CA advises i against taking that action. If ($Z_i \leq Z$) then the CA advises i to take the action. This recommendation is sent to the member's mobile device (e.g. smartphone) guiding the member's decision making. In our running scenario we consider the action to physically enter into an area. However, our model can be easily extended to other scenarios like evacuation of people from a building [1].

C. Threat Model

Since a health IoT system relies on information sharing from several entities, it is important to analyze an entity's behavior with regards to being trustworthy or untrustworthy. IoT devices generally behave in a trustworthy manner in order to benefit personally from the health IoT system and remain in it. Furthermore, the effort required by IoT devices is minimal, as measurement and communication is done by devices without intervention. However, a malicious member may show untrustworthy behavior to further its interests. For example, a member may send an incorrect location rating to the CA in order to minimize the traffic flowing into the location by other members in that area. Furthermore, a member may be reluctant to waste its resources for the benefit of the health IoT system. Moreover, faulty sensors can give incorrect readings due to malfunction. Thus, our trust management protocol is to overcome these incorrect readings and provide the most trustworthy data that matches the actual environment for a given location for accurate decision making.

Our threat model also considers malicious attackers who aim to break down the health IoT system. That is, a malicious attacker will always send incorrect readings to the CA about the measured phenomenon at a location. A malicious attacker will also send false location rating feedback/information to further disrupt the health IoT system. Our threat model does not consider collusion behavior as in [7], i.e. malicious nodes collude to provide bad-mouthing attacks to good nodes to ruin their trust score, while providing ballot-stuffing attacks toward each other to boost their trust scores. This will leave as a future research extension.

TABLE I: Notation.

Symbol	Meaning
$R^x_{i,j}$	Rating / report data from member i about location x regarding phenomenon j
$Q^x_{i,j}$	Query from member i about location x regarding phenomenon j
$WR^x_{i,j}$	Aggregated rating intended for querying member i about location x regarding phenomenon j
$TR^x_{i,j}$	Aggregated trust of rating intended for querying member i about location x regarding phenomenon j
$LE^x_{k,j}$	Location experience that increases a member $k's$ rating trustworthiness when rating phenomenon j at location x
$\lvert A^x_j \rvert$	Total number of reports about phenomenon j in location x
$T^x_{k,j}$	Trust of member k for sensing phenomenon j at location x
∂	decay factor (decaying over time)

IV. PROTOCOL DESIGN FOR HEALTH IOT SYSTEMS

In this section, we describe our protocol design for a health IoT system. Each entity in the health IoT system will execute the protocol for effecting trust-based decision making. Table I lists the notation used in our protocol design.

A. Location Ratings

As illustrated in Figure 4, each health IoT device can send the sensed data from its PAN to the CA. Let $R^x_{i,j}$ denote a rating (or report) sent from member i about location x regarding phenomenon j where $R^x_{i,j}$ is in the range of [0, 1]. Here we note that the phenomenon is measured by a particular IoT device that is known to the IoT system. We will use j to denote the IoT device or simply the phenomenon measured by the IoT device. The CA receives the ratings sent from various IoT members and stores them in the cloud.

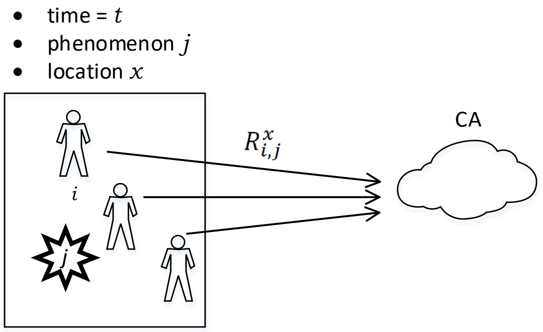


Figure 4: Member $\boldsymbol{i}$ sending location rating $\boldsymbol{R^x_{i,j}}$ at time $\boldsymbol{t}$ to the CA.

B. Query Proessing by the CA

As illustrated by Figure 5, a member, say member i, can obtain information regarding a particular location x by sending a query to the CA, denoted by $Q^x_{i,j}$, which represents a query from member i about location x regarding phenomenon j.The CA must examine its stored reports about location x and form a query reply $QR^x_{i,j}$ to supply member i with necessary information for decision making. It derives the aggregate rating for the location, taking into consideration of the associated trustworthiness scores of raters for the aggregate rating. More specifically, let $WR^x_{i,j}$ denote the *aggregated rating* about location x regarding phenomenon j, defined as follows:

$$WR^x_{i,j} = \frac{\sum_{k\in A^x_j} C_{k,j} \times LE^x_{k,j} \times \partial \times R^x_{k,j}}{\sum_{k\in A^x_j} C_{k,j} \times LE^x_{k,j} \times \partial} \tag{2}$$

where ∂ is a decay factor based on when $R^x_{k,j}$ was issued. Location ratings from members that have more experience in location x should be considered more trustworthy in rating the location's phenomenon. We call this factor "location experience" $LE^x_{k,j}$ which is the experience that increases a member's rating trustworthiness when rating phenomenon j at location x, defined as:

$$LE^x_{k,j} = \frac{\left|A^x_{k,j}\right|}{\left|A^x_j\right|} \tag{3}$$

where $\left|A^x_j\right|$ is the total number of reports received about phenomenon j in location x and $\left|A^x_{k,j}\right|$ is the total number of reports about phenomenon j in location x reported by member k. The capability of the device used by member k to sense phenomenon j denoted by $C_{k,j}$ is expressed by a range between 0 and 1 where $C_{k,j}$ closer to 1 means that the device is more capable of capturing accurate readings for phenomenon j. The CA is responsible for inferring $C_{k,j}$.

