Experience Modelling For Ubiquitous Computing: A Mathematical Approach

Nalini A. Mhetre*[a], Arvind V. Deshpande[b], Parikshit N. Mahalle[c], and Pravin A. Thakre,[d]

[a] Asst. Professor, Dept. of Computer Engg., Sinhgad College of Engg., Pune, India
[b] Principal, Smt. Kashibai Navale College of Engineering, SPPU., Pune, India.
[c] Professor, Dept. of Artificial Intelligence and Data Science, Vishwakarma Institute of Information Technology, Pune, India.
[d] Professor, Zeal College of Engg And Research, Pune, India.
[a] nalini.mhetre@gmail.com, [b] principal.skncoe@sinhgad.edu, [c] aalborg.pnm@gmail.com, [d] thakrepa@rediffmail.com

Article History: Received: 10 November 2020; Revised 12 January 2021 Accepted: 27 January 2021; Published online: 5 April 2021

Abstract: In ubiquitous computing environment, nodes communicate in dynamic, heterogeneous and distributed environment. Support for wireless technologies further extends the association between devices to interact with each other. For mobile nodes, many a times associations are volatile in nature. There is always a risk associated with such transactions when there is no experience and trust with each other's' reputation. From security perspective, there is requirement of a proper mechanism to build trust and experience so that nodes can interact with each other for safe sharing of their resources. So far, several trust and reputation models have been proposed to secure the such communication. However, important factor ubiquity exhibiting mobile nature of node and its impact on trust and experience is not much investigated.

In this paper, experience model for ubicomp nodes has been proposed. The novel concept of ubiquity and impact of access network type on trust relationship is presented. This model calculates experience score for a node using ubiquity and other parameters like history, reliability and transitivity. Further, experience model is formulated and evaluated with mathematical approach. Evaluation results show that model effectively calculates experience score of the ubicomp node with respect to parameters considered. This experience model can easily be incorporated with various self-regulating access control systems.

Keywords: Experience Model, History, Reliability, Transitivity, Trust, Trust Model, Ubiquitous Computing, Ubiquity

1. Introduction

Since its introduction in 1988 by M.D. Weiser, Ubiquitous Computing (UbiComp) (Weiser, 1999) now becomes a buzzword in today's technology world. It's a paradigm, an innovation that touched every aspect of our life and still functions in the background, providing value to a user without getting in the way. Internet of Things (IoT) is a subset of UbiComp which refers to a broad range of internet-connected devices capable of communicating with each other and networks. These devices are either multifunctional or doing single specific tasks, but their inherent value is the information they collect to perform certain tasks. The Majority of IoT devices have the capability to process data still some are only intended to sense data and transmit it elsewhere to process. Take an example of a smart thermostat, which senses outside temperature, humidity and starts air conditioner when both are high or adjust air conditioner temperature accordingly while in operation. This type of smart and ubiquitous nature is appealing to users as these devices can engage in a kind of learning that empowers them to collect and recall information which allows them to adjust individual tastes.

Statistics (BusinessInsider, n.d.) predict, there will be 41 billion IoT devices by 2027 and that's a huge number. Their need to gather and analyse a huge amount of data will demand more sophisticated and secure edge data points. They should be capable of directing the resulting digital information within a secured, trusted, and self-regulating communication network of devices. There is always a risk associated with transactions when there is no prior experience and familiarity with each other's reputations. In other words, devices need to start the trust-building process with zero trust or limited trust. In UbiComp environment, conventional relationship with a network provider may no longer exist. It might have been replaced by a considerably fuzzier connection with so many unknown entities, network nodes, and service providers. Moreover, these devices could be mobile in nature. Due to mobility, there will be change in network dynamics and adaptation to it is significant. To manage this type of uncertainty and risks in UbiComp environments, there is an urgent demand of designing adequate and suitable strategies. These strategies should support trust as well as assist communicating entities to complete reliable transactions in secure way.

In human behaviour, the notion of trust develops as experience grows. Trust is a crucial factor when dealing with things in everyday life. When we buy any item, we select particular brands because we trust in them, compared to unknown brands for quality and other factors. This trust in them comes from our experience of

using their products, or from the reputation they received from other people or the recommendation of our friends or family. Variations in experience affect trust relationships.

In distributed UbiComp, nodes establish a communication channel with each other directly, cooperate with each other by shared information and resources. These types of nodes form communities dynamically and establish relations with unknown and unrelated peers. Groups or communities can improve the scalability and robustness of the network by improving task delegation amongst a smaller set of trusted nodes. Traditional static association methods are not suitable for such groups because of the dynamic and decentralized nature of the network and hence trust and reputation have demonstrated importance in dynamic association formation. However, there will be a trade-off between the flexibility of the environment with high risk and privacy disclosures. Because, much of the node's context is continually being recorded, transmitted, and stored by wireless devices (sensors, access points, and so on). Thus, in a UbiComp environment, securing private resources is a major concern for devices. These types of networks are majorly ad-hoc in nature and lack initial direct trust.

But the question is, how to build such trust? There has been a lot of research done on how to establish trust through reputable third parties. Recommendations from trustworthy peers can be used for establishing trust between unknown entities. But in ubiquitous environments, due to their dynamic and open nature, numerous malicious nodes who give biased recommendations for their gains can also exist. Hence, incorporating means to avoid or decrease the effect of biased recommendations is an ultimate problem for trust models in ubiquitous systems. Furthermore, reliability of node is important attributes for trustworthy communication. There is no point in granting resources to those un-reliable nodes which are consistently engaged in unsuccessful communication. Ubiquitous nature and mobility of participating nodes also affects overall trustworthiness.

In this paper we have proposed experience computation model. It considers interaction history, reliability, transitivity, and ubiquity of the node. This model considers human notion of trust to build experience by considering above mentioned parameters. Also, mathematical model has been proposed for experience calculation. A novel approach has been proposed to investigate impact of node mobility on trust and overall experience with respect to various network technologies.

The remaining section of the paper is organized as follows: Section 2 explains the motivation for our study. A literature review of the traditional approaches regarding various trust models in UbiComp along with their merits and demerits is explained in section 3. Section 4 reflects the proposed experience model. Section 5 explains mathematical model for experience. 6 incorporates results and a discussion. Conclusively, section 7 concludes the paper.

