Trust Assessment of Smart Health Devices

Alexis Davidson
Fachbereich Mathematik und Informatik
Institut für Informatik
Freie Universität Berlin, Deutschland
Advisor: Emmanuel Baccelli

***Abstract*—With the increasing omnipresence of IoT in everyday life, IoT devices take a big place in our environment. In order to function properly, it is crucial to be able to trust our environment and IoT devices. In some domains like Smart Health, IoT can have a decisive influence on people's life and impact them fatally. In these scenarios particularly, it is important to trust these devices our lives depend on.**

In this paper, we present an overview of the current state of smart health devices in IoT. We describe some characteristics of trust in general, in the context of IoT and introduce the importance of trust management. We present the overall architecture of smart health monitoring systems, underlying the different units and risks coming with them. We then take an in-depth look at the aspects of human trust assessment and a specific trust quantifying method called TNA-SL using trust networks. Based on this method, we present some interesting mathematical and geometrical expressions of trust scenarios. The main problem with this method is that a lot of data is required for it to be meaningful. Most importantly, this method is one of many and underlines the complexity that trust quantifying represents.

We reviewed one method for human trust quantifying but many questions remain open. IoT systems are complex and especially health IoT systems need to be trustable on every layer of the architecture. This means that trusting the final overall product is not enough since every single component of the system has different levels of trust.

***Index Terms*—Trust Management, IoT, Smart Health, Trust Networks, Health Monitoring Systems.**

I. Introduction

A. Motivation

In the past decades, smart health systems evolved rapidly. Unlike most of the other IoT domains, smart health devices have the potential to impact people's life fatally. A patient who has bradycardia has a heart problem in which the heart rate becomes too slow. This patient can wear a pacemaker that will provide electrical impulse, causing the heart to beat and keep the heart rate from dropping below. A pacemaker is not necessarily an IoT device but it can be. In this case, machines having a connection are allowed to exchange information with hospital staff and doctors. Its activity can be remotely monitored, and eventual fatal cases can be detected and avoided. This function seems like an improvement but would it be wise to replace regular visits when the patients use to come to the doctor's office for a check with the remote monitoring? How far can we trust in smart health devices to be properly functioning at all times and how can we asses trust in them?

There are many different types and goals of smart health devices which can go from saving life to improving life or performance and monitoring data. To achieve a small overview over these, we will introduce some of them briefly in a section below.

B. Problem

Trust is a very complex subject and as we can see in the next section, many works proposed methods to represent it and quantify it with abstract and mathematical methods. In this paper, we choose to focus on one aspect of trust which is human trust by taking an in-depth look at a quantifying method called TNA-SL covered in different works in literature. Even if this method does not target smart health specifically, it can be applied for IoT and smart health as a subset of it.

C. Plan

To understand the functioning of smart health IoT, we first introduce some specific use cases of smart health systems. Then we describe some characteristics of trust in general, in the context of IoT and introduce the importance of trust management. After that, present the overall architecture of smart health monitoring systems, underlying the different units and risks coming with them. We then take an in-depth look at the aspects of human trust assessment and a specific trust quantifying method called TNA-SL using trust networks. Based on this method, we present some interesting mathematical and geometrical expressions of trust scenarios.

II. Related Works

In [21], the authors introduce a specific IoT environment called personal space IoT and propose 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. Their work do not address trust in Health-IoT.

The authors of [16] propose a novel security and privacy mechanism for health devices in IoT. Even if trust is directly linked to security and privacy, these are not the main focuses of this paper.

In [5], the authors consider multiple trust properties with which they propose a trust management protocol in the context of service composition. They analyze the effect of trust parameters on trust assessment accuracy and more. This paper touches trust in IoT but does not cover trust in smart health devices.

The authors of [24] address the challenges about effective integration of scattered devices and technologies. Their paper are focused on the technology and architecture of Health-IoT, which we are interested in, but do not address trust.

In [18], the authors investigate the impact of this health technology on the relationship between management and operatives, the formulation of health and safety rules and the risk perception and risk behavior of operatives. While these aspects play a role in trust assessment of health devices, organizational issues are not the focus of this paper.

Many works analyze trust as an abstract concept [1], [12], [14], [34]. Some works focus on trust in the context of IoT [17], [19], [27], [31]. For the in-depth look into trust, we choose to follow [10], [11] which present a trust quantifying method called TNA-SL that can be used in IoT, smart health devices and human trust networks.

III. Use cases of smart health devices

Before diving into the subject of trust in IoT in smart health devices, we need to get a general idea about smart health systems and their practical uses. In this chapter, we briefly introduce two specific domains of smart health: smart cards and health monitoring.

A. Smart Cards

Whether for money withdrawing, for a fitness membership or for timestamp controlling at work, we're all familiar with smart cards and we use them every day. In the context of healthcare, smart cards carry personal and health information and act as an access key to the patients' data [20].

