iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL
FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 Issue: V Month of publication: May 2023

DOI: https://doi.org/10.22214/ijraset.2023.51959

Trust Based Service Management for Social Internet of Things: The Implementation

Prof. Y. B. Jadhao[1], Ms. Farisa Fatema[2], Ms. Vaishnavi D. Chaudhari [3], Ms. Aarti G. Khodke[4], Ms. Samruddhi J Pol[5]
[1]Assistant Professor, Department of Computer Science & Engineering, Padm. Dr. V.B.K.C.O.E. Malkapur, Maharashtra, India
[2, 3, 4, 5]Student, Department of Computer Science & Engineering, Padm. Dr. V.B.K.C.O.E. Malkapur, Maharashtra, India

Abstract: A social internet of things (Iot) system can be seen as a union of normal peer-to-peer networks and social networks, where "things" freely establish the social relations according to the owners' social networks, and search trusted "things" that can provide services stand in need of when they come into contact with each other aggressively. We have suggested and study the design notion of many easily flexible trust management system for social Internet of Things systems in which social relationships progress are not stable but they are variable among the owners of Internet of Things devices. We have been give away the planned trade-off between trust confluence vs. trust contrast in our old easily adaptive trust management protocol design. With our regular easily adaptable trust operation principals, the social Internet of effects(SIOT) operations can fluently elect the stylish trust r settings in response to changing Internet of effects social parameters similar that not only trust assessment is accurate but also the application performance is enhanced. We have propose a table-lookup method to apply the analysis results dynamically and demonstrate the practicability of our proposed adaptive trust management scheme with two actual social IoT service construction applications.

Keywords: Trust Management, Internet of Things, Social Networking, Performance Analysis, Adaptive Control, Security .

I. INTRODUCTION

The Internet of Things (IoT) provides a platform to combine a large number of distributed heterogeneous systems. common computing is the backbone of IoT, indicate a network of uniquely detecteble interrelated smart objects using standard communication protocols . These resource-constrained smart devices communicate and co-operate in various factors. However, IoT is not just a global network of smart devices, but also enclose a set of supporting technologies along with the necessary services and group of applications . IoT can be handle as a network whose prime aim is to include devices or nodes which can request or provide services. Moreover, nodes can work together to provide a single service . Since the begining of IoT, there has been progress in this pattern at an unmatched rate result in the innovation of many different visions and contexts such as ‘‘Social Internet of Things’’ (SIoT), industrial IoT, and IoT in the healthcare sector. Internet of Things enables various devices to communicate and co-operate while providing or recieving different services. However, this co-operative interaction can lead to trust challenges between devices, be in need of a decentralized, mobile, beneficial, low latency, lightweight and extensible trust management framework. The merging of ‘‘social networks’’ and the ‘‘internet of things’’ leads to the understanding of SIOT , which has been identify by the heterogeneity of the software and hardware components and a variety of hardware architectures. In SIoT these different devices collaborate and cooperate with each other to achieve a common target . Social Internet of Things is a broad term that includes connection entirely between people, between ‘‘things’’, or between people and things . Geographically spread different objects can be proficiently detect through the use of SIOT. Social IoT includes both peer-to-peer networks and social relationships amongst multiple self-governing systems, where nodes act as service providers (SPs) or service requesters/ consumers (SRs or SCs).

Every object or node on a social network obtain valid responses to their requests as compared to the objects or nodes working indivially , The basic goal of Social IoT is to p on things from people and allow them to self-organize – to share computational resources, information, and services. Every Entity must decide on the type of connection it has with other objects. Social IoT applications are likely stablized toward a service align architecture where each thing plays the role of either a service provider or a service requester, or both, according to the rules set by the owners. Unlike a conventional service-oriented Peer-to-peer network(P2P), social networking and social relationship plays an important role in a social IoT, since things (real or virtual) are necesariliy operated by and work for humans. Therefore, social relations among the owners must be taken into account during the compose phase of social IoT applications. A social internet of things system thus can be seen as a P2P owner-centric community with devices (owned by humans) request and give services on behalf of the owners.

IoT devices establish social relationships autonomously with other devices based on social rules set by their owners, and interact with each other excessive as they come into contact. It is out of our imagination that the future social Internet of things will be connect large amount of smart Objects in our physical world including RF identification (RFID) tags sensors ,actuators ,Personal Digital Assistance and smartphones as well as virtual objects in cyber space such as data & virtual Desktop on the different cloud. The Emerging paradigm of the social Internet of things has attracted a large amount of variety of application running on the top of it including Smart Home, Smart City ,E-health and smart community. We will have to use the term things objects and device mutually in the paper .Such future social internet of things applications are likely oriented towards a service oriented architecture where each thing plays the role of either a specific service provider and a service requester (the person who request the service) or both , according to the principles set by the owners .Not likely a traditional service oriented Peer to Peer network , social networking and social relationship play an vital role in a social internet of thing , since things (virtual or real) are approximatelly operate by the work for us (Humans). Therefore , Social relationship among the users or owners must be taken into account during the design phase of social internet of things application.

A Social IOT system thus can be seen as the Peer to peer owner-centric community with the devices (acquired by human) requesting and providing different services on the behalf of the owners . Internet of things devices based on the social principles set by their owners , and interact with one another opportunistically as they come into contact . to best satisfy the service requester and maximize application performance , it is crucial to evaluate the trustworthiness of service provider in social internet of things environment .

II. LITERATURE SURVEY

We have Served recently proposed trust management protocols for IOT systems. We have contrast and compare our work with old/existing work so as to make difference in our work from the existing work and identify unique features and contributions of our trust management protocol design and trust based sevice management design for the Internet of things systems. There is a small work on trust management in Internet of Things in environments for security enhancement ,especially for dealing with misbehaving owners of Internet of things devices that provides different services to other Internet of things devices in the system.[14] proposed a trust management model which is based on the fuzzy reputation for the Internet of Things environment populated with the wireless sensor only , so they will only considered Quality of Service trust metrics like the packet forwarding /delivery ratios and energy consumption for measuring trust of sensors. On the other hand our , work will consider both QoS trust deriving from communication networks And social trust deriving from social networks which give to th social relationship of owners of IoT devices in the social Internet of things environment . Said et al .[**36**] proposed a context aware and multi-service approach for the trust management in IoT environments . Relative[**36**] to our trust protocol is totally distributed without requiring ant centralized trusted entity. Bao and Chen [5] proposed a trust management protocol considering both social trust metrices and use both direct observation and indirect recommendation to update in Internet Of Things systems .

However the adaptivity issue adjusts trust evaluation in response to dynamically changing as to cope with misbehaving node and maximize the IOT applications performance running on the top of trust management was not addressed related to cited above[5] we do not only consider multiple trust properties for Social Internet Of Things (SIOT) environment, but also analyze the tradeoff between the speed of trust convergence and fluctuation of trust to identify the best protocol parameter setting for trust propagation and aggregation to best exploit this tradeoff fot minimize the trust bias.