2. Motivation

Experience, as a social concept, can be obtained using past interactions between two entities. After each interaction, an entity is aware of the behaviour of others (i.e., as per the expectation or not). Definition of experience according to Merriam-Webster dictionary is - “direct observation of or participation in events as a basis of knowledge”. Another version from the same dictionary defines experience as “the fact or state of having been affected by or gained knowledge through direct observation or participation”. X naturally trusts entity Y after several successful interactions that include both entities. Experience is the outcome of aggregate awareness about the behaviour which represents inter-relationship between entities. The larger the experience better it helps in the trust evaluation. Thus, the experience must be proportional to trust. Experience is thus the process of getting knowledge through events, actions, observations, and/or sensing. In other words, it means something that happens which leaves certain impressions behind. The term experience typically follows trust-related literature.

For device-to-device communication in a ubiquitous environment, the human analogy of experience and trust is equally applicable. Basically, the experience is subjective and context-dependent in nature. It means that the experience of a particular device may be different for its peers with the same context. It is may also be possible that experience may be different depending on the context between the same pair of devices. When there is no previous direct communication history between two entities, a trust relationship can be formed using transitive experiences generated from the peer chain in the form of recommendations. In the ubiquitous environment, the experience can be modelled using interactions/events between devices. The logs of these interactions/events can be stored and analysed to perceive the experience.

Recent technological advancements bring new challenges when nodes in networks are more mobile and form a Mobile ad hoc Network (MANET). All major literature considers trust and reputation as budling blocks for modelling experience. However, a much important aspect or property, the ubiquity of node is less discussed (Raikwar, 2012) while establishing trust between nodes. In our model, the experience of a node is calculated by

considering the ubiquity factor with equal importance. Thus, our model uses properties like history, reliability, transitivity, ubiquity to compute overall experience which is discussed in further sections.

3. Related work

3.1. Literature Review

Various methods have been developed to formalize trust in different domains like P2P networks (Kamvar, Schlosser, & Garcia-Molina, 2003) (Tahta, Sen, & Can, 2015), pervasive computing (D'Angelo, Rampone, & Palmieri, 2017), IoT (I. R. Chen, Guo, & Bao, 2014). Recent methods (Liu, Tredan, & Datta, 2014) (Taylor, Barakat, Miles, & Griffiths, 2018) started using a machine learning approach for generalizing and formalizing trust models compared to exiting methods which are tailored to limited context or domain-dependent. These models can be broadly categorized as centralized and distributed.

In (Ruan, Durresi, & Uslu, 2018)**,** proposed distributed trust management scheme based on direct interactions between edge nodes. The trust model is constructed to transfer jobs from malicious edge nodes to trustworthy nodes. Beta distribution along with Measurement theory is used in the model to estimate trustworthiness. A supplementary attribute, confidence, is used along with direct interactions to measure uncertainty in the model. The model used the weighted mean method to calculate final trust and provided more weight to incoming interactions compared to outgoing. In (D. Chen et al., 2011), for the IoT scenario, the author proposed a fuzzy logic-based trust management model (TRM-IoT), to increase cooperation and decision making among the sensor devices. This model is based on direct trust and reputations, where direct trust is considered as subjective probability value and reputation as objective and acknowledged value. Each node develops a direct trust in the other node by witnessing an end-to-end packet forwarding ratio, packet delivery ratio, and energy consumed. The indirect reputation about nodes is constructed based on the recommendations received from the peer nodes. The final trustworthiness score is processed by employing the fuzzy theory on the direct and indirect interactions. Models in (Ruan et al., 2018), (D. Chen et al., 2011) lacks context-awareness factors. In (Mahalle, Thakre, Prasad, & Prasad, 2013)**,** introduced a fuzzy approach, for context-aware trust-based access control in IoT (FTBAC). In their work, trustworthy ness is computed using fuzzy membership over linguistic information of devices based on the Mamdani scheme (If-else rule relationships). Trust calculation in their work is based on three parameters, experience, knowledge, and recommendation. NS2 based simulation is used to validate the proposed approach with the example of temperature application.

Distributed Trust Management Scheme (DTMS) - The main objectives of major techniques are establishing trust between communicating nodes either devices or humans and detecting malicious behaviour of nodes. In (Mendoza & Kleinschmidt, 2016) author proposed distributed trust management scheme which is based on decentralizing architecture to provide various services in IoT. Trust value calculation is based on direct interactions where initial trust is zero or neutral. All nodes broadcast services provided to other agents at certain intervals. The scheme works based on reward and penalty, where the reward is provided in terms of the increased trust when the agent provides the requested service in time, and the penalty is imposed when it failed to do so. In author (Truong, Lee, Askwith, & Lee, 2017) represented a trust evaluation model based on reputation, experience as direct interactions, and knowledge. This model emphasis on SIoT environment and covers multidimensional aspects of trust by adding heterogeneous information from direct observations, personal experience, and global reputation.

The context-based Social Trust Model for the Internet of Things (CBSTM-IoT) (Rafey, Abdel-Hamid, & El-Nasr, 2016) is designed to increase the collaboration among trusted nodes and limit the interaction of malicious nodes. This model has two components node transaction factor and social relationship. The node transaction factor relies on context importance, computation power, confidence, and feedback, where the social relationship is based on owner trust and SIoT relationship. Trust is calculated for each node in the range of [0-1] when they have interaction. This trust is the result of a combination of direct and indirect trust. When there is no prior interaction default trust value assumes to be 0.5 and if any sort of communication is identified, the value is set to 1. In case of no prior history, it calculates trust by recommendations from other nodes in a specific context. CBSTM-IoT is adaptive in nature and can adjust to changes in a network environment. Major issue in this model is, it cannot control malicious node which acts sometimes fairly and allocate higher trust values to other nodes. Hence more indirect recommendation decreases accuracy and performance of trust calculation.

Trust-based Adaptive Security in the IoT (TAS-IoT) model (Hellaoui, Bouabdallah, & Koudil, 2016) - In the TAS-IoT model extra authentication is added to each message at the device level. The device decides whether to authenticate the message or not based on its association with the message sender. This model considers direct interactions, recommendations, and observations. No transitivity level and mobility are considered during trust evaluation.

