Trust Management for Service-Oriented SIoT Systems

Roopa M S*
IoT Lab, University Visvesvaraya College of Engineering, India

Puneetha R
IoT Lab, University Visvesvaraya College of Engineering, India

Vishwas H K
IoT Lab, University Visvesvaraya College of Engineering, India

Rajkumar Buyya
University of Melbourne, Melbourne, Australia

Venugopal K R
Bangalore University, Bangalore, India

Iyengar S S
Florida International University, Miama, USA

Patnaik L M
National Institute of Advanced Studies, Bangalore, India

ABSTRACT

With the proliferation of fairly powerful mobile devices and ubiquitous wireless technology, there is a transformation from traditional ad hoc networks into a new era of service-oriented Internet of Things (IoT) networks wherein an object can provide and receive services. One of the principal conceptions of IoT is to socialize the objects. A social IoT system is a mixture of IoT and social networks, where objects inde- pendently create social relationships among other objects in the vicinity and search the most trusted objects to render services required when they remain connected with each other. We propose a service-oriented trust management scheme for detecting the adversarial attacks that ex- ist in the SIoT network to build a reliable system. The proposed scheme integrates multiple constituents such as trust metrics, intended trust and recurrent trust update to determine the trust score among objects. We aggregate all the trust metrics to select the best metric for assessing each object that provides service; thus, an object with the lesser score is identified and filtered out efficiently. Simulation results demonstrate the efficacy of the proposed trust management scheme against co-relative service attack.

CCS CONCEPTS

• **Information systems —> Information systems applications;;** • **Security and privacy —> Intrusion/anomaly detection and malware mitigation.**;

KEYWORDS

Co-relative Service Attack, Social IoT, Trust Management, Trustworthy Service, Trust Metrics

ACM Reference Format:
Roopa M S*, Puneetha R, Vishwas H K, Rajkumar Buyya, Venugopal K R, Iyengar S S, and Patnaik L M. 2020. Trust Management for Service-Oriented SIoT Systems. In *2020 The 8th International Conference on Information Technology: IoT and Smart City (ICIT 2020), December 25–27, 2020, Xi'an, China.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3446999.3447635

ICIT 2020, December 25–27, 2020, Xi'an, China

ACM ISBN 978-1-4503-8855-9/20/12…$15.00
https://doi.org/10.1145/3446999.3447635

1 INTRODUCTION

The rapid growth in mobile devices, along with ubiquitous wireless technology, has made tremendous transmute in computing technology. The emerging technology that is gaining more momentum due to the outcome of this is the Internet of Things. IoT is an innovative model that is swiftly growing along with wireless telecommunication. The tremendous growth in the IoT has positively impacted several aspects of a users' day to day life. IoT has a noticeable effect in many of the fields, from industries to domestics. Some of the examples being, assisted living, domotics, enhanced learning, e-health [1.] etc.

IoT being a distributed environment it is a challenging task to achieve system goals such as reliability, availability, scalability and reconfigurability. The objects in an IoT environment can change their locations and configure themselves. An IoT network comprises of mobile objects that are wireless in which the networks are formed temporary without any centralized aid for infrastructure, and the communication among objects is via multi-hops. Designing security based protocols for service-based IoT devices pose many technical hurdles, in terms of constraints with limited memory, battery life, bandwidth and computational power. The distinct wireless characteristics also impose a constraint for the design of protocols. Some of them are eavesdropping, shortage of precise ingress and exit points, security threats, swift changes in the topologies due to mobility of objects and the users. With increased powerful computing capabilities of mobile devices, traditional devices are now getting migrated into Service-Based Systems [2.].