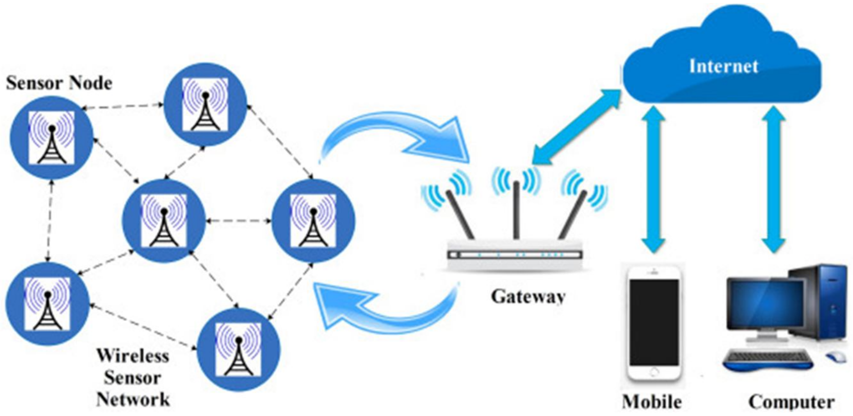


Figure 1. Social Internet Of Things (SIOT) Structure

Further more .it addresses the problem of trust formation for application performance maximization using service composition as an application example. Recently, Nitti *et al.* [32] had considered social relationships of owners of Internet of Things devices for trust management S IoT systems. They are proposed two models for trustworthiness management. First one ,*subjective model* deriving from social networks, with each node compute the trustworthiness of its friend on the basis of its own experience and on the opinion of friendly recommenders, and second is *objective model* derived from Peer 2Peer communication networks with each node stores and retrieves trust information towards its peers in a distributed hash table structure, so that any node can make use of the same information. Their objective model requires a pre-trusted nodes be in place for maintaining the hash table, which is questionable in IoT environments. Their subjectivemodel is also similar in spirit to our trust model taking into consideration for the social relationships between owners of IoT devices. The fundamental main difference is that our model of *objective trust* is based on ground truth or actual status, and our trust protocol dynamically adapts to changing environments by adjusting the best protocol settings to minimize trust bias (it is the difference between subjective trust and objective trust) and to maximize application performance. Security has taken the attention in IoT research [14, 15,34, 35, 42]. Roman *et al*. [35] Has discussed about threats to IoT, such as compromising botnets trying to hinder services and the domino effect in between intertwined services and user profiling .Conventional network approaches to the network security ,ie data and privacy management ,to identify management and fault tolerance wii no be accommodate the requirement of IOT due to the scalability lack and inability to cope with a high variety of relationship and identity type[35].There is a possible solution proposed for each security problem, but specific protocols and analysis was not given. Ren proposed [34]a compromise-resilient key management scheme for heterogeneous wireless IoT. The proposed key managementprotocol includes key agreement schemes and key evolution policies (forward and backward secure key evolution). The author also designed a quality of service (QoS) aware enhancement to the proposed scheme. However, the proposed scheme doesn't take social relationships among IoT identities into consideration. Chen and Helal [15] proposed a device-centric approach to enhance the safety of Internet Of Things. They were design a device description language i.e. DDL in which each device can specify its own safety concerns, constraints and knowledge .Nevertheless, their approach is specifically designed for sensor and actuator device, and does not consider social relationships among device owners. Zhou and Chao [42]proposed a architecture on media-aware traffic security for IOT .First ,the authors designed multimedia traffic classification and then develop this media aware traffic security architecture to achieve good trade-off between efficiency and flexibility of the system. A limitation of their work is that they only considered direct observations to traffic without considering indirect recommendations. Relative to the security and design/mechanism cited above ,our approach is to use trust to implement security against malicious attacks .We note that our trust system can work orthogonally with this security designs and mechanism to further enhance security of Social Internet Of Things(SIOT) systems.

III. SYSTEM MODEL

A. *User-Centric Social IoT Environments*

We consider a user-centric social IoT environment with no centered trusted authority. Each IoT device has its unique specification which can be gain through standard techniques such as PKI. A device communicates with other devices through the overlay social network protocols, or theunderlying standard communication network protocols(wired or wireless). Every device has an owner who could have many devices. Social relationships between owners is translated into social relationships between IoT devices as follows: Each owner has a list of friends (i.e., other owners), showing its social relationships. This friendship list varies dynamically as an owner makes or oppose other owners as friends. If the owners of two nodes are friends, then it is likely they will be collaborative with each other. A device may be carry or operated by its owner in certain community-interest environments (e.g., work vs. home or a social club). Nodes belonging to a similar set of sections likely share similar interests or capabilities.

Our social Internet of Things model is based on social relations among humans who are owners of IoT devices. We note that the device-to-device autonomous social relationship is also a portale for the social IoT paradigm or pateern.

B. *Attack Model*

A malicious node is fraudulent and socially uncollaorative in nature and can break the basic functionality of the social IoT system. A malicious node can perform the following trust-related attacks

1) *Self-promoting Attacks*: a malicious node can promote itsimportance (by providing good advice for itself) so as to be selected as the service provider, but then it provides malfunctioned(crash) service. Our trust protocoldeals with self-promoting attacks by considering honestyas a trust property to detect self-promoting attacks.

2) *Whitewashing Attacks*: a malicious node can pass from side and reconnect the application to wash away its bad reputation. Our trust protocol deals with whitewashing attacks by remembering trust information of each identity, and by performing trust decay over time to account for node inactivity during the period in which a node disappears from the Internet of Things system.
3) *Discriminatory Attacks:* a malicious node can discriminatively attack non-friends or nodes without strong social ties (without many common friends) because of human nature or propensity towards friends insocial Internet of Things systems. Our trust protocol deals with prefrential attacks by considering cooperation and community-interest as trust properties.
4) *Bad-mouthing Attacks*: a malicious node can ruin thereputation of a well-behaved node by providing bad proposal against the good node so as todecrease the chance of this good node being selected as aservice provider. This is a form of *collusion attacks*, i.e., it can collaborate with other bad nodes to ruin the reputation of a good node. Our trust protocol deals with bad-mouthing attacks by considering honesty as a trust things.
5) *Ballot-stuffing Attacks*: a malicious node can increase the reputation of another bad node by providing good suggestions for it so as to boost the chance of this bad node being selected as a service provider. This isalso a form of *collusion attacks*, i.e., it can collaborate with other bad nodes to boost the reputation of eachother. Our trust protocol deals with ballot-stuffing attacks by considering honesty as a trust property

A collusion attack means that the malicious nodes in thesystem boost their allies and focus on particular victims in the system to victimize. Bad-mouthing and ballot-stuffing attacks both are a form of collusion attacks to ruin thereputation of (and thus to victimize) good nodes, and to boost the reputation of malicious nodes. A malicious node can perform Sybil and identity attacks, and in general can perform communication protocol attacks to disrupt IoT network operations. We assume such attacks will be handled by intrusion detection techniques [16, 31] and the attackers will be evicted from the system upon detection

IV. ADAPTIVE TRUST MANAGEMENT

Table I lists the parameters used in the paper. A design parameter is one that adaptive trust management can control to optimize performance. A derived parameter is one that is generated during runtime as a result of running the trust protocol. An input parameter is one that the operating environment dictates.

The components of adaptive trust management for asocial IoT system are shown in Figure 1. Our protocol

Symbol	Meaning	Type
$T^{x}(t)$ ij	trust of *i* towards *j in X* at time *t*	derived
$D^{X}(t)$ ij	direct trust of *i* towards *j in X* at time *t*	derived
$R^{X}\ (t)$ jk	recommendation from *k* toward *j in X* at *t*	derived
$T_{ij}(t)$	overall trust or overall trustworthiness scoreof *i* towards *j* at time *t*	derived
α	weight on direct trust w.r.t. experience	design
β	weight on recommendation w.r.t. experience	design
NT	number of IoT devices	input
NH	number of owners	input
NG	number of user communities	input
□	average interaction inter-interval time	input
□	percentage of malicious nodes	input
□c	node compromise time period	input

Figure 2. list of parameters

Addresses all aspects of trust management: the trust *composition* component addresses the issue of how to selectmultiple trust properties according to social IoT application requirements. The trust *propagation* and *aggregation* component addresses the issue of how to disseminate and combine trust information such that the trust assessment converges and is accurate. The trust *formation* component addresses the issue of how to form the overall trust out of individual trust properties and how to make use of trust in order to maximize application performance. Essentially adaptive trust management is achieved by (1) selecting the best trust propagation and aggregation parameter setting to achieve trust accuracy and convergence and (2) selecting the best trust formation parameter setting to maximize application performance, in response to an evolving IoT environment.

Adaptive trust management must be distributed as asocial IoT system frequently consists of free-will entities without a centralized mediator. Each node maintains itsown trust assessment towards other nodes. A node is more likely to share common interests with those nodes it recently interacts with or it believes to be trustworthy. For an IoT node with a limited storage, it will only keep trust and recommendation information for a limited set of nodes which it is most interested in. In this paper we do notconsider the use of caching to mitigate the limited storage issue. We refer the readers to [8] for a scalable caching storage management design to effectively utilize limited storage space without compromising trust accuracy and convergence properties. Adaptive trust management is interaction-based as well as activity-based, meaning that thetrust value is updated dynamically upon an interaction event or activity. Two nodes involved in a direct interaction activity can directly observe each other and update their trust assessment. They also exchange their trust evaluation results toward other nodes as recommendations.

