Asian Journal of Information Technology 15 (20): 3957-3964, 2016
ISSN: 1682-3915

Towards Trustworthy and Secure Communications in Social Internet of Things (SIoT)

A. Meena Kowshalya and M.L. Valarmathi
Department of Computer Science and Engineering, Government College of Technology, Coimbatore, Tamil Nadu, India

Abstract: The world has faced three ICT (Information and Communication Technology) revolutions and the third ICT wave led to Internet of Things, the notion of anything, everything, anytime and everywhere. Out of the many visions of IoT, one revolutionary concept is to make IoT sociable i.e., incorporating social networking within internet of things. This revolution has led to the notion of Social Internet of Things (SIoT). Establishing a SIoT network or community is not so simple and requires integration of heterogeneous technology and communication solutions. This study focuses on establishing a secure and reliable communication over nodes in SIoT by computing trust dynamically among neighboring nodes. Trust management is an important area that has attracted numerous researches over the past few years. The proposed DTrustInfer computes trust based on first hand observation, second hand observation, centrality and dependability factor of a node. Properties of trust such as honesty, cooperativeness, community interest and energy of a node are considered for computing trust. Also, this study ensures secure communication among SIoT nodes through simple Secret Codes. Experimental results show that the proposed DTrustInfer out performs the existing trust models significantly.

Key words: Internet of Things (IoT), Social Networks (SN), Social Internet of Things (SIoT), trust, secret codes

INTRODUCTION

Social Internet of Things (SIoT) is a new paradigm that integrates two technologies namely Internet of Things (IoT) and Social Networks (SN). Internet of things has enabled integration of various heterogeneous technologies and communications together; social networks are evolutions beyond internet of things. A different perspective and visualization of internet of things is to make it social by giving IoT a social structure and adding social responsibilities to the Things. This concept has led to what is called Social Internet of Things (SIoT). Social internet of things enable collaboration among objects via owners, the objects are not only smarter but also socially responsible. Bao and Chen (2012) defines social internet of things as a social network of intelligent objects. The SIoT concept was introduced very recently and little research has been carried out in this field. Various frameworks and solutions exist for IoT, not all suits for SIoT. Chen *et al*. (2011) has reported evolutions, applications, architecture, challenges and solutions for internet of things. Establishing a successful social internet of things community is a complex task. Challenges like data management, data discovery, interoperability, trust management, security, privacy, heterogeneit and fault tolerance has to be handled. Social internet of things attracts enormous research work in these areas. Valarmathi has surveyed research challenges, architectures, design issues and platforms available for social internet of things. Sherchan *et al*. (2013) has surveyed trust and its properties for social networks. The proposed research focuses on establishing reliable communication with peer members of the SIoT community. Trust management is considered crucial for SIoT. A node has to compute trust among its neighbors in order to enable trustworthy communications. A SIoT network is subject to sybil attacks very commonly. Social networks grow enormously every year and thus malicious users also grow. A secure way of communication between nodes in a SIoT can be achieved by managing trust among nodes. If a noe is trustworthy, it is assumed to be honest and give honest recommendations. The real challenge is to determine honest nodes and dishonest nodes. This study exclusively presents DTrustInfer that computes trust of nodes dynamically and uses secrete codes to provide secure and reliable communication between nodes. The major contributions of the study are as follows.

Corresponding Author: A. Meena Kowshalya, Department of Computer Science and Engineering, Government College of Technology, Coimbatore, Tamil Nadu, India

Establish trustworthy communications between nodes to ensure that the SioT network comprises of majority of honest nodes. Few malicious nodes may be present in the network, since the SIoT network needs to be robust and a check for robustness should be made periodically. Establish secure and reliable conversation between trustworthy nodes by using simple secrete codes.

