On Trust Evaluation in Mobile Ad Hoc Networks

Dang Quan Nguyen[1], Louise Lamont[1], and Peter C. Mason[2]

[1] Communications Research Centre, Canada
{Dang.Nguyen,Louise.Lamont}@crc.gc.ca
[2] Defence Research & Development, Canada
Peter.Mason@drdc-rddc.gc.ca

Abstract. *Trust* has been considered as a social relationship between two individuals in human society. But, as computer science and networking have succeeded in using computers to automate many tasks, the concept of *trust* can be generalized to cover the reliability and relationships of non-human interaction, such as, for example, information gathering and data routing. This paper investigates the evaluation of trust in the context of ad hoc networks. Nodes evaluate each other's behaviour based on observables. A node then decides whether to trust another node to have certain innate abilities. We show how accurate such an evaluation could be. We also provide the minimum number of observations required to obtain an accurate evaluation, a result that indicates that observation-based trust in ad hoc networks will remain a challenging problem. The impact of making networking decisions using trust evaluation on the network connectivity is also examined. In this manner, quantitative decisions can be made concerning trust-based routing with the knowledge of the potential impact on connectivity.

Keywords: Ad hoc networks, security, trust evaluation, connectivity.

1 Introduction

A Mobile ad hoc network (MANET) consists of auto-configuring nodes that communicate with each other using wireless equipment. Such networks are infrastructureless, self-deploying and do not require a centralized entity. These advantages make MANETs suitable for critical uses: tactical military networks, disaster recovery, etc. Messages between two out-of-range nodes are routed in a multi-hop way, through intermediate nodes selected by MANET routing protocols (e.g. OLSR [1]).

These characteristics have a deep impact on security issues as they pose new challenges to the design of security solutions. One of these issues is concerned with trust management. The ad hoc environment is distributed and changing, meaning nodes can join and leave the network at any time. Therefore, traditional identification schemes based on a centralized authentication server are generally unsuitable for ad hoc networks. Ad hoc networks require new trust management designs to support a distributed environment and to be more robust against topology changes. One of the main components of trust management is *trust*

A.U. Schmidt and S. Lian (Eds.): MobiSec 2009, LNICST 17, pp. 1–13, 2009.

evaluation, or how to estimate the degree of trust between two nodes in an ad hoc network.

In this paper, we focus on the evaluation of trust. We define trust in the context of ad hoc networks and show how observations can be used to build an accurate estimate of trust. We also investigate the effect of decisions, based on trust evaluation, on one of the important properties of ad hoc networks which is connectivity. Indeed, trust decisions based on strict selection policy may result in few nodes selected, thus the network topology made of trusted nodes may be disconnected.

The remainder of this paper is organized as follows. In Section 2, we describe the existing work on trust computation. We start our study by giving a new definition of trust in ad hoc networks in Section 3 and discuss some aspects of this definition. Trust evaluation and estimation accuracy are explained in Section 4. We investigate the effect of trust evaluation on the network connectivity in Section 5. We conclude this paper in Section 6.

2 Related Work

There has been a significant amount of work done on trust. One of the earliest results on the topic within computer science [2] shows that trust can be formalized as a computational concept. Since then, research on trust has evolved in two main directions: *trust evaluation* and *trust sharing*.

Trust evaluation is concerned with the problem of estimating the trustworthiness of an entity (called a *node*) within a system, usually viewed as a network of interacting nodes. In [3], the authors propose a model for trust computation. This model defines trust as a subjective expectation a node has about another node based on the history of their encounters. This definition is probably closest to the one we will present. However, the work done in [3] is limited in the sense that it only takes into account a node's binary actions (cooperate or defect)– that is, the trust is discrete.

In [4], the authors use entropy to measure the uncertainty in trust relationship. This entropy is obtained from the probability that a node will perform some action. Such a probability is useful because it can be used as factor in predicting the behaviour of a node; that is, it can be used to estimate its trustworthiness. The authors do not, however, specify how this probability of node's compliance is arrived at in the first place.