The Context-based Trust Management System for the Social Internet of Things (CTMS-SIOT) (Ben Abderrahim, Elhedhili, & Saidane, 2017) - In this model author used feedback system parameters, for successful, uncertain, and failed transactions. When malicious behaviour was detected, the object gets punishment by reducing trust value by double to discourage malicious behaviour. Different weights are assigned to transactions based on context to avoid gaining high trust by doing high interaction volume on low-priority services. In the trust computation process, initial trust values are assigned by direct peers based on their shared relationship. This model works on different relationships among nodes like ownership, domestic and social. In the first two types of relationships, the relationship is formed based on common owner and common workspace and considered as most trusted. While the social relationship is formed due to the mutual interest which is prone to malicious behaviour.

3.2. Challenges and Gaps

The problem of trust evaluation was effectively solved using the recommendations in many pieces of literature. But in many cases, they lack to identify the unfair recommenders when recommenders trust themselves low. Thus, trust and experience models seem to be deficient on evaluating the confidence on transitive trust and reliability of requester. Another important factor which is less investigated is ubiquity of the node. In existing models, typically the impact of ubiquity on the end experience of the device communication poses several inadequacies. This subsequently result in non-trustworthy and unsecured device communication ecosystem, hence there exist a need to provide a context-aware, self-regulating and experience-based device to device communication ecosystem. The model representing and catering to such scenario is proposed in this paper

4. Proposed Experience Model

4.1. Fundamental Concept

It will be beneficial to formalize the idea of experience which empowers us to develop solutions efficiently. The node, which requests or sends the request to another node is called a requester or subject, and who satisfies the received request is called a service owner or object. We denote a requester by B, and owner by A.

The experience of node A on requester node B is a real number between 0 and 1. We denote the experience of node A on node B as $E_{A,B} \in [0,1]$. If $E_{A,B} = 1$, means node A has a very strong positive experience with requester B and if $E_{A,B} = 0.5$ (default) means node A has neutral experience. There is also a case when node A has a very bad experience with node B and which can be denoted as $E_{A,B} = 0$.

4.2. Attributes of Experience Model

In this section, we propose an experience model with history, reliability, transitivity, and ubiquity attributes as shown in Figure 1. The level of experience a node can have on another node is represented by the experience score. A higher value of experience score suggests a greater probability of node's trustworthiness.

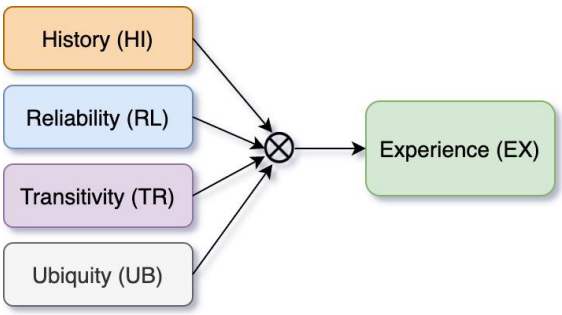

Figure.1. Attributes of experience

4.2.1. History (HI)

The history or History attribute of a node is computed on a basis of the number of past interactions node A had with requester node B. It is assumed that a device maintains a communication history between A and B in the form of an interaction log about every device it communicates with. Each interaction is evaluated further to decide whether it was good or bad depending on its success or failure. If the number of historical interactions is not adequate to compute the history attribute with sufficient confidence, reputations (history of interactions of B with other nearby nodes) may be used. This type of statistical trust approaches like BRS (Josang, Audun and Ismail, 2002), TRAVOS (Teacy, Patel, Jennings, & Luck, 2006) uses both direct and indirect interactions to compute trust. If the number of interactions with a specific target device is large and consistently good, it could

be derived that the target is more trustworthy. Even though existing approach models trust effectively they come with fundamental problems (Şensoy, Yilmaz, & Norman, 2016), bootstrapping and whitewashing. Bootstrapping problem features when new nodes join UbiComp systems for the first time, lacks any past history. In such a situation history attribute cannot be calculated from direct or indirect interactions. In this case, ignorance value can be assigned which can be updated during the course of future interactions or if an existing external model is available for calculating the priory value of History attribute like (Şensoy et al., 2016) can be used

4.2.2. Reliability

"Reliability" is defined as "*the ability of an item to perform a required function under stated conditions for a stated time period*" (Bauer & Adams, 2012). Reliability shows how much a particular device is reliable or credible depending on the evaluations of its past interactions in particular time. It is derived from history by considering good as well as bad interactions. Suppose in scenario 1, node A had only 2 past interactions with node B and both were successful. Similarly, Node A had 100 interactions with node C, and 100 were successful. In both case success percentage is 100% but longevity of relation is different. In human notion, same thing is valid, more the interactions more the reliable is relationship.

The larger the base of interactions, the more accurate reliability is. It is also possible that even if the history contains a large number of interactions with a requester node but all are failed then experience with the device will be considered as unreliable. In (Jøsang & Presti, 2004), Josang et al. discussed context independent reliability trust and context dependent decision trust. According to them, Context independent reliability is observed reliability by other party regardless of situation which trustor might consider as risk. Whereas, reliability in particular context adds relatively more confidence to take risk, even negative consequences are possible. Reliability is essential for effective communication in UbiComp, as sensing, processing, and transmission of information in time play a crucial role. Rapid development in communication systems demands high reliability to ensure trustworthiness in the overall system. Certain factors affecting reliability are scale, ubiquity, and heterogeneity. Scale impact can be handled by changing or updating physical network infrastructure. Ubiquity will be discussed in the section 4.3.4

4.2.3. Transitivity

Transitivity indicates an inter-device trust relationship between the requester node and trusted peers in the network in the given relevant context. It is a measure indicating the transitive nature of the node. One of the most important and controversial properties of experience is transitivity, based on the concept of recommendation of someone that is not directly known. Transitivity is expressed in the form of recommendations from trusted peer nodes about the experience of the requester node. For example, As shown in Figure 2, if node A trusts node B, and node B trusts node C, then A may trust C if B recommends C as a trusted one to it.