The aggregated trust for answering member i about location x regarding phenomenon j is defined as:

$$TR^x_{i,j} = \frac{\sum_{k\in A^x_j} T^x_{k,j}}{\left|A^x_j\right|} \tag{4}$$

where $\left|A^x_j\right|$ is the total number of reports about phenomenon j in location x and $T^x_{k,j}$ is the trust score the CA has toward member k about sensing phenomenon j at location x. This is to be discussed later in Section IV.C.

C. $WR^x_{i,j}$ as G and $TR^x_{i,j}$ as p for Decision Making

Our protocol uses $WR^x_{i,j}$ and $TR^x_{i,j}$for decision making. The parameter $WR^x_{i,j}$ corresponds to probability of health loss (G) since G is derived from sensing data, while parameter $TR^x_{i,j}$ corresponds to reliability trust (p) in the decision graph (shown in Figure 2). For our running scenario, the CA then can make a decision whether or not the user should enter location x based on if member $i's$ Z_i value falls below or above the decision plane (Z, p, G) defined by Equation 1.

Alternatively, the CA can send this information to i which can use this aggregated information for decision making (as opposed to receiving a yes/no decision from CA). Specifically, the CA can send the following information to member i: the time-decayed location rating list $D = \{\partial R^x_{1,j}, \ldots, \partial R^x_{n,j}\}$ and the trust list $T = \{T^x_{1,j}, \ldots, T^x_{n,j}\}$ containing the information about the n IoT devices that have sensed phenomenon j at location x and have sent their ratings to CA. Member i can then process this information locally for decision making. An advantage of this method is to enable the user to personalize the receiving information by further applying its own measurements of trust scores towards other entities such as its relatives and close friends which could be given higher trust by default and their information could be considered more trustworthy.

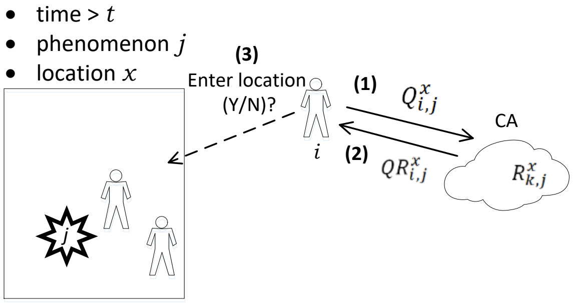


Figure 5: Steps for member decision making in the health IoT system: (1) Member $\boldsymbol{i}$ querying CA; (2) CA replying with decision or decision making information; (3) Member $\boldsymbol{i}$ decides based on obtained information and risk model (and possible local assessment), whether or not to enter location $\boldsymbol{x}$.

D. Trust Score Computation

To calculate the aggregate trust for answering member i about location x regarding phenomenon j (as in Equation 4) the CA needs to know whether the sensing report sent by each node k for sensing phenomenon j at location x is trustworthy. A member's trust score is time dependent, and more recent assessments of its trustworthiness contribute more to its current trust. The CA therefore must periodically calculate every member's trust score. If a node's updated trust score falls below a threshold, T_{thresh}, it is deemed untrustworthy and detected as malicious by the system. Let $T^x_{k,j}$ be the trust score of member k for sensing phenomenon j at location x, as computed by the CA, and $RR_{k,I}$ be the trust score given by the

CA in the I^{th} period. Then the overall trust score $T_{k,j}^{x}$ can be computed based on the trust scores of all intervals as:

$$T_{k,j}^{x} = \frac{\sum_{I=1}^{trc} \partial_I \times RR_{k,I}}{\sum_{I=1}^{trc} \partial_I} \tag{5}$$

where trc is the total number of periodic trust computations that have been performed by the CA, and $\partial_I$is the decay factor for the trust score computed in the I th interval. Member k's trust score at the I th interval, $RR_{k,I}$, is based on assessing three trust scores and is derived as:

$$RR_{k,I} = \alpha \times RR_{k,I}^{loc\_rating} + \beta \times RR_{k,I}^{rater} + \gamma \times RR_{k,I}^{loc\_verif} \tag{6}$$

where α, β and γ (with α+ β + γ = 1) are weights to prioritize three different trust scores, namely, $RR_{k,I}^{loc\_rating}$ for location rating trust score, $RR_{k,I}^{rater}$ for rater trust score, and $RR_{k,I}^{loc\_verif}$ for witness trust score, for computing the overall trust score $T_{k,j}^{x}$. Below we discuss these trust scores.

$RR_{k,I}^{loc\_rating}$ (Location Rating Trust Score): Every location rating given by a rater k is judged by the query issuer i whenever i actually enters location x and makes a self-observation itself, as shown in Figure 6. This way i can provide a feedback about k's rating, represented by $f_i(R_{k,j}^{x})$ = $R_{i,j}^{x}$ in Figure 6, allowing the CA to judge if k's location rating $R_{k,j}^{x}$was malicious or fabricated. Member i's mobile device and equipped sensors can automatically provide a feedback to the IoT cloud. Specifically we define:

$$RR_{k,I}^{loc\_rating} = \frac{\sum_{j\in K_j} \sum_{x\in K_x} \sum_{i\in FS(R_{k,j}^{x})} T_{i,j}^{x} \times \partial_{afr} \times d(f_i(R_{k,j}^{x}), R_{k,j}^{x})}{\sum_{j\in K_j} \sum_{x\in K_x} \sum_{i\in FS(R_{k,j}^{x})} T_{i,j}^{x} \times \partial_{afr}} \tag{7}$$

where K_j is the set of all location ratings reported by member k regarding phenomenon j, $K_x$is the set of all ratings reported by member k regarding location x, $FS(R_{k,j}^{x})$ is the feedback set of all members who had used the location rating $R_{k,j}^{x}$ provided by member k, and $T_{i,j}^{x}$ is the trust score of i for sensing phenomenon j at location x. Since i can be malicious and provides a false feedback to ruin the reputation of k, the CA takes $T_{i,j}^{x}$ into consideration as it computes $RR_{k,I}^{loc\_rating}$.