On the other hand, trust sharing is concerned with the problem of sharing the estimation of a node's trustworthiness with other (usually distant) nodes and, conversely, of synthesizing all the received estimations. In [5], the authors propose an algorithm allowing indirect neighbours to estimate the trustworthiness of each other based on the trustworthiness of direct neighbours, as long as there exists a path between them. This algorithm of trust sharing treats it as a single real value between 0 and 1. It also assumes that trust propagation is multiplicative. Thus, given a node k which is a direct neighbour of nodes i and j, the level of trust node i puts in node j is the product of the trust values of node i in node

k and that of node k in node j. Trust sharing models such as this assume some transitivity of trust, but put stronger emphasis on information obtained from direct neighbours while attenuating trust values received via a multi-hop route. That is, local information carries a greater weight yet can still contribute to a global trust-sharing model.

In [6], the authors take a different approach to sharing trust values by considering trust as an opinion composed of a pair of real numbers (*trustvalue*, *confidence*) $\in [0,1] \times [0,1]$. While *trustvalue* is the estimation of the trustworthiness that node i puts in node j, *confidence* is the accuracy of the *trust value* assignment. In other words, *confidence* can be viewed as the quality of the estimation of trust. Therefore, when a node synthesizes opinions about a distant node, it must take into consideration the confidence value of each local *trustvalue*. We believe that this approach can give a more objective result of trust estimation than in [5] because it recognizes the subjectivity of each local trust estimation. This type of approach would lend itself well to a trust model that used a fuzzy logic reasoning engine.

In this paper, we consider the problem of trust evaluation and show how the quality of trust estimation can be quantified. To start, we state our definition of trust in the next Section.

3 Definition of Trust

Many existing definitions of trust are derivatives of authentication techniques which require encryption and a centralized authentication server. While authentication can provide a quick and efficient way to identify a node, implementing a practical and efficient authentication algorithm in an ad hoc environment remains an open problem [7]. We wish to decouple aspects of trust from authentication so that we may create an additional factor to be used as a tool in securing MANETs. One of the advantages of having a quantifiable and continuous value of trust available is that it allows flexibility in making certain security decisions so that trade-offs between security and functionality can be taken into consideration. We will return to this concept in Section 5.

We define the notion of trust of a given node in a MANET as the consistency of the node's behaviour. The behaviour is observed by other nodes in what is known as a watchdog approach [8]. A consequence of the watchdog approach is that it is observer-dependent; that is, an observed node can have different observational outcomes from the perspective of different neighbours. Let us define the *capacity* of a node to be the innate properties of that node. The node's behaviour will then be inherently tied to, and should reflect, its capacity. If a node behaves inconsistently, it is either because the node is being unfaithful to its capacity, in which case it is acting in an untrustworthy manner, or external factors (e.g. multipath and fading) are affecting its performance. In the latter case, we will assume that the observing nodes are also monitoring the environment and the link quality, can detect such factors, and compensate for them when making their observations.

Some examples of a node's behaviour related to security could be:

- The node's ability to reliably transmit periodic status updates that reflects parameters such as battery level, location and configuration.
- Forwarding packets in a timely manner based on management information base (MIB) bounded delay.
- The difference in the amount of data that should be forwarded and that is actually forwarded.

Our working definition of trust is meant to extract all aspects related to the capacity (as we have defined it) of a node from previous trust models. We do this for the purpose of allowing a quantitative measure of trust to be made which can then be used for making analytical decisions that affect network security. With this new definition of trust, nodes can proactively measure the trustworthiness of their neighbours through observation, without the need of challenging them. Moreover, the network does not need any centralized authentication server to assert signatures.

This definition of trust also allows us to decouple a node's capacity and its trustworthiness. For example, a node may have a large response delay because the throughput aspect of its capacity is low, but this node can still be trusted by other nodes as long as its response delays remain consistently large. As a result, for certain tasks nodes in the network could be selected as a function of both their trustworthiness and their capacities, e.g.: selecting highly capable nodes among those who are above a specified trust threshold.