A. Trust Composition

While there is a success of social trust metrics available [38], we choose *honesty*, *cooperativeness*, and *community- interest* as the most obvious metrics for characterizing social IoT systems, as illustrated in Figure 1 (2nd level). These trust properties are considered orthogonal but complementary to each other to characterize a node. Each trust property is evaluated separately as follows:

1) The *honesty* trust property represents whether or not a node is honest. In IoT, a malicious node can be dishonestwhen providing services or trust recommendations. We select *honesty* as a trust property because a dishonest node can severely disrupt trust management and service continuity of an IoT application. In an IoT application, a node relies on direct evidence (upon interacting) andindirect evidence (upon hearing recommendations vs. own assessment toward a third-party node) to evaluate the honesty trust property of another node.

2) The *cooperativeness* trust property represents whether or not the trustee node is socially cooperative [28] with the trustor node. A node may follow a prescribed protocol only when interacting with its friends or nodes with strong social ties (with many common friends), but become uncooperative when interacting with othernodes. In an IoT application, a node can evaluate the cooperativeness property of other nodes based on social ties and select socially cooperative nodes in order toachieve high application performance.

3) The *community-interest* trust represents whether or not the trustor and trustee nodes are in the same social communities/groups (e.g. co-location or co-work relationships [3]) or have similar capabilities (e.g., parental object relationships [3]). Two nodes with a degree of high community-interest trust have more chances and experiences in interacting with each other, and thus can result in better application performance

We note that while transaction importance or degree of friendship can complement or refine the above three trust properties, we will not consider them in this paper for simplicity. In Section 3.2 below we discuss in detail how a node evaluates other nodes in *honesty*, *cooperativeness*, and*community-interest* trust properties by combining first-handdirect observations (discussed in Section 3.2.1) and second-hand recommendations (discussed in Section 3.2.2).

Trust Propagation and Aggregation

Adaptive trust management is a ongoing process which constant aggregates past information and new information. The new information includes both direct observations (first-hand information) and indirect guidance (second-hand information). The trust assessment of node i towards node j at time t is denoted by

$T(t)$ where X = *honesty*, *cooperativeness*, or *community*

ij

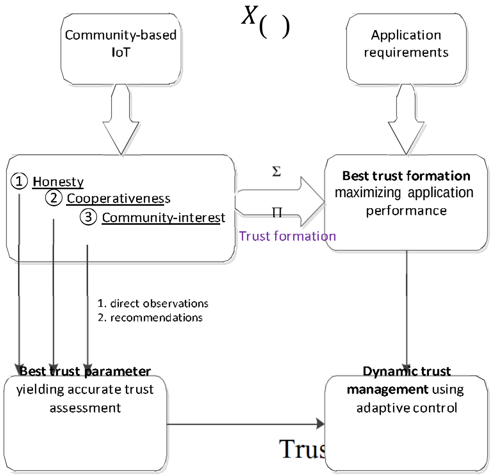

X( )
Community-based IoT
Application requirements
① Honesty
② Cooperativeness
③ Community-interest
Σ
Π
Trust formation
Best trust formation maximizing application performance
1. direct observations
2. recommendations
Best trust parameter yielding accurate trust assessment
Dynamic trust management using adaptive control
Trus

Figure 3: Components of adaptive trust management for a social IoT system: (1) trust composition – *honesty*, *cooperativeness*, and *community-interest*, (2) trust propagation and aggregation – combining first-hand (direct observations) and second-hand information (recommendations), (3) trust formation – forming the overall trust out of three individual trust properties, (4) adaptive trust management – adaptively adjusting parameter settings to improve trust evaluation accuracy and trust formation to maximize application performance.

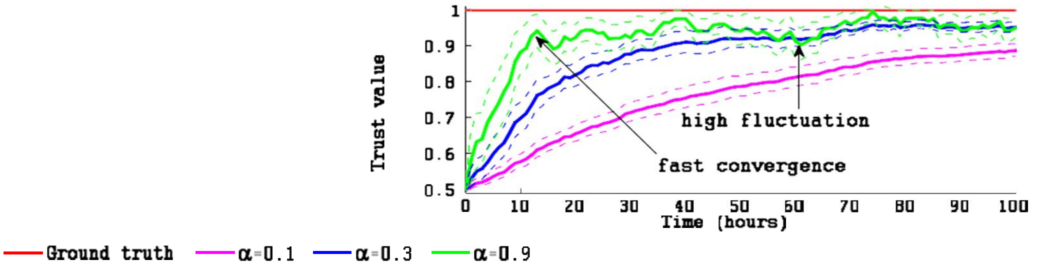
And 0 distrust. In IoT infrastructure, nodes interact with$_{ij}$ each other when they detect the presence of each other, via IoT discovery protocols such as [33]. When evaluating (t), we adopt the following notations: node *i* is the trustor, node *j* is the trustee, node *k* is a recommended to provide its feedback about node *j* to node *i*.

V. PROTOCOL PERFORMANCE EVALUATION

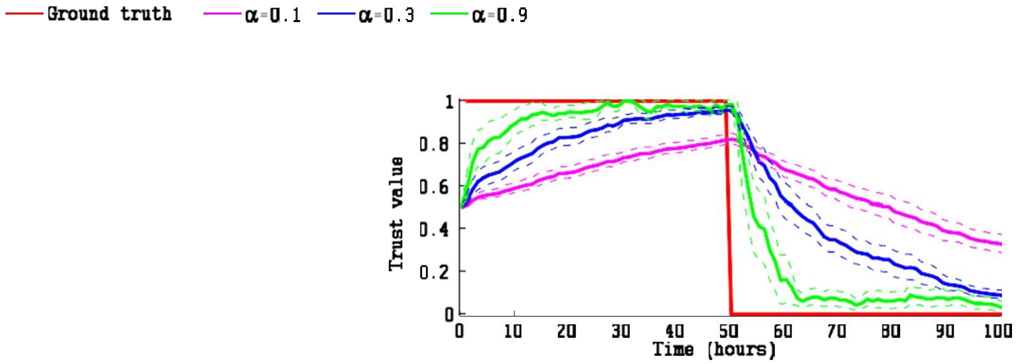
In this section, we asses our proposed adaptive trust management protocol based on ns3 simulation to validate the junction, accuracy, and flexiblity properties of our protocol design. The readers are referred to [6] for a formal proof. Later in Section 5, we will illustrate the utility of our adaptive trust management protocol design with two real-world social IoT applications.

A. Social IoT Environment Setup

In our experimental setup the status of each node is changing dynamically. The input is specified by a set of input instructions in Table 1. We consider a hostile environment where the percentage of malicious nodes $\lambda \in$ [10, 90%] is arbitariliy selected out of all IoT devices. The default value of λ is 30% and we will test the sensitivity of performance results with respect to λ. A node selected to be in this "malicious" population is benign initially, but turns malicious after a period of time $Tc \in$ [0, 100 hrs] randomly generated is elapsed, after which it will perform attacks as described in Section 2. On the other hand, a node not selected in this "malicious" population remains benign all over the simulation. With this setup, while the objective trust or ground truth of a good node remains constant, the objective trust or ground truth of a malicious node changes dynamically. We consider a social internet of things environment with NT=50 heterogeneous smart objects/devices with all of them providing various services. These devices are randomly distributed to NH=20 owners. The social cooperativeness relationship among the devices is characterized by a friendship relationship (matrix) [28] among device owners. That is, if the owners of devices i and j are friends, then there is a 1 in the ij location. While our protocol allows



a) Trust of a good node randomly picked.



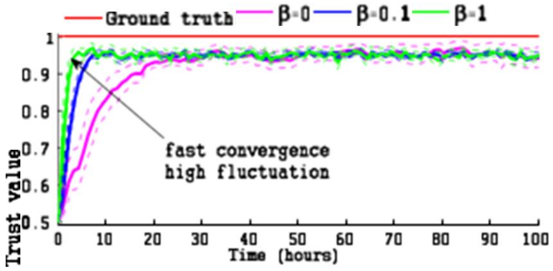
b) Trust of a malicious node randomly picked.

