ATM: Automated Trust Management for Mobile Ad-hoc Networks Using Support Vector Machine

Wenjia Li, Anupam Joshi and Tim Finin
Department of Computer Science and Electrical Engineering
University of Maryland, Baltimore County (UMBC)
Baltimore, MD 21250
{wenjia1, joshi, finin}@cs.umbc.edu

***Abstract*—Mobile Ad-hoc NETworks (MANETs) are extremely susceptible to various misbehaviors and a variety of trust management schemes have been proposed to detect and mitigate them. Most schemes rely on a set of pre-defined weights to determine how the extent of each misbehavior is used to evaluate the trustworthiness. However, due to the extremely dynamic nature of MANETs, it is not possible to determine a set of weights that are appropriate for all contexts. In this paper, an Automated Trust Management (ATM) system is described for MANETs that uses a support vector machine classifier to detect malicious MANET nodes. The ATM scheme is resilient to attempts by a malicious MANET node to hide its nature by varying its misbehavior patterns over time. The performance of the ATM scheme is evaluated via an extensive simulation study and compared with existing approaches.**

***Keywords*-security; trust management; mobile ad hoc network; support vector machine**

I. Introduction

Mobile Ad-hoc NETworks (MANETs) are generally more vulnerable to malicious attacks and random failures than traditional infrastructure-based wireless and wired networks. Node misbehavior is a common security threat for MANETs. To cope with node misbehaviors in MANETs, an *Automated* Trust Management (*ATM*) scheme is proposed to better evaluate the trustworthiness of nodes in MANETs. Unlike the traditional trust management schemes such as [1], [2], [3], [4], the ATM scheme neither uses a fixed formula to calculate the trustworthiness of mobile nodes, nor does it rely on a set of pre-defined weights to punish various misbehaviors at different rates. Instead, an SVM classifier is trained and then used in ATM scheme to determine the trustworthiness of the nodes in an automated manner.

II. Related Work

In the past decade, significant research efforts have been made to address the security needs for MANETs by means of trust management. In [1], Buchegger et al. proposed a protocol, namely CONFIDANT (Cooperation Of Nodes, Fairness In Dynamic Ad-hoc NeTworks), to encourage the node cooperation and punish misbehaving nodes. Michiardi et al. [2] presented a mechanism with the name CORE to identify selfish nodes and then compel them to cooperate in the following routing activities. Patwardhan et al. [3] studied an approach in which the reputation of a node is determined by data validation.

In our previous research work [4], [5] we proposed a *multi*-dimensional trust management scheme for MANETs. In this framework, the trustworthiness of a node is judged from different *perspectives* (i.e., *dimensions*), and each dimension of the trustworthiness is derived from various sets of misbehaviors according to the nature of those misbehaviors. Compared to the previous trust management schemes [1], [3], [6], the multi-dimensional trust management scheme can assess the trustworthiness of mobile nodes in a more accurate manner because it is able to precisely determine whether or not a node is trustworthy in terms of one or a set of specific behaviors that it should conduct, such as cooperativity, normative policy adherence, and honesty. However, each dimension of trustworthiness is still derived from a pre-defined formula with a set of fixed weights, which can not adapt to complicated scenarios or changes in the context.

III. ATM: Automated Trust Management Scheme

In the ATM scheme there are two major functional modules: *behavior data collection* and *trust management* as shown in Figure 1. The output of the behavior data collection module module is the processed behavioral data collected by each node (i.e., *direction* observation) and the behavioral data collected by its neighbors (i.e., *indirect* observation). If the scheme is at the training stage, then the behavioral data will be labeled because the set of misbehaving nodes is pre-defined. In contrast, we use the unlabeled behavioral data at the testing stage.

The trustworthiness of each node is then assessed in the trust management module. In the ATM scheme, we train and then use a SVM classifier to evaluate the trustworthiness of the nodes. The trust management module supports the following two modes for the SVM classifier: training mode and testing mode. In the training mode, several known adversaries exhibiting known misbehaviors are deployed in the network to generate the training dataset so that a SVM classifier can be learned from this dataset. In the testing mode, we randomly choose a set of nodes as malicious nodes. These malicious nodes will behave differently from those in the training mode. This ensures that the adversary models used in the training

This work was partially supported by awards from the Air Force Office of Scientific Research (MURI FA9550-08-1-0265) and the National Science Foundation (0910838).