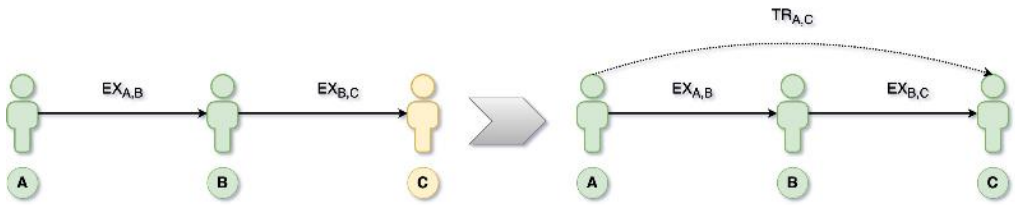

Figure.2. Transitive Nature of Experience

Certainly, in real life trust is not always transitive but works only in specific contexts. In (Jøsang & Pope, 2005) explained the necessity to have similar and semantically consistent trust purposes along transitive trust paths. This means if device A trusts device B in a certain context and device B trusts device C in the same context then only a trust path can be created between A and C for the same context. In a ubiquitous environment with a huge number of devices there are high chances that there is no interaction between any two nodes, i.e., there is no history data. This makes it difficult to calculate reliability also. Hence, transitivity is an important component for experience calculation especially when there is no or less history about the target. Each device that has previous interactions with the target device shares its experience to other devices on request. The transitivity attribute of the requester is an aggregate experience of trusted peers. Secondly, it is a safety requirement that is based on personal experience and first-hand evidence and it should be communicated in a trusted referral. Communicating indirect trust based on second-hand evidence can result in incorrect trust derivation.

4.2.4. Ubiquity

Ubiquity specifies whether the node is ubiquitous or not to indicate its mobile nature. When a node has more mobility, we can say that node is more ubiquitous and when a node is static or moves in a restricted speed, we can say the node is less ubiquitous. Based on observations in (Raikwar, 2012), when node speed increases, packet drop also increases. Hence ubiquity can be treated as a correction factor, for calculating experience.

Suppose there's a trustor node that wishes to send the packet to the destination. If the node is in the static state during transmission of all packets, the experience of the node will be calculated assuming the node is in a stable state. If we assume now node to be moving while packet transfer, packet drop will increase, decreasing the experience value. Packet drop is proportional to the speed of node, more is speed more will be packet drop. Based on observations, change in the ubiquity of the device affects the overall experience of communication hence ubiquity factor UB is introduced in the experience model.

Fixed devices always have ubiquity factor 1, which means these devices are more trustworthy as packet loss will be negligible. During movement, if the speed of the node is between minimum speed and average speed Ubiquity attribute is set to 1. When this attribute is weighted with the remaining experience model properties, the experience score will be unchanged. The value of the Ubiquity attribute will be reduced linearly with an increase in the speed of the node. If the speed of the node pasts the maximum allowed speed, the Ubiquity attribute of the node reduced to 0, stopping the node from taking part in further interactions by reducing its experience score value to 0.

Variation in the access network shows the ubiquity of the device. Fixed devices connected using Ethernet, DSL, FTHH, Wi-Fi are almost stationary in nature. They are not ubiquitous and more trustworthy. But the mobile devices connected using 3G, 4G, or hotspots based on these technologies are ubiquitous in nature. Such devices, due to their mobility and ability to connect through different modes, are less trustworthy.

4.3. Proposed Experience Model

The proposed model is shown in Figure 3. It comprises three different types of entities.

- Resource Oner (A) : These types of entities represent nodes that have resources and share them with other nodes the in network on request. The resources could be any information, for example, files or services.
- Requester B) : These are the clients requesting resources or services. They request a particular resource from the resource owner.

Peers (D1,D2 … Dn) : Peers provides their experience about B to resource owner A, when A request for recommendation about B to its peers.

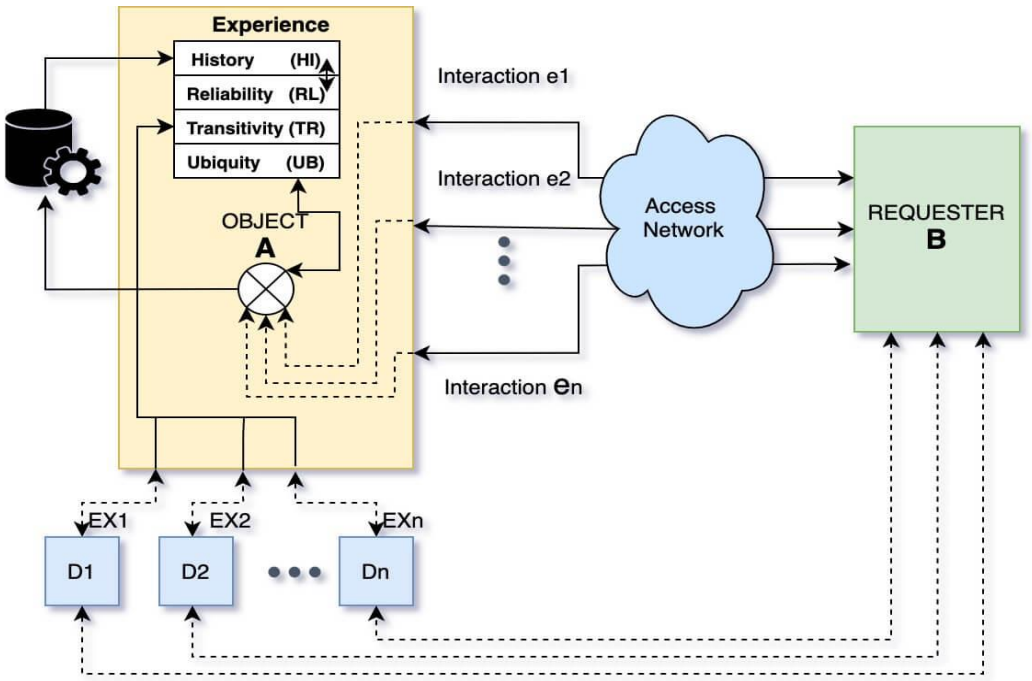

Figure.3. Experience model

5. Computation of Experience

For conceptual experience model shown in Figure 3, Experience can be computed as in eq.1 using the following components: interaction history, reliability, transitivity, and ubiquity.

$$EX_{A,B} = f\left(HI_{A,B}, RL_{A,B}, TR_{A,B}, UB_{A,B}\right) \quad (1)$$

Hereafter, assuming device to device communication between A and B nodes, all the above parameters are referred as *EX*, *HI*, *RL*, *TR*, and *UB* resp.