Figure 2: Effect of α on honesty trust evaluation (a) toward a good node and (b) toward a malicious node which turns bad at $\boldsymbol{T_c}$=50 hours. Trust converges in both cases. There is an inherent trade-off between trust convergence time vs. trust fluctuation. Specifically, as the value of α increases, the trust value converges to ground truth faster, but the trust fluctuation also becomes higher

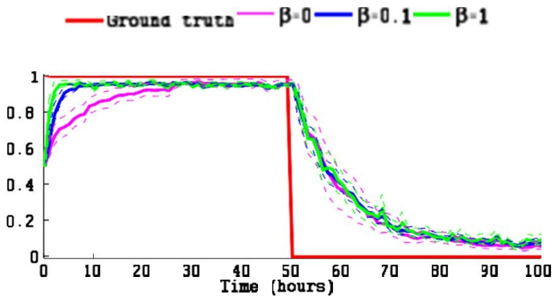
Dynamic friend lists, the friend list kept by each device is simulated initially and remains the same throughout the simulation. Devices are used by their owners in one or more social groups. A device can belong to up to NG=10 communities or groups. This is also simulated and remains fixed all over the simulation. We assume that the encounter or interaction pattern follows a bounded power law allocation ([10mins, 2 days]) with the slope equal to 1.4, resulting in the average interaction-contact time T being 4 hours. The settings are close to those obtained from real traces [25]. The all simulation time is 100 hours. The initial trust value of all devices is set to ignoring with a trust level of 0.5. Our aim is to show that an IOT device upon hostility changes can adaptively select trust protocol settings in terms of α and β to best tradeoff the trust convergence rate and trust varition rate to obtain an acceptable mean absolute error (MAE) between the trust value obtained vs. ground truth.

B. Effect of α on Trust Evaluation

We first investigate the effect of design parameter α on trust evaluation. Recall that α is the weight associated with direct trust with respect to past experience in Equation 1. For sensitivity analysis of α, we vary α by selecting different values (0.1, 0.3, and 0.9) and set β to 0 to isolate its effect. The percentage of spiteful nodes λ is 30%. Here we only give the results for the honesty trust property evaluation. The other two trust properties follow the same style. Figure 2(a) shows the effect of α on honesty trust estimation toward a "good" node whose ground truth status does not change as time increases. The ground truth honesty status for this good node is constant at 1. The dash lines show the empirical confidence intervals with 90% confidence. We can see that the trust evaluation approaches ground truth as time expand. Further, we observe that as the value of α increases, the trust value converges to ground truth faster, but the trust variation also becomes higher. Here we observe that the trust convergence time is 5 to 10 hours because the average inter-arrival activity time following a bounce power law distribution is set to 4 hours (as listed in Table 1). Figure 2(b) shows the results of trust estimation for honesty toward a "malicious" node a arbitrarily selected whose status goes from benign to malicious after Tc = 50 is elapsed. We can see that after the status change, the trust evaluation converges towards the new ground truth status. In addition, as the value of α boosted, the trust evaluation converges to the new ground truth status faster, albeit with a higher fluctuation. This result validates the convergence, accuracy, and resiliency properties of our protocol design.



A) Trust of a good node randomly picked



B) Trust of a malicious node randomly picked

Figure 5: Effect of Q on honesty trust evaluation (A) toward a goodnode and (B) toward a malicious node which turns bad at $\boldsymbol{T_c}$=50 hours. Trust converges in both cases. There exists a trade-off between trust convergence time vs. trust fluctuation. As Q increases, the trust evaluation converges to the ground truth faster, but the trust fluctuation becomes higher. The effect of Q is not as significant compared to the effect of a.

C. Effect of Q on Trust Evaluation

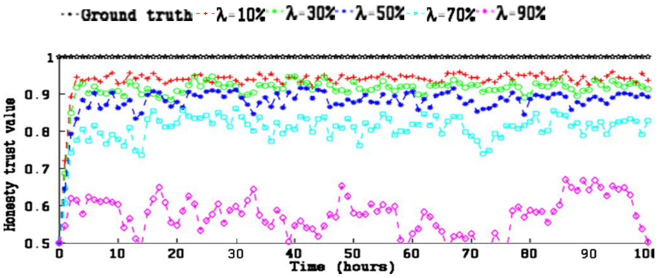
Next, we search the effect of design parameter β on trust evaluation. Recall that β is related to γ by Equation 3, represents the weight associated with the indirectly recommendation with respect to past experience in Equation 2. For sensitive analysis of β, we vary β by selecting different values (0, 0.1, and 1), and set α to 0.5 to separate its effect.

Figure 3(a) shows the effect of β on honesty trust evaluation of a good node. Again, we can see that our trust evaluation approaches ground truth status as time increased. We also observe that as β increases, the trust evaluation cross to the ground truth faster, but the trust alteration becomes higher. The reason is that using more recommendations (higher β) helps trust convergence through effective trust propagation. However, one can see that the effect of β is inconsiderableS compared to the effect of α

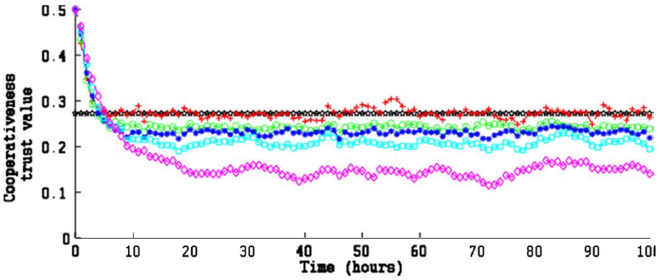
The reason is that very often in a social IoT environment, the chance of a trustor interacting with a recommender is higher than the chance of the trustor directly interacting with a trustee. As long as $\beta > 0$, adaptive trust management is able to effectively aggregate trust using recommendations from a large number of suggestion, thus making the effect of further increasing the value of β insignificant. Figure 3(b) shows the effect of β on honesty trust evaluation of a malicious node randomly selected whose status goes from benign to malicious after $Tc = 50$ hours is progressed. Again, we see that after the ground truth status changes, our trust protocol quickly converges towards the new ground truth status. Initially using more recommendations ($\beta > 0$) in trust evaluation helps trust convergence. However, after the status change, the convergence behavior is about the same regardless of β. This is partly because the effect of β (Figure 3(b)) is negligible compared to the effect of α (Figure 2(b)) and partly because an honest recommender can adversely provides obsolete and inaccurate trust recommendations toward a malicious node, as it has not interacted with the malicious node since the malicious node's status change. As the trustor will not exclude these inaccurate recommendations from good nodes, using more recommendations does not accelerate the pace of trust convergence.

D. Adaptive Trust Management in Response toDynamically Changing Hostility Conditions

From Figures 2 and 3, one can see that the trust evaluation quickly converges and it is remarkably close to the ground truth status, demonstrating its resiliency against trust attacks. We further validate resiliency of our adaptive trust management protocol toward trust attacks in IoT environments with a vary degree of antagonistic. We consider five different apposed environments with the percentage of evil nodes λ being 10%, 30%, 50%, 70%, and 90%.



E. Honesty Trust



Cooperativeness trust

Figure 6 Effect of hostility on dynamic trust evaluation of a good node toward another good node. Our adaptive trust management protocol can react to changing hostility by dynamically choosing the best (α, Q) values to tradeoff the trust convergence rate and trust fluctuation rate to obtain an acceptable MAE between the trust value obtained vs. ground truth.

Figures 4(a), 4(b) show trust evaluation resultsof a good node one by one picked toward another good node also randomly picked for honesty (ground truth trust = 1), cooperativeness (ground truth trust = 0.28), and community-interest (ground truth trust = 0.38), respectively. One can see that the trust evaluation quickly converges and it is surprisingly close to the ground truth status (marked with solid lines) with MAE less than 10% when $\lambda \leq 50\%$, demonstrating our protocol's high resiliency to trust attacks. As λ increases, the MAE of trust evaluation naturally increases because of more false suggestions from malicious nodes. Even when most nodes are malicious with λ going from 70 to 90%, the Mean Absolute Error only goes from 12 to 40%. This show our protocol's high resiliency toward attacks even in extremely hostile environments.

