Trust-based Content Distribution for Mobile Ad Hoc Networks

Mentari Djatmiko, Roksana Boreli, Aruna Seneviratne
NICTA
University of New South Wales
Sydney, Australia
{*mentari.djatmiko, roksana.boreli, aruna.seneviratne*}*@nicta.com.au*

Sebastian Ries
CASED
Technische Universität Darmstadt
Darmstadt, Germany
ries@cased.de

***Abstract*—We propose a novel trust and probabilistic node selection mechanism for content distribution in mobile ad hoc networks, which aims to achieve trustworthy node selection and to preserve mobile node resources. The proposed mechanism is evaluated against selected alternative trust schemes, with the results showing that our proposal achieves its goals.**

***Keywords*-ad hoc networks; node selection; trust evaluation;**

I. Introduction

Mobile ad hoc networks will enable future mobile users to share and distribute content using direct mobile-to-mobile wireless connections. Since such networks will need to be based on an open environment, selecting the appropriate nodes for interactions is a major challenge, especially when some of the nodes may be misbehaving. Considering that mobile devices have limited resources (i.e., available battery power, processing power and the available bandwidth), interacting with misbehaving nodes will waste these resources and reduces the usable time of mobile devices.

Trust-based solutions provide a method to select neighbours based on their trust value which is derived from previous interactions. There have been a number of trust mechanisms proposed for mobile [1]–[4] and peer-to-peer networks [5]–[7]. Most of these mechanisms are distributed and favour the most trustworthy neighbour.

In this paper, we propose a novel probabilistic node selection model which provides a load balancing within the population of nodes. Hereby, a node's probability for being selected for an interaction will correspond to its trust value. Furthermore, it gives unknown nodes the opportunity to be selected, thus enabling these nodes to contribute to the community. Eigentrust [5] briefly discusses a similar selection model, but it does not provide an analysis of the model's impact on the quality of interactions and it allocates the lowest possible trust value to unknown nodes.

Since our proposed model may select a misbehaving node, we also propose a generic trust evaluation mechanism to alleviate this problem. We introduce the concept of real-time trust evaluation, which continually evaluates trust value during an interaction and allows interaction to terminate if the selected node misbehaves, with a strong bias towards recently observed behaviour.

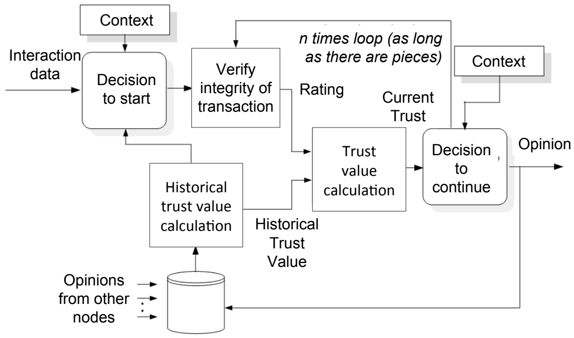


Figure 1. Proposed Real-Time Trust mechanism

II. Proposed Mechanism

We assume that in ad hoc content distribution networks, nodes download the required content from their immediate wireless neighbours and hence all the communications are single hop. Furthermore, we assume that all neighbours have the required content and that content is sub-divided into several pieces. We propose Real-Time Trust (ReTT), a novel distributed trust evaluation mechanism that continuously evaluates trust during an interaction. The mechanism is based on the assumption that an interaction between two nodes will consist of a number of steps which can be individually analysed in real time.

Figure 1 shows an overview of the proposed mechanism. ReTT introduces two decision points, the decision to connect to a node (decision to start) and the decision to stay connected after the interaction has started (decision to continue). The term real time reflects the notion that newly received information is immediately evaluated to form an evolving evaluation of trust.

The decision to start is determined by a historical trust value of the content-providing node and the context of the interaction. This value is calculated by aggregating the opinions of the selecting node and the recommendations by other nodes. Let us assume that node d has to make a decision whether to interact with node i. Given that $O_{j,i}$ is the opinion sent to node d by node j on node i, W_j is node d's weighting on $O_{j,i}$, and node d has opinions on i from k nodes (including its own opinion), then the historical trust value T_i^H of node d for node i is calculated as follows:

$$T_i^H = \frac{\sum_{j=1}^{k} W_j \times O_{j,i}}{\sum_{j=1}^{k} W_j} \tag{1}$$

$O_{j,i}$ is the average number of good integrity pieces received by node j from node i in a transaction. The decision to start considers a level of *openness*, which allows the mechanism to be flexible depending on the context and introduces a trust level threshold. In a fully open system, this threshold would be the lowest possible trust value, and thus, all available content-providing nodes are considered as candidates. The remainder of the paper assumes a fully open system.