Literature review

Trust management in P2P networks: The trust management solutions of P2P networks served as the foundations for trust management in SIoT. Numerous researches have been proposed for improving trust among peers. This study reveals very recent and successful algorithms for trust management in P2P systems. Xong and Liu (2004) proposed a reputation based Trust for peer to peer communities. It includes a coherent and adaptive trust model for comparing trust based on feedback. The algorithm uses feedback, total number of transaction, creditability of the feedback sources, transaction context factor and community context factor to compute trust. This algorithm is highly effective for a P2P environment and cannot be extended to IoT or SIoT where objects are dynamic. But these solutions can be modified to suit SIoT systems. Another interesting research proposed by Despotovic and Aberer improves and encourages trust among P2P communities by managing peers reputations. It uses maximum likelihood probabilistic technique that reduces implementation overhead and ambiguous trust related semantics. Though simple and efficient, this technique is not pretty well scalable. And, hence such a research cannot be extended for a SIoT system. Bao *et al.* (2012) proposed a highly scalable cluster based hierarchical trust management protocol for Wireless Sensor Networks (WSN) which detects malicious and selfish nodes. This protocol uses multi dimensional trust attributes derived from social networks. This research served as a basic protocol for (Nitti *et al.*, 2014) classifying trust as objective and subjective trust. This research was the first technique to derive social trust from social networks in addition to Quality of Service (QoS) trust derived from communication networks. This study considers (Bao *et al.*, 2012) as the source in computing trustworthiness of nodes. The researchers Zhou and Hwang (2007) present gossip trust which is a reputation aggregation scheme for unstructured P2P networks. By aggregating local trust this protocol computes global trust concurrently. With minor modification this protocol can be extended to structured P2P networks also. In a P2P system each peer shold have the knowledge of other peers in order to decide whether or not to trust them. The researchers Yu *et al.* (2004, 2008) and Yu (2011) proposed a robust reputation mechanism for large scale P2P system where a peer combines several testimonials of other peers to determine trustworthiness. Without third party involvements this mechanism improves trust levels, identify malicious nodes and unreliable peers in a P2P system. For P2P networks a distributed scheme for inference of trust was proposed by Sherwood *et al.* (2006). The technique stores reputation information's about users in a decentralized manner and uses this information to identify non cooperative users in a NICE system. Using this scheme, individual users can infer trust of other users thus leading to network reliability and trustworthiness. Trust and reputation may seem the same but the researchers by Wang and Vassileva (2003) differentiate these two and propose a Bayesian network based trust model for P2P systems. Since the requirement of peers is different at various circumstances this approach uses Bayesian networks to identify differentiated trust and combine different aspects of trust. The researchers have tested the model for a file sharing scenario and it is the successful approach that used multiple facets of trust.

MATERIALS AND METHODS

Trust management in SioT: This section summarizes recent trust management solutions and strategies adopted for SIoT network. Nitti *et al.* (2014) presents an algorithmic approach of computing trust from behaviors of online social network. This study also lists measurable trust metrics. The researchers Saied *et al.* (2013) combine inferences to arrive at trust and distrust among nodes even if the nodes do not know each other. Mahalle *et al.* (2013) presents a distributed trust management system for internet of things according to the three layering architecture method. DuBois *et al.* (2011) proposed a dynamic trust management scheme for communication based SIoT environment. Multiple complex social relationships and basic properties of trust were used for dynamic trust management. As an extension of the previous study, the researchers Mahaue *et al.* (2013) consider two types of community of interest namely inter community of interest and intra community of interest. Given these two as inputs the approach achieves best trust protocol settings. This protocol is scalable when compared to the researcher's previous work (Wang *et al.*, 2013). Bao *et al.* (2013) proposed a trust and a reputation model that improves collaboration among nodes. Fuzzy sets were used to analyze the trust