Here we note that given information of environment hostility (expressed in terms of λ), our adaptive trust management protocol can react to change hostility by mightly choosing the better (α, β) values to swap the trust convergence rate and trust fluctuation rate to obtain an acceptable MAE between the trust value obtained vs. ground truth. We will discuss how one may apply the analysis results at runtime in Section 6.

VI. IOT APPLICATION PERFORMANCE

To illustrate the effectiveness of our proposed trust protocol for IoT systems, we consider two real-world social Internet of Things applications [2, 3, 4] which require dynamic service composition and binding [19, 29]. Such social IoT applications running on top of our trust protocol aim to first compose a service plan (this is the service composition part) and then select the most trustworthy IoT nodes (this is the service binding part) for providing services requested such that the trustworthiness score representing the goodness of the service composition is maximized. We compare the performance of trust-based service composition with two baseline approaches:

1) Ideal Service Composition: it returns the maximum achievable trustworthiness score by always knowingly selecting service providers with the highest "ground truth" trustworthiness scores (based on the actual status). This scheme in practice is not achievable because we do not know ground truth status
2) Random Service Composition: it selects service providers randomly without regard to trust

A. Smart City Air Pollution Detection

We examine a smart city IOT application running on Alice's smartphone for air pollution detection [4]. Alice tries to avoid stepping into high air pollution areas (in terms of the levels of carbon dioxide, PM10, etc.) for health reasons. Alice's smartphone is a member of the air pollution awareness social network. She decides to invoke her smartphone to connect to sensor devices in an area she is about to step (or drive) into. Alice knows that many IoT devices will respond, so she needs to make a decision on which sensing results to take. She instructs her smartphone to gain results only from n=5 most "trustworthy" sensors and she will follow a trust-weighted mass voting result. That is, each yes or no recommendation is counted as 1 weighted by Alice's trust toward the recommender. If the total trust-weighted "yes" score is higher than the total trust-weighted "no" score, Alice will step into the area; otherwise, she will make a detour to avoid the area.

This smart city air pollution detection application is essentially a simple trust-based service composition IoT application in which Alice will simply select n=5 IoT devices for which she trusts the most. Therefore, the trustworthiness score of this service composition application which it aims to maximize is simply the sum of the individual trustworthiness scores. Since this application involves a simple binary decision (yes or no), we consider a simple trust formation design as follows. If a selected service provider does not pass the minimum honesty trust

;

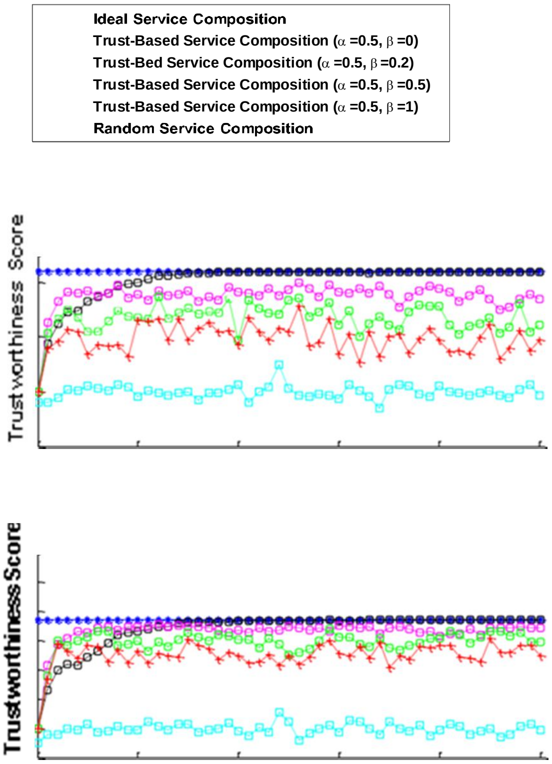


Figure 7. Performance comparison for the smart city air pollutiondetection application.

Threshold, the trustworthiness score is zero; otherwise, the trustworthiness score is determined by the social ties between the service provider and the service requester, i.e., a higher trustworthiness score is given if they have more common friends, or if they share more community interests. The rationale of using honesty trust to screen service providers is to avoid malicious service. The rationale of using cooperativeness and community interest trust to subsequently rank service providers is that trustee nodes with which a trustor node has good social ties can most likely provide good service in social IoT environments. Alice decides to set the minimum honesty trust threshold as 0.5. With the above given reasons, her smartphone (as node i) guess the trustworthiness score $T(t)$ toward each service provider (node j) as follows:

$$0, \qquad if\ T^{honesty}(t) \leq 0.5$$

$$ij^{(4)}$$

$$T_{ij}(t) = \qquad T^{cooperativeness}(t),$$

$$\min(\quad ij \qquad), \quad if\ T^{honesty}(t) > 0.5$$

$$T^{community-interest}(t) \qquad ij$$

$$ij$$

Figure 5 diffrentiate trust-based service state against two baseline service comparison methods (random and ideal). The expolatory setup is the same as that in Section 4. The performance metric is the combined trustworthiness score for n=5 service providers selected. We consider 4 kinds of trust-based service composition by selecting 4 various sets of design parameters: (α, β) = (0.5, 0), (α, β) = (0.5, 0.2), (α, β) = (0.5, 0.5), and (α, β) = (0.5, 1) for the need of testing the effect of (α, β)on application performance.

VII. RELATED WORK

In this section, we survey recently proposed trust management protocols for IoT systems. We contrast and compare our work with existing work so as to differentiate our work from existing work and identify unique features and contributions of our trust protocol design and trust- based service management design for IoT systems.

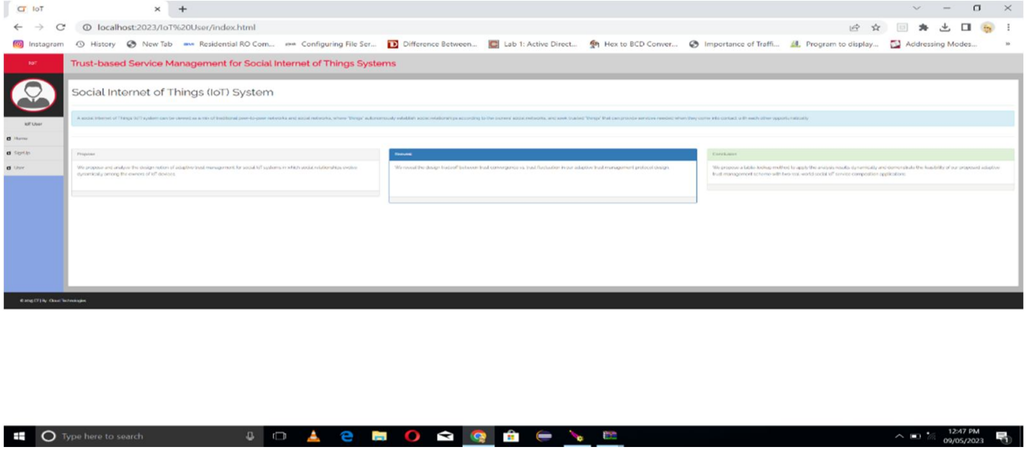
There is little work on trust management in IoT environments for security enhancement, especially for dealing with misbehaving owners of IoT devices that provide services to other IoT devices in the system. Chen et al. [14] proposed a trust management model based on fuzzy reputation for IoT systems. However, their trust management model considers a very specific IoT environment populated with wireless sensors only, so they only considered QoS trust metrics like packet forwarding/delivery ratio and energy consumption for measuring trust of sensors. On the contrary, our work considers both QoS trust deriving from communication networks and social trust deriving from social networks which give rise to social relationships of owners of IoT devices in the social IoT environment. Saied et al. [36] proposed a context-aware and multiservice approach for trust management in IoT systems against malicious attacks. However it requires the presence of centralized trusted servers to collect and disseminate trust data, which is not viable in IoT environments. Relative to [36], our trust protocol is totally distributed without requiring any centralized trusted entity. Bao and Chen [5] suggest a trust management protocol considering both social trust and QoS trust metrics and by using both direct observations and indirect suggestion to update trust in IoT systems. However the issue of adaptively adjusting trust evaluation in response to dynamically changing conditions so as to cope with misbehaving nodes and maximize the performance of IoT applications running on top of the trust management was not addressed. Relative to [5] cited above, we not only consider multiple trust properties for social IoT environments, but also analyze the tradeoff between trust convergence speed and trust fluctuation to identify the best protocol parameter settings for trust propagation and aggregation to best exploit this tradeoff for minimizing trust bias. Furthermore, it addresses the issue of trust formation for application performance maximization using service composition as an application example.