If the selecting node decides to interact with a content-providing node, it then downloads the first piece and evaluates the piece's integrity. In this paper, a piece is considered to have good integrity if it is received as requested and it does not contain a virus. The integrity verification result is then combined with historical information to decide whether to download the next piece (i.e., decision to continue in Figure 1). Given $T_{i,m}$ is node i's calculated trust value after m^{th} piece in the current interaction, $T_{i,m-1}$ is the trust value after receiving the previous piece (in the case of $m = 1$, $T_{i,m-1} = T_i^H$) and $R_{i,m}$ is the verification result of the current piece, then real-time trust value is calculated as:

$$T_{i,m} = \alpha T_{i,m-1} + \beta R_{i,m} \quad, m \in \{1, 2, ..., n\} \tag{2}$$

α and β are the weights, with both being positive numbers which sum up to one. Since having $\beta > \alpha$ will ensure that the mechanism quickly responds to changes in behaviour, in our simulations we use $\alpha = \frac{1}{3}$ and $\beta = \frac{2}{3}$. If the selecting node decides to continue ($T_{i,m} \geq$ threshold), then the next piece is downloaded and evaluated using the same process. After the loop is terminated, the selecting node generates an opinion combining the most current experience and the old opinion (previous history). This opinion is distributed to other nodes which can then re-distribute it further. To prevent excessive control traffic, any opinions will only be forwarded a maximum of two times.

We also propose a novel node selection model which probabilistically selects content-providing nodes based on their trust value, which aims to achieve load balancing while still having an appropriate tradeoff for interacting with nodes with low trust value. To this end, the selecting node evaluates the trust values T of the set of all available content-providing nodes C. The node probabilistically selects a node from this set C, where the probability of selecting a node n, P_n, is:

$$P_n = \frac{(T_n^H)^x}{\sum_{i=1}^{|C|} (T_i^H)^x} \tag{3}$$

The impact of the difference in trust values on the node choice is regulated by the value of parameter x, which for the simulations is $x = 3$. For an unknown node, we define $T_n^H = 0.5$ only for the selection process, to ensure that unknown nodes are preferred over known misbehaving nodes.

Table I
NS-2 SIMULATION PARAMETERS

Parameter	***Value***
Piece size	$100kB$
Number of pieces sent in one interaction	5
Interval between interaction sessions	$10s$
Interval of neighbour discovery and recommendation dissemination (PERIOD)	$15s$
Maximum number of opinions in a recommendation (MAX_OPINIONS)	20

III. Evaluation

A. Simulation Environment

We simulate a one-hop ad hoc content distribution network in ns-2 version 2.34 [8]. The simulation contains 50 nodes, with the simulation area of $500 \times 500m$ and duration of $18000s$. We assume a flash crowd scenario and idealised wireless links, where all nodes are within range of each other. To minimise the control traffic overhead, opinions required for trust evaluation (as per Section II) are attached to control messages which are also used for neighbour discovery.

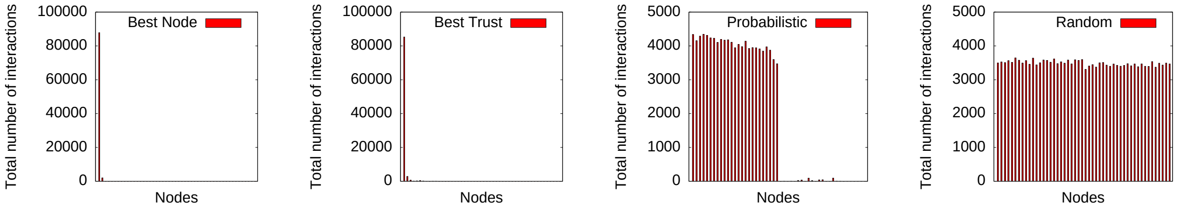
We model power use based on the experimental results for power consumption of Android phones using 802.11g link [9]. The results show that there is a close to linear relationship between battery consumption and transmitted data. Furthermore, the uplink uses more power than the downlink, which provides an incentive for selfish behaviour. Assuming the mobile has a full battery at the start of the simulation, the percentage of battery power P can be expressed as:

$$P = 1 - \frac{x_d}{X_d} - \frac{y_u}{Y_u} \tag{4}$$

where x_d and y_u are download and upload volume respectively, and X_d and Y_u respectively correspond to maximum download and upload volume (roughly $8GB$ and $5.5GB$). Table I presents other simulation parameters.