On the assumption that nodes can monitor the behaviour of their neighbours using a variety of metrics, we will, for the rest of this paper, denote the outcome of a behaviour observation by X, a continuous random variable. X takes values between 0 and 1, thus the outcomes are normalized in the entire network. X is obtained by direct observation by a node i on a node j's behaviour. Values of X can be propagated to the other nodes in the network who can use them as they see fit. Therefore, a given node k can obtain many observation results of a distant node i from different sources (or observers).

The above assumption demands that the observers accurately report all observation results and the use of some cryptography mechanisms prevents the observation results from being modified while they are propagated in the network. The first assumption requires *objectivity* and the second *trust propagation*. These are strong assumptions and it is well recognized that both issues are themselves complex problems in MANET security that need to be addressed separately.

4 Accuracy of Trust Evaluation

In this Section, we are interested in trust as a measure of the consistency of a node's behaviour as objectively observed by one or many different observers.

4.1 Estimation of a Node's Capacities

Let $X_1, X_2, \ldots, X_n$ be different observation outcomes of a node i reported by different sources to a node j. If node j computes a weighted average of these values to

estimate the capacity of i, then our main concern is how accurate this estimation would be when compared to node i's true capacity. We can subsequently quantify the number of observations needed by node j in order to achieve an acceptable level of confidence in its estimation of node i's capacity. Node j can then decide whether it should trust node i to have such an estimated capacity.

Let $Y = c_1X_1 + c_2X_2 + \ldots + c_nX_n$ be an estimation of node i's capacity, with $0 \leqslant c_i \leqslant 1$ and $\sum_{i=1}^{n} c_i = 1$. We introduce the weights c_i to allow node j to assign different importance to the values X_i, for example: recent observations are more important than old ones. All random variables X_i are assumed to be independent and identically distributed.

Since X measures the observational outcomes of a node's behaviour, $\mu = E[X]$ represents the capacity of this node. Our problem can be formulated as follows: given $\delta \geqslant 0$ and $\epsilon \geqslant 0$, what is the probability that an estimation Y of μ can achieve an accuracy of δ, and conversely, how many observations (n) are needed in order to achieve an estimation of accuracy δ with the probability $1 - \epsilon$?

Theorem 1 (Chernoff bound). *Let* $\mu = E[X]$. *Denote by* $\phi_X(s) = \int_{-\infty}^{\infty} \mathrm{e}^{sx} f_X(x)dx$ *the moment generating function of* X. *We have*

$$P\left[|Y - \mu| \geqslant \delta\right] \leqslant \min_{s \geqslant 0} \left(\mathrm{e}^{-s(\delta+\mu)} \prod_{i=1}^{n} \phi_X(c_i s) \right) + \min_{s \geqslant 0} \left(\mathrm{e}^{-s(\delta-\mu)} \prod_{i=1}^{n} \phi_X(-c_i s) \right)$$

Proof. We have

$$P\left[|Y - \mu| \geqslant \delta\right] = P\left[Y - \mu \geqslant \delta\right] + P\left[Y - \mu \leqslant -\delta\right].$$

Apply Chernoff bound to random variable Y in the first term yields

$$P\left[Y - \mu \geqslant \delta\right] = P\left[Y \geqslant \delta + \mu\right] \leqslant \min_{s \geqslant 0} \left(\mathrm{e}^{-s(\delta+\mu)} \phi_Y(s) \right).$$

Since X_i are independent and identically distributed random variables:

$$\phi_Y(s) = \phi_{\sum_{i=1}^{n} c_i X_i}(s) = \prod_{i=1}^{n} \phi_{c_i X_i}(s) = \prod_{i=1}^{n} \phi_X(c_i s).$$

And hence

$$P\left[Y - \mu \geqslant \delta\right] \leqslant \min_{s \geqslant 0} \left(\mathrm{e}^{-s(\delta+\mu)} \prod_{i=1}^{n} \phi_X(c_i s) \right).$$

Similarly, applying the Chernoff bound to the random variable $Z = -Y$ in the second term yields

$$P\left[Y - \mu \leqslant -\delta\right] \leqslant \min_{s \geqslant 0} \left(\mathrm{e}^{-s(\delta-\mu)} \prod_{i=1}^{n} \phi_X(-c_i s) \right)$$

which ends the proof. □

If X is a gaussian random variable with mean μ and variance σ^2, then we have the following result.