1) Typical scenario: When a patient arrives at a doctor's reception, he hands over his card at the desk and is immediately identified. Previous records and related documents are read and the patient is guided to the waiting room while its name gets appended to the list of waiting patients.

On entering the consulting room, the patient hands over his card again and the doctor can rapidly use it to retrieve previous care encounters, tests, and reports.

The doctor, having special rights, is then allowed to record drugs prescriptions and an encounter summary on the patient's card.

2) Health insurance: In some countries, having a health insurance is mandatory. The health smart card is provided by the insurance company and also serves as a proof for insurance cover. Thanks to this, transaction and data transmission between medical care providers, health insurance companies and drugstores is simplified, accelerated and more cost-effective. A patient only needs to bring his card to the doctor's office and the bill is redirected to the insurance company via the insurance card.

In 2006 the European health insurance card has replaced the health insurance card in most EU countries [8]. Another advantage here is gained: patients are allowed to continue their stay and receive treatment in foreign countries. They do not have to return home for medical care.

B. Health Monitoring

Health monitoring systems can have very different uses and impacts on patients or users. Following are some examples of health monitoring devices and their uses.

1) Smart vest: A smart vest is a wearable physiological monitoring system in the form of a washable shirt, using sensors connected to a central processing unit and firmware [23]. Data like body's temperature, heart rate, blood pressure and more is collected and can be used to produce an overall picture of the wearer's health [4]. For example, patients with lungs injuries and diseases can wear a smart vest to monitor the development of their condition and be warned when confronting endangering situations.

2) Smart home for elderly: To assist the large percentage of the elderly people that live independently, specific smart home technology has been developed. Sensors, cameras, pulse rate and blood pressure are used to measure weight, light and temperature data. Also the presence of gas or smoke, fall risk and moisture can be detected in the home [3], [26].

IV. Trust in IoT

The interconnection of devices in IoT makes the use of them unavoidable in the every day life. It even came to a point where tasks solely depend on the ability of IoT devices to perform, which is why trusting IoT devices can be so important in some domains, especially in smart health.

Trust is complicated and touches many different concepts like confidence, belief, expectation, reliability, integrity, security, dependability, ability, and more [38]. Aspiring trust as an IoT device is very challenging. In general, an IoT system is composed in three layers: a physical layer, an application layer and a network layer [22]. All of these layers are interconnected and the whole system relies on the cooperation among layers and other properties like security, privacy and more. If if the trustworthiness of one IoT layer is ensured, it does not say the same for the other layers automatically.

A. Factors influencing trust

There are various definitions of trust to be found in literature. In [30], the authors define trust as "a state involving confident positive expectations about anothers motives with respect to oneself in situations entailing risk", highlighting three attributes of trust:

- A trust relationship involves two or more entities: a trustor and a trustee
- Trust involves risk since there is no guarantee that the trustee will live up to the trustor's expectation.
- The trustor believes in the trustee's honesty and benevolence

Factors influencing trust can be summarized into the five following categories [36].

- Trustee's objective properties: safety, reliability, utility and maintainability.
- Trustee's subjective properties: benevolence, motivations and honesty.
- Trustor's subjective properties: confidence, expectation, belief and gratification.
- Trustor's objective properties: purpose, assessment, regulation and standards.
- Context: situation, environment and risk.

B. Characteristics of trust

In their work on adoption of a multidisciplinary view on trust, the authors of [28] observe common characteristics of trust. Trust is:

- directed: The trust relationship between the trustor and the trustee is an oriented relationship.
- subjective [9].
- context-dependant.
- measurable.
- influenced by past experience.
- dynamic: may change with time.
- conditionally transferable: information about trust can be transmitted and received.
- a composite property: "trust is really a composition of many different attributes: reliability, dependability, honesty, truthfulness, security, competence, and timeliness, which may have to be considered depending on the environment in which trust is being specified" [9].

C. Trust modeling and trust management

A trust model specifies, evaluates and sets up trust relationships amongst entities in order to calculate trust [36]. It can help answer the problem of trust measurement in a variety of ways. In their work, the authors of [2] proposed a trust model based on online virtual communities maintaining global knowledge about entire networks. The authors of [25] founded their trust model focusing on cryptographic technologies. Some trust models target only specific trust properties, such as risk and reputation [32].

Trust management can be achieved through trust modeling. It concerns itself with "collecting the information required to make a trust relationship decision; evaluating the criteria related to the trust relationship as well as monitoring and reevaluating existing trust relationships; and automating the process" [9]. [37] proposes the four following aspects to be included in trust management:

- Trust establishment: establish the trust relationship between a trustor and a trustee
- Trust monitoring: monitor the performance of the trustee to collect evidence for trust assessment
- Trust assessment: evaluate the trustworthiness of the trustee.
- Trust control and re-establishment: control or re-establish the trust relationship in case it was broken before.