In the recent past, the challenges in IoT is handled by the integration of the two network paradigms IoT and social networks termed as Social Internet of Things (SIoT) [3.]. In SIoT, objects independently build social relationships with the owners social networks and inquire trusted objects that can afford required services while they associate with each other opportunistically [4.]. In a service-oriented SIoT system, a device act as a service provider (SP) as well as service requester (SR). Peer-to-Peer service systems with a dynamicity in composing a service plan and binding the service is an instance of service-oriented SIoT. The prime concern

of a service-oriented SIoT is the existence of malicious objects acting in support of malicious owners. The aim of malicious owners is to collude with other malicious objects to maximize their gain and hold the service. In this paper, we use the concept of trust for service-oriented SIoT, where the trust levels of each SP is analyzed by the SR, with which it interacts and the assessed trust value is passed on to the other objects as a recommendation. This ensures that a well-behaving object is selected to provide the requested service and an untrustworthy SP is detected and isolated from the network.

Trust is a vital concept for addressing reliable, secure, seamless interactions and services. Devices must be analyzed based on their behaviour capabilities to predict its performance over time. Behaviour-based analysis in terms of trust management is provided by analyzing the entities or devices based on their past behaviour, by taking a recommendation from other entities or with their reputation gained over time in the network. In order for a device to be trustworthy, it must prevent itself from being affected by the activities performed by malicious devices. Also, management of trust possesses a key challenge in Social IoT systems, in order to guarantee to analyze the reliability of data, to ensure eligible services and user security. Trust management for SIoT systems helps users to surface and surpass their doubts and uncertainty, which leads users to accept and consume IoT services and its applications.

The contributions of the paper are summarized as follows:

- Compute the trust score among objects to develop a trustworthy service- oriented SIoT network.
- Evaluate the intended trust based on Correlation coefficient to predict the expected behaviour of an object and gives higher possibilities to distinguish malicious objects
- Demonstrate the effectiveness of the proposed trust management scheme against co-relative service attacks by comparing with the existing systems.

The rest of the paper is organized as follows. A summary of related works in trust management of SIoT are discussed in Section 2. The system model and the proposed trust management scheme for service-oriented SIoT system is presented in Section 3. Section 4, emphasizes on the performance evaluation and analysis of the proposed method. The concluding remarks are addressed in Section 5.

2 RELATED WORK

In this section, we present the research works for trust management in Social IoT. Chen et.al., [5.] introduced a service recommendation system for detecting malicious attacks and rendering efficient service composition in SIoT environment. It takes transaction properties and social relationships between the devices to estimate access service in dynamic settings and an energy-aware mechanism to balance network. However, it could not achieve better performance and render quality service coping with dynamic behaviour and unstable network status.

Abderrahin et.al., [6.] presented a clustering structure called TMCOI-SIOT based on similarity interest where a single admin controls each cluster. It uses on-off and Kalman filter-technique for trust prediction and to eliminate the course of attacks that are inhibited by malicious nodes. It fails to detect more attacks in the existing architecture.

Rafey et.al., [7.] proposed a context-based social trust model that takes into account social relationships to evaluate trust employing direct and indirect observations. It provides accurate trust assessment and increase the trust convergence speed but was prone to a linear decrease in efficiency due to the collusive attacks from malicious objects. However, it does not explore trusts like cooperativeness and other failures created without malicious purposes.

Truong et.al., [8.] suggested a trust-based model which evaluates human trust information process and establishes the social relationship among the entities. It uses the fuzzy-based algorithm for knowledge trust metrics and a personalized multi-criteria utility for calculation of overall trust score. The disadvantage of this model is that it restricts the trustors' preferences taking part in the final process of trust calculation. Further, it does not enable the reputation system to publish their feedbacks securely, and more safely that can eliminate the risk of trusted attacks. It also fails to employ an intelligent fuzzy expert system that selects the best algorithm autonomously to adapt to the changes in the context.

Kogias et.al., [9.] offered a trust and reputation model that combines the standard explications granted for peer-to-peer and mobile ad-hoc networks. It examines the trust model by operating the state-of-the-art simulator and increases its feasibility in terms of analyzing the performance. However, it does not verify the model in terms of real-world use case situations and implements the probabilistic analysis of the COSMOS project.