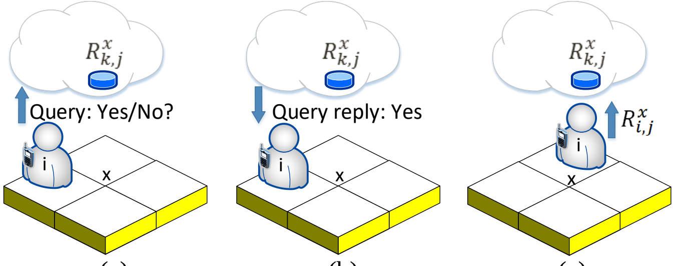
The basic idea of Equation 7 is to effectively judge the phenomenon measurement that should have been there with what was actually seen once there by i (supposedly). A restriction can be added to examine the most recent feedbacks and ratings only, thus limiting the number of feedbacks and ratings that need to be examined and stored. In Equation 7, ∂_{afr} is a feedback factor parameter defined as:

$$\partial_{afr} = \lambda^{\sigma} \tag{8}$$

where 0.9 < λ < 1.0 and σ is the standard deviation of the difference between time of assessment $t(RR_{k,I})$ vs. time of feedback $t\left(f_i(R_{k,j}^{x})\right)$ and time of location rating $t(R_{k,j}^{x})$. The basic idea of Equation 8 is that the closer these three timings are from each other, the higher the weight applied to the similarity comparison between the rating and its feedback. This keeps the comparison more relevant at the time of assessment (to minimize weight of old data) and keeps the comparison fair (so that ratings cannot be expected to be similar to current feedback ratings if there is a large time gap). The comparison of the rating and its feedback in Equation 7, $d(f_i(R_{k,j}^{x}), R_{k,j}^{x})$, is in the range of [0, 1], and defined as:

$$d(f_i(R_{k,j}^{x}), R_{k,j}^{x}) = 1 - \left|f_i(R_{k,j}^{x}) - R_{k,j}^{x}\right| \tag{9}$$

Based on Equation 9, suppose k reported a low phenomenon rating at location x, e.g. a low level of Particulate Matter (PM), resulting in a scaled value of $R_{k,j}^{x}$ = 0.2, and i relies on this rating and enters x only to find that the level of PM sensed by i ($R_{i,j}^{x}$ or $f_i(R_{k,j}^{x})$ in this context) maps to a high scaled value of 0.9, then we find $d(f_i(R_{k,j}^{x}), R_{k,j}^{x})$ results in a low similarity of 0.3. This low similarity contributes to a low location rating trust score for k (i.e., $RR_{k,I}^{loc_rating}$in Equation 7) because it is used as a weight in Equation 7.



(a). (b). (c).

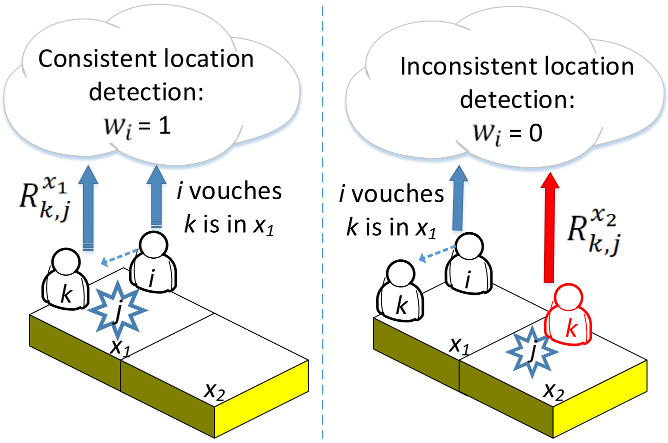
Figure 6: The process of assessing node k's location rating trust score: (a) i requests entering location x; (b) CA responds with agreement; (c) i enters location x and sends its own location rating to CA who uses it to judge if k (any node that has provided a rating of location x) has provided a true location rating.

$RR_{k,I}^{rater}$ (Rater Trust Score): This trust score assesses if node k is accurate as a rater. The basic idea is to compare node k's feedback with the majority of feedbacks about the same phenomenon in a location. Assume that k gave a feedback about $R_{i,j}^{x}$ provided by member i and that other feedback providers (each represented by u) also gave their feedbacks about the same phenomenon. Then, the rater trust score of node k is computed by:

$$RR_{k,I}^{rater} = \frac{\sum_{\substack{\forall i\ \forall x\ \forall u\in FS(R_{i,j}^{x}) \\ AND\ k\in FS(R_{i,j}^{x})}} T_{u,j}^{x} \times \partial_{aff} \times d(f_u(R_{i,j}^{x}), f_k(R_{i,j}^{x}))}{\sum_{\substack{\forall i\ \forall x\ \forall u\in FS(R_{i,j}^{x}) \\ AND\ k\in FS(R_{i,j}^{x})}} T_{u,j}^{x} \times \partial_{aff}} \tag{10}$$

where ∂_{aff} and $d(f_u(R_{i,j}^x), f_k(R_{i,j}^x))$ are defined in a similar way as in Equations 8 and 9. With Equation 10, an untrustworthy member fabricating its feedback will result in a low similarity with the majority of member feedbacks, thereby resulting in a low rater trust score.

$\boldsymbol{RR_{k,I}^{loc\_verif}}$ **(Witness Trust Score):** At every interval I, the CA examines the trustworthiness of its received ratings by all members since the last time interval. It relies on data from members that vouch for the correctness of the claim that another member was in fact in a location at a specific time. This can be verified since they were able to communicate over short range transmission (functioning as a substitution for physical eye sight) and this is can be relayed (piggybacked) back to the CA periodically. The benefit is twofold. First, Members that have been seen by other members in the reported location gain trust. Second, it can detect misbehavior in reported location ratings, including the case in which a member sending a rating is from two distant locations at the same time, or the case in which a member claiming to be at a location is seen elsewhere.


