Trustworthiness Management in the Social Internet of Things: first theoretical analysis

Michele Nitti, Roberto Girau, Luigi Atzori, *Senior Member, IEEE* Department of Electrical and Electronic Engineering - University of Cagliari, 09123 Cagliari, Italy
{*michele.nitti, roberto.girau, l.atzori*}*@diee.unica.it*

***Index Terms*—Internet of Things, social networks, trustworthiness management**

Herein we provide an analysis of the performance of the subjective model, whose objective is to discriminate benevolent nodes from malicious ones with the minim error. The resulting trustworthiness formula is made of three additive elements (**??**), namely the centrality, the direct opinion, and the indirect opinion, each one contributing to isolating malicious nodes.

The subjective centrality measures how much a node is central in another node "life". If we calculate the average centrality of node p_i over all its friendships $\mathcal{N}_i$, we obtain

$$R_i = \frac{\sum_{j=1}^{|\mathcal{N}_i|} \frac{|\mathcal{K}_{ij}|}{\left(|\mathcal{N}_i|-1\right)}}{|\mathcal{N}_i|} = \frac{\sum_{j=1}^{|\mathcal{N}_i|} |\mathcal{K}_{ij}|}{\left(|\mathcal{N}_i|-1\right)|\mathcal{N}_i|} \tag{1}$$

that corresponds to the local clustering coefficient for node p_i, and then gives an indication of how close node p_i's neighbors are to being a clique, i.e. a complete graph.

As there are no models to represent the behavior of the nodes in creating and updating the clusters of friends, we do not have the basis to compute the efficiency of this parameter, but evidences of its capacity to isolate malicious nodes can be found in literature. In [1] the authors state that "trust is to be built based not only on how well you know a person, but also on how well that person is known to the other people in your network" and then they show that, using local clustering for email filtering, it is possible to classify correctly up to 50% of the messages. Moreover, in [2], the authors show how trust networks are highly related to the creation of cluster.

When the nodes start to exchange services, they still do not have any information about how much they can trust each other. However, they can rely on the centrality and, for what concerns direct and indirect opinion, on the relationship factor and on the computation capabilities. When N_{ij} becomes high, the dependence of the direct opinion on the relationship factor and the computation capabilities decreases whereas that related to the past transactions increases. The feedback generated for each received service is provided by (**??**). To simplify the analysis, as done in the simulations, we assume a binary feedback system is used. When analyzing the received service, the client may introduce some errors due to several reasons and mostly because of the intrinsic difficulty in evaluating the quality of the received service. We then introduce probability e that a node gives the wrong feedback, so that the probability to give the correct feedback is $h = 1 - e$. The probability that p_i generates k correct feedback ($f_{ij} = 1$ when p_j is benevolent and $f_{ij} = 0$ when p_j is malicious) over n transactions with p_j, follows a binomial distribution

$$P(k) = \binom{n}{k} h^k (1-h)^{(n-k)} \tag{2}$$

Note that if we consider feedback having the same weights, the long term and short term opinions $O_{ij}^{lon/rec} = k$ if p_j is benevolent and $O_{ij}^{lon/rec} = 1 - k$ if p_j is malicious. Accordingly, these follow a binomial distribution as well, where the expected value is h if node p_j is benevolent, and $1 - h$ if it is malicious, and the variance is $h(1 - h)$. This distribution can be approximated with a gaussian one (when $n > 30$) with the same variance and average values. When adding the two contributions from the short and long term opinions, considering $\gamma = 0.5$ as in the simulations, we obtain that the direct opinion is still a gaussian distribution with the same mean value ($\mu_b = p$ and $\mu_m = 1 - p$ based on the behavior of node p_j) and a variance equals to $h(1 - h)/2$.

To calculate the distribution of the indirect opinion, we assume for simplicity that the credibility for all the nodes is the same; in this case, it is the sum of gaussian-distributed variables, so it follows a gaussian distribution as well. Considering that x% of the nodes are malicious, the average value for the indirect opinion is $(1 - 0.x)\mu_{b,m} + 0.x\mu_{m,b}$ while its variance is $\sigma^2 / |\mathcal{K}_{ij}|$.

Using the $erfc$ function to calculate the error when estimating the trustworthiness of a node, we obtain the results shown in Table I for different values of the error probability and $x = 25\%$. Both the parameters can achieve low error probability. Indeed, the direct opinion is the parameter that most affects the trustworthiness calculation, and that leads to the smallest errors. However, when services start to circulate in the network, the first parameter that varies and gives actual information about the trustworthiness of a node is the indirect opinion. This happens because, if node p_i wants to evaluate the trustworthiness of node p_j, it is simply more probable that it can obtain information from one of the common friends $\mathcal{K}_{ij}$ than from a direct transition between p_i and p_j. Moreover, with the combination of these two parameters, it is possible to achieve more reliable results than using only one of them.

REFERENCES

[1] O. P. Boykin and V. Roychowdhury, "Personal Email networks: an effective anti-spam tool," *Condensed Matter cond-mat/0402143*, 2004.

TABLE I
PROBABILITY TO MISJUDGE A NODE

Direct opinion

e	μ benevolent	μ malicious	σ^2	error
0.1	0.9	0.1	0.045	$3.15 * 10^{-17}$
0.15	0.85	0.15	0.064	$9.63 * 10^{-7}$
0.2	0.8	0.2	0.08	$1.016 * 10^{-5}$

Indirect opinion

e	μ benevolent	μ malicious	σ^2	error
0.1	0.7	0.3	0.024	$6.56 * 10^{-15}$
0.15	0.675	0.325	0.034	$1.084 * 10^{-5}$
0.2	0.65	0.35	0.043	$1.14 * 10^{-2}$

Direct + Indirect opinion ($\alpha = 0.6$ **and** $\beta = 0.4$)

e	μ benevolent	μ malicious	σ^2	error
0.1	0.82	0.18	0.017	$8.72 * 10^{-77}$
0.15	0.78	0.22	0.024	$2.04 * 10^{-29}$
0.2	0.74	0.26	0.03	$8.31 * 10^{-14}$

[2] W. Yuan, D. Guan, Y.-K. Lee, S. Lee, and S. J. Hur, "Improved trust-aware recommender system using small-worldness of trust networks," *Knowledge-Based Systems*, vol. 23, no. 3, pp. 232–238, 2010.