Wang et.al., [10.] devised a trustworthy crowdsourcing model to address the security issues in SIoT. It detects the social data links based on the social awareness mechanism. It performs the winner selection and payment decision introducing an auction mechanism and evaluates the reliability of the participants that rule out the cause of unreliability. However, the trustworthiness of transmission of sensed data and interpretation of the results is not addressed.

Chen et.al., [11.] recommended a trust management protocol for rendering direct and indirect applications for managing services in SIoT systems. It is distributed in nature and only updates trust towards other nodes based on its desired level of interest and resilient to misbehaving attacks and trades off convergence pace of trust from inconstancy. However, it is not viable for the dynamically varying environment to improvise its performance in terms of accuracy, convergence and resilient properties. Further, the statistical method to eliminate recommendation outliers to overcome trust variation and improve the trust convergence to design the protocol is not addressed.

Truong et.al., [12.] proposed a model composed of a triad of trust indicators for trust evaluation and creates reputation methods for E-commerce services in social networks. The model uses three computational trust factors, namely reputation experience and knowledge measured from direct observations to recommendations. The disadvantage is that it does not have a scheme that combines the information to demonstrate the trusts subjectivity; it just calculates the trustworthiness of the entities instances.

Kowshalya et.al., [13.] devised a context-aware model that handles dynamic behavior of objects during bad mouthing attack. Moreover, it collects past behaviors and predicts future behaviors making it a case of prevention from malicious objects. However the trust

selective forwarding objects is better in terms of recovery of trust value of malicious objects and the complete isolation of on-off attacks is not being discussed in this paper.

3 SYSTEM MODEL

In this section, we discuss the system model that includes the SIoT network model, adversarial model with the different types of attacks that the IoT objects can perform and the proposed service-oriented trust model for SIoT systems.

3.1 SIoT Network Model

An object in service-oriented SIoT has two important roles: a service provider to offer services and a service requester to request for a service. The requested service may be a composition of other small services which requires dynamic service binding. The service requests are based on the social network among the owners of the IoT objects in which they establish various types of relationships between the friends and their objects in the proximity to seek services and information. The relationships constitutes Parent-object relationship (POR), CoWork object relationship (CWOR), Social-object relationship (SOR), Owner-object relationship (OOR), and Co-location object relationship (CLOR) [14., 15.]. The service request may be a single query or a sequence of multiple individual requests, which we address as abstract services. Each of the service requests can be broadly divided into three phases: Service Advertisement, Service Composition and Service Binding.

1. Service Advertisement: When the service request is placed by the SR, each of the SPs in the SIoT broadcasts its service availability. The SP will broadcast its availability only if it is capable of providing the requested service.
2. Service Composition: Once the SP broadcasts its availability, the responsibility of the SR is to decide on which SP to choose and further SR will construct a plan for executing the service. The service plan is the information on how each service has to be executed, i.e. each service may be a single request or a set of abstract services and the execution may occur sequentially or concurrently.
3. Service Binding: Service binding is the commitment for the SP to ensure its availability to the service request. Once the services are bound, it is the sole responsibility of the SP to complete the service as requested by the SR. If SP does not meet the expectations of the SR, then SP will be rated with negative feedback.

The purpose of composition and binding phases of service is to select the best service provider among available service providers to the customer who issued the request at that particular time.

3.2 Adversarial Model

As in the cases of other network-based models, even a Social IoT environment has its own set of threats. In Social IoT, not every object exhibits the same type of behaviour; few objects may act adversarial for its gain. The behaviour may vary depending on time and place. The various types of attacks exhibited by a malicious IoT objects are as follows:

1. *Self Promotion Attack (SPA)*: A malicious object will report a false quality of service information to promote its importance so that its chance of getting selected increases as a service provider. Once its objective is achieved, it starts to provide service of low quality.
2. *Opportunistic Service Attack (OSA)*: The objects behave opportunistically under different circumstances. That is, when a object observes that its reputation is decreasing, it may provide just enough good service to get selected as SP and then behave absurdly.
3. *Bad Mouthing Attack (BMA)*: A malicious object might bombard with other bad objects to spoil the status of a good object by giving false ratings so that the chance of good object is being chosen as SP decreases.
4. *Ballot Stuffing Attack (BSA)*: A malicious object might bombard with other bad objects to enhance the status of a malicious object by giving false ratings so that probability of bad objects is being chosen as SP increases.
5. *Co-relative Service Attack(CSA)*: A malicious object act as a SP, wherein it ensures its co-relative presence in the proximity for some SR proving false service quality information and increases its chance of being selected as a SP and then try to enter the vicinity.