Consistent location detection:
w_i = 1
$R_{k,j}^{x_1}$
i vouches k is in x_1
k
i
j
x_1
x_2
Inconsistent location detection:
w_i = 0
i vouches k is in x_1
$R_{k,j}^{x_2}$
k
i
k
j
x_1
x_2

(a). (b).

Figure 7: (a) CA detects location consistency when *i* vouches for *k* at location $\boldsymbol{x_1}$ and *k* reports a location rating about *j* also from location $\boldsymbol{x_1}$; (b) CA detects inconsistency when *i* vouches for *k* at location $\boldsymbol{x_1}$but CA receives a location rating from *k* about *j* in location $\boldsymbol{x_2}$.

Let $OS_{k,t}^{x_1}$ be the set of witnesses that have come in contact with member k at time t at location x_1 while k had sent rating $R_{k,j}^{x_2}$ to the CA regarding j at location x_2. For each witness i, if $x_1 = x_2$ then i's claim is consistent with k' s claim in terms of k' s location at time t and hence the CA sets the weight of $w_i = 1$ to increase i's witness trust. Otherwise, $x_1 \neq x_2$, and $k's$ rating is considered suspicious based on information supplied by i, so the CA sets $w_i = 0$. Figure 7 illustrates the witness trust score assessment process. This is done for every witness i that has claimed to be in the vicinity of k at time t. In case there is no observation for or against i, the CA sets $RR_{k,i}^{loc\_verif}$ to a neutral value of 0.5. Thus we have:

$$RR_{k,I}^{loc\_verif} = \begin{cases} \dfrac{\sum_{i \in OS_{k,t}^x} T_{i,j}^x \times w_i}{\sum_{i \in OS_{k,t}^x} T_{i,j}^x}, & |i \in OS_{k,t}^x| \neq \emptyset \\ 0.5\,, & |i \in OS_{k,t}^x| = \emptyset \end{cases} \tag{11}$$

With Equation 11, favorable observations will increase the witness trust score, anomalous and suspicious observations will decrease the witness trust score, and absence of information will result in a neutral (0.5) witness trust score.

E. Protocol Description in Pseudo Code

```
CA Execution:
Get next event
if event is $T_{period}$ timer then
    For each member k
        determine trust rating for interval $RR_{k,I}$ by
        Equation 6 from calcualting
            location rating score $RR_{k,I}^{loc\_rating}$ by Equation 7)
            rater score $RR_{k,I}^{rater}$ by Equation 10
            witness score $RR_{k,I}^{loc\_verif}$ by Equation 11
        update the overall trust score $TR_{i,j}^x$ by Equation 5
        if $(TR_{i,j}^x < T_{thresh})$ identify node as malicious
         for eviction
else if event is location query arrival $Q_{i,j}^x$ then
    detemine aggregate location rating $WR_{i,j}^x$ by
     Equation 2
    detemine the overall trust score $TR_{i,j}^x$
    by Equation 4
     find decision point Z where
            $G = WR_{i,j}^x$ and $p = TR_{i,j}^x$ by Equation (1)
    Retrieve $H_i$ for member i from
     the database and set $Z_i = 1 - H_i$
    if $Z_i \leq Z$
        return approval message
    else
         return dissapproval message
else // event is location rating message arrival $R_{k,j}^x$
    extract and store location rating of location x by k
    extract and store vector of seen members at
     location x by k
    update location experience $LE_{k,j}^x$ for member k
     by Equation 3

Member Execution:
Get next event
if event is arrival at location x then
    send rating message $R_{k,j}^x$ to CA including measured
        phenomenon j rating and seen members vector
        send location query for next movement to CA
    if CA returns approval message
        move to location
    else
        try another location/wait/take min risk location
```

The CA interacts regularly with all health IoT members, answering their queries and storing all reports necessary for decision making. The protocol description specifying the actions to be taken by the CA and the members in response to dynamically changing environments and events is shown above in pseudo code format. Lines 3-9 contain the procedure followed by the CA to compute the trust of each IoT device in every T_{period} interval. The overall trust score of a given member is computed by finding the location rating trust score (line 6), rater trust score (line 7), and the witness trust score (line 8), which are then used to update the overall trust score (line 9). If the node's trust value falls below the minimum trust threshold T_{thresh} the node is identified as malicious for eviction. Lines 10-18 contain the procedure followed by the CA in the event of a query arrival. The CA finds the aggregate rating of the location (line 11) and the associated trustworthiness (line 12) as the values of G and p respectively. The decision point Z is then derived (line 13) and the CA replies with a query reply approval or disapproval response based on the stored querying member's health (lines 13-18). In the case of a location rating message arrival (lines 19-22) the CA stores the location information along with the vector of seen members. The member's location experience is then updated. Lines 24-32 show the operation of a member. In the case of a member arriving at a location (assuming prior approval from CA), the member sends the phenomenon rating along with the seen members vector to the CA (line 27). The next action the member takes is when it is near a new location and wants to know if it should enter the new location (28-32), it sends a location query to the CA and takes action based on the returned result.

V. Performance Evaluation

In this section we perform ns3 simulation for performance evaluation of our trust-based decision making protocol, and conduct a comparative analysis with two baseline decision making protocols. Our performance metric is the correct decision ratio (CDR), i.e., the ratio of the number of correct decisions over the total number of decisions, by a user. This performance metric is measured dynamically. As more information is collected regarding the trustworthy behavior of nodes in the system, more correct decisions will be made, so CDR should converge to a high value as time progresses.

TABLE II: Parameters for Performance Evaluation.