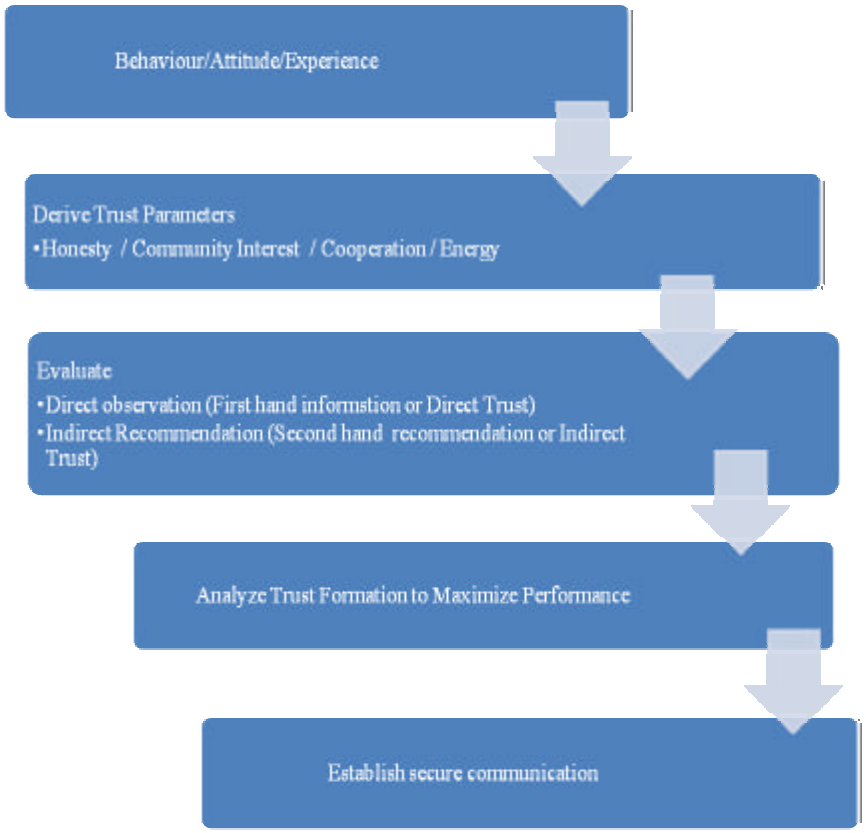

Fig. 1: Process of deriving trust

and reputation models. Bachi *et al.* (2012) proposed a fuzzy based approach to evaluate trust level across nodes in IoT. The same can be extended for SIoT. This fuzzy based approach is scalable and energy efficient. The researchers Atzori *et al.* (2010, 2012) have created a framework for inferring trust and distrust relationships in online social networks. The network is decomposed into ego trust sub network and mined for trust and distrust relationship. Graph data mining algorithms are employed for this purpose. Its possible to derive various trust metrics from behavior of objects/nodes/things. The proposed research takes into account honesty, cooperativeness, community interest and energy as primitive trust properties. According to these trust parameters, trust is calculated based on first hand information and second hand recommendation. Unlike Bao and Chen (2012) this study doesn't derive trust from a subjective model and an objective model. A dependability factor is introduced along with direct trust, recommendation and centrality for trust calculation which helps in improving the application performance. The main difference between this study and (Bao *et al.*, 2012) is that the use of the dependability factor which is the history of nodes behavior from other similar application environment.

Deriving trust: This study proposes a novel secure framework for deriving trustworthiness among nodes in SIoT. The framework is shown in Fig. 1. From the experience of the user, we derive four properties of trust namely honesty, cooperativeness, community interest and energy. Using these properties direct trust and indirect trust are computed. The computed trust is analyzed based on varying weighing factors to maximize the application performance and establish a secure communication.

Deriving trust parameters: The trust parameters are helpful to characterize a node according to its behavior, attitude and experience. Each trust property (honesty, cooperativeness, community interest and energy) is complimentary to each other and hence needs to be evaluated separately.

Table 1: List of parameters used

Parameter	Description
D_{ij}^{X} (t)	Direct trust of i towards j at time t in X
R_{kj}^{X} (t)	Recommendation of k from j time t in X
T_{ij}^{X} (t)	Trust between i and j at time t in X
G_{ij}^{X}	Centrality of a node
D_{ik}^{X} (t)	Direct trust of i towards k at time t in X
DP_{ij}^{X}	Dependability factor
α, β, λ	Weighing factors

Honesty: Honesty of a node in the range (0,1) is considered as a prime factor since an honest node is assumed to always give proper and correct recommendation about its neighbors. This assures that the node is not malicious and helps improve the trustworthiness of the network. To evaluate honesty, a node relies on firsthand information i.e., direct trust. Direct trust is obtained by a nodes interacting with other node directly.

- $D_{ij}^{honesty}$ (t) is the direct trust calculated between node i and j. Here i is the trustor and j is the trustee at time t. Node i computes $D_{ij}^{honesty}$ (t) between itself and node j.