5.1. Compute HI

Suppose node A wants to calculate the HI attribute for node B for nth interaction in context *c*. Interactions between A and B are noted as *e = {e1,e2, ... en}* , which are recorded as positive or negative results according to their time of occurrence . A compute the sum of all previous positive and negative interactions with B as P_B and F_B as shown in eq. 2 and eq. 3 resp.

$$P_{B=\sum_{i=1}^{n} e_i} \quad \text{where } ei = 1 \quad (2)$$

$$F_{B=\sum_{i=1}^{n} |e_i|} \quad \text{where } ei = -1 \quad (3)$$

P_B and F_B are the input parameters to a beta probability density function (PDF), whose expected value is the estimate of the Bs behaviour.

The confidence (*cnf*) , in B is expected behaviour based solely on their previous interactions denoted by cnf_B, is calculated as in eq. 4.

$$cnf_B = \frac{P_B}{P_B + F_B + 2} \quad (4)$$

When there is less or no knowledge, there will be always uncertainty about the success of interactions. Uncertainty plays an important role. Uncertainty occurs due to a lack of knowledge about the node for which the uncertainty factor u_B is calculated. A decision made on less knowledge may be a bad decision. u_B is calculated as shown in eq. 5.

$$u_B = \frac{2}{P_B + F_B + 2} \quad (5)$$

Uncertainty factor varies between [0,1]. When uncertainty is closer to 1 means, there are fewer interactions between A and B. If it's near to 0 then there are sufficient interactions to calculate the HI attribute.

When a new node introduced in-network, there is no evidence of history, a default value 'a' needs to be provided. We can take this default as a fixed value or introduce a new model like (Şensoy et al., 2016) to calculate the default value as per eq. 6.

$$a = \begin{cases} x & if\ model\ is\ available \\ 0.5 & default\ value \end{cases} \quad (6)$$

HI attribute for interactions of B with A is calculated using eq. 7.

$$HI_{A,B} = cnf_B + (u_B \times a_B) \quad (7)$$

Similarly, the HI attribute for interactions between A and B in context *c* is calculated using eq. 8.

$$HI^c_{A,B} = cnf^c_B + (u^c_B \times a_B) \quad (8)$$

Then P_B and F_B calculation will consider only interactions related to context c.

5.2. Compute RL

Highly reliable node may attribute to good experience. Node B is reliable to node A if B gives consistently good results to A. Here reliability of node B can be calculated by node A on the basis of set of interactions witnessed between A → B.

Let the node B interacts with node A nr times in an interaction window *W* then overall reliability attribute regardless of context between A & B can be calculated as shown in eq. 9.

$$RL_{A,B} = log_e(nr + 1) \times \frac{Pr_B}{nr} \times \frac{1}{log_e(W)} \quad (9)$$

where $RL_{A,B} \in [0,1]$,

W = max number of past interactions under consideration for reputation calculation

nr = Total number of recent interactions such that ($0 < nr \leq W$)

Pr_B = Number of recent successful interactions.

If the reliability attribute of node A about node B is close to 1, then B is reliable to A because many previous interactions were successful. If the reliability attribute closes to 0, then many previous interactions were unsuccessful.

Reliability attribute for particular situation or context c can be calculated as in eq. 10.

$$RL_{A,B}^{c} = log_e(nr^c + 1) \times \frac{Pr_B^c}{nr^c} \times \frac{1}{log_e(W^c)} \quad (10)$$

where,

W^c= max number of past interactions under consideration for reputation calculation in context c

nr^c= Total number of recent interactions such that ($0 < nr \leq W^c$)

Pr_B^c = Number of successful interactions

5.3. Compute TR

Indirect experience computation holds key importance when the object owner has no previous interaction with the requester to calculate direct experience.

If there are no sufficient interactions between B and A, then A can ask experiences about B to its other active peers in the network. Let, there be another node C and

$EX_{A,C}$ is Experience of A about C

$EX_{C,B}$ is Experience of C about B

When B request resource/service from A, A observes that there is no previous interaction history between them. So, A broadcast recommendation request to all its trusted peers to send their experience about B. A gets a response from C with its experience score about B. If A founds this experience is sufficient to honour the request of B, then access to a resource will be provided to B and a transitive trust path between A and B will get established as

$TR_{A,B}$ is Experience of A about B

i.e. the transitive experience score $TR_{A,B}$ will be calculated as $min(E_{A,C}, E_{C,B})$. When node A receives responses from multiple peers j = (1,2,3… n) the transitive experience will be calculated as shown in eq. 11.

$$TR_{A,B} = \frac{\sum_{j=1}^{n} \min(E_{A,j}, E_{j,B})}{n} \quad (11)$$

5.4. Compute UB

Theoretically, it can be inferred that if the speed of node is between the minimum speed V_{min} and the calculated average speed V_{avg}, mobility factor mf is set to 1. When this mf is 1 in experience calculation, experience value will not be affected. Thus, it can be inferred that the experience value will be unaffected when node is static or moving at allowed min speed. mf decreases with increase in speed and when node crosses maximum speed V_{max}, it will become 0, resulting in low experience. Thus, mf ranges between 0 and 1 i.e. ($0 \leq$ mf ≤ 1)

$$mf \propto \frac{1}{V_{current}}$$

where $V_{current}$ = Current speed of node

i.e., with increase in speed , experience will be decreased. This means that if node is stable, experience will be good and if node is at high speed or moving, experience of node will be impacted accordingly. Mobility factor mf is given as in eq. 12.

$$mf = \frac{(V_{max} - \min(\max(avg(V_{min}, V_{max}), V_{current}), V_{max}))}{avg(V_{min}, V_{max}) - V_{min}} \quad (12)$$

where,

V_{max} = Maximum allowed speed of node.

V_{min} = Minimum speed of node.

It is further possible to assign correction factor cf based on access networks, i.e., if connectivity is ethernet then node is static and cf will be 1. Similarly, for other access networks cf values can be assigned as shown in Table 1. Ubiquity attribute can be calculated as shown in eq. 13.

$$UB = mf \times cf \quad (13)$$

Table.1. Correction Factors based on Access Network

	Access Network	**Correction Factor (*cf*)**
1	Ethernet	1.0
2	WIFI	0.95
3	WiMAX	0.9
4	Cellular(2G/3G/4G)	0.7

5.5. Computation of EX Score

$EX_{A,B} = f(HI_{A,B}, RL_{A,B}, TR_{A,B}, UB_{A,B})$, this function works on weighted average of *HI*, *RL*, *TR*, *UB* which can be calculated using weighted average function viz.