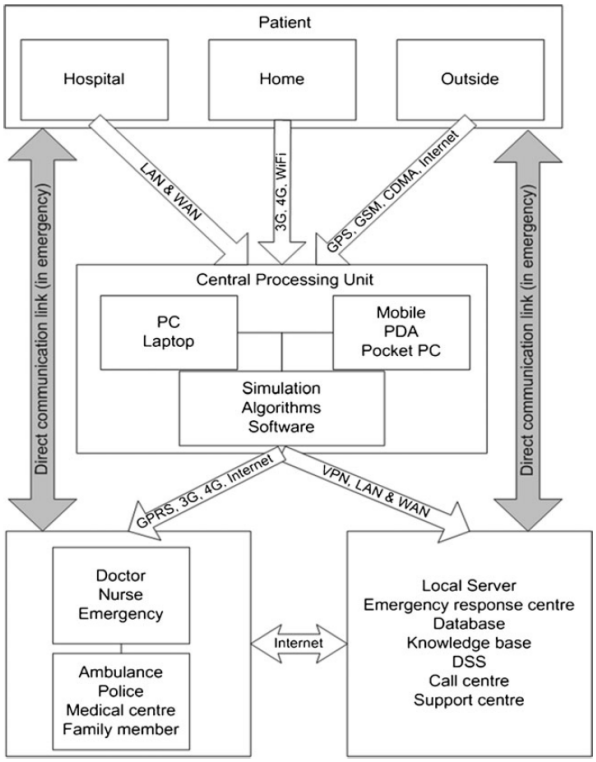

Fig. 1. Overall architecture of smart health monitoring systems [4]

V. Architecture and risks of health monitoring systems

In order to go in depth into trust assessment in smart health, we need to narrow down our field of work. Mainly based on the work [4], we choose to focus on trust in the context of health monitoring systems.

A. Architecture of smart health monitoring system

The overall architecture of smart health monitoring systems is represented in Fig. 1. It is composed in three main parts: the Patient Unit, the Central Processing Unit and the Doctor and Emergency Units. For the whole system to work, it is important that each unit is properly working and has a functioning communication with the other units at all time.

1) The Patient Unit: Whether the patient is at home, outside or in a hospital, the used wearable health monitoring devices remain in communication with the Central Processing Unit. The only distinguishing factors are the communication channels. From a hospital, LAN & WAN are used to communicate with the Central Processing Unit. From home, the WiFi, the 3G or the 4G. From outside: GPS, GSM, CDMA, Internet. At all times, the patient needs to be able to contact the Doctor and the Emergency Unit directly.

2) The Central Processing Unit: The Central Processing Unit fetches all data coming from the monitoring health devices of the patients. Data are gathered, sorted, and interpreted using the right algorithms. The results are then transferred to the Doctor Unit for monitoring and to the Emergency Unit to be stored in a knowledge database.

3) The Doctor and Emergency Units: The Doctor Unit receives incoming data from the Central Processing Unit for monitoring. When receiving an alert, a doctor can contact the Emergency Unit directly to take action. Also, both the Doctor and the Emergency Units have a direct communication channel with the Patient Unit.

B. Risks

To understand the value of being able to trust such a health system, we can take the example of the smart vest and review the possible catastrophic outcomes when a single component within the IoT system fails.

1) System shutdown: If a system e.g. a monitoring PC in the Central Processing Unit fails, incoming data from patients cannot be fetched and transferred to the Doctor and Emergency Units. If the patient were to enter a state where a doctor would interpret a fatal danger, it would go unnoticed.

A typical way to bypass this problem is to provide backup systems to relay a failing component.

2) Software error: No software is bug free and that applies to the algorithms fetching data from patients and interpreting them as well. The software might still be running and not explicitly return any error, but the results given back may contain some. In the worst case, the software could return a false negative which means that it interprets that a patient is fine when it actually is in a endangered situation. In the case of a false positive, the algorithm interprets a danger where there is not. This might cause an emergency situation where there is not and costs but not put a life in danger.

One strategy to limit this problem is to develop the same software or algorithm twice from completely independent teams. To avoid error redundancy, these teams are not allowed to contact each other. This strategy is one of many used in the development of reliable airplane software [7].

3) Communication: If a communication channels ends up unreliable, critical data may end up not being sent and a dangerous situation may end up not being detected.

4) Personal: Not only machines but also people are part of the smart health monitoring system. If a doctor does not read the output of a software right, or misjudges the condition of a patient calling, help can not be sent when it is actually needed.

For developers, making an IoT health system trustable is about making sure that these scenarios as little chance to happen as possible when patients use it. As a patient, trust in an IoT health system is about being convinced that none of these scenarios is bound to happen when using it.

VI. Human trust

To fully trust a smart health system, every component of the network must be trustable at each level. E.g. for a health monitoring system, each aspect represented in the Fig. 1 must be trustable: the software, the hardware, the communication channels, the energy sources and the personal operating behind the machines. In this chapter, we take an in-depth look at the aspects of human trust assessment and trust quantifying methods using trust networks.