Cooperativeness: Cooperative trust represents whether or not the trustee node is socially cooperative with the trustor. It's assumed that nodes with common friends are cooperative and behaves differently with others. In a SIoT environment, nodes cooperativeness can be predicted by its social ties. Socially cooperative nodes improves the application performance. Each device/object possesses a list of friends likely to be cooperative. This list will be updated by owners periodically. According to Bao and Chen (2012) the $D_{ij}^{cooperativeness}$ (t) is calculated as follows:

$$\frac{\text{Friends(i)} \cap \text{Friends(j)}}{\text{Friends(i)} \cup \text{Friends(j)}}$$

Community interest: Community interest as proposed by (Atzori *et al*., 2012) is another factor that enables communication between objects of communal interest. The objects are classified according to their parental relationships, Co-work or Co-location relationships. Objects with the same community interest are supposed to interact with each other very often leading to increased application performance. According to Bao and Chen (2012) the $D_{ij}^{cooperativeness}$ (t) is calculated as follows:

$$\frac{\text{Community(i)} \cap \text{Community(j)}}{\text{Community(i)} \cup \text{Community(j)}}$$

Energy: Energy of a node also plays an important role in communication and sharing of information. Almost all devices in SIoT are low power devices and less energy efficient devices. Thus energy of a node is to be given prime importance for collaboration purpose. Energy of a node is calculated as the product of power and time.

Evaluate direct observations and indirect recommendations: To improve trustworthiness among SIoT nodes two types of trust are evaluated namely First hand observation or direct trust and second hand recommendation or indirect trust. Table 1 illustrates the parameters used for calculating trust. When nodes i and j interact directly with each other the trust is calculated as follows:

$$T_{ij}^{X}(t) = \alpha T_{ij}^{X}(t)(t-\Delta t) + \alpha D_{ij(t)}^{x} + \beta G_{ij}^{x} + \alpha\beta DP_{ij}^{x} \quad (1)$$

Where:

X = Honesty, cooperativeness, community interest and energy

T_{ij}^{x} (t) = The past trust between i and j with respect to X

Δt = The time elapsed since the last trust update

Node i will use direct observation T_{ij}^{x} (t) and its past trust) $T_iIJ'X(t)$ (t-Δt) towards node j. Along with these two parameters node i also uses the centrality and dependability factor to compute trust. The centrality of a node is computed according to Eq. 2:

$$\text{Centrality } G_{ij}^{X} = \frac{\text{Set of common friends between i and j}}{\text{Neighbors between i, j}} \quad (2)$$

Dependability factor is in the range (0, 1) which is obtained by the service provider of another similar SIoT environment. The behavior of the same node (past history) in a different environment is used to evaluate the trustworthiness. Nodes are identified by their semantics. The cost associated with retrieving the dependability factor is negligible and in few cases dependability factor will be 0 if the same objects do not participate anywhere in the outside world. When node i witnesses node k which has already experienced transaction with node j, then trust is computed according to Eq. 3. Node i uses k's recommendation to judge node j. Node i will not have any direct interaction with node j instead use recommendation of k towards j R_{kj}^{X} (t) and the past trust value $T_iIJ'X(t)$ (t-Δt) to access j:

$$T_{ij}^{X}(t) = \gamma T_{ij}^{X}(t)(t-\Delta t) + \gamma D_{ik}^{X}(t) + \gamma R_{kj}^{X}(t) + \beta G_{ij}^{X} \quad (3)$$

Where:

T_{ij}^{X} (t)(t-Δt) = The past trust value

R_{kj}^{X}(t) = The recommendation that node k provides to node i about node j

There are possible chances of node k being malicious. If node k is not malicious R_{ij}^{X} (t) equals D_{ik}^{X}. If node k is malicious it can perform bad mouthing attacks and propagate the same to node i. To prevent this happening, node i uses direct trust to access node k D_{ik}^{X} (t) (Bao and Chen, 2012). Together with these parameters, the trust is computed using centrality and dependability factor discussed in Eq. 2 and 3.

