RraR: Robust Recommendation Aggregation using Retraining in Internet of Things

Avani Sharma, Emmanuel S. Pilli, Arka P. Mazumdar
Department of Computer Science and Engineering
Malaviya National Institute of Technology, Jaipur, India
Email: *avnisharma2010@gmail.com*, {*espilli.cse, apmazumdar.cse*}*@mnit.ac.in*

***Abstract*—Trust and Reputation Systems (TRS) have been witnessing the most promising solutions to ensure the security of a system in the presence of insider adversaries. The methodology behind TRS is to analyze the behavior of entities in the system to compute trustworthiness on them by the mean of direct (using own experience) and indirect (using recommendations from the others) trust computation. For the Internet of Things (IoT), where devices collaborate with each other to offer multiple services, TRS solve the issues of access control, decision making, reliable service delivery etc. The focus of this paper is towards robust indirect trust computation in a service-oriented, dynamic IoT environment. We propose a robust recommendation aggregation scheme which alleviates the effect of false or dishonest recommendations in indirect trust computation by performing the objective and subjective evaluation. In the objective evaluation, the value of a received recommendation is weighted by computing deviation from the average value of all the recommendation received. Subjective evaluation is performed to weight the recommender based on their age of interaction. The scheme deploys a retraining module which retrains the credibility of a recommender based on the dissimilarity experienced with the outcome of recommendation. The effectiveness of the proposed scheme has been demonstrated by the results of the simulation.**

***Index Terms*—Trust, Recommendations, Dishonest, Reliability, Freshness, Retraining**

I. Introduction

The growing era of ubiquitous and seamless connectivity giving rise to new technologies to accomplish user demands with satisfaction services. Internet of Things (IoT) is one of such emerging technologies which enables communication between heterogeneous physical objects (called IoT devices) by connecting them to the internet. The devices in the IoT system have embedded intelligence which makes them capable to offer multiple services. One important issue to be addressed in the deployment of IoT is to maintain security in the system for reliable service provisioning. Trust and Reputation Systems (TRS) provide the solution for such kind of problem by providing reasoning over the observed behavior of entities [1]. In the systems like IoT, the importance of TRS has been analyzed along multiple dimensions like facilitating access control, accelerating decision-making power of devices, ensuring reliability over the services etc. [2]. In TRS, the behavior of entities has been analyzed to compute trustworthiness on them directly by using self-observations and experience gained from the previous transaction instances, or indirectly by asking recommendations from the other entities in the system. Importance of indirect trust computation lies in the case where there is a lack of familiarity between the entities.

978-1-5386-4980-0/19/$31.00 ©2019 IEEE

This work focuses on indirect trust computation in IoT, in which trustworthiness of a device is computed by aggregating recommendations received from the other entities in the system. Reliance on the recommendations to derive trustworthiness about an unfamiliar device can lead to the spurious result in the presence of dishonest recommenders. A recommender can mislead the decision by reporting falsely about the trustworthiness of a device being evaluated. Such type of recommenders is called a traitor, which either increase the recommendation of a misbehaving device, called ballot stuffing attack or decrease the recommendation value of a well-behaving device, called bad mouthing attack. To deal with these type of attacks, we propose a robust recommendation aggregation scheme in which the evaluator device performs an objective and subjective evaluation to weight the received recommendation and recommender's credibility respectively. The objective evaluation is a deterministic way to compute weight on the received recommendation based on the deviation seen from the average value of recommendations, called *Reliability of Recommendation (RREL)* whereas, the subjective evaluation is a probabilistic approach to weight the recommender based on the age of its last interaction, called *Freshness of Recommender (RFRS)*. A retraining module works along the scheme which retrains the credibility (observed behavior of recommender by evaluator device) of recommenders, based on dissimilarity experienced with the response/outcome of recommendation. The remaining paper is organized as follow. The related work on the existing solutions has been given in Section II. Section III presents our proposed scheme along with the explanation of each computation phase. Results of simulation have been given in Section IV. Section V concludes the paper followed by the suggestions for future work.