Corollary 1. *Let* $\xi = \sum_{i=1}^{n} c_i^2$. *If* $X \sim \mathrm{G}(\mu, \sigma^2)$, *then*

$$P\left[|Y - \mu| \geqslant \delta\right] \leqslant 2\exp\left(-\frac{\delta^2}{2\sigma^2\xi}\right)$$

Proof. If $X \sim \mathrm{G}(\mu, \sigma^2)$ then $\phi_X(s) = \exp\left(\mu s + \frac{\sigma^2 s^2}{2}\right)$.

Therefore

$$\begin{aligned}\prod_{i=1}^{n} \phi_X(c_i s) &= \prod_{i=1}^{n} \exp\left(\mu c_i s + \frac{\sigma^2 c_i^2 s^2}{2}\right) \\ &= \exp\left(\mu \textstyle\sum_{i=1}^{n} c_i s + \frac{\sigma^2 \sum_{i=1}^{n} c_i^2 s^2}{2}\right) \\ &= \exp\left(\mu s + \frac{\sigma^2 \xi s^2}{2}\right).\end{aligned}$$

And hence

$$\min_{s \geqslant 0}\left(\mathrm{e}^{-s(\delta+\mu)} \prod_{i=1}^{n} \phi_X(c_i s)\right) = \min_{s \geqslant 0}\left(\exp\left(-\delta s + \frac{\sigma^2 \xi s^2}{2}\right)\right).$$

The expression $-\delta s + \frac{\sigma^2 \xi s^2}{2}$ has a minimum value of $-\frac{\delta^2}{2\sigma^2\xi}$ when $s = \frac{\delta}{\sigma^2 \xi} \geqslant 0$.

Thus

$$\min_{s \geqslant 0}\left(\mathrm{e}^{-s(\delta+\mu)} \prod_{i=1}^{n} \phi_X(c_i s)\right) = \exp\left(-\frac{\delta^2}{2\sigma^2\xi}\right).$$

Similar calculations give

$$\min_{s \geqslant 0}\left(\mathrm{e}^{-s(\delta-\mu)} \prod_{i=1}^{n} \phi_X(-c_i s)\right) = \exp\left(-\frac{\delta^2}{2\sigma^2\xi}\right).$$

The assertion thus follows from Theorem 1. □

An interesting conclusion we can draw from Corollary 1 is that the accuracy of the Y-estimation does not depend on the true capacity μ of the subject node. That is, in other words, if node j has received n observations $X_1, \ldots, X_n$ of node i, then it can estimate the capacity of node i with a certain degree of confidence, even if this estimation indicates that node i's capacity is low. Conversely, when some early-arriving reports indicate that node i's capacity is rather high, node j should not rely entirely on this small number of observations to conclude this with a high degree of confidence. Since this result shows that the capacity μ of a node and the estimation accuracy (represented by δ) are statistically unrelated, we do not need to have *a priori* knowledge of a node's capacity in order to draw conclusions about its trustworthiness.

4.2 Number of Observations Required

The following corollary gives a lower bound on the number of observations needed in order to achieve a desired degree of confidence in the estimation.