3.3 Trust Model for Service-Oriented SIoT

The constituents of the trust management scheme for a service-oriented SIoT system are illustrated in Figure 1. The trust metrics constituent addresses the notion of multi-trust that expresses the multiple dimensions of trust according to the SIoT application specifications. The numerous aspects of the trust accurately separate the features contributing to the successful execution of a service request under the service composition phase. Once the trust is estimated, it decides the best trust parameter yielding the best decision. In the service binding phase, the overall trust formation constituent discusses the process to determine the overall trust from the direct and indirect assessment of the trust metrics. It presents the means of distributing and consolidating trust information to converge the trust assessment and accuracy for maximizing the application performance. The trust update constituent updates the trust score after completion of each time slot δ_t, the period over which the trust scores are combined to a single value. Once the overall trust is assessed, the SR chooses the SP satisfying all the trust requirements and its criterion.

3.3.1 Trust Metrics. While there is several social trust metrics available the honesty, cooperativeness, community of interest, competence and integrity are examined. Trust metrics honesty, cooperativeness and community of interest are concerned with the trust evaluation of objects communicating in a service-oriented SIoT. Whereas, competence and integrity are the measures of service composition, *i.e.* competence measures the capability for delivery of service, and the integrity measures the compliance of the service protocol. The trust metrics are estimated as follows:

1. *Honesty (H)*: It denotes the authenticity of an object in service-oriented SIoT. An object may be dishonest when offering trust recommendations or while providing services. The reason for choosing honesty as a trust metric is that an

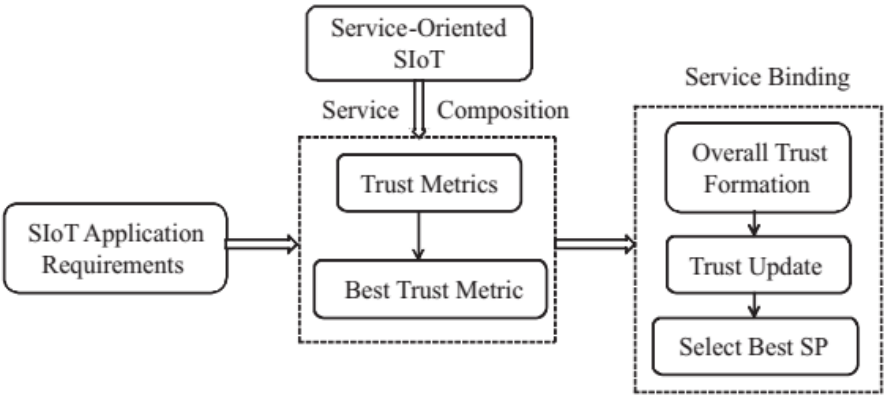

Figure 1: Components of a Service-Oriented SIoT System

object exhibiting dishonest behaviour may severely disturb the trust management and service stability of IoT applications. The honesty property of another object is evaluated based on direct evidence i.e. through interaction, and via indirect evidence, that is based on recommendation.

2. *Cooperativeness (CO):* It represents the social ties between the objects in SIoT applications. It assesses the social cooperativeness of the trustee object with the trustor object. An object may be cooperative only with few objects while interacting with strong social relations and may behave uncooperative with other objects.
3. *Community of Interest (CoI):* The community of interest property represents the co-location or co-work relationships, i.e. whether or not objects are in the same social communities. The object with a higher community of interest has more chances of interacting with other objects and thus results in a more incredible performance.
4. *Competence (C):* Competence refers to the ability of the SP to serve the requested service so that SR is satisfied.