II. Related Work

Trust and Reputation Systems (TRS) has been examined as an important aspect of security for various domains [3] [4]. By driving decision making over the observed behavior (directly or indirectly) of entities, these systems serve manifold purposes like access control, identity management, intrusion detection, reliability measurement etc. For IoT, an extensive survey on trust is presented by Yan et al. [2] explaining the

various objectives that can be achieved by trust management. Although these systems are intended to offer various advantages, vulnerability towards insider adversaries is still a challenging issue while designing such systems [5]. Lopez et al. [6] and Mousa et al. [7] gave an assessment of the vulnerability of TRS in the presence of false or dishonest recommendations. A dishonest recommender can perpetrate good recommendation value about a dishonest entity or it can decrease recommendation of a well-behaving entity to decrease its chances for being selected as trustworthy. The defense approaches for such type of attacks are broadly classified as detection-based, which apply filtering techniques or machine learning methods to detect the attacker from legitimated entities, and prevention-based, which aim to reduce the influence of attack by applying some weight to the computation [8].

Iltaf et al. [9] proposed a detection mechanism for dishonest recommendations in indirect trust computation. The mechanism first removes trust values with zero frequencies by constructing a histogram, passes the value of the histogram from a deviation function to find out dissimilarity factors and then classify recommended trust into two subsets. The subset with a higher value of dissimilarity is considered a malicious one. The authors assume that a dishonest recommendation has less probability to occur in the recommendation set. An advancement over the above mechanism is presented in [10] where authors use a trust value of recommenders in dissimilarity function. A smoothing function is then used to find a set of dishonest recommenders. Denko et al. [11] proposed a filtering method based on the deviation function for unfair recommendations. The method first computes an average of all recommendation received and then finds the absolute difference between the recommendation trust an average value. If the value of the difference is larger than the chosen threshold value, the recommendation is filtered out. The filtering based detection approaches are not well suitable for the dynamic environment like IoT in which the behavior of a device may not be the same for all type of services. A device performing well for a lightweight service may not serve the same for a service which requires more resources for computation.

The most common widely adapted approach to mitigate the influence of dishonest recommendations in indirect trust computation is to use the weighted aggregation of recommendation to derive a trust score. Chen et al. [12] used reputation computation of the recommender by considering quality and quantity of recommendation for weighting the recommendations. The authors in [13] used global reputation score to weight the local reputation assuming that the entity having high reputation will provide an honest recommendation as compared to the lower one. A recent work proposed by Qussai et al. [14] presents an approach for mitigation of collusion attacks caused by dissemination of false information in IoT using a fog computing layer. Their methodology for detecting false information, while performing aggregation, is to weight the each received reading with the deviation from the average value of all the reading. All these works compute weight deterministically on the received recommendation neglecting the probabilistic measures for a device being dishonest. Also, each new request of recommendation does not keep the influence of previously observed dissimilarity with the recommender. To overcome these limitations, we proposed a robust recommendation aggregation scheme based on both objective and subjective measures for IoT environment. Our scheme uses a subjective evaluation to assign weight to the recommender based on the age of last interaction. Also, the dissimilarity seen with each computation is used to retrain the credibility of recommender to ensure the reliability of future interactions.

III. Robust Recommendation Aggregation using Retraining

We propose a robust recommendation aggregation scheme with retraining, RraR, which performs an objective and subjective evaluation to alleviate the effect of dishonest recommendation in recommended trust score (indirect trust) of a device being evaluated. RraR deploys a retraining module which retrains the credibility of recommenders to propagate the effect of dissimilarity experienced in future recommendation request. Figure 1 depicts the overview of the proposed scheme along with each computation phase.

A. System Model

For a service-oriented IoT environment, the device can act as a service requester, service provider, or recommender. To perform the reliable collaborative task and to ensure the success of the future transaction, the service requestor (evaluator) computes trustworthiness of an unfamiliar service provider (device being evaluated) by relying on the recommendations received from the previously interacted devices. A trust computational model is assumed to exist on each device which computes the trust score, denoted as observed trust score (*OTS*), on each interacting device. We considered our proposed trust computation model [15] designed for IoT environment. The value of *OTS* with existing model ranges between 0 to 1, where the value towards 1 represents most trustworthiness. For each interacting device D_{id}, information about *OTS* along with the time of computation, t, and context (the type of service) of computation, S, stored in the local repository of the evaluator device.