Weighted Average = $\frac{\sum_{i=1}^{n} x_i w_i}{\sum_{i=1}^{n} w_i}$

Where, x denotes the distribution and w denotes the weights. Experience of A with B is calculated as shown in eq. 14.

$$EX_{A,B} = \frac{(W1 * HI_{A,B}) + (W2 * RL_{A,B}) + (W3 * TR_{A,B}) + (W4 * UB_{A,B})}{w_1 + w_{2+} w_3 + w_4} \quad (14)$$

When every parameter is given equal weightage , eq. 14 can be re-written as eq. 15.

$$EX_{A,B} = avg(\ HI_{A,B}, RL_{A,B}, TR_{A,B}, UB_{A,B}) \quad (15)$$

6. Results and Analysis

We have taken 6 scenarios of having 30 interactions between 2 nodes A and B. For each scenario from 1 to 6, out of 30 interactions the successful interactions count taken as 30, 28, 25, 20, 15, 6 respectively. i.e., count of unsuccessful interactions is 0, 2, 5, 10, 15, 24 respectively. Recent transaction window size (*W*) taken as 20. Table 2 shows scenarios details. With this interaction data, we verified proposed model and its attributes w. r. t. changes in number of successful and unsuccessful interactions.

Table.2. Scenario details

Scenario	**Total Interactions**	**Successful Interactions**	**Unsuccessful Interactions**
1	30	30	0
2	30	28	2
3	30	25	5
4	30	20	10
5	30	15	15
6	30	6	24

Figure 4 shows graphs of 6 scenarios depicting impact on HI attribute. From graph in Figure 4, we can see that as number of unsuccessful interactions increased, HI attribute declines towards 0. For scenario 1, all 30 interactions were successful hence HI observed stable with value 1. In scenario 6, count of unsuccessful interactions increased considerably hence HI also declined significantly towards 0.

Figure 5 shows 6 scenarios depicting impact on Reliability attribute (RL) . We fixed recent transaction window size W to 20, i.e., node A should have at least 20 interactions happened with B to decide B as reliable/unreliable. For scenario 1, all 30 interactions were successful but from transactions 1 to 20 reliability increased steadily towards 1. This scenario explains that for any node to be reliable, there must be sufficient interactions history available. In scenario 6, count of unsuccessful interactions increased considerably hence HI also declined consistently towards 0.