A. Transitivity and reflexivity

To some extent, trust is transitive. For example, if a patient A trusts a health smart watch because of a previous positive experience, he can recommend it to a patient B who will in turn, depending on its relationship with patient A, gain some level of trust towards the device [17].

In general trust may not be reflexive. If a patient trusts its doctor for an operation, it is not implied that the doctor trusts its patient for an operation or something else. While in some areas there might be tendencies of mutuality or equality, health and smart health are domains that do not aspire reflexivity in trust.

B. Psychological aspects of risk and risk assessment

Recognizing and assessing risks is not easy. Since many actors take part in the creation of an IoT device, it is difficult to recognize whether this IoT device is part of an hostile environment or is safe. On top of that, humans suffer from wishful thinking and have problems associating risks with abstract things like the computers and the internet.

The authors of [33] analyzed the psychology of security and report that ”People tend to believe they are less vulnerable to risks than others. People also believe they are less likely to be harmed by consumer products compared to others. It stands to reason that any computer user has the preset belief that they are at less risk of a computer vulnerability than others.”

In [29], the authors point that people tend to exaggerate spectacular but rare risks, people have trouble estimating risks for anything not exactly like their normal situation, and more.

We can take from this that trust is not a product from rational thinking but a sum of emotions and complex thinking behaviours.

C. Reputation

Directly linked with transitivity, reputation can be good or bad and is a decisive factor for trust. This is used in marketing where one usually attempts to associate a product with a known public figure or expert. That way unknown devices or services gain trust by transitivity even if the consumers have not tried it yet [27]. Reputation in IoT can also be built on an amount of opinions, like for example groups in social network.

D. Quantifying trust

We explained to some extent why it is not always possible to trust software, hardware, devices and services. Furthermore, when adding malicious intent to the equation, an IoT environment can be very dynamic and hostile. On top of that, the human aspects adds to the complexity and emotional responses can override rational thinking.

With all the factors that we named previously, it seems quite difficult to quantify trust meaningfully. In the following section we investigate a promising model for quantifying trust using trust relationships in the context of a trust network analysis.

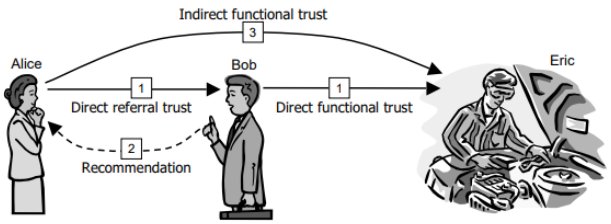

Fig. 2. Transitive trust principle [11]

VII. Trust networks

As we can see in other works, trust quantifying happens by using an abstract trust model [1], [19], [31]. In this chapter, we review a method for trust network analysis using subjective logic (TNA-SL) proposed in [11]. The trust networks consist of transitive trust relationships between people, organizations and possibly software agents. In out Smart Health IoT perspective, these entities could relate to each other and communicate via channels represented in Fig. 1. First we will make some definitions, then we will present a structured notation and finally use these to go into subjective logic.

A. Transitivity

Transitivity means that if Alice trusts Bob and Bob trusts Eric, then Alice trusts Eric (see Fig. 2). This is called a *recommendation*.

A *Trust scope* is a specific type of trust in a trust relationship. For example, if Bob trusts Eric for fixing cars, Bob will not necessarily trust him for being a good doctor.

In Fig. 2, we can see different kind of trusts represented with the arrows. The ability to recommend represents *referal trust*. The trust in the ability of being a good car repairer represents *functional trust*. In this case the scope of the trust is the same, which is to be a good car mechanic. Since Bob recommends Alice directly, this referal trust is considered *direct*. The same goes for the trust of Bob in Eric to be a good car mechanic. Alice trusts Eric because of Bob's recommendation. Alice does not know Eric and has not experienced his skills so this trust is considered *indirect*.

B. Parallel trust combination

Collecting advice from several sources helps to be better informed when making decisions. It can be modelled as *parallel trust combination*. In Fig. 3, Alice needs to find a good doctor. Alice asks Bob and David for an opinion. They both reply that they know Claire, who recommended Eric to them. Alice does not know Claire but since she received two recommendations for her as an advisor, Alice's trust in Claire is stronger than if she only had one recommendation. The effect of parallel combination of positive trust is to strengthen the derived trust.

The case where the parallel combinations are conflicting, that is one recommendation is positive and the other one negative will be covered in a following subsection.