Name	Value	Name	Value
$M \times M$	10×10(1km×1km)	S_{ph}	0.2m/s
N_T	100	T_{period}	1hr
P_m	$[0, 30\%]$	T	[20,30] hrs
S_N	1m/s	T_{comp}	[5,10,15]
H	[0.25, 1]	T_{thresh}	0.3

Table II lists the parameters used in the simulation. In our experimental setup we consider an environmental health IoT system with N_T=100 members, each using a smart IoT device for simplicity.

The percentage of malicious nodes is specified by a parameter $P_m \in [0, 30\%]$ to test the effect of malicious population on performance. The malicious nodes are randomly selected out of all IoT devices. A node selected to be in this "malicious" population remains malicious throughout the simulation. All nodes move randomly in an *M*-cell by *M*-cell operational area. A hazardous condition is created and is moving at a slower speed S_{ph} =0.2m/s than the average node mobility S_N=1m/s. A node issues a query before it steps into a cell. Based on the CA's recommendation, the node decides to enter the cell or not. The mobility route changes as a result if the recommendation is no. The CA calculates the trust scores of all members of the health IoT system in every T_{period} = 1 hour, and the total simulation time is *T*=20 hours so we can observe the CDR convergence behavior. We set the trust rating factor weights to $\alpha = \beta = \gamma = 1/3$.

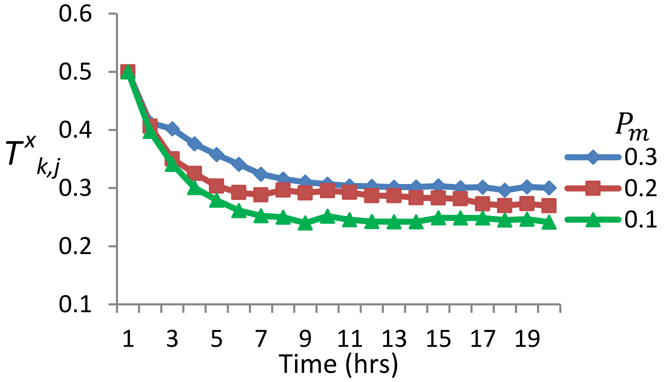


Figure 8: $\boldsymbol{T^x_{k,j}}$ vs. time for a randomly selected malicious node *k*.

Figure 8 shows $T^x_{k,j}$ (the trust score of *k* for sensing phenomenon *j* at location *x*) vs. time for a malicious node *k* randomly selected. We see that as time progresses, the trust score of this malicious node decreases and finally converges to a low value reflecting the untrustworthiness status of the malicious node. This demonstrates the effectiveness of our designed mechanisms against malicious attacks.

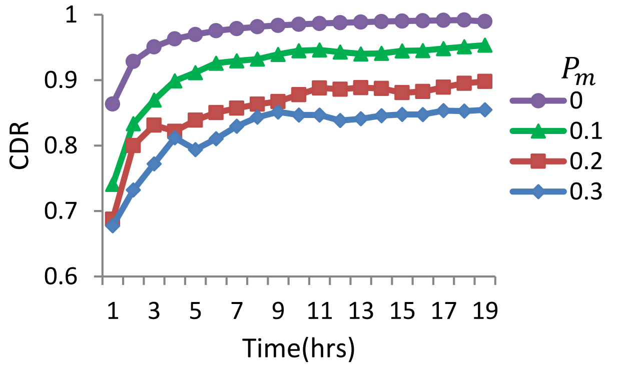


Figure 9: CDR vs. time for a good node randomly selected over a range of $\boldsymbol{P_m \in [0, 30\%]}$.

Figure 9 shows CDR vs. time for a good node randomly selected over a range of $\boldsymbol{P_m \in [0, 30\%]}$ in increment of 10%.

Here the decision made at time $\boldsymbol{t}$ for member $\boldsymbol{i}$ to decide whether or not to enter location $\boldsymbol{x}$, given $\boldsymbol{i}$ ' $\boldsymbol{s}$ health $\boldsymbol{H_i}$ as input, can be verified against the correct decision using the ground truth rating of the sensed phenomenon for which CDR=1. Hence, we can verify whether $\boldsymbol{i}$ had made a correct decision by comparing it with the decision using ground truth information at simulation time. More specifically, we first use Equation 1 to find the Z value calculated as $\boldsymbol{Z}\left(\boldsymbol{TR}^{\boldsymbol{x}}_{\boldsymbol{i,j}}, \boldsymbol{WR}^{\boldsymbol{x}}_{\boldsymbol{i,j}}\right)$ as well as the ground truth Z value calculated as $\boldsymbol{Z^{gt}} = \boldsymbol{Z}(\mathbf{1}, \textbf{ground truth rating})$. Then, a correct decision is defined as whether the logical operation $(\boldsymbol{Z_i} \le \boldsymbol{Z}) \equiv (\boldsymbol{Z_i} \le \boldsymbol{Z^{gt}})$ returns true. The outcome is reflected in the CDR value as shown in Figure 9.

We see that when there is no malicious node in the system, i.e. $P_m = 0\%$, CDR converges fairly quickly as more information is collected as time progresses. The convergence time increases as P_m increases. However, we see that CDR eventually converges to a high value even when P_m is as high as 30%. We attribute this to the ability of our trust protocol to discern malicious nodes from good nodes and the effectiveness of our trust-based decision making protocol to make correct decisions based on the relationship between the patient's risk classification (Z), the decision's reliability trust (p), and the loss of health probability (G).