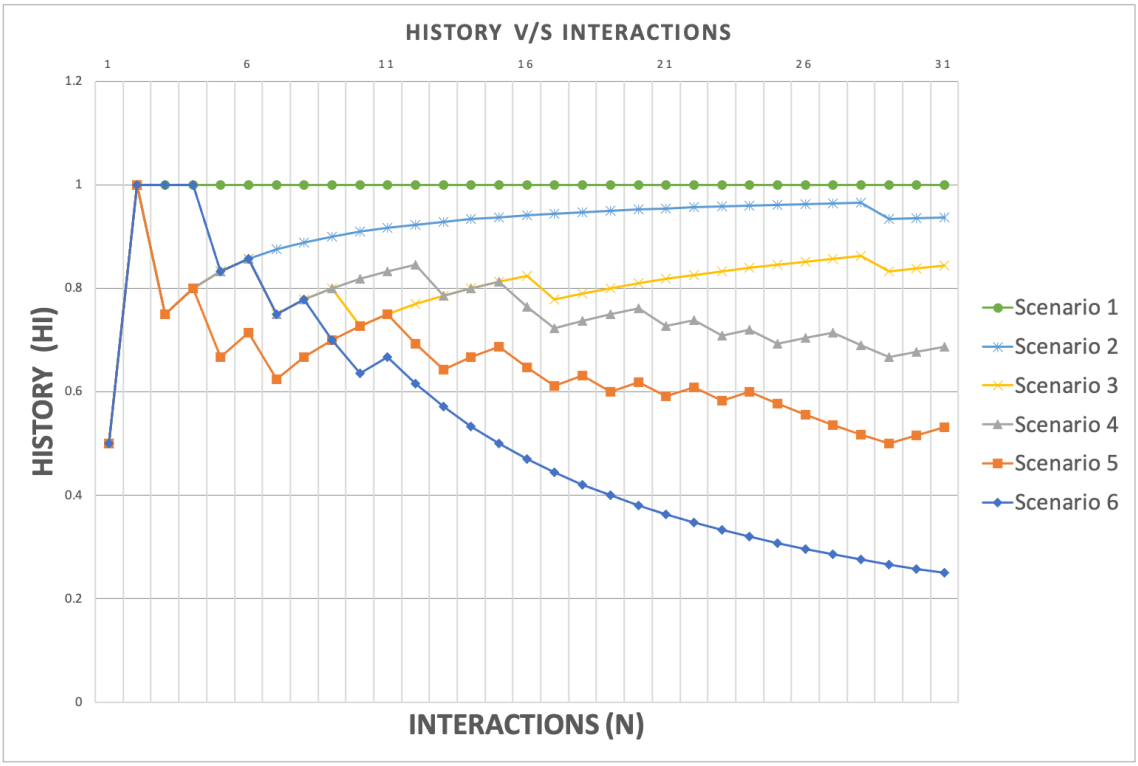

Figure.4. Comparison of scenario 1-6 for HI property

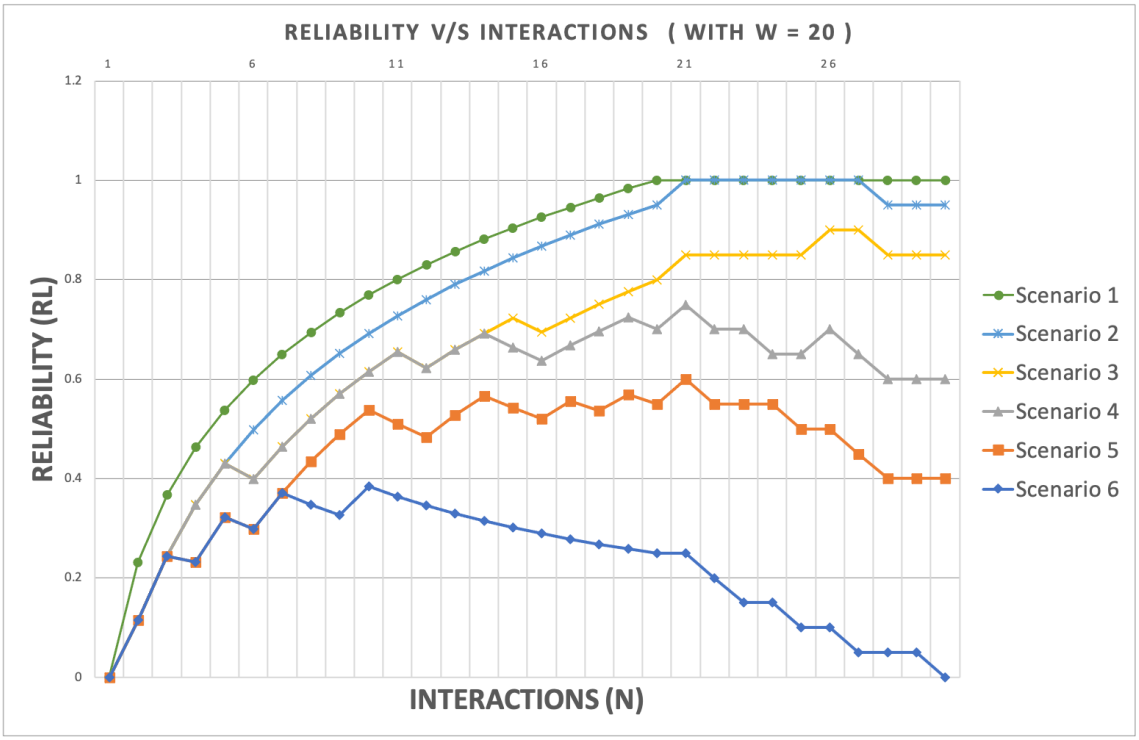

Figure.5. Comparison of scenario 1-6 for RL property

Impact of ubiquity on overall experience score:

Here, we assumed EX in absence TR as a function of HI, RL and UB parameters along with weightage of 0.2, 0.4, and 0.4 resp. to each of them i.e. EX = (HI*0.2) + (RL*0.4) + (UB*0.4). For this equation, we have considered scenario 5 only from Table 2 to check impact of UB on overall EX. Note that the weights assigned here for each parameter can be adjusted as per different applications and scenarios. In this scenario we considered V_{min} is 10 and V_{max} = 80 and calculated V_{avg} = 45. Node a move from 1st interaction to 11th interaction with in range of min and average speed and from 11th interaction onwards starts incising speed and reaches max speed at 18th interaction. From Figure 6, it can be concluded that if node speed increases above average speed, then ubiquity gradually reaches to 0 which also causing decreased value of overall experience to certain extent.

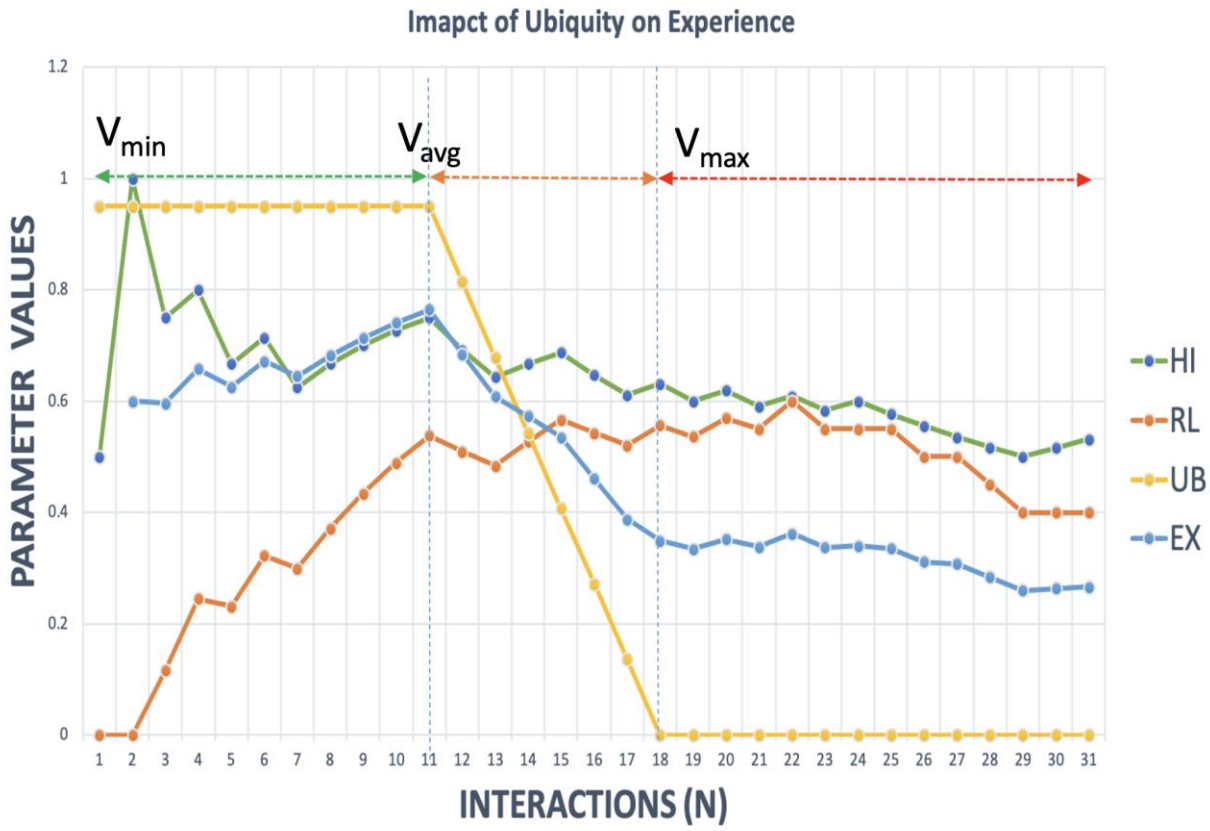

Figure.6. Impact of UB for scenario 5 on EX

7. Conclusion

In this paper, experience model is presented to calculate experience score of UbiComp devices using history, ubiquity, reliability, and transitivity parameters. Further, experience model is formulated and validated with mathematical approach. Outcomes of the validation show that the experience of a device is directly proportional to trust. Novelty of the contribution is in terms of impact of ubiquity on experience. It suggests that as mobility of the node increases the overall trust and experience decreases. Further, the type of the access network along with mobility also has proportionate influence on overall experience. Other parameters such as history, reliability and transitivity proportionately contribute in experience. The proposed model can be used in self-regulating security systems. Future work includes implementation of this model with suitable security system to validate the findings.