To compute trustworthiness of an unfamiliar service provider j, evaluator device i initiates the recommendation request about j with the context of computation S^l to all the devices listed in its local repository. Upon receiving a recommendation request, a recommender device k searches its local repository to find OTS_{kj} which is the observed trust score on j by k for the service S^l and sends this value as recommendation R_{kj} to the device i. Let T is time at which recommendation request has been raised and the total number of recommenders is N for the device i.

B. Computation of Recommended Trust Score

The recommended trust score of j for i, i.e. RTS_{ij} is computed by performing weighted aggregation on the recom-

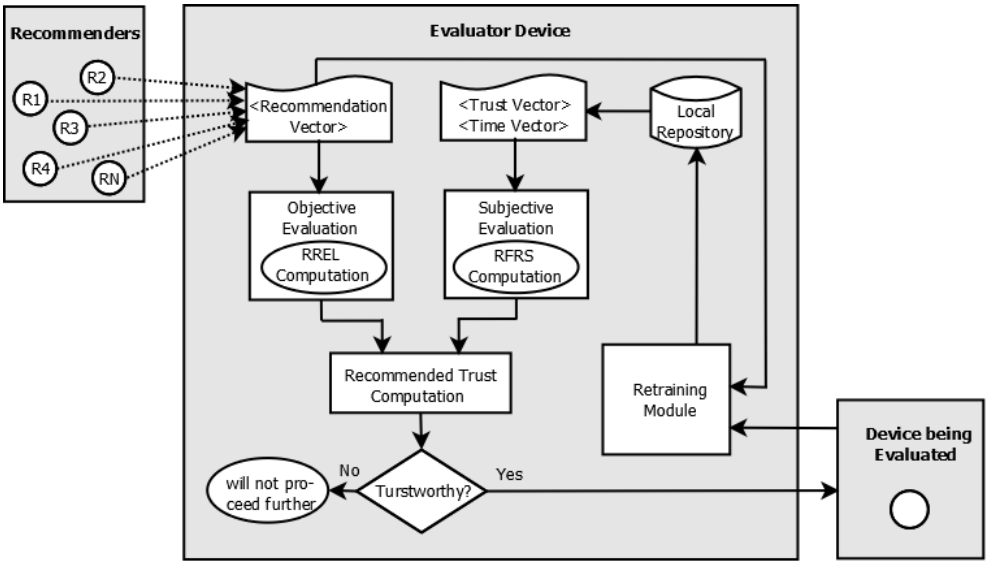

Figure 1: Overview of Proposed Scheme

mendations received by i from N number of recommenders. The evaluator i weight the recommendations and recommender by performing Objective and Subjective Evaluation, given in Algorithm 1 and 2 respectively.

Algorithm 1 Objective Evaluation

Input: $< R_{1j}, R_{2j}, \ldots R_{Nj} >$
Output: OE

1: Compute average: $R_{avg} = \frac{R_{1j}+R_{2j}+..+R_{Nj}}{N}$
2: **for** $k \leftarrow 1$ to N **do**
3: $\quad D_{kj} = |R_{avg} - R_{kj}|$
4: $\quad RREL_{kj} = 1 - D_{kj}$
5: $\quad$ **return** $RREL_{kj}$
6: $OE = \frac{\sum_{k=1}^{N} R_{kj} * RREL_{kj}}{\sum_{k=1}^{N} RREL_{kj}}$

In Objective Evaluation, the reliability on a recommendation received from device k about j, i.e. $RREL_{kj}$ is computed based on the deviation from the average value of recommendations. This $RREL_{kj}$ is used to weight the received recommendation R_{kj} having a higher value of reliability for the recommendation with less deviation. A Subjective Evaluation is performed by the i to weight the credibility of the recommender k, stored in the local repository of i as OTS_{ik} along with the time of computation t_{ik}, based on the age of last interaction between i and k. The device i first assign the rank to the recommenders based on the time difference $T - t_{ik}$. The freshness of recommender, i.e $RFRS_{ik}$, is then computed based on rank assigned to the recommender. A factor α, having the value between 0 to 1, is used with the normalized value of rank to control the decay of weight with the rank. The value of $RFRS_{ik}$ will be high for the recommender having the recent interaction with i.