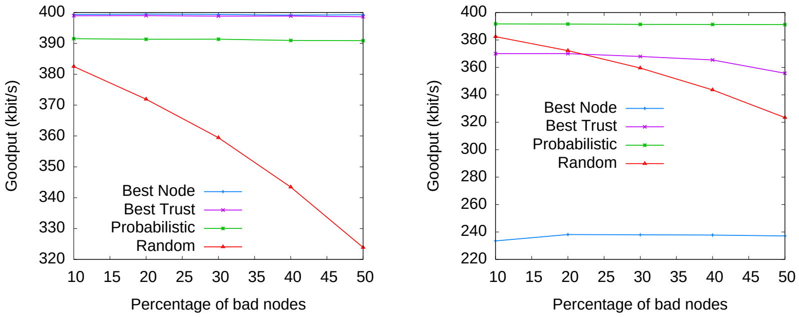
The node behaviour includes two aspects, integrity and selfishness. Integrity determines the utility of the data downloaded from that node. It is defined by core integrity behaviour, which determines the interaction outcome and can either be *well-behaving (good integrity)* or *misbehaving (bad integrity)*, and adherence probability, which determines the probability that a node will adhere to the core integrity behaviour and is randomly assigned in the uniformly distributed range of [0.8, 1.0]. Selfishness relates to whether or not a node contributes to the collaborative content sharing irrespective of its integrity. We assume that all nodes cooperate at the beginning and only become selfish after the available battery power falls to 60% of full capacity.

We compare our node selection mechanism to three other node selection models. *Objective best node* selection model is an artificial model which selects a node with the highest objective probability for providing a good interaction, which is equal to adherence probability $P(A)$ for good nodes and



(a) Best Node (b) Best Trust (c) Probabilistic (d) Random

Figure 2. These diagrams show the selected nodes based on different models. In each graph the nodes are ordered according to their probability of providing good interactions with the higher values on the left side. Note that the scales shown in the graph significantly differ.



(a) No resource constraints (b) Limited power leading to selfish behaviour

Figure 3. Results for goodput without resource constraints and with limited power leading to selfish behaviour

$1 - P(A)$ for bad nodes. It assumes the knowledge of the good interaction probability of other nodes. We also utilise the *random* selection model which only uses trust values for the *decision to continue* (see section II). Finally, *best trust* selection scheme, which selects a node with the highest trust value, is also considered. Note that all the schemes use our proposed trust evaluation mechanism to calculate trust values.

The criteria used to evaluate our selection mechanism are load balancing and quality of the content distribution service. For load balancing, we evaluate the workload, that is the total number of interaction requests that a node has to handle, and the fairness of resource sharing within the community, which is measured by power failure (since the simulation is designed to prevent overloading of 802.11g link capacity). Quality of the content distribution service is represented by goodput, that is the average good integrity download data rate, which reflects the trust mechanism's accuracy and load balancing.

B. Results

First, we evaluate the workload on a per node basis without considering resource constraints. Figure 2, shows the results for a single run, where for each graph the nodes are sorted in descending order of providing good service from left to right. Note that there are equal numbers of good and bad nodes. The *best node* and *best trust* selection schemes result in a strong imbalance in the distribution of workload amongst nodes. The *random* selection scheme results in equal workload distribution, however, the number of interactions with good and bad nodes are equal, which leads to an unacceptably low service quality as we will show later. In contrast, the *probabilistic* selection scheme provides a balanced workload among the good nodes while the number of interactions with the bad nodes is low, indicating that it is able to identify well-behaving nodes in the network.

Table II
EVALUATION: POWER FAILURE

	Fully Connected	
	Time to first failure [sec]	No. of node failures
Best Node	2140	8
Best Trust	2582	7.78
Probabilistic	–	–
Random	–	–

Next, we consider the case where nodes have limited power and hence, we evaluate the potential for one or more nodes to run out of battery. Table II shows the time to first failure and the number of node failures in the total simulation time. The simulation results are averaged over five scenarios (where the percentage of bad nodes is increased from 10% to 50%) with 50 simulation runs for each scenario. The result for the *best node* selection scheme indicates that 8 out of 25 (32%) of the good nodes run out of battery in the simulation period. If the best nodes learn over time that they are being exploited, this may cause the nodes to become selfish. In the extreme case, it may lead to a breakdown of the content-sharing network as no node is willing to be one of the best nodes. The results for the *best trust* are very similar to the *best node* scheme. For the *probabilistic* and *random* schemes, we can see that there is no power failure in the observed period. These results clearly indicate that the *probabilistic* scheme outperforms the *best node* selection scheme. Although the *random* scheme shows good results, this scheme is considered to be unsuitable for the collaborative environment as it cannot detect misbehaving nodes and consequently has substandard performance, which we will demonstrate next.