Dtrustinfer algorithm: A SIoT network is a graph G (V,E) where V represents the number of vertices (objects/things/humans) and E represents the edges between them. The DTrustInfer algorithm takes input a sub graph G (V,E). When a node wants to establish communication with another node, it computes and estimates the trustworthiness of the neighboring node. The node with the highest centrality is chosen as the authenticator A_i. The authenticator node A_i manages generation and distribution of Secret codes that are to be padded with the messages. It also verifies user credentials during user churn. The algorithm begins by computing trust between nodes that need to communicate. When found to be trustworthy, the sender node pads the secret key along with the message. At the destination, the destined node separates message and secret key compares the secret key with the one that was distributed by the Authenticator A_i. Thus a check is made to ensure authentication of messages. Both trust and authentication make the SIoT network more robust. A SIoT network need not always possess honest nodes; malicious nodes may also be present within the network.

Few false positives (labeling honest nodes as "Sybil's") and false negatives (labeling sybil's as "honest") do exist in the network (Yu *et al*., 2008) but considered less harmful. This is needed for the system to tolerate some amount of malicious node behavior. It is proved that honest nodes are fast mixing (Yu *et al*., 2004) and sybil's are not fast mixing enough like honest ones. Due to this nature, there exists a small cut in the graph between the honest region and Sybil region. This helps us easily identify the sybil region.

Algorithm: DTrustInfer
Input: Subgraph G(V,E)
Output: Trust scores between nodes and Sybil Region
When node i wants to communicate with node j directly,
Compute trust using equation (1).
Else,
Compute trust using equation (3).
Choose the node with the highest centrality to be the Authenticator node A_i, use equation (2)
For all neighboring nodes of A_i,
    Allocate secret codes to each,
For i to establish communication between j,
    Check trustworthiness between i and j,
    Perform walks on the sub graph to identify small cuts
    if cut present
        The region is Sybil Region and contains attack edges
    Else
        Start communication by padding the secret code along the message
Repeat until done

RESULTS AND DISCUSSION

To conduct our experiments large number of traces of objects were required. SWIM (Small World In Motion) simulator is used to generate traces of mobility of objects. The Brigtkite dataset and the Epinions dataset which are location based online social networks comprising of 1023 and 1088 nodes each were used. These traces where modified for the purpose of modeling objects that mimic human behavior. The Table 1 shows trust values for the subjective model, objective model of (Bao and Chen, 2012), the adaptive trust model of (DuBois *et al*., 2011) and the proposed DTrustInfer. The configuration parameters used for the simulation environment is listed in Table 2. A detailed comparative study between (Nitti *et al*., 2014; Bao *et al*., 2013) and the proposed research was done. The results are tabulated in Table 3. Experimental results show that the proposed method outperforms the other two methods and leads to increased application performance.

The subjective model uses direct trust to compute trustworthiness of nodes. The trust of the nodes was found to be 91% since only direct interactions were involved to compute trust. This approach is the simplest and efficient method to derive trustworthiness between nodes. Since SIoT is composed of heterogeneous devices trust has to be derived even if nodes are far apart i.e., with no direct communication. The objective model uses direct trust and indirect trust. The trust worthiness of nodes was

Table 2: Configuration parameters for brightkite dataset

Variables	Values
Nodes	1023
Node radius	0.00948
Knowing time	1728000
Simulation seconds	950400
Cell distance weight	0.8
Node speed multiplier	1
Waiting time exponent	1.35
Waiting time upper bound	216000
Buckets per side	14

Table 3: Configuration parameters for epinions dataset

Variables	Values
Nodes	1088
Node radius	0.009348
Knowing time	1327030
Simulation seconds	955460
Cell distance weight	0.8
Node speed multiplier	1
Waiting time exponent	1.35
Waiting time upper bound	216000
Buckets per side	14

Table 4: Comparison of trust between subjective, objective, adaptive trust and dtrust infer

Model	Technique used	Final trust value (%)	
		Brigtkite dataset	Epinions dataset
Subjective model	Direct trust	91.04	92.56
Objective model	Direct trust and recommendation	85.87	88
Adaptive trust model	Direct trust and recommendation	92.56	93.23
	Direct trust , recommendation and depend ability factor		
Dtrustinfer	Trust between i and j-direct interaction	97.45	97.56
	Trust between i and j-indirectly using k	97.12	98.21

Table 5: Range of sybil and honest nodes

Degree of nodes	Brightkite	Epinions
Minimum degree	1	1
Maximum degree	289	267
Average value	16.32	16.23
Range of degree of sybil nodes	1-5	1-4
Range of degree of honest nodes	1-289	1-267