3.3.2 Overall Trust Formation. The trust assessment information about object p towards object q is denoted as $T_{p,q}$ for direct and indirect observations is computed as a weighted average of trust metrics such as honesty, cooperativeness, the community of interest and competence:

$$T_{p,q} = w_1 H_{p,q} + w_2 CO_{p,q} + w_3 CoI_{p,q} + w_4 C_{p,q} \quad (1)$$

Where w_1, w_2, w_3, and w_4 are the weights to adjust the trust value in the range of 0 to 1. $H_{p,q}$ is referred as the belief of object p on object q based on p's direct interaction experiences or through a recommendation from the other objects, $CO_{p,q}$ represents the degree of cooperativeness of objects which is calculated as the ratio of common friends between object p and object q. $CoI_{p,q}$ is the similar interests of objects or of a community which is calculated as the ratio of common interests between object p and object q. $C_{p,q}$ is about object p's mean direct trust toward object q is computed as the ratio of the number of positive observations to the number of negative observations [16.].

The computed trust of an object need not be the same as the intended trust in the near future, *i.e.* a non-malicious object in the exhibition may shift to malicious and vice-versa. Hence to overwhelm this, the intended trust is presented. The intended trust of an object q with respect to object p denoted as $IT_{p,q}$ is computed to discriminate between legitimate and malicious objects according to the correlation coefficient [17.].

$$T_{p,q} = \frac{cov(p,q)}{\delta_p . \delta_p} \quad (2)$$

$$IT_{p,q} = \frac{\sum_{i=1}^{N} (x_i - M_p)(y_i - M_q)}{\sum_{i=1}^{N} (x_i - M_p)^2 (y_i - M_q)^2} \quad (3)$$

Where δ_p and δ_q are the standard deviation object p and q 's behaviour respectively. *cov(p,q)* is the covariance of p and q 's behaviour, and x_i and y_i, denotes p and q ' s values respectively. The mean value of object p and q are estimated as $M_p = \sum_{i}^{N} x_i / N$ and $M_q = \sum_{i}^{N} y_i / N$ respectively and N denotes the number of objects in the vicinity, striving to build relationships for rendering services. The intended trust is in the range of *[0, 1]*, we consider the absolute value of the correlation coefficient. Thus, the overall trust of object p on q is the product of estimated trust $T_{p,q}$ and the intended trust $IT_{p,q}$

$$OT_{p,q} = T_{p,q} * IT_{p,q} \quad (4)$$

Considering the estimated trust $T_{p,q}$ and the intended trust $IT_{p,q}$ is in the scope of *[0-1]*, the highest value of overall trust is 1.

3.3.3 Trust Update. Trust scores are updated periodically for every time interval δt considering the behaviour of the objects. The new trust score is $TU_{p,q}(t)$ is computed at time t based on the current, previous and intended trust score of the object.

$$TU_{p,q}(t) = (T_{p,q} * T_{p,q}(t - \delta t) * IT_{p,q}) * \alpha + 1 \quad (5)$$

Where $\alpha \in [0,1]$, $T_{p,q}$ is the computed current trust score, $T_{p,q}(t - \delta t)$ is the previous trust and $IT_{p,q}$ is the intended trust of an object q with respect to object p.