The value of recommended trust score of j by the device i,

Algorithm 2 Subjective Evaluation

Input: $< t_{i1}, t_{i2}, \ldots t_{iN} >$,$< OTS_{i1}, OTS_{i2}, \ldots OTS_{iN} >$
Output: SE

1: For each k, find time difference: $T - t_{ik}$
2: Sort the list of recommenders according to the ascending value of time difference
3: Assign the highest rank, starting from 1, to the device having least time difference
4: **for** $k \leftarrow 1$ to N **do**
5: $\quad Rank_k$ = get rank of k using step 3
6: $\quad NRank_k = [\frac{Rank_k - Rank_{min}}{Rank_{max} - Rank_{min}}] * \alpha$
7: $\quad RFRS_{ik} = 1 - NRank_k$
8: $\quad$ **return** $RFRS_{ik}$
9: $SE = \frac{\sum_{k=1}^{N} OTS_{ik} * RFRS_{ik}}{\sum_{k=1}^{N} RFRS_{ik}}$

i.e. RTS_{ij}, is computed by aggregating the value of OE and SE, calculated using the Algorithm 1 and 2 above, as:

$$RTS_{ij} = \beta * OE + (1 - \beta) * SE \quad (1)$$

Here, β is a scaling factor used to assign weight to the different evaluations, having the value between 0 to 1. For a higher value of β, weight of objective evolution will be more in final recommended trust computation as compared to subjective evaluation.

C. Retraining Module

The evaluator i proceeds to interact with the unfamiliar j based on the outcome of recommended trust score computed by equation 1. A threshold value, $Trust_{th}$, is used to decide the outcome as trustworthy or not by comparing it with the computed score. After gaining access to device j, i retrains the credibility of each recommender devices k (stored as

OTS_{ik} in the local repository of i) based on the dissimilarity seen between recommended and observed trust score on j. A retraining factor ρ^j_{ik} is used to penalize the credibility of k as:

$$\rho^j_{ik} = (1 - D^j_{ik})\delta^j_{ik} \quad (2)$$

Here, D^j_{ik} is a decision parameter which will be 1, if the outcome of OTS_{ij} is same as provided by R_{kj}, otherwise will be 0. The value of δ^j_{ik} is the dissimilarity measured between the values of OTS_{ij} and R_{kj}. The value of ρ^j_{ik} will be 0 if the recommended behaviour matches with observed one. Otherwise, the credibility of the recommender k will be reduced by the factor ρ^j_{ik} for new recommendation request.

IV. Experiments and Results

A. Simulation Setup

We created a service-oriented IoT network of M number of nodes(IoT devices) in the ns3 simulator where a device can be service requestor, provider or recommended. Having unique identities, these devices communicate with each other using low power protocol stack, given in Table I along with the other simulation parameters, designed especially for IoT environment [16]. To know about the trustworthiness of an unfamiliar service provider, a service requestor aggregates recommendations received from N number of recommenders about the device being evaluated. All the simulations are performed for a specific context of communication. The analysis on the effectiveness of RraR is done by randomly choosing the devices to disseminate dishonest recommendations from the list of recommender. Also, the probability of a device being dishonest lies less with the recommender whose behavior is seen recently.

Table I: Simulation Parameters

Layer	**Protocol**
Physical Layer	IEEE 802.15.4
Link Layer	IEEE 802.15.4e
Network Layer	IPv6 Addressing, RPL
Transport Layer	UDP Traffic
Communication/ Adaptation Layer	6LoWPAN Connectivity
Simulation Area	1000*1000
M	200
N	100
$Trust_{th}$	0.5
β	0.5
α	0.1, 0.2, 0.3