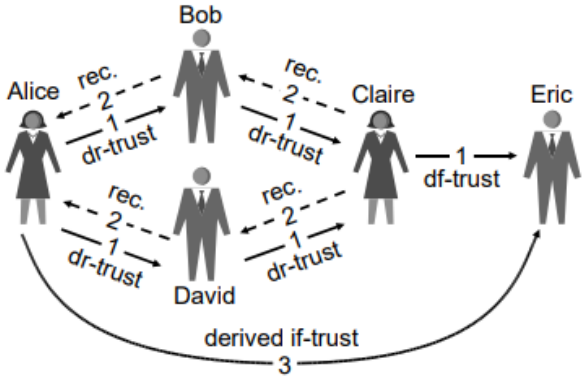

Fig. 3. Parallel combination of trust paths [11]. *rec.* stand for *recommendation*, *dr-trust* for *direct referal trust*, *df* for *direct functional trust* and *if-trust* for *indirect functional trust*.

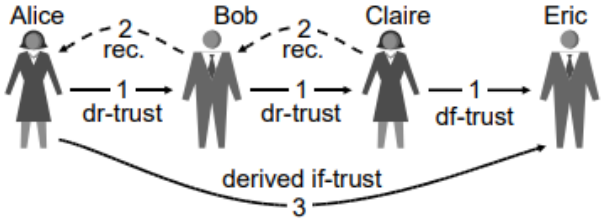

Fig. 4. Transitive trust arcs [11].

C. Structured notation

To represent many different entities, we will drop the names such as Alice and Bob and use capitals letters A, B, C, D and E instead.

A trusts B can be noted as [A,B]. The symbol ":" denotes a transitive connection.

In the simple case shown in Fig. 4, A trusts B, B trusts C and C trusts E, so A trust E.

Using these notations, we can express the case of Fig. 4 with an implicit scope as:

$$([A,E]) = ([A,B] : [B,C] : [C,E])$$

A trust scope is denoted as σ. The functional variant is denoted by "fσ" and the referal variant by "rσ". To distinguish between a direct trust and an indirect trust, we can prefix the trust scope respectively by "d" (dσ) or "i" (iσ). Combined with referral and functional trust, for example a direct functional trust is denoted "dfσ". We can include the scope in the trust notation like this: $[A,B,df\sigma]$. Taking scope into account, the trust network in Fig. 4 can be expressed as:

$$([A,E,if\sigma]) = ([A,B,dr\sigma] : [B,C,dr\sigma] : [C,E,df\sigma])$$

To express parallel paths in the context of parallel trust, the symbol "$\diamond$" is used. The trust graph of Fig. 2 combined of two parallel trust paths from Alice to Eric is expressed as:

$$([A, E, if\sigma]) = (([A, B, dr\sigma] : [B, C, dr\sigma])\diamond$$
$$([A, D, dr\sigma] : [D, C, dr\sigma])) :$$
$$[C, E, df\sigma]$$

Using the short notation, the same trust graph is expressed as:

$$([A, E]) = (([A, B] : [B, C])\diamond$$
$$([A, D] : [D, C])) : [C, E]$$

Fig. 2 contains two paths. We can express the two paths separately, as:

$$([A, E]) = ([A, B] : [B, C] : [C, E])\diamond$$
$$([A, D] : [D, C] : [C, E])$$

The problem with this expression is that the arc [*C*, *E*] is appearing twice. In some combination models, this expression has a different meaning than the one where [*C*, *E*] is appearing once. Generally, the desirable expression of a graph will be the one where an arc only appears once. This expression is called a *canonical expression*.

With these structured notations, large trust networks can be expressed, containing information of source, target and scope.

D. Subjective logic

Subjective logic is a belief calculus used for calculative analysis trust networks. In this subsection we point out how to derive trust with the belief calculus of subjective logic, which is required for TNA-SL.

Belief theory is related to probability theory but the probabilities over the set of possible outcomes do not always add up to 1. *Belief calculus* can be used to approximate reasoning in situations where there is partial ignorance regarding the truth of a certain given proposition.

Specific belief calculus can be represented by *subjective logic*, using a belief metric called *opinion* in order to express beliefs [10]. An opinion is denoted as:

$$\omega_x^A = (b, d, u, a)$$

where *A* is the trustor of the statement *x*. *b* represents belief, *d* represents disbelief and *u* represents uncertainty, where $b, d, u \in [0, 1]$ and $b + d + u = 1$. The parameter $a \in [0, 1]$ is called the base rate and it represents the initial trust put in any member of the community before any positive or negative experience was observed. The base rate is used to compute an opinion's *probability expectation value* that can be expressed as:

$$E(\omega_x^A) = b + au$$

where *a* determines how uncertainty will contribute.

An opinion space can be mapped into the inside of an equal-sided triangle. For an opinion $\omega_x = (b_x, d_x, u_x, a_x)$, the position of the point in the triangle representing the opinion is determined by the parameters b_x, d_x and u_x. In Fig. 5, we can see such an equal-sided triangle with an example opinion $\omega_x = (0.7, 0.1, 0.2, 0.5)$ positioned within.