Node XL Version 1.0.1.229

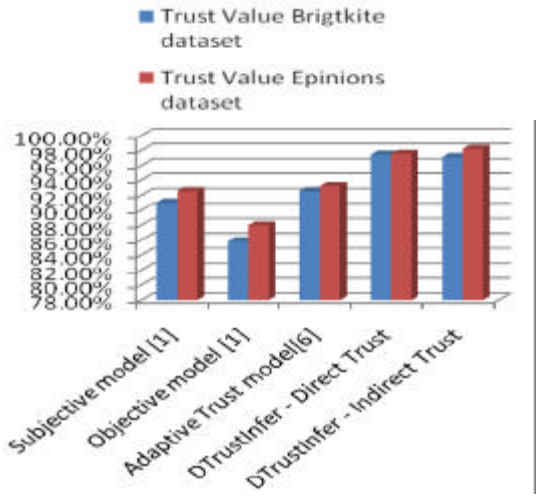

Fig. 2: Comparison of trust values

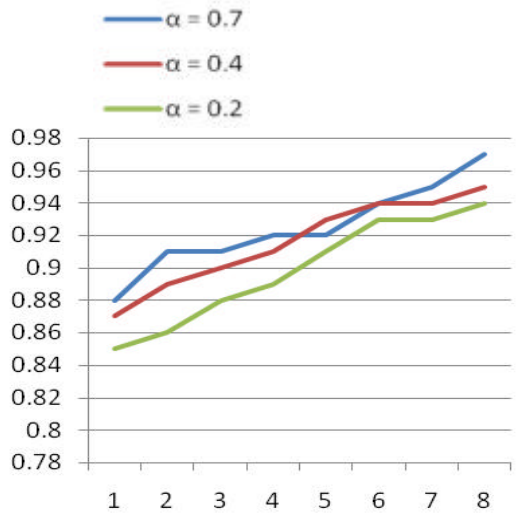

Fig. 3: Non malicious nodes with varying a values 0.2, 0.4 and 0.7. Larger the a, better the performance

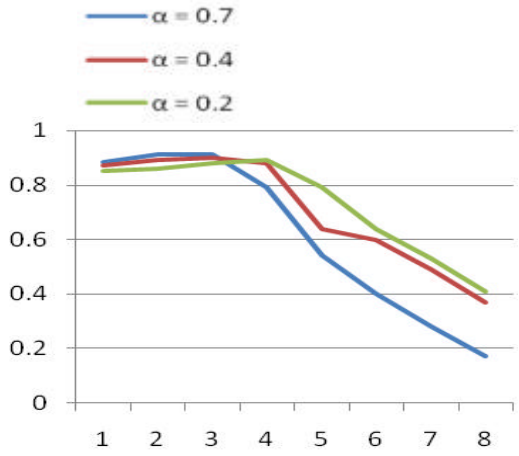

Fig. 4: Malicious nodes with varying a values 0.2, 0.4 and 0.7

found to be 85%. The recommendations of nodes may differ from one node to other i.e., opinions differ. This model requires trust to be globally stored by pre trusted objects and fetched from a dynamic hash Table 4 that is practically not feasible in a SIoT environment. The adaptive trust model (Bao *et al*., 2013) achieves 92% trust worthiness of nodes by combining direct observation and indirect recommendations. The proposed model achieves 97% of trustworthiness between nodes. This outperforms the subjective, objective and the adaptive trust model. Figure 2 compares the subjective model, the objective model, the adaptive trust model and the proposed model. A subset of 100 nodes was chosen randomly from the generated traces of 1000 nodes and the weights were varied to analyze the performance (Table 5). For nodes i and j interacting with each other directly according to equation 1, α values were chosen to be 0.2, 0.4 and 0.7 and the β value was kept to be 0 to isolate its effect. The performance was compared between a non malicious node and a malicious node. The larger the α value, application performance increases. The reason of larger α is that it has greater impact on the direct trust according to Eq. 1. Figure 3 and 4 shows the behavior of non malicious and malicious node, respectively. It can be noted that the fluctuations are very high in Fig. 5 and 6. Similarly when nodes i interact with k for evaluating node j as in Eq. 4, λ values chosen to be 0.2, 0.4 and 0.7 and β