B. Simulation Results

The effectiveness of RraR has been analyzed with the varying number dishonest recommenders. We used Computation Error (CR) as the performance matrix which is computed as:

$$CR = \frac{|GTS - RTS|}{|GTS - RTS| + 1} \quad (3)$$

Here, GTS is the ground trust score of a device being evaluated. GTS represents the actual behavior of a device in the absence of an attack. We considered the value of GTS as 1 for a trustworthy device and 0 for an untrustworthy device. The value of RTS is the recommended trust score computed by aggregating the recommendations in the presence of an attack. The results of the simulation have been compared with the one existing work, collusion attack detection using fog computing (CADF) [14], which uses deviation from the average readings as the weight for each received reading while aggregating all the values. For having equal weight over objective and subjective evaluation, we choose value of β as 0.5. To analyze the effect of retraining module on the credibility of dishonest recommenders along with the objective and subjective evaluation, results have been traced for the following five cases:

1) 5% of N are attackers
2) previous 5% + new 10% = 15% of N are attackers
3) previous 15% + new 10% = 25% of N are attackers
4) previous 25% + new 10% = 35% of N are attackers
5) previous 35% + new 10% = 45% of N are attackers

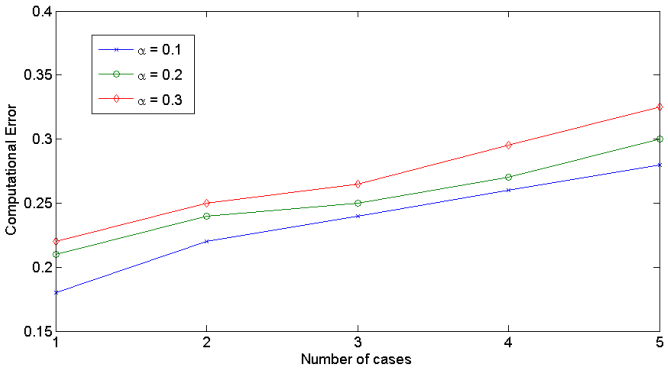

Figure 2: Performance of RraR with different values of α

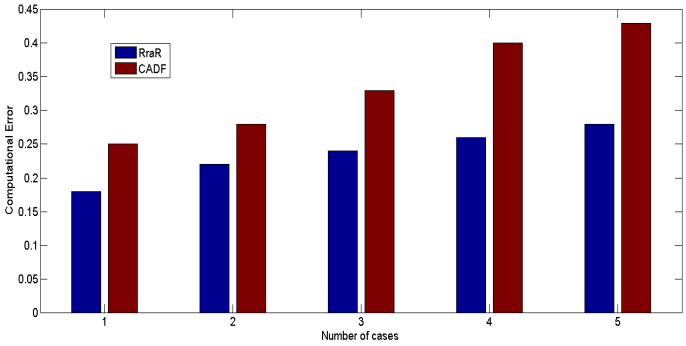

Figure 3: Performance comparison between RraR and CADF

With each case, simulation is performed over 5 runes and their average value is used to show the results. An analysis on the effect α on CR is performed to choose the appropriate value. Figure 2 shows that with having less value of α, CR is comparatively low. The comparison of our proposed scheme

RraR with the existing CADF is presented in Figure 3. These results have been traced having $\alpha = 0.1$ in the scenario of Bad Mouthing Attack, where a dishonest recommender tries to decrease the trustworthiness of a well-behaving device by providing low recommendation value. Results show that computation error is less with proposed RraR as compared to existing CADF. As we considered the scenario in which the probability of a device being dishonest is more with the device having more age over the interactions. Our subjective evaluation handle this issue while assigning more weight to the recently interacted recommender. Although this error increases with an increase in the number of dishonest recommendations, the percentage increase in error is less with proposed RraR because of the retraining of recommender's credibility based on the dissimilarity seen with the observed behaviour. With each new case, the retraining factor will reflect the influence of dissimilarity observed with the previous recommendation request.