Figure 10 demonstrates the effectiveness of our strategy in identifying and evicting untrustworthy users. In Figure 10, we show the percentage of malicious nodes being detected over time under varying initial malicious node populations ($P_m \in [0, 30\%]$). As time progresses the system is able to discern malicious nodes from good nodes based on the computation of trust scores reflecting the behavior of the nodes. Once a malicious node's trust score falls below a threshold T_{thresh} it is deemed untrustworthy and identified as malicious by the system. We find that in all cases ($P_m \in [0, 30\%]$) a near 100% of malicious nodes will be detected as untrustworthy, and the higher the P_m the longer it takes for the system to identify all malicious nodes.

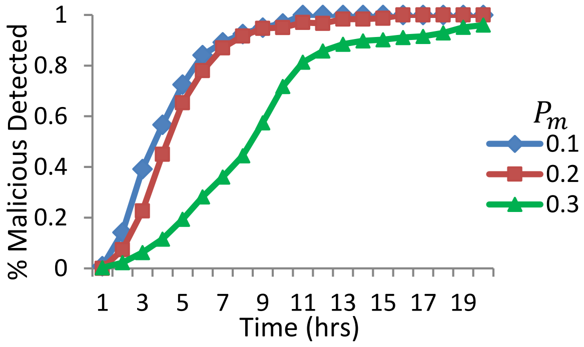


Figure 10: Percentage of malicious nodes detected vs. time over a range of $\boldsymbol{P_m} \in [\mathbf{0}, \mathbf{30}\%]$ with $\boldsymbol{T_{thresh}}$=0.3.

In Figure 11, we show how our trust system measures the trust score of a good node, k, turning into malicious after T_{comp} (ranging from 5hrs to 15hrs) is elapsed. We observe that in all cases our trust system is quick to adapt to the changing behavior of node k by decreasing its trust score $T^x_{k,j}$. As soon as k turns into malicious, $T^x_{k,j}$ decreases rapidly. We observe that the speed at which k's trust score decreases is about the same for all three curves as soon as k turns malicious. We attribute this to the desirable accuracy property of our trust score computation method.

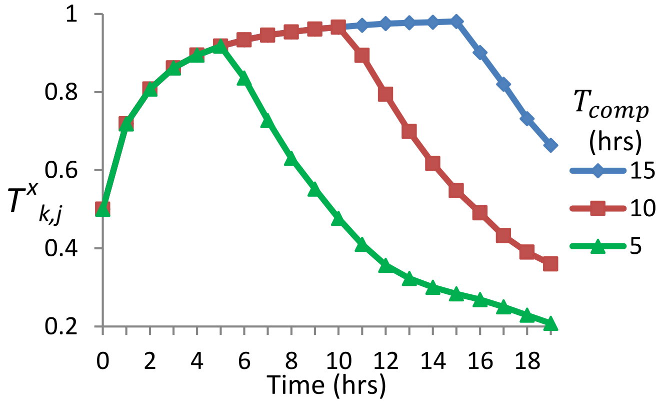


Figure 11: $\boldsymbol{T^x_{k,j}}$ vs. time for a randomly selected good node $\boldsymbol{k}$ turning malicious after a duration of $\boldsymbol{T_{comp}}$.

Figure 12 shows the effect of a member's health status on CDR. For a randomly selected good member, we examine CDR under varying member health (H) and percentage of malicious nodes in the system (P_m). For example, the red curve shows CDR vs. time under $(P_m, H) = (0.2, 0.5)$. An interesting trend is that the lower the health of the member (lower H) the more sensitive it is to attacks by malicious nodes (higher P_m) and, consequently, the higher the chance of this member making an incorrect decision. CDR is improved by our protocol as it effectively detects and lowers the trust scores of malicious nodes within the system, thus forcing malicious nodes to be evicted once a minimum trust threshold has been reached. Unlike CDR, the resulting trust level of a node is not dependent on the node's health status.

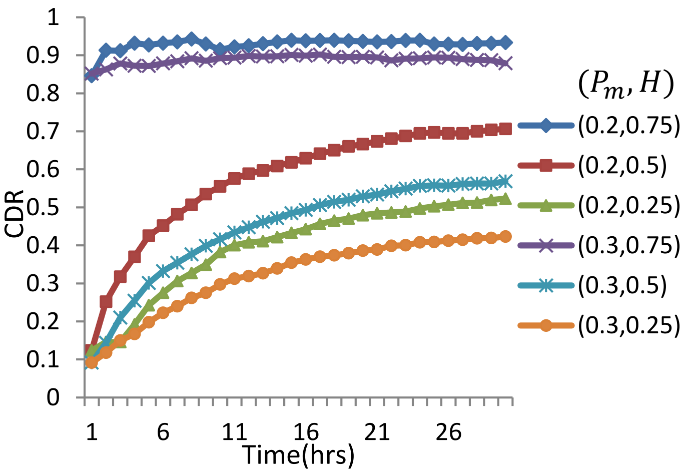


Figure 12: Effect of a member's health status on CDR.

In Figure 13, we show the Mean Squared Error (MSE) between the actual phenomenon rating and the aggregate phenomenon rating based on the location ratings collected from IoT devices. We perform this evaluation under varying node compromise percentages with $P_m \in [0, 20\%]$. We observe that in all cases the MSE decreases with time and finally converges to a low value.

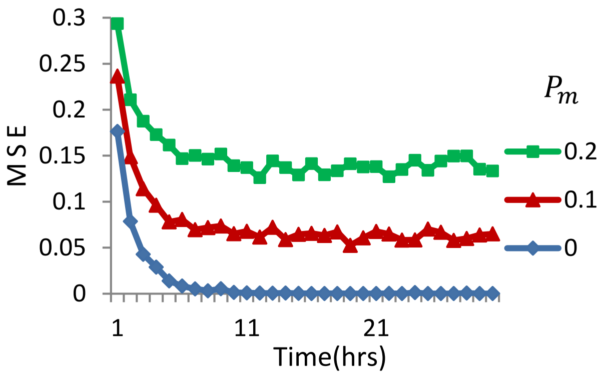


Figure 13: MSE vs. time for the aggregate phenomenon measurements of the $\boldsymbol{M} \times \boldsymbol{M}$ area selected over a range of $\boldsymbol{P_m} \in$ [0, 20%] in increment of 10%.