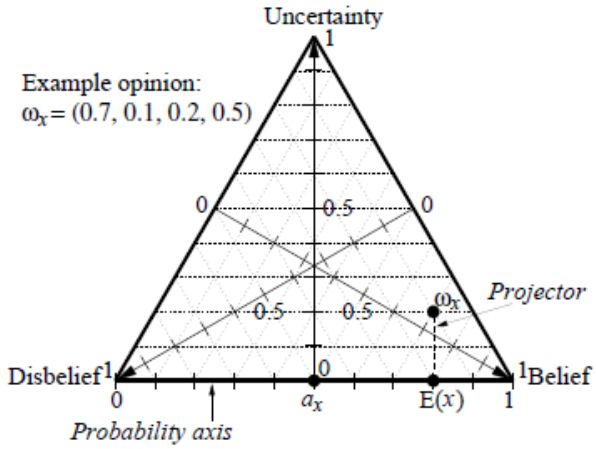

Fig. 5. Opinion equal-sided triangle with example opinion [11]. The top vertex represents uncertainty, the bottom left vertex represents disbelief and the bottom right vertex represents belief.

A linear function on the triangle takes the value 0 on the edge joining uncertainty and disbelief and takes the value 1 at the belief vertex. On the segment represented by this linear function, the parameter b_x is placed. The parameter a_x on the other hand is placed on the *probability axis* joining disbelief and belief. On this axis, the projection of ω_x corresponds to the value of the probability expectation value $E(\omega_x^A)$.

There are different criteria that can be used to order opinions. Two opinions ω_x and ω_y can be ordered following rules by priority [10]:

- The opinion with the greatest probability expectation is the greatest opinion.
- The opinion with the least uncertainty is the greatest opinion.
- The opinion with the least base rate is the greatest opinion.

The probability density function (PDF) can express the probability density over opinion spaces. It is denoted as (α, β). If *r* represents a number of positive past observations and *s* represents a number of negative past observations, with *a* expressing the initial base rate, α and β are expressed as [6]:

$$\alpha = r + 2a, \beta = s + 2(1 - a)$$

[6], [15] show that the parameters of an opinion and the parameters of a PDF can be determined as:

$$\begin{cases} b_x = r/(r+s+2) \\ d_x = s/(r+s+2) \\ u_x = 2/(r+s+2) \\ a_x = \text{base rate of } x \end{cases} \iff \begin{cases} r = 2b_x/u_x \\ s = 2d_x/u_x \\ 1 = b_x + d_x + u_x \\ a = \text{base rate of } x \end{cases} \quad (1)$$

E. Assessing trust with reputation systems

These trust mathematical expressions and representations are compatible with the reputation representation of Bayesian reputation systems. Thanks to this, we can use reputation systems to determine or assess trust measures. In this subsection, we briefly go over the complex method of Bayesian reputation systems presented in [13], [14], [34], [35].

In Bayesian reputation systems, agents rate other agents in transactions. They can rate positively and negatively in any amounts and take the form of a vector:

$$\rho = \begin{bmatrix} r \\ s \end{bmatrix}, \text{ where } r \geq 0 \text{ and } s \geq 0$$

For example, we can have a simple binary rating system with $\rho^+ = [1, 0]$ for a positive transaction and $\rho^- = [0, 1]$ for a negative transaction [12].

We denote a single particular rating as ρ^X_{Z,t_R} where *X* is the rating of *Z* at a time t_R.

1) Aging ratings: Agents and human agents tend to change their behaviour over time. To work with this, we can attribute a greater weight to more recent ratings. To do this, we add a parameter λ called *longevity factor*, controlling the rate at which old ratings are no more meaningful.

$$\rho^{X,t}_{Z,t_R} = \lambda^{t-t_R} \rho^X_{Z,t_R}, \text{ where } 0 \leq \lambda \leq 1$$

and where t is the current time and t_R the time at which the rating was taken into account.

2) Aggregating ratings: Aggregating ratings can be done by simply adding the rating vectors. $\rho^t(X, Z)$ is the aggregate rating of two ratings *X* and *Z* and is expressed as:

$$\rho^t(X, Z) = \sum \rho^{X,t}_{Z,t_R}, \text{ where } t_R \leq t$$

So if we want to aggregate the ratings for Z for an entire agent community C, it can be expressed as:

$$\rho^t(Z) = \sum_{X \in C} \rho^t(X, Z)$$

3) The reputation score: $R^t(Z)$ is called *Z*'s reputation score at time *t* and is defined as [11]:

$$R^t(Z) = E[\text{beta}(p^t(Z))] = \frac{r + 2a}{r + s + 2}$$

with $0 \leq R^t(Z) \leq 1$. The reputation score represents the probability indicating the reliability of a specific agent Z in the future.

The role of the base rate parameter a is interesting to observe in this equation. If the base rate *a* is high, that means the initial trust in the agent is relatively high, a single negative rating *s* will have more impact on the reputation score than a single positive rating *r*. On the other hand, if the base rate *a* is low, a single positive rating will have more impact than a single negative rating. As pointed out in [11], this behaviour models an intuitive observation from everyday life: "it takes many good experiences to balance out one bad experience".