V. CONCLUSION

Relying on the recommendations to derive reputation of a device is one of the most effective and adopted strategy for Trust and Reputation Systems (TRS). One concerned issue is to handle dishonest or falsely recommendation by the adversary which results in erroneous aggregation of recommendations. The proposed work provides an effective scheme which reduces the effect of dishonesty by assigning weight to the recommenders by performing an objective and subjective evaluation. A retraining module is used to fine tune the recommender's credibility based on the dissimilarity seen in the behaviour of recommender. Simulation results show that the scheme works well to alleviate the effect produced by the dishonest adversaries. For future work, we would like address other recommendation related attacks like selective behavior attack and self-promoting attack. We will try to present examination of proposed scheme on the other important factors like communication overheads and network bandwidth. Also, we would like to maintain the effectiveness of the proposed scheme in the presence of a large number of dishonest recommenders in the system.

REFERENCES

[1] L. Rasmusson, and S. Janssen, "Simulated Social Control for Secure Internet Commerce," in ACM New Security Paradigms Workshop, California, USA, Sep., 1996, pp. 18-25.

[2] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for Internet of Things," Journal of Network and Computer Applications, vol. 42, pp. 120-134, Jan. 2014.

[3] K. Chang, J. L. Chen, "A Survey of Trust Management in WSNs, Internet of Things and Future Internet," KSII Transactions on Internet and Information Systems, vol. 6, no. 1, pp. 5-23, Jan. 2012.

[4] 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, pp. 618-644, Mar. 2007.

[5] Hoffman, Z. Kevin, David, N. Rotaru, "A Survey of Attack and Defense Techniques for Reputation Systems," ACM Computer Survey, vol. 42, no. 1, pp. 1-31, Dec. 2009.

[6] J. Lopez, R. Roman, I. Agudo, and C. F. Gago, "Trust management systems for wireless sensor networks: best practices," Computer Communications, vol.33, no. 9, pp. 1086-1093, June 2010.

[7] H. Mousa, S. B. Mokhtar, O. Hasan, O. Younes, M. Hadhoud, and L. Brunie, "Trust management and reputation systems in mobile participatory sensing applications: a survey," Computer Network, vol. 90, pp. 49-73, Oct. 2015.

[8] D. Wang, T. Muller, Y. Liu, and J. Zhang, "Towards robust and effective trust management for security: A survey," in Proc. of 13th International Conference on Trust, Security and Privacy in Computing and Communications, TRUSTCOM, Sep. 2014, Washington, USA, pp. 511–518.

[9] N. Iltaf, A. Ghafoor, and U. Zia, "A mechanism for detecting dishonest recommendation in indirect trust computation," EURASIP Journal on Wireless Communications and Networking, vol. 1, pp. 1-13, June 2013.

[10] Zakirullah, M. H. Islam, and A. A. Khan, "Detection of dishonest trust recommendations in mobile ad hoc networks," in 5th International Conference on Computing, Communications and Networking Technologies (ICCCNT), Hefei, Chaina, Nov. 2014, pp. 1-7.

[11] M. K. Denko, T. Sun, and I. Woungang, "Trust management in ubiquitous computing: a Bayesian approach," Computer Communication, vol. 34, no. 3, pp. 398-406, Mar. 2011.

[12] M. Chen, J. P. Singh, "Computing and using reputations for internet ratings," in 3rd ACM Conference on Electronic Commerce, Florida, USA, Oct. 2001, pp. 154–162.

[13] R. Zhou, and K. Hwang, "Powertrust: a robust and scalable reputation system for trusted peer-to-peer computing," IEEE Transactions on Parallel and Distributed Systems, vol. 18, no. 4, pp. 460-473, Apr. 2007.

[14] Q. Yaseen, Y. Jararweh, M. A. Ayyoub, and M. AlDwairi, "Collusion attacks in Internet of Things: Detection and mitigation using a fog based model," IEEE Sensors Applications Symposium (SAS), Glassboro, NJ, 2017, pp. 1-5.

[15] A. Sharma, E. S. Pilli and A. P. Mazumdar, "Obviating capricious behavior in internet of things," International Conference on Advances in Computing, Communications and Informatics (ICACCI), Udupi, India, Sep. 2017, pp. 480-486.

[16] M. R. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L. A. Grieco, G. Boggia, and M.Dohler, "Standardized protocol stack for the internet of things," IEEE Communications Surveys & Tutorials, vol. 15, no. 3, pp. 1389-1406, Jul. 2013.