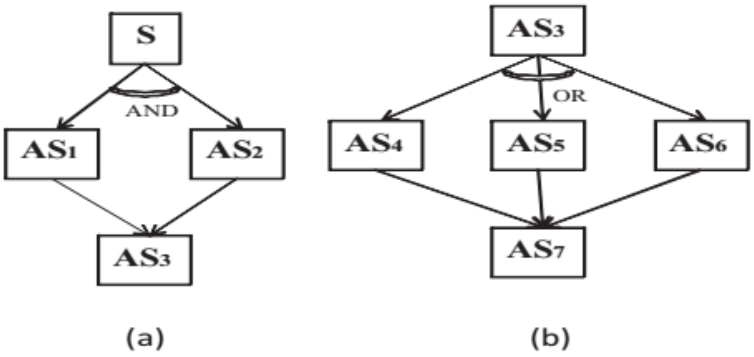

Figure 2: Service Flow Structure (a) Parallel Structure (b) Sequential Structure

3.4 Use Case Scenario

To effectively determine the proposed trust management for service-oriented SIoT systems, we examine an instance of a real-world scenario of a travel map assistance, which requires dynamic service composition as well as binding. Consider a travel map assistance SIoT application in which user John is new to the city and is concerned about the service quality he would receive during his visit to different places. He is in a smart city; hence he enrolls his smartphone in a SIoT based social network. He downloads an IoT map assistance application on his smartphone that would assist him in exploring the city, with the help of Near field communication (NFC). The map application automatically connects John's phone to IoT devices that it encounters during the travel. The objects discovered during the interaction provide information on maps, eateries, entertainments and transport services. John directs his phone to make decisions dynamically. John's phone makes the following actions: (i) Create a service composition plan based on the assembled events and (ii) Based on John's service request, invoke the required services. Suppose John makes a request, such as, *Serve me a best-grilled chicken under a budget of 250 rupees within 30 minutes.* There will be multiple service providers competing to offer the service, John's phone formulates the best service composition plan and selects the best among them.

The Figure. 2 illustrates the service flow structure for travel map assistance. Here the service requests are divided into chunks of multiple abstract services, each performing a dedicated task denoted as AS_i. The abstract services can be taxi provider or grilled chicken service. The execution of services takes place simultaneously or sequentially depending upon the service selected by John. Here AS_1 and AS_2 are the different service providers proposing information about which is the best restaurant that offers the grilled chicken within the budget and time constraints (250 rupees and 30 minutes). The abstract services are connected by a AND structure, indicating that they must be executed simultaneously as seen in Figure. 2. Once John selects the best service, the next step is to execute the sequential service choosing the service of the preferred choice, as shown in Figure. 2. The sequential services are performed once the services at the upper level are completed *i.e.* when the upper-level service binding is executed; sequential services are conducted one after the other. The purpose of the service composition and binding application based on trust is to choose the best honest IoT object that offers the specified services and qualifies to be a trustworthy provider identifying the presence of the CSA attack in the vicinity.

3.5 Performance Analysis

In this subsection, we discuss the comparative analysis of the proposed Trust Management for Service-Oriented SIoT scheme (TMSOS) with multi-trust based adaptive trust management for SIoT systems (ATMS) [11.] through simulations. The proposed service-oriented trust scheme is evaluated and validated for adversarial attacks using ns3 simulation tool. To conduct the simulation, we created the synthetic data using Small World In Motion (SWIM) mobility model [18.] on the location-based online social network Brightkite dataset [19.]. We chose to run the transactions for 100 objects, assuming that each user maintains a relationship with a maximum of 5 objects, where each object can request a service from its neighbouring objects and provide upto 3 services in the time slot of 0 and 60 seconds. Social relationships are built based on ownership relations. Two distinct behaviours of the objects are considered in the social network one is the cooperative, which offers good service, and the other is opportunistic, which provides bad service. The environment is modelled by changing the percentage of malicious nodes in the range of [10-60 %] with the default value set to 20% and executes the attacks outlined in the adversarial model. In the implementation, the initial threshold value of trust is set to 0.4 for all the objects.