This is due to the ability of our trust system to recognize malicious nodes and decrease their trust scores, thereby resulting in the aggregate phenomenon rating closer to the actual phenomenon rating. This demonstrates the effectiveness of our trust management protocol in collecting sensed data from health IoT devices to create a map of a phenomenon which can guide health-based decision-making for individual health IoT members.

We conduct a comparative analysis of our protocol with two baseline approaches:

- No Trust (NT): The first baseline protocol does not have trust management in place to evaluate the trustworthiness of information sources, and merely uses location ratings provided by the sources. Under NT, we use $1 - G$, where $G = WR^x_{i,j} = \frac{\sum_{k \in A^x_j} \partial \times R^x_{k,j}}{\sum_{k \in A^x_j} \partial}$ representing the average location rating weighed on time decay, to make a decision. Then, a correct decision is defined as whether the logical operation $(Z_i \leq 1 - G) \equiv (Z_i \leq Z^{gt})$ returns true, with $(Z_i \leq Z^{gt})$ being the ground truth decision.
- No Member Health (NMH): The second baseline protocol uses the traditional trust score (as in [17, 18]) to filter untrustworthy information sources but does not consider the relation between the member's health and the derived level of harm from the phenomenon, i.e., it does not relate Z_i with G. In other words, NMH merely uses filtered "trustworthy" location ratings to make decisions. Under NMH, we use $p \times (1 - G)$ to make decisions, with $p = TR^x_{i,j} = \frac{\sum_{k \in A^x_j} T^x_{k,j}}{|A^x_j|}$ and $G = WR^x_{i,j} = \frac{\sum_{k \in A^x_j} \partial \times R^x_{k,j}}{\sum_{k \in A^x_j} \partial}$, where p represents the reliability trust of sources and G represents the average location rating weighted on time decay. Then, a correct decision is defined as whether the logical operation $\left(d_{thresh} \leq p \times (1 - G)\right) \equiv (Z_i \leq Z^{gt})$ returns true, where d_{thresh} is the health decision threshold. Thus, the decision maker simply takes the decision if the outcome is generally perceived to be safe (above d_{thresh}). In this case, a member may overestimate required health (when using large d_{thresh}) or underestimate required health (when using small d_{thresh}).

Figure 14 compares our protocol (labeled "Our") with NT and NMH in terms of CDR, with $P_m \in$ [20, 30%] and $H_i \in$ [0.25, 1.0] for member i to make decisions. To simulate an unknown member health value, we set a fixed d_{thresh}=0.5 under the NMH protocol.

We first observe that a higher P_m results in a lower CDR because they are more false location rating reports to filter out. We clearly see that our protocol outperforms NT and NMH as time progresses due to its ability to recognize malicious nodes and thus effectively filter out untrustworthy ratings, and its design to consider member i's health status when making decisions. While NT takes member health into account when making decisions, it does not distinguish false ratings from true ratings, and thus its CDR is highly dependent on P_m. NMH also has a low CDR since it does not use a health value close to member i's health status as a third design dimension for decision making.

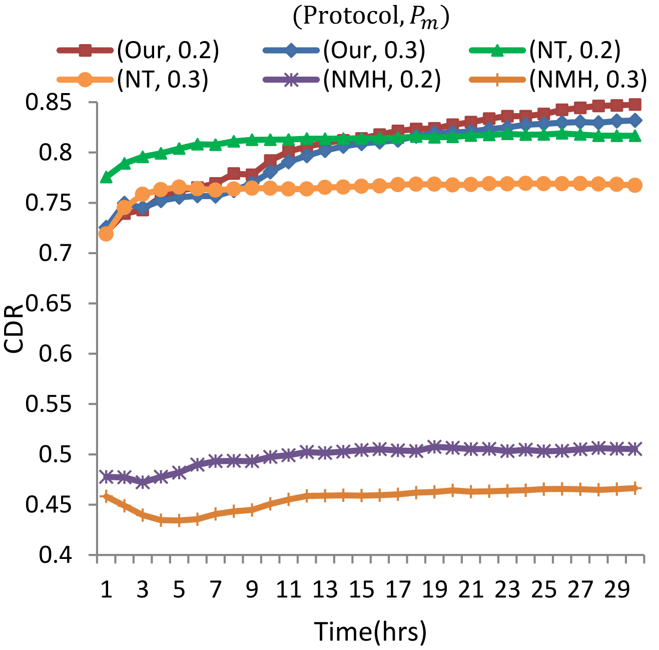


Figure 14: Performance comparison of our protocol vs. NT and NMH under varying $\boldsymbol{P_m} \in$ [20, 30%].

VI. Conclusion

In this paper we proposed and analyzed a trust-based decision making protocol for health IoT systems. We described the problem and thus the motivation to create a trust-based decision making protocol for a health IoT system. Our trust-based health IoT protocol considers risk classification, reliability trust, and loss of health probability as three design dimensions for decision making. We developed a trust computation protocol for a health IoT system to assess the reliability trust of individual IoT devices. We also developed a method to aggregate sensing data and derive the probability of health loss, should the user enter a given location at a given time. Based on the user's vulnerability our system then assesses if the risk is low or high enough to support or refute the user's request of entering the location specified in the query. Our simulation results demonstrated the feasibility of our approach with a high correct decision ratio (CDR) relative to the ground truth case with CDR=1 despite increasing malicious node population in a health IoT system. We also conducted a comparative performance analysis of our proposed trust-based health IoT protocol with two baseline protocols (NT and NMH) with convincing results.