Very recently, Nitti et al. [32] considered social relationships of owners of IoT devices for trust management in social IoT systems. They proposed two models for trustworthiness management. Namely, a subjective model deriving from social networks, with each node computing the trustworthiness of its friends on the basis of its own experience and on the opinion of friendly recommenders, and an objective model deriving from P2P communication networks with each node storing and retrieving trust information towards its peers in a distributed hash table structure, so that any node can be make use of the same information. Their objective model requires pre-trusted nodes be in place for maintaining the hash table, which is questionable in IoT environments. Their subjective model is similar in spirit to our trust model taking into consideration of the social relationships between owners of IoT devices. The fundamental difference is that our model of objective trust is based on ground truth or actual status, and our trust protocol dynamically adapts to changing environments by adjusting the best protocol settings to minimize trust bias (the difference between subjective trust and objective trust) and to maximize application performance.

Security has drawn the attention in IoT research [14, 15, 34, 35, 42]. Roman et al. [35] talk about threats of Internet of Things, such as compromising botnets tries to hinder services and the domino effect in between intertweaved services and user profiles. Traditional approaches to network security, data and privacy management, identity management, and fault tolerance will not accommodate the requirements of IoT due to lack of scalability and not being able to cope with a high variety of identity and relationship types [35]. Possible solutions were proposed to each security problem, but no specific protocol or analysis was given. Ren [34] presents a compromise-resilient key management plan for diverse wireless IoT. The proposed key management protocol includes key agreement schemes and key evolution policies (forward and backward secure key evolution). The author also designed a quality of service (QoS) aware enhancement to the proposed scheme. However, the proposed scheme does not take social relationships among IoT identities into consideration. Chen and Helal 15 proposed a device-centric approach to enhance the safety of IoT. They designed a device description language (DDL) in which each device can specify its safety concerns, constraints, and knowledge. Nevertheless, their approach is specifically designed for sensor and actuator devices, and does not consider social relationships among device owners. Zhou and Chao [42] proposed a media-aware traffic security architecture for Internet of Things. The authors first designed a multimedia traffic classification, and then developed this media-aware traffic security architecture to achieve a good trade-off between system flexibility and efficiency. A limitation of their work is that they only considered direct observations to traffic without considering indirect recommendations.

Relative to the security designs/mechanisms cited above, our approach is to use trust to implement security against malicious attacks. We note that our trust system can work orthogonally with these security designs/mechanisms to further enhance security of social IoT systems.