Corollary 2. *Suppose that* $X \sim \mathrm{G}(\mu, \sigma^2)$. *Given* $0 < \epsilon < 1$, *the minimum number of observations needed in order to achieve an estimation of accuracy* δ *with the probability* $1 - \epsilon$ *is*

$$n \geqslant \frac{2\sigma^2}{\delta^2} \ln\left(\frac{2}{\epsilon}\right)$$

Proof. The inequality in Corollary 1 can be rewritten as

$$P\left[|Y - \mu| \geqslant \delta\right] \leqslant \min_{\xi}\left(2\exp\left(-\frac{\delta^2}{2\sigma^2\xi}\right)\right)$$

where $\xi = \sum_{i=1}^{n} c_i^2 \geqslant \frac{1}{n}$ by Cauchy-Schwartz inequality. Equality occurs when $c_1 = \ldots = c_n = \frac{1}{n}$.

Therefore

$$P\left[|Y - \mu| \geqslant \delta\right] \leqslant 2\exp\left(-\frac{\delta^2 n}{2\sigma^2}\right).$$

And hence

$$P\left[|Y - \mu| < \delta\right] \geqslant 1 - 2\exp\left(-\frac{\delta^2 n}{2\sigma^2}\right) \geqslant 1 - \epsilon$$

yields the desired result. □

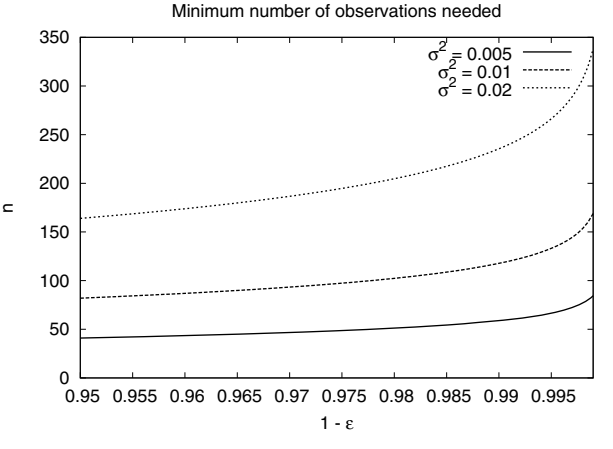


Fig. 1. Minimum number of observations needed to satisfy probability $1 - \epsilon$, with $\delta = 0.03$

Figure 1 shows the minimum number of observations needed in order to achieve an estimation having an accuracy of ± 0.03 ($\delta = 0.03$) with probability at least 95%, for three different values of the variance, σ^2.

Corollary 2 shows that the minimum number of observations required is proportional to the maliciousness of a node which is represented by the standard deviation σ. The deviation measures the lack of consistency in a node's behaviour and we assume intentionally inconsistent behaviour is malicious or untrustworthy. The more inconsistently a node behaves, the more observations we need in order to accurately estimate its capacity. This implies that a greater number of observations are required in order to identify untrustworthy nodes, a fact that makes doing so a more onerous task.

Corollary 2 also gives a lower bound on the number of observations needed to perform an accurate estimation. This lower bound is obtained when equal weights are assigned to each of the observations. Equal weighting of observations is an unlikely scenario: it is more likely a node will grant more importance to recent observations than to stale ones, or more importance to its own observations than to the ones reported by the other nodes. Therefore, the minimum number of observations needed will be higher but will still be accurately quantifiable.

An additional parameter of interest that can be extracted from our calculations is the number of observations required to achieve different accuracies in trust assessment of a node. Figure 2 shows the probability of having an estimation achieve an accuracy δ as a function of the number of observations for a given variance. This figure shows that achieving a very high level of confidence in an assessment comes at great cost with respect to the number of observations required. In this example, it only requires approximately twenty observations to achieve an accuracy of within 4% ($\delta = 0.04$) with 80% confidence but doubling the accuracy to 2% at the same confidence level increases the number of required observations by a factor of six, to $n = 120$. Again, a goal of this work is to allow