In this work, we considered the case in which there is a centralized cloud collecting and analyzing sensing reports submitted by individual IoT devices. In the future, we plan to extend our analysis to the case in which IoT devices themselves form a distributed cloud and cooperate for storage and processing. We also plan to consider social IoT characteristics for peer-to-peer trust assessment, and take the pairwise trust assessment results into consideration to enhance the accuracy of trust-based decision making for health IoT systems.

Acknowledgment

This work was supported and funded by Kuwait University Research Grant #QS01/15.

References

[1] P. Fraga-Lamas, T. Fernández-Caramés, M. Suárez-Albela, L. Castedo, and M. González-López, "A Review on Internet of Things for Defense and Public Safety," *Sensors,* vol. 16, no. 10, p. 1644, 2016.

[2] S. Raza, P. Misra, Z. He, and T. Voigt, "Building the Internet of Things with bluetooth smart," *Ad Hoc Networks,* 2016.

[3] E. Borgia, "The Internet of Things vision: Key features, applications and open issues," *Computer Communications,* vol. 54, pp. 1-31, 2014.

[4] Adafruit Industries, New York City, NY, USA. Adafruit Industries products.2017.[Online].Available: https://learn.adafruit.com/category/adafruit-products [Accessed: 25- Apr- 2017].

[5] Sensorcon, Williamsville, NY, USA. Sensorcon Sensing Products by Molex. 2017. [Online]. Available: http://www.sensorcon.com [Accessed: 25- Apr- 2017].

[6] I. R. Chen, F. Bao, and J. Guo, "Trust-based service management for social internet of things systems," *IEEE Transactions on Dependable and Secure Computing,* vol. 13, no. 6, pp. 684-696, 2016.

[7] 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.

[8] K. Habib, A. Torjusen, and W. Leister, "Security analysis of a patient monitoring system for the Internet of Things in eHealth," in *Proceedings of the International Conference on eHealth, Telemedicine, and Social Medicine*, 2015.

[9] S. C. Mukhopadhyay and N. Suryadevara, "Internet of Things: Challenges and Opportunities," in *Internet of Things*: Springer, 2014, pp. 1-17.

[10] A. B. Pawar and S. Ghumbre, "A survey on IoT applications, security challenges and counter measures," in *IEEE International Conference on Computing, Analytics and Security Trends*, 2016, pp. 294-299.

[11] 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.

[12] J. Guo, I. R. Chen, and J.J.P. Tsai, "A survey of trust computation models for service management in internet of things systems," *Computer Communications,* vol. 97, pp. 1-14, 2017.

[13] M. Nitti, R. Girau, and L. Atzori, "Trustworthiness management in the social internet of things," *IEEE Transactions on knowledge and data engineering,* vol. 26, no. 5, pp. 1253-1266, 2014.

[14] Y. B. Saied, A. Olivereau, D. Zeghlache, and M. Laurent, "Trust management system design for the Internet of Things: A context-aware and multi-service approach," *Computers & Security,* vol. 39, pp. 351-365, 2013.

[15] B. P. Wong and B. Kerkez, "Real-time environmental sensor data: An application to water quality using web services," *Environmental Modelling & Software,* vol. 84, pp. 505-517, 2016.

[16] A. Morales-Torres, I. Escuder-Bueno, I. Andrés-Doménech, and S. Perales-Momparler, "Decision Support Tool for energy-efficient, sustainable and integrated urban stormwater management," *Environmental Modelling & Software,* vol. 84, pp. 518-528, 2016.

[17] P. Sharma and P. D. Kaur, "Effectiveness of web-based social sensing in health information dissemination - a review," *Telematics and Informatics,* vol. 34, no. 1, pp. 194-219, 2017.

[18] H. Anumala and S. M. Busetty, "Distributed Device Health Platform Using Internet of Things devices," in *2015 IEEE International Conference on Data Science and Data Intensive Systems*, 2015, pp. 525-531.

[19] S. H. Chang, R. D. Chiang, S. J. Wu, and W. T. Chang, "A Context-Aware, Interactive M-Health System for Diabetics," *IT Professional,* vol. 18, no. 3, pp. 14-22, 2016.

[20] A. Jøsang and S. L. Presti, "Analysing the relationship between risk and trust," in *International Conference on Trust Management*, 2004, pp. 135-145.

[21] M. K. Kim, H. Ter Jung, S. D. Kim, and H. J. La, "A Personal Health Index System with IoT Devices," in *IEEE International Conference on Mobile Services*, 2016, pp. 174-177.

Hamid Al-Hamadi received the Bachelor degree in Information Technology from Griffith University, Brisbane, Australia in 2003, the Master degree in Information Technology from Queensland University of Technology, Brisbane, Australia in 2005, and the PhD degree in Computer Science from Virginia Tech, USA, in 2014. His research interests include security, Internet of things, mobile cloud, wireless sensor networks, and reliability and performance analysis. Currently he is an assistant professor in the Department of Computer Science, Kuwait University, Khaldiya, Kuwait.

Ing-Ray Chen received the BS degree from the National Taiwan University, and the MS and PhD degrees in computer science from the University of Houston. He is a professor in the Department of Computer Science at Virginia Tech. His research interests are primarily in service and trust management as well as reliability and performance analysis of mobile systems and wireless networks, including Internet of Things, wireless sensor networks, service-oriented peer-to-peer networks, ad hoc networks, mobile social networks, mobile web services, mobile cloud services, and cyber physical systems. Dr. Chen currently serves as an editor for *IEEE Transactions on Services Computing, IEEE Transactions on Network and Service Management, The Computer Journal*, and *Security and Network Communications*. He is a recipient of the IEEE Communications Society William R. Bennett Prize in the field of Communications Networking and a recipient of the U.S. Army Research Laboratory (ARL) Publication Award.