A Protocol to Increase the Security in a MANET Based on Trust and Reputation

Ana E. Fernández and Jens Hardings

Departamento de Ciencia de la Computación, Pontificia Universidad Católica de Chile
Vicuña Mackenna 4860 (143), Macul, Santiago, Chile
{asfernan, jhp}@ing.puc.cl

Abstract

The security of wireless and mobile networks has a very important role on the performance of mobile infrastructure. The protocol presented in this paper keeps a record of the history of a node and its level of participation in order to identify its reliability for a securer exchange of packages. Simulation results support our proposal by a significantly lower bit error ratio in the exchange of information between nodes.

Introduction

A mobile ad-hoc network (MANET) is a multi-hop wireless network where all nodes cooperatively maintain network connectivity. Due to the limited transmission range of wireless nodes, as well as the rapid change in network topology, multiple hops may be needed for one node to exchange data with another across the network. The most common cost metric used for determining the optimum routing path is shortest delay or fewest number of hops, as in the case of DSDV [1], AODV [2]. However, these algorithms do not take reputation of nodes into consideration; therefore valuable information about past transactions is not taken into account.

Reputation is an interdisciplinary concept that has been used in many different contexts from social to finance. Schneider et al. [3] explain how information about reputation assists in daily human interactions. They provide a solution to evaluate a user's trustworthiness in a mobile and wearable community [3].

Grajek et al. [4] discuss the origins of trust in an individual's psychological feelings and the necessity of IT services' reputation. In their work, trust is related as a measurement used to estimate the consequences of the expected behaviours.

Barber et al. [5] face out the existing issues facing trust and reputation. The trust models having higher accuracy generally need more complicated computations and more information; nevertheless, the systems associated with reputation evaluations can expand their security effectively.

Klusch [6] proposes an agent-based technology to acquire, mediate, and maintain pertinent information about the common user, and thereby to work out the users' records to form their reputations. Thus, there are significant costs to applying reputation evaluations and it is crucial to find the right balance.

This paper presents a protocol to increase the security of a MANET, understood as the reliability in the delivery of messages. The provided solution is based on trust and reputation applied to wireless and mobile networks. Previous research work on the problem involving reputation of peers has led to a static communication scheme. However future communication networks require an allocation scheme that is a dynamic and flexible according to demand.

The paper in organized as follows. First there is a description of the system model. In the second part we present a trust-based routing algorithm followed by simulation results followed by conclusions and future work.

Description of the System Model

A MANET is a collection of autonomous mobile nodes without any infrastructure. Due to the dynamic and distributed nature, the end-to-end communication may require routing information via several intermediate nodes.

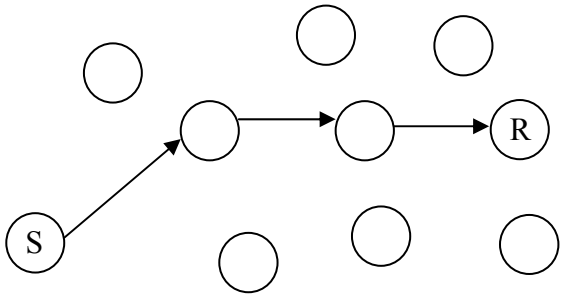

Figure 1. Example of a MANET network.

A typical example of a MANET network is shown in Figure 1, in this case with eleven nodes.

Node S and R represents the sender and receiver nodes respectively and the information sent requires two intermediate nodes in order to cooperate for the transmission of the message.

In a MANET network based on trust we have nodes that use their community partners to communicate between each other and the nodes chosen will depend on their level of trust.

The network model proposed makes the following assumptions:

- The geographic position of each node is known all the time. This can be easily implemented by having a GPS device in every node.
- Nodes can communicate with each other using a multi-hop architecture.
- The reputation of nodes is managed centralized and all nodes have access to the central trust system at all times.
- The network must be equipped with an infrastructure of authorities for the assignment of certificates.

Key Generation

A node to be part of a network has to be properly authenticated by an association between its identity and its public key. Public key certificates are usually used for this purpose. Certificates will be associated with an identifier of the node such as IP address or MAC address. Thus we propose a mechanism of assignment of unique certificate for each node by a certifying authority.

Nowadays, key management schemes based on public key cryptography are not suitable for MANET networks because of its computation inefficiency and nodes resources constraints.