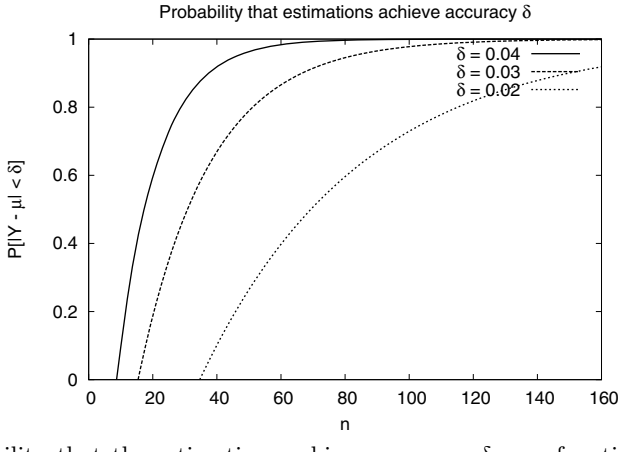


Fig. 2. Probability that the estimations achieve accuracy δ as a function of n, with $\sigma^2 = 0.01$

these tradeoffs to be understood so that decisions using trust as a parameter can be weighed appropriately.

5 Trust and Network Connectivity

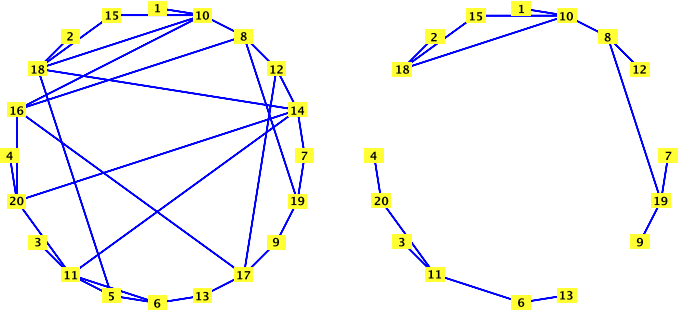
In this section, we study an example where decisions based on trust may have an effect on the connectivity of the network. In particular, we are interested in the probability of the network graph remaining connected if some nodes of the network are untrusted and thus either do not, or are not permitted to, participate in routing. This probability of connectivity is useful for the configuration of trust-based routing. Indeed, when a node extracts a trust topology out of the network graph by excluding nodes having insufficient trustworthiness, it may obtain a partitioned graph and hence trust-based routing may not be available to all destinations.

5.1 Connectivity of Trust-Based Networks

Network connectivity is an important issue in networking and distributed systems. Research on this topic ranges from graph theory [9,10,12] to physics-related domains such as percolation theory [11]. In [12], the authors show that if n nodes of a network are placed uniformly and independently in a unit disc, then the network is connected with a probability asymptotically tending to 1 if and only if each node has $\log n + c(n)$ neighbours and $c(n) \to \infty$ as $n \to \infty$.

In this section, we consider a connected random graph G characterized by n nodes and average density d (or number of neighbours per node). We derive an upper-bound of the connectivity probability for this graph when a subset S, $0 \leqslant |S| \leqslant n$, of randomly chosen nodes in G is untrusted and removed from G.

Figure 3(a) shows an example of a random graph having 20 nodes and average density 3. Nodes {5, 14, 16, 17}, randomly chosen, are untrusted and removed



(a) Initial network graph G

(b) Trust topology, nodes {5,14,16,17} are untrusted and removed from G

Fig. 3. A random graph composed of 20 nodes with 3 neighbours in average per node

from the original graph to obtain a trust topology of the network. This topology is partitioned into two components (see Figure 3(b)).

The following theorem gives us an upper bound of the probability that the trust topology remains connected.

Theorem 2 (Trust-based connectivity).
Let $\rho = \frac{|S|}{n}$*, the probability that* $G\backslash S$ *is connected is*

$$P\left[G\backslash S \text{ is connected}\right] \leqslant 1 - \left(\rho\left(2-\rho\right)\right)^{\frac{1}{2}d(1-\rho)}$$

Proof. We prove this theorem by first quantifying the number of edges that are removed from G due to the removal of nodes in S. Then, the remaining induced subgraph $G\backslash S$ is connected if and only if it still has at least one spanning tree.