F. Applying TNA-SL to smart health IoT

In this section we briefly presented simple mathematical representations of the TNA-SL method from [10], [11]. Trust quantifying can be very complex and many works present different mathematical methods going in depth. What we want to underline in this chapter is that trust can be represented mathematically and we can attribute probability for future outcomes of agents in a community.

Even if the method seems to be abstract, it is applicable on many areas, even in IoT and so smart health IoT. Even if we chose to go for the trust aspect of human trust, these networks are also applicable for IoT devices and other trust aspects.

VIII. Summing up and open issues

We have introduced smart health by describing use cases of some specific smart health devices. On this basis, we presented characteristics of trust in general and in the context of IoT, then introduced the importance of trust management. We presented the overall architecture of smart health monitoring systems, underlying the different units and risks coming with them. We took an in-depth look at the aspects of human trust assessment and a specific trust quantifying method called TNA-SL using trust networks. Based on this method, we were able to present some interesting mathematical and geometrical expressions of trust scenarios. The main problem with this method is that a lot of data is required for it to be meaningful. Most importantly, this method is one of many and underlines the complexity that trust quantifying represents.

We reviewed one method for human trust quantifying but many questions remain open. IoT systems are complex and especially health IoT systems need to be trustable on every layer of the architecture. This means that trusting the final overall product is not enough since every single component of the system has different levels of trust.

Smart Health IoT may not be as much concerned by malicious intent compared to other IoT domains, if malicious intent was added in the game, the consequences could be catastrophic. For this reason, smart health systems need a superior level of security, guarding against very rare but life-threatening attacks.

To continue the research on trust in smart health devices, one could review different trust quantifying methods and eventually find one working with less data than TNA-SL. One could research about the psychological difference when using an IoT smart devices and an IoT device from another domain and its effect on trust. One could take an in-depth look at each and every single aspect of the many factors influencing trust. Finally, looking at the overall architecture of smart health monitoring systems, one could go over each channel, each unit and make an in-depth analysis of the reliability of those, since they all contribute to the overall reliability and trustability of the smart health system.

References

[1] Alfarez Abdul-Rahman and Stephen Hailes. A distributed trust model. In *Proceedings of the 1997 workshop on New security paradigms*, pages 48–60. ACM, 1998.

[2] Alfarez Abdul-Rahman and Stephen Hailes. Supporting trust in virtual communities. In *Proceedings of the 33rd annual Hawaii international conference on system sciences*, pages 9–pp. IEEE, 2000.

[3] Amaya Arcelus, Megan Howell Jones, Rafik Goubran, and Frank Knoefel. Integration of smart home technologies in a health monitoring system for the elderly. In *21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07)*, volume 2, pages 820–825. IEEE, 2007.

[4] Mirza Mansoor Baig and Hamid Gholamhosseini. Smart health monitoring systems: an overview of design and modeling. *Journal of medical systems*, 37(2):9898, 2013.

[5] Fenye Bao and Ray Chen. Trust management for the internet of things and its application to service composition. In *2012 IEEE international symposium on a world of wireless, mobile and multimedia networks (WoWMoM)*, pages 1–6. IEEE, 2012.

[6] Morris H DeGroot and Mark J Schervish. *Probability and statistics*. Pearson Education, 2012.

[7] Dave E Eckhardt, Alper K. Caglayan, John C. Knight, Larry D. Lee, David F. McAllister, Mladen A. Vouk, and John P. J. Kelly. An experimental evaluation of software redundancy as a strategy for improving reliability. *IEEE Transactions on software engineering*, 17(7):692–702, 1991.

[8] Frank Gotthardt. Communication method of an electronic health insurance card with a reading device, July 28 2011. US Patent App. 12/935,008.

[9] Tyrone Grandison and Morris Sloman. A survey of trust in internet applications. *IEEE Communications Surveys & Tutorials*, 3(4):2–16, 2000.

[10] Audun Jøsang. A logic for uncertain probabilities. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 9(03):279–311, 2001.

[11] Audun Jøsang, Ross Hayward, and Simon Pope. Trust network analysis with subjective logic. In *Proceedings of the 29th Australasian Computer Science Conference-Volume 48*, pages 85–94. Australian Computer Society, Inc., 2006.

[12] Audun Jøsang, Shane Hird, and Eric Faccer. Simulating the effect of reputation systems on e-markets. In *International Conference on Trust Management*, pages 179–194. Springer, 2003.

[13] Audun Josang and Roslan Ismail. The beta reputation system. In *Proceedings of the 15th bled electronic commerce conference*, volume 5, pages 2502–2511, 2002.

[14] Audun Jøsang, Roslan Ismail, and Colin Boyd. A survey of trust and reputation systems for online service provision. *Decision support systems*, 43(2):618–644, 2007.

[15] Audun Jøsang, Simon Pope, and David McAnally. Normalising the consensus operator for belief fusion. In *Proceedings of the International Conference on Information Processing and Management of Uncertainty (IPMU2006)*. Paris, July, 2006.