We propose to use a symmetric key distribution scheme between mobile nodes like the one proposed in [7]. Such scheme distributes symmetric keys between mobile nodes in two steps: the distribution of certificates during the route request process and the dissemination of symmetric keys during the route reply process [7].

Reputation and Trust Calculation

In our model we identified two reputation factors that are directly correlated with the trust of a node in a MANET: activity level and past behaviour.

The first will be named participating reputation and will be calculated by a relative contribution factor which will be the amount of actions performed by a node over the amount of total actions. We will denote C_i^P as the relative contribution factor for participation which has been divided in m areas, where m represents the amount of participation dimensions. Each contribution should have different importance in the system, for such reason we will identify β_i as the importance weight of C_i^P. We then define the participating reputation R_P of node a as:

$$R_P(a) = \sum_{i=1}^{m} \beta_i C_i^P(a) \qquad (1)$$

The second factor will be named peer reputation and represents the rates from other nodes. Nodes in the system can be qualified by others with a positive or negative qualification depending on the correctness of the information transmitted by them.

Records of the last h rates of every node will be kept and when a new qualification $h+1$ arrives, the oldest one comes out of the list like a FIFO array. Q_a stores the rates for node a where $Q_a[1]$ is the oldest rate and $Q_a[h]$ is the most recent. Nodes will behave more probably like they did in their most recent transactions. Therefore we chose a metric called BlurredSquared [8] which computes a weighted sum of all past ratings. The older a rating is, the less it influences the current reputation. In our particular case the reputation will only be calculated with the last h qualifications. The peer reputation R_Q of node a will then be defined by the formula:

$$R_Q(a) = \sum_{j=1}^{h} \frac{Q_a[j]}{(h-j+1)^2}. \qquad (2)$$

Our model computes the global reputation or trust of a peer based on two factors: past qualifications and level of activity. The chosen model is based in the one described in [9]. The essential distinction between that metric and ours is that this novel metric considers qualifications from other nodes assigning more importance to the most recent ones. Trust for node a will be calculated as:

$$Trust(a) = \frac{R_Q(a)^{1+R_P(a)} - 1}{R_Q(a) - 1}. \qquad (3)$$

Trust-Based Routing Algorithm

To send a package between two peers it is necessary to find the appropriate path for the message in order to reach its goal with the highest probability of success. Once the path is selected, the message is sent. The algorithm proposed in this paper identifies the best path for a message based in

three factors: reputation of nodes, distance between them and integrity of the wireless connection.

The strength of the wireless connection between two nodes A and B is expressed by the signal-to-noise ratio (SNR). The connection between these two nodes has a score $Score_{AB}$ which is calculated as a weighted sum of the distance between them d_{AB} and the stregth of the signal SNR_{AB}, with $\lambda \in [0,1]$ a scalar between zero and one according to Equation (4).

$$Score_{AB} = \lambda \cdot SNR_{AB} + (1-\lambda) \cdot d_{AB} \qquad (4)$$

The pseudocode for the proposed algorithm is the following which returns the most adequate path for a message between two nodes.

Protocol 1: A Trust-Based Routing Algorithm

```
path [ ] ← insert (initial_node);
current_node ← initial_node;
while (current_node ≠ final_node) do
  selected_nodes[ ]← good_neighbours (current_node);
  max_trust ← selected_ nodes[0];
  for j = 0…size (selected_ nodes[] do
   if (selected_ nodes[j] = final_node) then
     max_trust ← selected_ nodes[j];
   else
     if (trust (selected_ nodes[j]) > trust (max_trust)) then
       max_trust ← selected_nodes[j];
  path [ ] ← insert (max_trust);
  current_node ← max_trust;
return path[];
```

Protocol 1 is used for the transmission of a package from an initial node to a final node in a MANET network and returns the path with the highest level of trust for such message.

In the beginning an initialization of the path and current node is performed. After that an iterative instruction is performed while the current node is different from the final node. Inside that loop we identify the good neighbours of the current node using the connection score and for all selected nodes we choose the one with the highest trust. By 'neighbours' of a node we mean all nodes in the network that are one-hop distance from the node. After that selection we include the chosen node into the path and then jump to the node with highest credibility. Finally the function returns the path with the highest level of trust.

Every received message is checked to verify its integrity. In a real-world implementation this could be done by a checksum. Such qualification will go to all nodes that are part of the selected path. Figure 2 shows a transmission between nodes A and B which involves two other nodes as part of the path. Node B after receiving the message rates the three nodes involved in the communication.