References

[1]. Bauer, E., & Adams, R. (2012). *Reliability and Availability of Cloud Computing*. Hoboken, NJ, USA: John Wiley & Sons, Inc. https://doi.org/10.1002/9781118393994

[2]. Ben Abderrahim, O., Elhedhili, M. H., & Saidane, L. (2017). CTMS-SIOT: A context-based trust management system for the social Internet of Things. *2017 13th International Wireless Communications and Mobile Computing Conference, IWCMC 2017*, 1903–1908. https://doi.org/10.1109/IWCMC.2017.7986574

[3]. BusinessInsider. (n.d.). THE INTERNET OF THINGS 2020. Retrieved from www.businessinsider.com website: https://www.businessinsider.com/internet-of-things-report?IR=T

[4]. Chen, D., Chang, G., Sun, D., Li, J., Jia, J., & Wang, X. (2011). TRM-IoT: A trust management model based on fuzzy reputation for internet of things. *Computer Science and Information Systems*, *8*(4), 1207–1228. https://doi.org/10.2298/csis110303056c

[5]. Chen, I. R., Guo, J., & Bao, F. (2014). *Trust Management for SOA - based IoT and Its Application to Service Composition*. *9*(3), 482–495. https://doi.org/10.1109/TSC.2014.2365797

[6]. D'Angelo, G., Rampone, S., & Palmieri, F. (2017). Developing a trust model for pervasive computing based on Apriori association rules learning and Bayesian classification. *Soft Computing*, *21*(21), 6297–6315. https://doi.org/10.1007/s00500-016-2183-1

[7]. Hellaoui, H., Bouabdallah, A., & Koudil, M. (2016). TAS-IoT: Trust-Based Adaptive Security in the IoT. *Proceedings - Conference on Local Computer Networks, LCN*, 599–602. https://doi.org/10.1109/LCN.2016.101

[8]. Josang, Audun and Ismail, R. (2002). The Beta Reputation System. *Proceedings of the 15th Bled Electronic Commerce Conference*, *5*, 2502–2511. https://doi.org/10.1.1.60.5461

[9]. Jøsang, A., & Pope, S. (2005). Semantic constraints for trust transitivity. *Conferences in Research and Practice in Information Technology Series*, *43*, 59–68.

[10]. Jøsang, A., & Presti, S. Lo. (2004). Analysing the relationship between risk and trust. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *2995*, 135–145. https://doi.org/10.1007/978-3-540-24747-0_11

[11]. Kamvar, S. D., Schlosser, M. T., & Garcia-Molina, H. (2003). The Eigentrust algorithm for reputation management in P2P networks. *Proceedings of the Twelfth International Conference on World Wide Web - WWW '03*, 640. New York, New York, USA: ACM Press. https://doi.org/10.1145/775152.775242

[12]. Liu, X., Tredan, G., & Datta, A. (2014). A generic trust framework for large-scale open systems using machine learning. *Computational Intelligence*, *30*(4), 700–721. https://doi.org/10.1111/coin.12022

[13]. Mahalle, P. N., Thakre, P. A., Prasad, N. R., & Prasad, R. (2013). A fuzzy approach to trust based access control in internet of things. *2013 3rd International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace and Electronic Systems, VITAE 2013 - Co-Located with Global Wireless Summit 2013*, 2–6. https://doi.org/10.1109/VITAE.2013.6617083

[14]. Mendoza, C. V. L., & Kleinschmidt, J. H. (2016). Defense for selective attacks in the IoT with a distributed trust management scheme. *Proceedings of the International Symposium on Consumer Electronics, ISCE*, (2), 53–54. https://doi.org/10.1109/ISCE.2016.7797367

[15]. Rafey, S. E. A., Abdel-Hamid, A., & El-Nasr, M. A. (2016). CBSTM-IoT: Context-based social trust model for the Internet of Things. *2016 International Conference on Selected Topics in Mobile and Wireless Networking, MoWNeT 2016*. https://doi.org/10.1109/MoWNet.2016.7496623

[16]. Raikwar, A. K. (2012). Effect of mobility on trust in mobile ad-hoc network. *Advances in Intelligent and Soft Computing*, *167 AISC*(VOL. 2), 673–684. https://doi.org/10.1007/978-3-642-30111-7_64

[17]. Ruan, Y., Durresi, A., & Uslu, S. (2018). Trust assessment for internet of things in multi-access edge computing. *Proceedings - International Conference on Advanced Information Networking and Applications, AINA*, *2018-May*, 1155–1161. https://doi.org/10.1109/AINA.2018.00165

[18]. Şensoy, M., Yilmaz, B., & Norman, T. J. (2016). Stage: Stereotypical trust assessment through graph extraction. *Computational Intelligence*, *32*(1), 72–101. https://doi.org/10.1111/coin.12046

[19]. Tahta, U. E., Sen, S., & Can, A. B. (2015). GenTrust: A genetic trust management model for peer-to-peer systems. *Applied Soft Computing Journal*, *34*, 693–704. https://doi.org/10.1016/j.asoc.2015.04.053

[20]. Taylor, P., Barakat, L., Miles, S., & Griffiths, N. (2018). Reputation assessment: a review and unifying abstraction. *The Knowledge Engineering Review*, *33*, 1–28. https://doi.org/10.1017/s0269888918000097

[21]. Teacy, W. T. L., Patel, J., Jennings, N. R., & Luck, M. (2006). TRAVOS: Trust and reputation in the context of inaccurate information sources. *Autonomous Agents and Multi-Agent Systems*, *12*(2), 183–198. https://doi.org/10.1007/s10458-006-5952-x

[22]. Truong, N. B., Lee, H., Askwith, B., & Lee, G. M. (2017). Toward a Trust Evaluation Mechanism in the Social Internet of Things. *Sensors*, *17*(6), 1346. https://doi.org/10.3390/s17061346

[23]. Weiser, M. (1999). The computer for the 21 st century . *ACM SIGMOBILE Mobile Computing and Communications Review*, *3*(3), 3–11. https://doi.org/10.1145/329124.329126