[16] KANG Kai, Zhi-bo PANG, and WANG Cong. Security and privacy mechanism for health internet of things. *The Journal of China Universities of Posts and Telecommunications*, 20:64–68, 2013.

[17] Geir M Køien. Reflections on trust in devices: an informal survey of human trust in an internet-of-things context. *Wireless Personal Communications*, 61(3):495–510, 2011.

[18] Gerd Kortuem, David Alford, Linden Ball, Jerry Busby, Nigel Davies, Christos Efstratiou, Joe Finney, Marian Iszatt White, and Katharina Kinder. Sensor networks or smart artifacts? an exploration of organizational issues of an industrial health and safety monitoring system. In *International Conference on Ubiquitous Computing*, pages 465–482. Springer, 2007.

[19] Matthew KO Lee and Efraim Turban. A trust model for consumer internet shopping. *International Journal of electronic commerce*, 6(1):75–91, 2001.

[20] Roderick Neame. Smart cardsthe key to trustworthy health information systems. *Bmj*, 314(7080):573, 1997.

[21] Tham Nguyen, Doan Hoang, and Aruna Seneviratne. Challenge-response trust assessment model for personal space iot. In *2016 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops)*, pages 1–6. IEEE, 2016.

[22] Huansheng Ning, Hong Liu, and Laurence T Yang. Cyberentity security in the internet of things. *Computer*, 46(4):46–53, 2013.

[23] PS Pandian, K Mohanavelu, KP Safeer, TM Kotresh, DT Shakunthala, Parvati Gopal, and VC Padaki. Smart vest: Wearable multi-parameter remote physiological monitoring system. *Medical engineering & physics*, 30(4):466–477, 2008.

[24] Zhibo Pang. *Technologies and Architectures of the Internet-of-Things (IoT) for Health and Well-being*. PhD thesis, KTH Royal Institute of Technology, 2013.

[25] Radia Perlman. An overview of pki trust models. *IEEE network*, 13(6):38–43, 1999.

[26] MW Raad and Laurence Tianruo Yang. A ubiquitous smart home for elderly. *Dept. of Comput. Eng., King Fahad Univ. of Pet. & Miner., Dhahran, Saudi Arabia*, 2008.

[27] Jon Robinson, Ian Wakeman, Dan Chalmers, and Ben Horsfall. Trust and the internet of things. In *Joint International Workshop on Trust in Location and Communications in Decentralised Computing (TruLoco10), Morioka, Japan*. Citeseer, 2010.

[28] Denise M Rousseau, Sim B Sitkin, Ronald S Burt, and Colin Camerer. Not so different after all: A cross-discipline view of trust. *Academy of management review*, 23(3):393–404, 1998.

[29] Bruce Schneier. *Beyond fear: Thinking sensibly about security in an uncertain world*. Springer Science & Business Media, 2006.

[30] D Susan and John G Holmes. The dynamics of interpersonal trust: Resolving uncertainty in the face of risk. *Cooperation and Prosocial Behavior; Cambridge University Press: New York, NY, USA*, page 190, 1991.

[31] Yao Wang and Julita Vassileva. Trust and reputation model in peer-to-peer networks. In *Proceedings Third International Conference on Peer-to-Peer Computing (P2P2003)*, pages 150–157. IEEE, 2003.

[32] Guo Wei, Xiong Zhongwei, and Li Zhitang. Dynamic trust evaluation based routing model for ad hoc networks. In *Proceedings. 2005 International Conference on Wireless Communications, Networking and Mobile Computing, 2005.*, volume 2, pages 727–730. IEEE, 2005.

[33] Ryan West. The psychology of security. *Communications of the ACM*, 51(4):34, 2008.

[34] Andrew Whitby, Audun Jøsang, and Jadwiga Indulska. Filtering out unfair ratings in bayesian reputation systems. In *Proc. 7th Int. Workshop on Trust in Agent Societies*, volume 6, pages 106–117, 2004.

[35] Ryan Wishart, Ricky Robinson, Jadwiga Indulska, and Audun Jøsang. Superstringrep: reputation-enhanced service discovery. In *Proceedings of the Twenty-eighth Australasian conference on Computer Science-Volume 38*, pages 49–57. Australian Computer Society, Inc., 2005.

[36] Zheng Yan and Silke Holtmanns. Trust modeling and management: from social trust to digital trust. In *Computer security, privacy and politics: current issues, challenges and solutions*, pages 290–323. IGI Global, 2008.

[37] Zheng Yan and Ronan MacLaverty. Autonomic trust management in a component based software system. In *International Conference on Autonomic and Trusted Computing*, pages 279–292. Springer, 2006.

[38] Zheng Yan, Peng Zhang, and Athanasios V Vasilakos. A survey on trust management for internet of things. *Journal of network and computer applications*, 42:120–134, 2014.