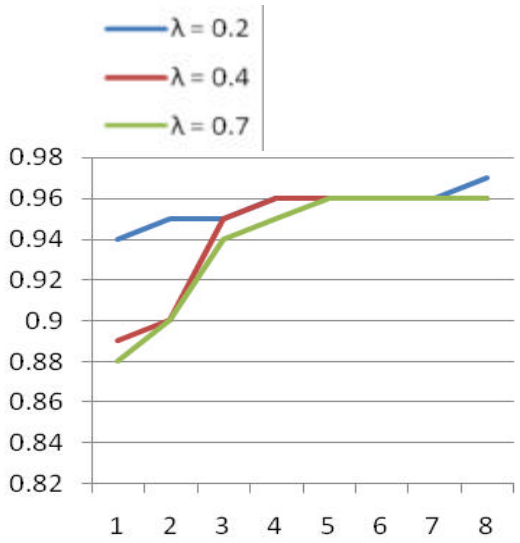

Fig. 5: Non malicious nodes with varying λ values 0.2, 0.4 and 0.7

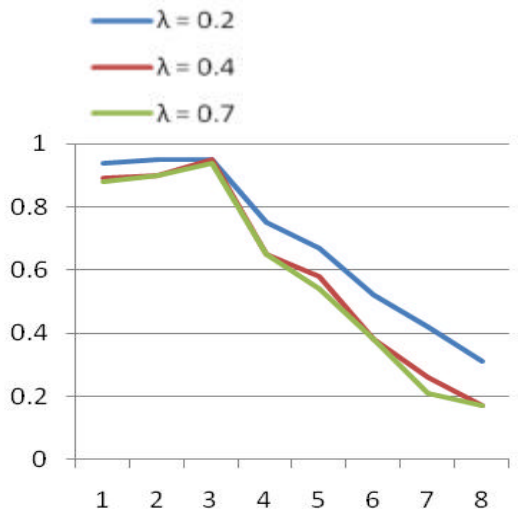

Fig. 6: Malicious nodes with varying λ values 0.2, 0.4 and 0.7

value was kept to be 0. β, does not show any significant impact on the performance. This experiment was carried only for the Brightkite dataset.

Table 5 shows the minimum and maximum degree of nodes in the topology, the average value and the range of degree of honest nodes and sybil nodes. NodeXL an open source social network analysis tool was used to explore the network graph. The version of NodeXL usd was 10.0.1.229.

CONCLUSION

This study proposes a novel framework for improving trustworthiness among nodes in a SIoT environment. Since the SIoT systems are dynamically changing, computing trust is not a simple task. The study has proposed a new model to compute trust among nodes in SIoT that uses firsthand observation (direct trust), second hand recommendation (indirect trust) Centrality and dependability of a node. The proposed model achieves 97% of trust when tested with the bright kite and Epnions dataset. This is 6, 12 and 5 times (for the Brightkite dataset) and 5, 9 and 5 times better (for Epinions dataset) when compared to the subjective, objective and the adaptive trust model which were the very recent trust models for SIoT. As an extension to this, the weighing factors were adjusted to analyze the best application performance. The weighing factors á affects directly the first hand observations and hence was chosen to analyze application performance. Also, messages between nodes were strictly authenticated by secret codes. The proposed method could also efficiently find sybil regions in the SIoT environment. As a future work, the same can be extended in a real time application.

REFERENCES

Atzori, L., A. Iera and G. Morabito, 2010. The internet of things: A survey. Comput. Networks, 54: 2787-2805.

Atzori, L., A. Iera and G. Morabito, 2011. Siot: Giving a social structure to the internet of things. IEEE. Commun. Lett., 15: 1193-1195.

Atzori, L., A. Iera, G. Morabito and M. Nitti, 2012. The social internet of things (siot)-when social networks meet the internet of things: Concept, architecture and network characterization. Comput. Netw., 56: 3594-3608.

Bachi, G., M. Coscia, A. Monreale and F. Giannotti, 2012. Classifying trust/distrust relationships in online social networks. Proceedings of the 2012 International Conference on Privacy, Security, Risk and Trust (PASSAT) and 2012 International Confernece on Social Computing (SocialCom), September 3-5, 2012, IEEE, Amsterdam, Netherlands, ISBN: 978-1-4673-5638-1, pp: 552-557.