Finally, we show the influence of the selection model on the service quality, represented by the average goodput of all nodes in Figures 3(a) and 3(b). In these figures, the percentage of bad nodes is increased from 10% to 50% and the value for each data point is averaged over 50 simulation runs. The confidence intervals are not shown since the variances are very small. We believe that the source of the variations between simulation run is adherence probability which determines the good interaction probability (since the nodes have the same set of content providing nodes to choose from). However, as mentioned in Subsection III-A, adherence probability is uniformly distributed and hence the values for different simulation runs do not significantly differ.

Figure 3(a) shows the results of the ideal case, assuming that nodes have no resource constraints. We can observe that the *best node* and *best trust* selection schemes are able to achieve the highest values for goodput. Furthermore, the *random* selection scheme comes with high costs especially when the number of malicious nodes is increased while the *probabilistic* scheme's results are only slightly worse than the *best node* and *best trust* schemes. However, to achieve these results, the *best node* and *best trust* selection schemes interact with only a few nodes (see Figure 2), leading to the high workload for these nodes.

Figure 3(b) shows the performance of the node selection schemes under the scenario where nodes have limited power and become selfish after their battery level reaches 60%. Compared to the ideal case from Figure 3(a), the *best node* and *best trust* schemes show a significantly reduced performance. *Best node* selection model performs the worst among all the schemes since the scheme continues to select the nodes with the highest probability of a good outcome, unaware that a node has reached its' interaction limit. The performance of the *best trust* scheme also decreases, as it is again over-utilizing the best nodes. However, this scheme is able to adjust quickly to the new situation. In contrast, the performance of the *probabilistic* model stays high and outperforms the other models. Additionally, we can observe that all schemes other than the *random* selection scheme do not depend on the number of bad nodes. This indicates again that the trust model is able to identify good nodes (given the conditions of the simulation).

IV. Conclusion and Future Work

This paper provides a novel trust evaluation and node selection model for a mobile ad hoc content distribution network. It presents the analysis and evaluation of this model and comparison with three other node selection models. The presented results show that models which select *only the best node* lead to significant imbalances with respect to the workload of the nodes, and the proposed *probabilistic* selection model helps to overcome this problem, while still enabling a high proportion of useful content downloaded from nodes correctly selected as trustworthy. For future work, we will compare our combined model with other trust evaluation models.

Acknowledgment

This research work has been supported by funding from National ICT Australia (NICTA). NICTA is a research organization funded by Australian Government research initiatives through Australian Research Council (ARC).

References

[1] P. Michiardi and R. Molva, "Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in *Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security: Advanced Communications and Multimedia Security*. Kluwer, BV, 2002, p. 121.

[2] S. Buchegger, "Coping with misbehaviour in mobile ad-hoc networks," Ph.D. dissertation, EPFL, 2004.

[3] S. Ries and A. Heinemann, "Analyzing the robustness of CertainTrust," in *2nd Joint iTrust and PST Conference on Privacy, Trust Management and Security*, Springer, 2008, pp. 51 – 67.

[4] R. Shankaran, V. Varadharajan, M. Orgun, and M. Hitchens, "Context-aware trust management for peer-to-peer mobile ad-hoc networks," in *Computer Software and Applications Conference, 2009. COMPSAC '09. 33rd Annual IEEE International*, vol. 2, 2009, pp. 188 –193.

[5] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The eigentrust algorithm for reputation management in p2p networks," in *Proc. of the 12th international conference on World Wide Web*. ACM Press, 2003, pp. 640–651.

[6] W. T. L. Teacy, J. Patel, N. R. Jennings, and M. Luck, "Travos: Trust and reputation in the context of inaccurate information sources," *Autonomous Agents and Multi-Agent Systems*, vol. 12, no. 2, pp. 183–198, 2006.

[7] X. Li, F. Zhou, and X. Yang, "A multi-dimensional trust evaluation model for large-scale p2p computing," in *Journal of Parallel and Distributed Computing*, vol. 2, 2011, pp. 188 –193.

[8] ns-2 Network Simulator, http://www.isi.edu/nsnam/ns/.

[9] H. Petander, "Energy-aware network selection using traffic estimation," in *Proceedings of the 1st ACM workshop on Mobile internet through cellular networks*, ser. MICNET '09. New York, NY, USA: ACM, 2009, pp. 55–60.