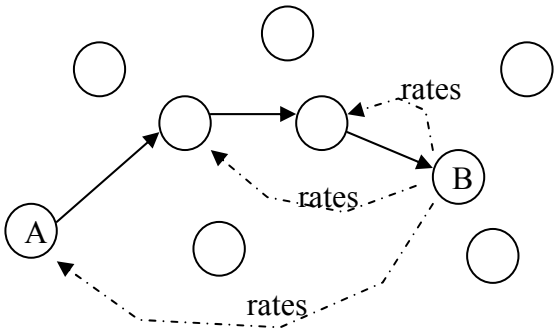

Figure 2. Transmission between nodes.

The reputation of nodes will change depending on their level of participation in number of messages exchanged as well as the integrity of the messages they send to other nodes. Eventually the reputation of peers will tend to represent their level of trustworthiness in the community. The higher the reputation is the better node for communication. A high reputation means that such node is a secure node to transmit messages in comparison with other nodes with lower reputation.

Simulation Results

We simulated several communities with different amount of nodes each. Each peer was given a random position in a two dimension map. The SNR of connections was assigned randomly because it is not necessarily related to distance since obstacles could be placed in the way.

To exemplify simulation we will show the results for a five node community. Every connection between any two nodes has a particular score as shown in Table 1. For simulation we used $\lambda = 0{,}5$ for the score formula described in (4).

Connection	SNR	Distance	Score
N_1 . N_2	13,24	6,25	3,50
N_1 - N_3	3,38	4,44	-0,53
N_1 - N_4	15,83	4,14	5,84
N_1 - N_5	5,65	6,54	-0,45
N_2 - N_3	12,46	6,42	3,02
N_2 - N_4	15,46	6,29	4,58
N_2 - N_5	5,92	4,87	0,53
N_3 - N_4	18,15	8,13	5,01
N_3 - N_5	3,34	9,39	-3,02
N_4 - N_5	2,60	3,39	-0,39

Table 1. Connection scores for a five-node community.

For this five-node community we simulated an event between two nodes (in this case N_2 sends a

message to N_5). The algorithm identified the best path as: N_2 - N_4 - N_1 - N_5. In Figure 3 we show the average bit error ratio (BER) for all paths between those two peers. We can see that any alternative path has a higher average bit error ratio than the one selected by the algorithm which is coloured differently from the rest.

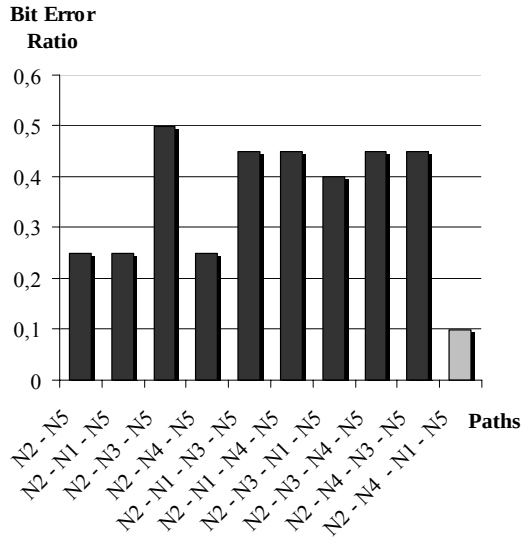

Figure 3. Average BER for paths between two nodes.

To simulate the final BER, each link has a convolutional code with a rate of ½. The mobile channel was set with a frequency of 900 Hz and a velocity of 500 meters per hour. The SNR for every connection is simulated randomly between 0 and 20 dB. The BER for each path is calculated between the message sent by the initial node and the message received by the final node.

Complexity Studies

A comparison of the complexities of other protocol algorithms such as TORA, ILS, the DUAL family, the GB full reversal algorithm, the LMR protocol, the DSDV protocol, and the WRP protocol are shown in Table 2.

These complexity computations are supported by [10] to which the reader is referred for details. Table 2 shows a comparison between Time Complexity (TC), defined as the number of steps required to perform a protocol operation, and the Communication Complexity (CC), defined as the number of messages exchanged in performing the operation.