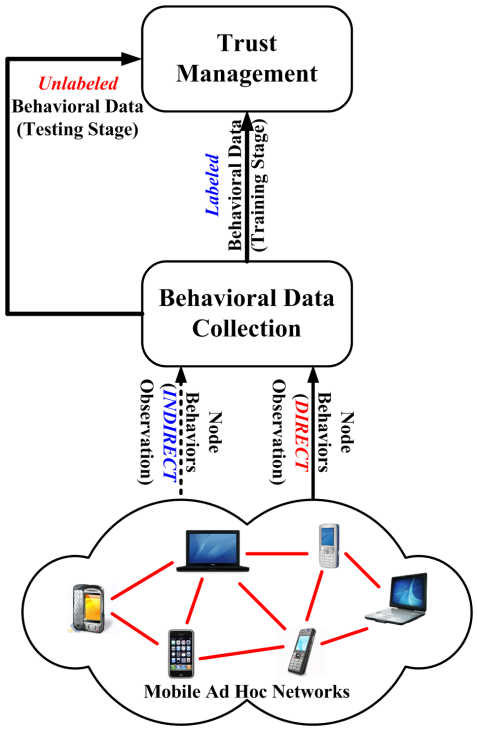

Fig. 1. Our automated trust management scheme has two primary components: behavior data collection and trust management.

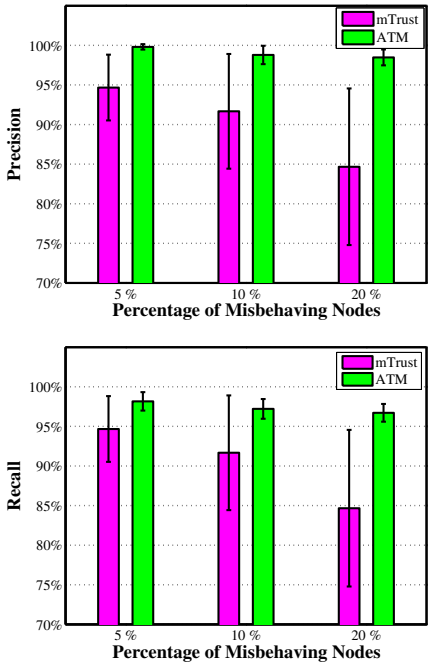

Fig. 2. Precision and recall of ATM vs. mTrust.

mode differ significantly from those in the testing mode, and the algorithm's ability to detect new misbehaviors is tested.

IV. Performance Evaluation and Analysis

In this section, we examine the performance of the ATM scheme and compare its performance to a baseline system – the *multi-dimensional trust management framework* (*mTrust*) discussed in [4]. The *mTrust* framework had been shown to outperform other well-known mechanisms by our prior work [4].

We use GloMoSim 2.03 [7] as the simulation platform . The SVM^{rank} system [8] was used to train the trust management module's classifier. We compute precision and recall measures to evaluate the performance of the ATM system, where precision is the fraction of the nodes judged to be malicious that actually are and recall is the fraction of all malicious nodes that were identified as such. Each simulation scenario has 30 runs with distinct random seeds, which ensures a unique initial node placement for each run. Each experimental result is the average over the 30 runs for this simulation scenario.

The performance of *ATM* is observed and compared to that of *mTrust* when there are different number of misbehaving nodes. The simulation results are showed in the Figure 2. From these results we find that: (1) In general, *ATM* achieves a good performance in terms of proper evaluation of node trustworthiness; and (2) *ATM* outperforms *mTrust* when there are a larger percentage of adversaries.

V. Conclusion

We described an automated trust management (ATM) scheme for MANETs that learn to categorize nodes as malicious or normal using a support vector machine (SVM). The result is a system that assesses the trustworthiness of nodes in an automatic and adaptive manner. Simulation results show that the ATM scheme achieves a good performance and it also outperforms the previous schemes.

References

[1] S. Buchegger and J.-Y. Le Boudec, "Performance analysis of the confidant protocol," in *MobiHoc '02: Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing*. New York, NY, USA: ACM, 2002, pp. 226–236.

[2] 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*. Deventer, The Netherlands, The Netherlands: Kluwer, B.V., 2002, pp. 107–121.

[3] A. Patwardhan, A. Joshi, T. Finin, and Y. Yesha, "A data intensive reputation management scheme for vehicular ad hoc networks," in *Proceedings of the 3rd Annual International Conference on Mobile and Ubiquitous Systems - Workshops, Mobiquitous '06.*, July 2006, pp. 1–8.

[4] W. Li, A. Joshi, and T. Finin, "Coping with node misbehaviors in ad hoc networks: A multi-dimensional trust management approach," in *Proceedings of the Eleventeenth International Conference on Mobile Data Management, 2010. MDM '10.* IEEE Computer Society, May 2010.

[5] W. Li, J. Parker, and A. Joshi, "Security through collaboration and trust in manets," *ACM/Springer Mobile Networks and Applications (MONET)*, pp. 1–11, 2010 (Online First).

[6] G. Theodorakopoulos and J. S. Baras, "Trust evaluation in ad-hoc networks," in *WiSe '04: Proceedings of the 3rd ACM workshop on Wireless security*. New York, NY, USA: ACM, 2004, pp. 1–10.

[7] X. Zeng, R. Bagrodia, and M. Gerla, "Glomosim: a library for parallel simulation of large-scale wireless networks," *ACM SIGSIM Simulation Digest*, vol. 28, no. 1, pp. 154–161, 1998.

[8] T. Joachims, *Making large-scale support vector machine learning practical*. Cambridge, MA, USA: MIT Press, 1999, pp. 169–184.