VIII. RESULT ANALYSIS

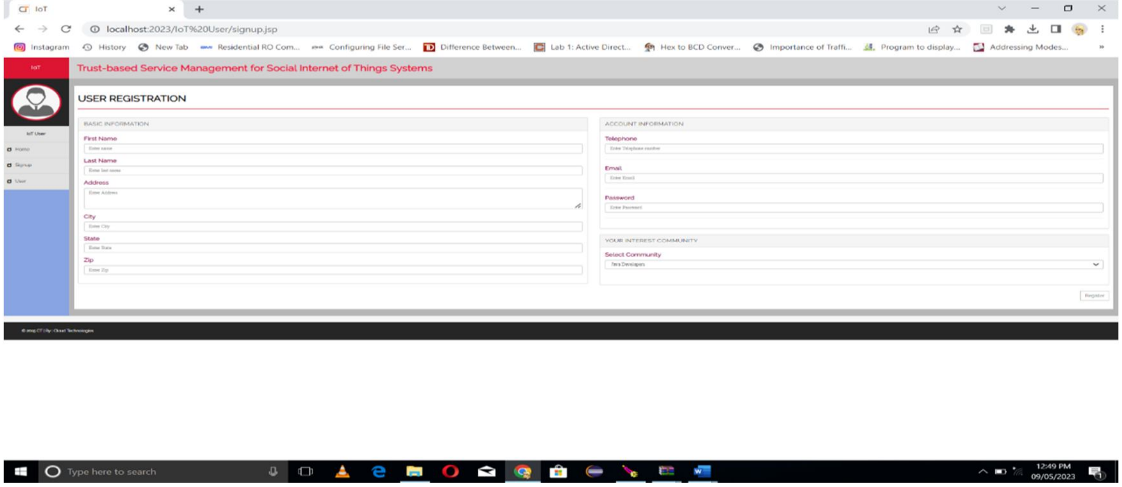


localhost:2023/IoT%20User/index.html

Trust-based Service Management for Social Internet of Things Systems

Social Internet of Things (IoT) System

Figure 8. HOME Page

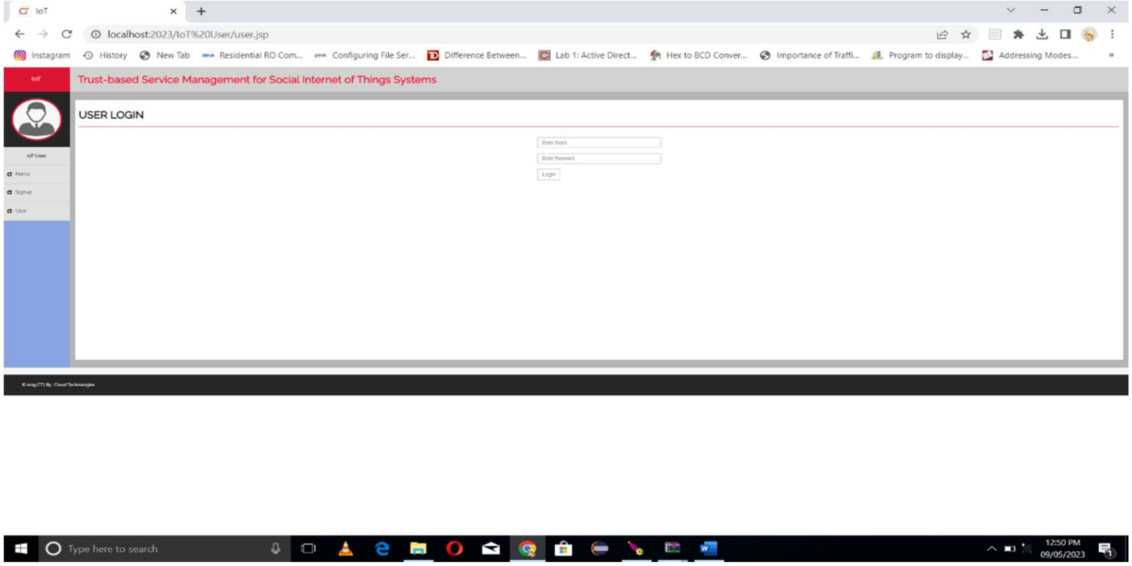


localhost:2023/IoT%20User/signup.jsp

Trust-based Service Management for Social Internet of Things Systems

USER REGISTRATION

Figure 9. User Registration

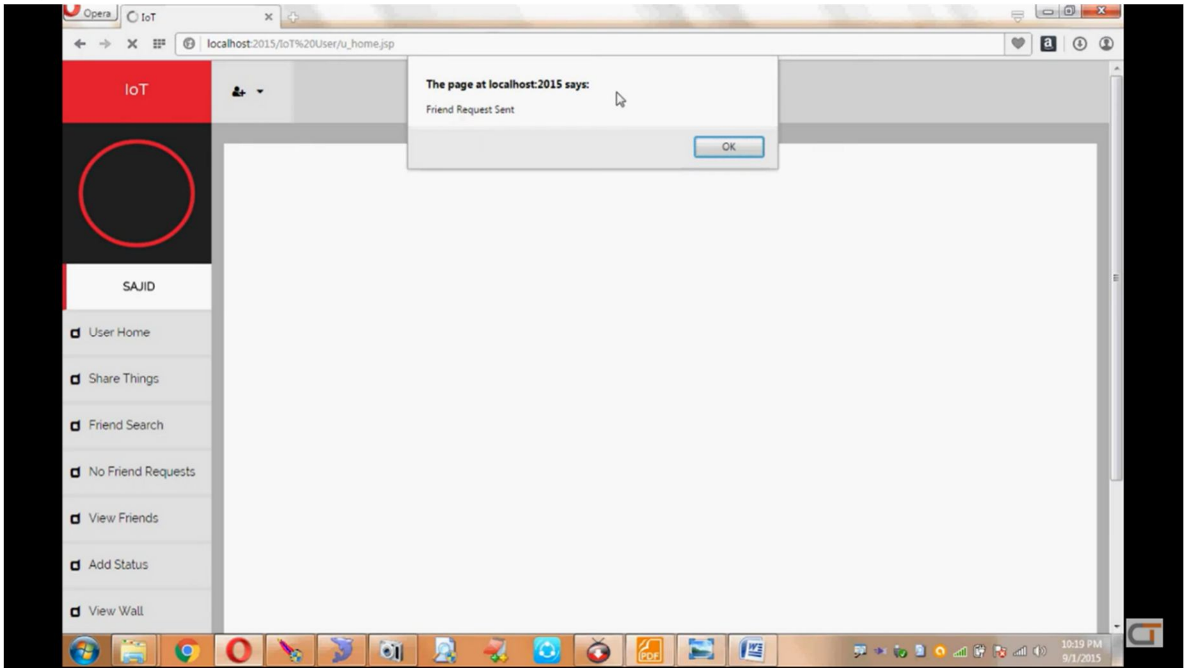


localhost:2023/IoT%20User/user.jsp

Trust-based Service Management for Social Internet of Things Systems

USER LOGIN

Figure 10. User LOGIN



The page at localhost:2015 says:

Friend Request Sent

Figure 8. Friend Request Send

IX. CONCLUSION

We developed and analyzed an adaptive trust management protocol for social Internet of thing systems and its application to service management. Our protocol is distinguished and each node only updates trust towards others of its interest upon encounter or agency events. The trust assessment is modernized by both direct observations and indirect suggestions, with parameters α and β being the respective design parameters to control trust propagation or aggregation there are two sources of information to improve trust assessment accuracy in response to dynamically changing conditions. We analyzed the outcome of α and β on the convergence, accuracy, and resiliency properties of our adaptive trust management protocol using simulation. The results demonstrate that (1) the trust estimation of adaptive trust management will convene and approach ground truth status, (2) one can tradeoff trust convergence speed for low trust oscillation, then (3) adaptive trust management its resilient to misbehaving attacks. We demonstrated the effectiveness of adaptive trust management by two real-world SIOT applications. The results showed our adaptive trust-based service composition scheme outperforms random service composition and approaches the maximum achievable performance based on ground truth. We attributed this to the capability of dynamic trust management being able to effectively choose the best design parameter settings in response to changing environment conditions.

We have study and provides a comprehensive analysis in the field of Social Internet of Things based on the trust management framework/models. Different social Internet of Things architectures are covered in the introduction section. Social relationships are the pillars of any Social Internet of Things architecture in any context. Therefore, this study also covers various social relationships which play an important role in the development of trust management frameworks as part of the introduction section. Our focus is on the examination of the trust management facets in social internet of thing that’s why this study covers all different facets of trust in detail.

Each trust management framework comprises Trust Attributes whose features are broadly classified as general trust properties and trust properties particularly related to the social aspects in the social internet of thing domain.

Our survey includes the classification of studies on the types of Trust Attributes ‘‘Social Trust’’ or ‘‘Quality of Service (QoS)’’ are used. Any trust management framework is based on there three general steps: trust computation, trust aggregation, and trust updates. the trust management framework is based on there are three general types trust computation, trust aggregation, and trust updates. The three general steps make use of Trust Attributes to perform the estimation. a local trust values are accumulated or aggregated to form an overall or global trust by using various trust aggregation schemes. Our research work also covers many distinguished trust computation and trust aggregate techniques in detail. The weighted Sum technique is one of the generally. Used techniques because of its low cost and easily operated.

REFERENCES

[1] Adali et al., "Measuring Behavioral Trust in Social Networks," IEEE International Conference on Intelligence and Security Informatics, Vancouver, BC, Canada, May 2010.

[2] L. Atzori, A. Iera, and G. Morabito, “The Internet of Things: A Survey,” Computer Networks, vol. 54, no. 15, Oct. 2010, pp. 2787- 2805.

[3] L. Atzori, A. Iera, G. Morabito, and M. Nitti, “The Social Internet of Things (SIoT) - When social networks meet the Internet of Things: Concept, architecture and network characterization,” Computer Networks, vol. 56, no. 16, Nov. 2012, pp. 3594-3608.

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

[5] F. Bao, and I. R. Chen, “Dynamic Trust Management for Internet of Things Applications,” 2012 International Workshop on Self-Aware Internet of Things, San Jose, California, USA, September 2012.

[6] F. Bao, Dynamic Trust Management for Mobile Networks and Its Applications, ETD, Virginia Polytechnic Institute and State University, May 2013.

[7] F. Bao, I. R. Chen, M. Chang, and J. H. Cho, “Hierarchical Trust Management for Wireless Sensor Networks and Its Applications to Trust-Based Routing and Intrusion Detection,” IEEE Trans. on Network and Service Management, vol. 9, no. 2, 2012, pp. 161-183.

[8] F. Bao, I. R. Chen, and J. Guo, “Scalable, Adaptive and Survivable Trust Management for Community of Interest Based Internet of Things Systems,” 11th IEEE International Symposium on Autonomous Decentralized System, Mexico City, Marc———h 2013.

[9] N. Bui, and M. Zorzi, “Health Care Applications: A Solution Based on The Internet of Things,” the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies, Barcelona, Spain, Oct. 2011, pp. 1-5.

[10] B. Carminati, E. Ferrari, and M. Viviani, Security and Trust in Online Social Networks, Morgan & Claypool, 2013.

[11] . R. Chen, F. Bao, M. Chang, and J.H. Cho, “Dynamic Trust Management for Delay Tolerant Networks and Its Application to Secure Routing,” IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 5, 2014, pp. 1200-1210.

[12] I. R. Chen, F. Bao, M. Chang, and J.H. Cho, “Trust-based intrusion detection in wireless sensor networks,” IEEE International Conference on Communications, Kyoto, Japan, June 2011, pp. 1-6.

[13] I.R. Chen, F. Bao, M. Chang, and J. H. Cho, “Trust management for encounter-based routing in delay tolerant networks,” IEEE Global Telecommunications Conference (GLOBECOM 2010), 2010, pp. 1-6.

[14] D. Chen, G. Chang, D. Sun, J. Li, J. Jia, and X. Wang, “TRM-IoT: ATrust Management Model Based on Fuzzy Reputation for Internet of Things,” Computer Science and Information Systems, vol. 8, no. 4, Oct. 2011, pp. 1207-1228.

[15] C. Chen, and S. Helal, “A Device-Centric Approach to a Safer Internet of Things,” the 2011 International Workshop on Networking and Object Memories for the Internet of Things, Beijing, China, Sep. 2011, pp. 1-6.

[16] J.H. Cho, I.R. Chen, and P. Feng “Effect of Intrusion Detection on Reliability of Mission-Oriented Mobile Group Systems in Mobile AdHoc Networks,” IEEE Trans. on Reliability, vol. 59, 2010, pp. 231- 241.

[17] J. H. Cho, A. Swami, and I. R. Chen, “Modeling and Analysis of Trust Management for Cognitive Mission-Driven Group Communication Systems in Mobile Ad Hoc Networks,” International Conference on Computational Science andEngineering, vol. 2, 2009, pp. 641-650.

[18] J. H. Cho, A. Swami, and I. R. Chen, “Modeling and analysis of trust management with trust chain optimization in mobile ad hoc networks,” Journal of Network and Computer Applications, vol. 35, no. 3, 2012, pp. 1001-1012.

[19] K. Dar, A. Taherkordi, R. Rouvoy, and F. Eliassen, “Adaptable Service Composition for Very-Large-Scale Internet of ThingsSystems,” ACM Middleware, Lisbon, Portugal, Dec. 2011.