Protocol	TC	CC
ILS	$O(d)$	$O(2\|L\|)$
DUAL (link failure, cost increase)	$O(x)$	$O(6Dx)$
DUAL (link addition, cost decrease)	$O(d)$	$O(\|L\|)$
DSDV (link failure)	$O(x)$	$O(Dx)$
DSDV (periodic update)	$O(l)$	$O(\|L\|)$
WRP (link failure, cost increase)	$O(h)$	$O(Dx)$
WRP (link addition, cost decrease)	$O(d)$	$O(\|L\|)$
GB (connected, postfailure)	$O(2l)$	$O(lDx)$
GB (disconnected, postfailure)	∞	∞
LMR (connected, postfailure)	$O(2l)$	$O(2Dx)$
LMR (disconnected, postfailure)	$< \infty$	$< \infty$
TORA (connected, postfailure)	$O(2l)$	$O(2Dx)$
TORA (disconnected, postfailure)	$O(3l)$	$O(3Dx)$

Table 2. Complexity comparison.

The complexity parameters mentioned previously are the number of network links $|L|$, the network diameter d, the number of nodes in a network x, the length of the longest directed path in the affected network segment l, the height of the routing tree h, and the maximum nodal degree D.

The routing protocol proposed in this paper has a similar complexity to ILS for it presents a time complexity of $O(d)$ and a communication complexity of $O(2|L|)$. This last value is due to the need of a past-transaction feedback about the reputation of a node in a package transmission. Although the complexity of algorithms such as DUAL is lower, the increase in complexity is minor compared to the enormous benefits reported by the use of ratings over past transactions. The proposed algorithm presents a low complexity accompanied by the identification of reliable nodes in the network which is very valuable for the general security in a wireless network.

Conclusions and Future Work

In this paper, we presented a secure reputation-based protocol that selects paths along nodes with a higher reliability expressed by its reputation and higher signal integrity with reduced complexity compared with other algorithms.

This algorithm ensures that nodes with lower trustworthiness are not selected on the communication paths and eventually be segregated from network operations. This leads to smaller error ratios in the transmission of messages as well as an improved reliability of the chosen paths depending in the characteristic of the channel. A direct consequence is an increased security and effectively in the network in the exchange of packages.

The proposed protocol is a symmetric key distribution scheme between mobile nodes that can be easily implemented due to its low complexity.

A futher step will be the implementation of this protocol in a real-world application. For future work we could incorporate a new security dimension for malicious attacks from intermediate nodes as well as the possibility to compare the reliability of different mobile ad-hoc networks.

Acknowledgements

The authors would like to thank CONICYT/PBCT Project ACT-11/2004 - Chile, and DICYT - Chile, Projects Nº 06-07HC33-OB and Nº 060917SG, for their financial support.

References

[1] C. E. Perkins and P. Bhagwat, "Highly Dynamic Destination Sequenced Distance Vector Routing (DSDV) for Mobile Computers", Proc. ACM SIGCOMM, Oct. 1994, pp. 234-244.

[2] C. Perkins and E. Royer, "Ad hoc On Demand Distance Vector Routing", in Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, Feb 1999.

[3] J. Schneider, G. Kortuem, and J. Jager, Eds., "Disseminating Trust Information in Wearable Communities", Personal and Ubiquitous Computing, Vol. 4, pp. 245–248, 2000.

[4] S. Grajek, P. Lynch and L. Cagnetta, "Why to market IT services and how to do it", Proceedings of the 30th annual ACM SIGUCCS conference on User services, pp. 251–253, 2002.

[5] K. S. Barber, J. Ahn, and S. Budalakoti, Eds., "Agent trust evaluation and team formation in heterogeneous organizations", Proceedings of international conference on Autonomous agents and multi-agent systems, pp. 1361–1362, 2007.

[6] M. Klusch, "Information agent technology for the Internet: A survey", Data and Knowledge Engineering, Vol. 36, pp. 337–372, 2001.

[7] H. Dahshan and J. Irvine, "Authenticated Symmetric Key Distribution for Mobile Ad Hoc Networks". 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems, 2008.

[8] A. Schlosser, M. Voss, and L. Brückner. "Comparing and Evaluating Metrics for Reputation Systems by Simulation". Proceedings of the IEEE Workshop on Reputation in Agent Societies, 2004.

[9] Y. Ren, A. Boukerche, "An Efficient Trust-Based Reputation Protocol for Wireless and Mobile Ad Hoc Networks: Proof and Correctness". Proceedings of the IEEE GLOBECOM, 2008.

[10] V. Park and M. S. Corson, "A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks", Proc. IEEE INFOCOM '97, Kobe, Japan, 1997.