The performance of the endeavoured service-oriented trust scheme that attack and defend against Co-relative Service Attacks is as shown in Figure. 3 and 3 3 respectively. The trust scores (without defending against attack) of ATMS and the proposed TMSOS trust management schemes are displayed in Figure. 3. The proposed method gave a small drift during a prior time interval due to the estimation of intended trust value; next during the other time slots, the trust scores remained similar. The trust scores of ATMS and the proposed TMSOS schemes that demonstrate the effectiveness of the proposed scheme against attacks is depicted in Figure. 3. At

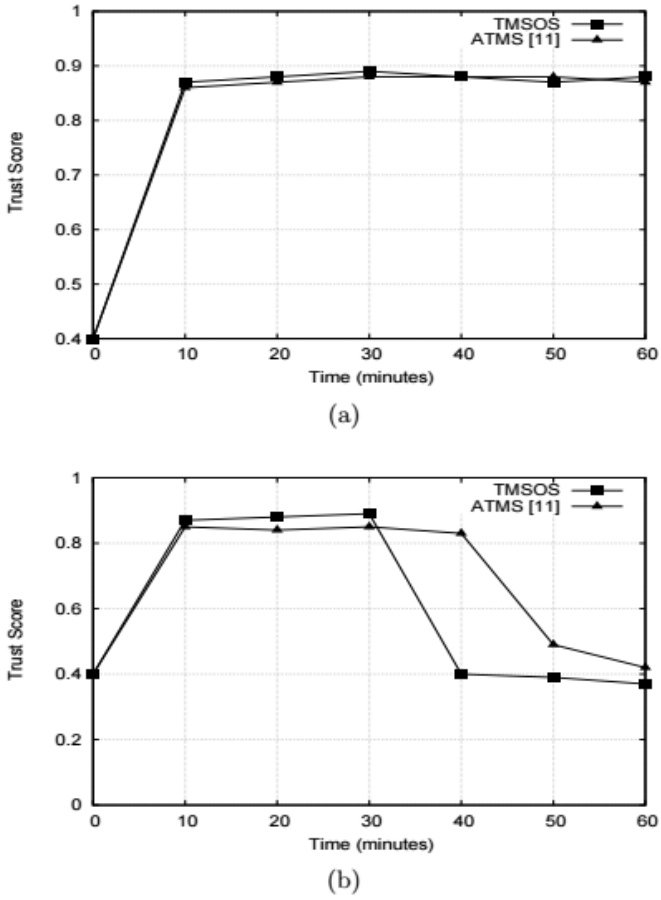

Figure 3: Performance Comparison of Trust Management Schemes that (a) Attack Co-relative Service Attack (b) Defend Co-relative Service Attack

each time slot, the adversary built a good reputation by offering a good service and then it stops providing a service. Experimental outcomes show that when the malicious object stops providing the service; the trust score is dropped from 0.89 to 0.4 in 10 minutes in the proposed scheme. Whereas, the trust score did not get the original state even if the malicious object continued providing service. The proposed scheme took lesser time to recognize co-relative service attack compared to ATMS scheme since it estimates the intended trust according to the correlation coefficient for differentiating the malicious and non-malicious objects.

3.6 Conclusions

In this paper, we examined the trust management in service-oriented SIoT systems. Discovering the trustworthy service provider among the available services is a critical issue in a service-oriented SIoT network. The proposed trust management scheme is based on the behaviour of objects that help to aid the services in a trustworthy process by regulating multiple aspects of trust and iteratively, combining the objects present and the past information. The simulation results have emphasized that the proposed trust scheme TMSOS outperforms as compared with the ATMS scheme following the study in isolating the co-relative attackers. In the future, we intend to address the more trust-related attacks in the SIoT systems by using machine learning based techniques. In this paper, a service provider was considered to be participating in one service request at a given point of time to reduce the load on a SP, since the heavy load can degrade service quality of a SP. The concurrent requests may give rise to schedule conflicts among multiple service requests. We further aim to propose a scheme, where a SP can handle service requests simultaneously at any given point of time.