Bao, F. and I.R. Chen, 2012. Dynamic trust management for internet of things applications. Proceedings of the 2012 International Workshop On Self-Aware Internet of Things, September 16-20, 2012, ACM, San Jose, California, ISBN: 978-1-4503-1753-5, pp: 1-6.

Bao, F., I.R. Chen, M.J. Chang and J.H. Cho, 2012. Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection. IEEE Trans. Network Service Manage., 9: 169-183.

Bao, F., R. Chen and J. Guo, 2013. Scalable, adaptive and survivable trust management for community of interest based internet of things systems. Proceedings of the 2013 IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS), March 6-8, 2013, IEEE, Mexico City, Mexico, ISBN: 978-1-4673-5069-3, pp: 1-7.

Chen, D., G. Chang, D. Sun, J. Li, J. Jia and X. Wang, 2011. TRM-IoT: A trust management model based on fuzzy reputation for internet of things. Comput. Sci. Inform. Syst., 8: 1207-1228.

DuBois, T., J. Golbeck and A. Srinivasan, 2011. Predicting trust and distrust in social networks. Proceedings of the 2011 IEEE Third International Conference on Privacy, Security, Risk and Trust (PASSAT) and 2011 IEEE Third Inernational Conference on Social Computing (SocialCom), October 9-11, 2011, IEEE, Boston, Massachusetts, ISBN: 978-1-4577-1931-8, pp: 418-424.

Mahalle, P.N., P.A. Thakre, N.R. Prasad and R. Prasad, 2013. A fuzzy approach to trust based access control in internet of things. Proceedings of the 2013 3rd International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace and Electronic Systems (VITAE), June 24-27, 2013, IEEE, Atlantic City, New Jersey, ISBN: 978-1-4799-0237-8, pp: 1-5.

Nitti, M., R. Girau and L. Atzori, 2014. Trustworthiness management in the social internet of things. IEEE. Trans. Knowl. Data Eng., 26: 1253-1266.

Saied, Y.B., A. Olivereau, D. Zeghlache and M. Laurent, 2013. Trust management system design for the internet of things: A context-aware and multi-service approach. Comput. Secur., 39: 351-365.

Sherchan, W., S. Nepal and C. Paris, 2013. A survey of trust in social networks. ACM. Comput. Surv. CSUR., 45: 1-33.

Sherwood, R., S. Lee and B. Bhattacharjee, 2006. Cooperative peer groups in NICE. Comput. Netw., 50: 523-544.

Wang, J.P., S. Bin, Y. Yu and X.X. Niu, 2013. Distributed trust management mechanism for the internet of things. Appl. Mech. Mater., 347: 2463-2467.

Wang, Y. and J. Vassileva, 2003. Bayesian Network Trust Model in Peer-to-Peer Networks. In: Agents and P2P Computing. Gianluca, M., C. Sartori and P.S. Munindar (Eds.). Springer Berlin Heidelberg, Berlin, Germany, ISBN: 978-3-540-24053-2, pp: 23-34.

Xiong, L. and L. Liu, 2004. PeerTrust: Supporting reputation-based trust for peer-to-peer electronic communities. IEEE Trans. Knowledge Data Eng., 16: 843-857.

Yu, B., M.P. Singh and K. Sycara, 2004. Developing trust in large-scale peer-to-peer systems. Proceedings of the IEEE 1st Symposium on Multi-Agent Security and Survivability, Aug. 30-31, IEEE Xplore Press, pp: 1-10.

Yu, H., 2011. Sybil defenses via social networks: A tutorial and survey. ACM. SIGACT. News, 42: 80-101.

Yu, H., M. Kaminsky, P. Gibbons and A. Flaxman, 2008. SybilGuard: Defending against sybil attack via social networks. IEEE. Trans. Netw., 16: 576-589.

Zhou, R. and K. Hwang, 2007. Gossip-based reputation aggregation for unstructured peer-to-peer networks. Proceedings of the IEEE. International Symposium Parallel and Distributed Processing, March 26-30, 2007, IEEE, Long Beach, California, ISBN: 1-4244-0909-8, pp: 1-10.