[20] T. Dubois, J. Golbeck, and A. Srinivasan, "Predicting Trust andDistrust in Social Networks," IEEE 3rd International Conference on Social Computing, Boston, MA, USA, Oct. 2011, pp. 418-424.

[21] A. Gluhak, S. Krco, M. Nati, D. Pfisterer, N. Mitton, and T. Razafindralambo, “A Survey on Facilities for Experimental Internet of Things Research,” IEEE Communications Magazine, vol. 49, no. 11, Nov. 2011, pp. 58-67.

[22] A. Gutscher, “A Trust Model for an Open, Decentralized Reputation System,” IFIP International Federation for Information Processing, vol. 238, 2007, pp. 285-300.

[23] A. J. Jara, M. A. Zamora, and A. F. G. Skarmeta, “An Internet of Things-Based Personal Device for Diabetes Therapy Management in Ambient Assisted Living (AAL),” Personal and Ubiquitous Computing, vol. 15, no. 4, 2011, pp. 431-440.

[24] A. Josang, R. Ismail, and C. Boyd, “A Survey of Trust and Reputation Systems for Online Service Provision,” Decision Support Systems, vol. 43, no. 2, March 2007, pp. 618-644.

[25] T. Karagiannis, J.-Y. Le Boudec, and M. Vojnović, “Power Law and Exponential Decay of Intercontact Times between Mobile Devices,” IEEE Transactions on Mobile Computing, vol. 8, no. 10, 2007, pp. 1377-1390.

[26] S. Lee, R. Sherwood, and B. Bhattacharjee, “Cooperative Peer Groups in NICE,” INFOCOM 2003, vol. 2, pp. 1272-1282, SanFrancisco, March 2003.

[27] X. Li, R. Lu, X. Liang, X. Shen, J. Chen, and X. Lin, “Smart Community: An Internet of Things Application,” IEEE Communications Magazine, vol. 49, no. 11, Nov. 2011, pp. 68-75.

[28] Q. Li, S. Zhu, and G. Cao, “Routing in Socially Selfish Delay Tolerant Networks,” IEEE Conference on Computer Communications, San Diego, CA, March 2010, pp. 1-9.

[29] L. Liu, X. Liu, and X. Li, “Cloud-Based Service Composition Architecture for Internet of Things,” International Workshop on Internet of Things, Changsha, China, August 2012, pp. 559-564.

[30] G. Liu, Y. Wang, M.A. Orgun, and H. Liu,“Discovering Trust Networks for the Selection of Trustworthy Service Providers in Complex Contextual Social Networks,” 19th IEEE International Conference on Web Services, 2012, pp. 384-391.

[31] R. Mitchell and I.R. Chen, “Effect of Intrusion Detection and Response on Reliability of Cyber Physical Systems,” IEEE Transactions on Reliability, vol. 62, no. 1, March 2013, pp. 199-210.

[32] M. Nitti, R. Girau, and L. Atzori, “Trustworthiness Management in the Social Internet of Things,” IEEE Transactions on Knowledge andData Management, vol. 26, no. 5, 2014, pp. 1-11.

[33] F. Paganelli and D. Parlanti, “A DHT-Based Discovery Service for the Internet of Things,” Computer Networks and Communications, vol. 2012, Article ID 107041, 11 pages, 2012.

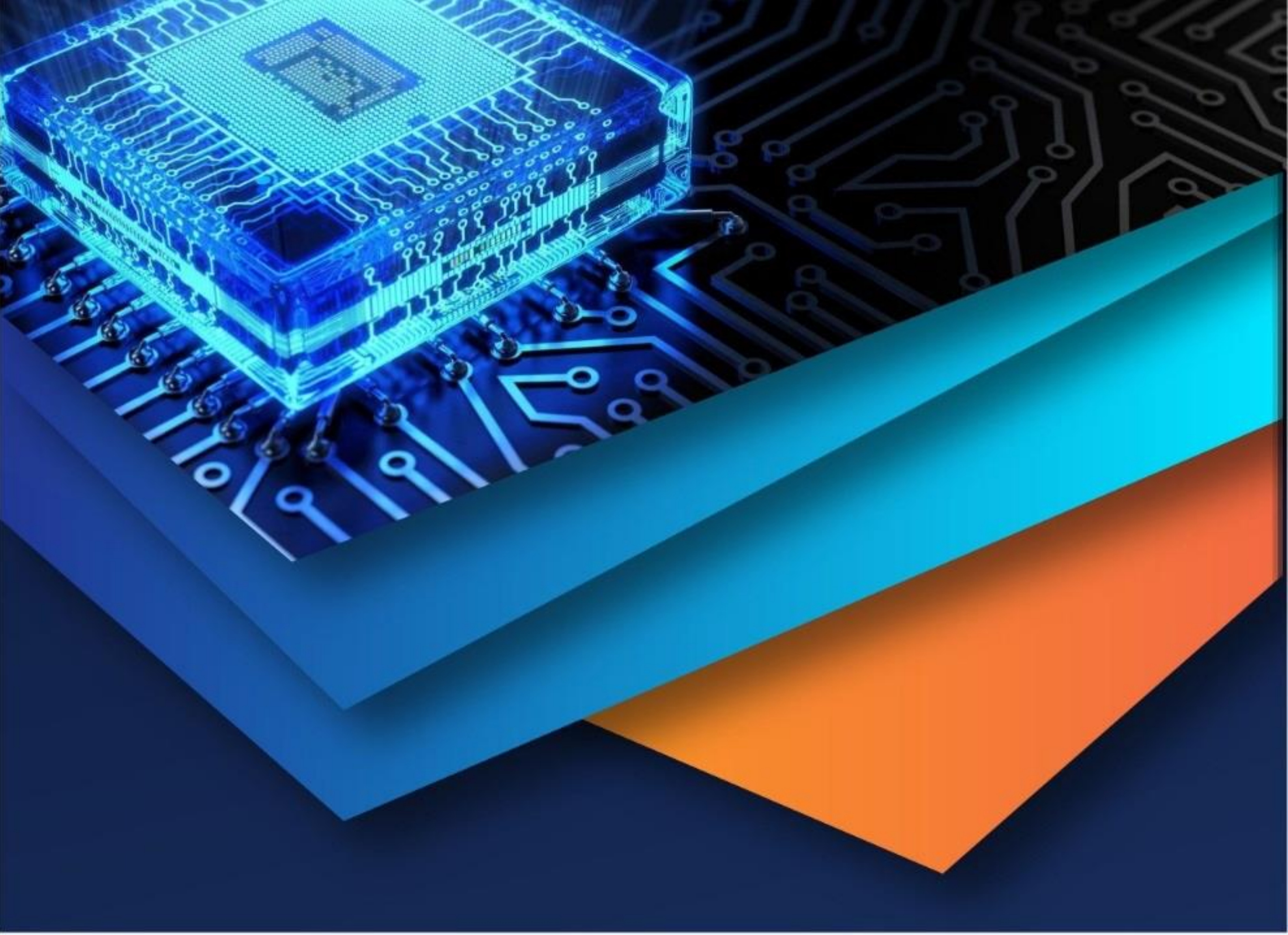
[34] W. Ren, “QoS-aware and compromise-resilient key management scheme for heterogeneous wireless Internet of Things,” International Journal of Network Management, vol. 21, no. 4, July 2011, pp. 284- 299.

[35] R. Roman, P. Najera, and J. Lopez, “Securing the Internet of Things,” Computer, vol. 44, no. 9, Sep. 2011, pp. 51-58.

[36] 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 and Security, vol.39, part B, Nov. 2013, pp. 351–365.

[37] A. A. Selçuk , E. Uzun , and M. R. Pariente, “A Reputation-based Trust Management System for P2P Networks,” Network Security, vol.6, no.3, May 2008, pp. 235-245.

[38] W. Sherchan, S. Nepal, and C. Paris, "A Survey of Trust in Social Networks," ACM Computing Survey, Vol. 45, No. 4, Article 47, August 2013.



10.22214/IJRASET

INDEX COPERNICUS
45.98

IMPACT FACTOR:
7.129

TOGETHER WE REACH THE GOAL
IMPACT FACTOR:
7.429