REFERENCES

[1.] Marques, G. Ambient assisted living and internet of things. In Harnessing the Internet of Everything (IoE) for Accelerated Innovation Opportunities, IGI Global, pp. 100-115 (2019)
[2.] Natchetoi, Y., Kaufman, V. and Shapiro, A. Service-oriented architecture for mobile applications. In Proceedings of the 1st international workshop on Software architec- tures and mobility pp. 27-32 (2008)
[3.] Roopa, M. S., Pattar, S., Buyya, R., Venugopal, K. R., Iyengar, S. S., & Patnaik, L.M. Social Internet of Things (SIoT): Foundations, thrust areas, systematic review and future directions. Computer Communications 139, pp. 32-57 (2019)
[4.] Roopa, M.S., Siddiq, A., Buyya, R., Venugopal, K.R., Iyengar, S.S. and Patnaik, L.M., Dynamic Management of Traffic Signals through Social IoT. Procedia Com-

puter Science 171, pp. 1908-1916 (2020)
[5.] Chen, Z., Ling, R., Huang, C.M. and Zhu, X. A scheme of access service recommendation for the Social Internet of Things. International Journal of Communication Systems, 29(4), pp.694-706 (2016)
[6.] Abderrahim, O.B., Elhdhili, M.H. and Saidane, L.T.S. A trust management system based on communities of interest for the social internet of things. In Proceedings of the 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), Valencia, Spain, pp. 26-30 (2017)
[7.] Rafey, S.E.A., Abdel-Hamid, A. and Abou El-Nasr, M. CBSTM-IoT: Context-based social trust model for the Internet of Things. In Proceedings of the 2016 Interna- tional Conference on Selected Topics in Mobile & Wireless Networking (MoWNeT) pp. 1-8 (2016)
[8.] Truong, N.B., Um, T.W. and Lee, G.M. A reputation and knowledge based trust service platform for trustworthy social internet of things. Innovations in clouds, internet and networks (ICIN), (2016)
[9.] Kokoris-Kogias, E., Voutyras, O. and Varvarigou, T. TRM-SIoT: A scalable hybrid trust and reputation model for the social internet of things. In Proceedings of the 2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA) pp. 1-9 (2016)
[10.] Wang, K., Qi, X., Shu, L., Deng, D.J. and Rodrigues, J.J. Toward trustworthy crowdsourcing in the social internet of things. IEEE Wireless Communications, 23(5), pp.30-36 (2016)
[11.] Chen, R., Bao, F. and Guo, J. Trust-based service management for social internet of things systems. IEEE transactions on dependable and secure computing, 13(6), pp.684-696 (2015)
[12.] Truong, N.B., Lee, H., Askwith, B. and Lee, G.M. Toward a trust evaluation mechanism in the social internet of things. Sensors, 17(6), p.1346 (2017)
[13.] Kowshalya, A.M. and Valarmathi, M.L. Trust management for reliable decision making among social objects in the Social Internet of Things. IET Networks, 6(4), pp.75-80 (2017)
[14.] Roopa, M. S., Valla, D., Buyya, R., Venugopal, K. R., Iyengar, S. S., & Patnaik, L. M. SSSSS: Search for Social Similar Smart Objects in SIoT. In 2018 Fourteenth International Conference on Information Processing (ICINPRO) pp. 1-6 (2018)
[15.] Roopa, M. S., S. Ayesha Siddiq, Rajkumar Buyya, K. R. Venugopal, S. S. Iyengar, and L. M. Patnaik. "DTCMS: Dynamic traffic congestion management in Social Internet of Vehicles (SIoV)." Internet of Things, 100311 (2020).
[16.] Wang, Y., Chen, R., Cho, J.H., Swami, A. and Chan, K.S. Trust-based service composition and binding with multiple objective optimization in service-oriented mobile ad hoc networks. IEEE Transactions on Services Computing, 10(4), pp.660-672 (2015)
[17.] Moustafa, N., Turnbull, B. and Choo, K.K.R. An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of internet of things. IEEE Internet of Things Journal, 6(3), pp.4815-4830 (2018)
[18.] Mei, A. and Stefa, J. SWIM: A simple model to generate small mobile worlds. In Proceedings of the IEEE INFOCOM pp. 2106-2113 (2009)
[19.] Leskovec, J., 2012. Brightkite dataset. URL http://snap. stanford. edu/data (accessed September 12, 2016), Stanford University.