Since G has n nodes and d neighbours per node on average, the probability that there exists a link between any two nodes is $\frac{d}{n}$. Therefore, the expected number of induced edges of $G\backslash S$, which has $(1-\rho)n$ nodes, is

$$\|G\backslash S\| = \frac{1}{2}\left((1-\rho)n\right)^2 \frac{d}{n} = \|G\|(1-\rho)^2.$$

Hence, the expected number of edges removed from G is

$$\begin{aligned}\|G\| - \|G\backslash S\| &= \|G\|\left(1-(1-\rho)^2\right)\\ &= \|G\|\rho(2-\rho)\end{aligned}$$

which means an edge of G is arbitrarily removed with probability $\rho(2-\rho)$.

Let k be the number of edge-disjoint spanning trees in $G\backslash S$. As each spanning tree in $G\backslash S$ has $(1-\rho)n-1$ edges, we have

$$k \leqslant k_{max} = \frac{\|G\|(1-\rho)^2}{(1-\rho)n-1} \approx \frac{1}{2}d(1-\rho).$$

$G\backslash S$ is disconnected if and only if all its k edge-disjoint spanning trees are disconnected, i.e. at least k edges must be removed from $G\backslash S$ to disconnect it. Hence

$$P\left[G\backslash S \text{ is disconnected}\right] \geqslant \left(\rho(2-\rho)\right)^k \geqslant \left(\rho(2-\rho)\right)^{\frac{1}{2}d(1-\rho)}$$

which ends the proof. □

5.2 Validation

We validate the above analysis by simulation. To start, we fix a value of ρ increasing from 0 to 0.95 by step 0.05, i.e. $\rho = 0, 0.05, 0.1, \ldots, 0.95$. For each value of ρ, we generate 10,000 random graphs. Each graph has 100 nodes and average density $\log_2(100)+1$. Therefore, we ensure that most of the initial graphs are connected (see [12]).

For each random graph G, $\lfloor \rho n \rfloor$ nodes are removed from G. The edges incident to these nodes are also removed. We calculate the percentage of graphs that

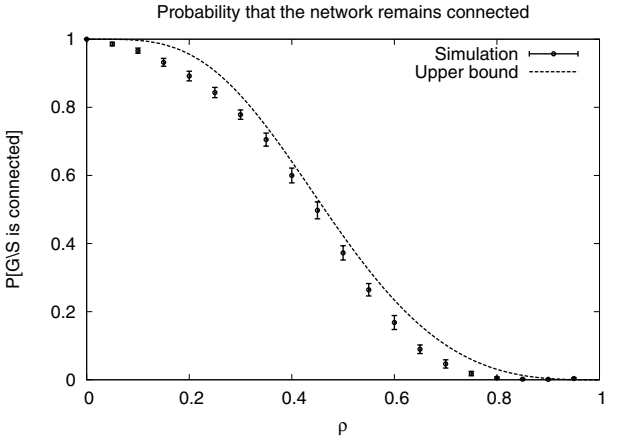


Fig. 4. Probability that a 100-node network ($d = \log_2(100) + 1$) remains connected in presence of a subset S of untrusted nodes, with $|S| = \rho n$

remain connected along with the standard deviation. In total, 200,000 random graphs are generated. The simulations are done using Maple software ([13]).

Figure 4 compares simulation results to analysis. We see that the probabilities of connectivity obtained by simulations closely follow the trend of the upper-bound probabilities obtained by analysis.

The results shown in Fig. 4 demonstrate the potential impact of using strict policies on trust to implement concepts like trust-based routing. If the threshold of required trust is set too high, there is a strong likelihood that a critical number of nodes will be excluded from the network, endangering connectivity. Knowledge of this relationship between trust-level and potential network segregation will allow security decisions to be made in which assuming different levels of risk (routing through less-trusted nodes) can be balanced against the value of increasing the probability of successful message transmission.

6 Conclusion

In this paper, we investigate the issue of trust evaluation and estimation accuracy for ad hoc networks. We start our study by giving a clear definition of trust in the context of ad hoc networks. This definition extracts the physically observable aspects of a nodes behaviour so that each node in the network can decide whether it can trust another node to have certain capacities. We then show that a node's true capacity and its estimation accuracy are statistically independent, given that a node's behaviour follows a normal distribution law. We also provide a minimum number of observations required in order to obtain an accurate estimation of a node's capacity. Given that this minimum number is large, we have shown that an implementation of an analytical trust model will require either a large number of independent observations done in parallel or

the ability to cache and safely propagate observation information through the network.

A motivation of this work is to quantify the trade-offs and requirements that will naturally arise by defining trust in this manner for ad hoc networks. To that end, we present an example showing what effect trust-based decisions may have on network connectivity. We derive an upper-bound probability of the network remaining connected when some nodes in that network are untrusted. This information could be used so that trust-based routing is available to as many nodes in the network as possible while simultaneously having an understanding of the measure of risk that is being assumed to do so.

In future work, we can study different mobility scenarios (e.g. time required to compute observations versus speed of nodes) as additional parameters to better understand the tradeoffs and practicability of using trust for security decisions. In addition, an examination of the avenues of attack on this trust model can be considered along with suggestions for mitigating their effects.

Acknowledgement

This work is funded by Defence Research & Development Canada (DRDC).

References

1. Adjih, C., Clausen, T., Jacquet, P., Laouiti, A., Minet, P., Muhlethaler, P., Qayyum, A., Viennot, L.: Optimized Link State Routing Protocol. RFC 3626, IETF (October 2003)
2. Marsh, S.P.: Formalising trust as a computational concept. PhD thesis, University of Stirling (1994)
3. Mui, L., Mohtashemi, M., Halberstadt, A.: A Computational Model of Trust and Reputation. In: Proc. of 35^{th} Hawaii International Conference on System Sciences, HICSS 2002, Hawaii, USA (January 2002)
4. Sun, Y., Yu, W., Han, Z., Ray Liu, K.J.: Trust Modeling and Evaluation in Ad Hoc Networks. In: Proc. of IEEE Global Telecommunications Conference, GLOBECOM'05, St, Louis MO, USA (December 2005)
5. Guha, R., Kumar, R., Raghavan, P., Tomkins, A.: Propagation of Trust and Distrust. In: Proc. of 13^{th} International Conference on World Wide Web, WWW 2004, New York NY, USA (May 2004)
6. Theodorakopoulos, G., Baras, J.S.: Trust Evaluation in Ad-Hoc Networks. In: Proc. of 3^{rd} ACM Workshop on Wireless Security, WiSe 2004, Philadelphia PA, USA (October 2004)
7. Tang, H., Salmanian, M.: Lightweight Integrated Authentication Protocol for Tactical MANETs. In: Proc. of IEEE TrustCom 2008, Zhangjiajie, China (November 2008)
8. Marti, S., Giuli, T.J., Lai, K., Baker, M.: Mitigating Routing Misbehavior in Mobile Ad Hoc Networks. In: Proc. of the Sixth Annual Conference on Mobile Computing and Networking, Boston, MA, USA (August 2000)
9. Gilbert, E.N.: Random Plane Networks. Journal of the Society for Industrial and Applied Mathematics 9(4), 533–543 (1961)

10. Philips, T., Panwar, S., Tantawi, A.: Connectivity Properties of a Packet Radio Network Model. IEEE Transactions on Information Theory 35(5), 1044–1047 (1989)
11. Meester, R., Roy, R.: Continuum Percolation. Cambridge University Press, Cambridge (1996)
12. Gupta, P., Kumar, P.R.: Critical Power for Asymptotic Connectivity in Wireless Networks. In: McEneany, W.M., et al. (eds.) Stochastic Analysis, Control, Optimization and Applications, pp. 547–566. Birkhauser, Boston (1998)
13. Maplesoft: Math Software for Engineers, Educators & Students, http://www.maplesoft.com