Ad Hoc Networks 11 (2013) 226–237

Contents lists available at SciVerse ScienceDirect

Ad Hoc Networks

journal homepage: www.elsevier.com/locate/adhoc

Intrusion detection in MANET using classification algorithms: The effects of cost and model selection

Aikaterini Mitrokotsa [a,*], Christos Dimitrakakis [b]

[a] Security and Cryptography Laboratory (LASEC), School of Computer and Communication Sciences, EPFL, Station 14, CH-1015 Lausanne, Switzerland
[b] Artificial Intelligence Laboratory (LIA), School of Computer and Communication Sciences, EPFL, Station 14, CH-1015 Lausanne, Switzerland

ARTICLE INFO

Article history:
Received 20 November 2011
Received in revised form 9 April 2012
Accepted 16 May 2012
Available online 7 June 2012

Keywords:
Intrusion detection
Classification algorithms
Cost-sensitive classification
Mobile Ad-hoc Networks (MANETs)

ABSTRACT

Intrusion detection is frequently used as a second line of defense in Mobile Ad-hoc Networks (MANETs). In this paper we examine how to properly use classification methods in intrusion detection for MANETs. In order to do so we evaluate five supervised classification algorithms for intrusion detection on a number of metrics. We measure their performance on a dataset, described in this paper, which includes varied traffic conditions and mobility patterns for multiple attacks. One of our goals is to investigate how classification performance depends on the problem *cost matrix*. Consequently, we examine how the use of uniform versusweighted cost matrices affects classifier performance. A second goal is to examine techniques for tuning classifiers when unknown attack subtypes are expected during testing. Frequently, when classifiers are tuned using cross-validation, data from the same types of attacks are available in all folds. This differs from real-world employment where unknown types of attacks may be present. Consequently, we develop a *sequential* cross-validation procedure so that not all types of attacks will necessarily be present across all folds, in the hope that this would make the tuning of classifiers more robust. Our results indicate that weighted cost matrices can be used effectively with most statistical classifiers and that sequential cross-validation can have a small, but significant effect for certain types of classifiers.

1. Introduction

Mobile Ad hoc Networks (MANETs) present many important advantages and have been employed in a broad range of applications such as emergency services [16], pollution monitoring [6] and vehicular networks [31]. MANETs are dynamic peer-to-peer networks, which employ multi-hop information transfer without requiring an *a priori* infrastructure. Due to their nature, they have unique security requirements. We must guard not only against usual attacks such as denial of service, but also against selfish and malicious nodes more generally. While intrusion prevention can be used as a first line of defence, these types of attacks cannot be prevented directly. In addition, intrusion detection can be used as a mechanism for indicating possible security failures in the system.

A simple way to perform intrusion detection is to use a classifier in order to decide whether some observed traffic data is "normal" or "abnormal". In the simplest case, the classification objective is to minimise the probability of error. However, in problems such as that of intrusion detection, authentication and fraud detection, the goal is not simply to predict the class with highest probability, but to actually take the decision with the lowest expected cost. For example, in intrusion detection, the cost of having an undetected attack is usually much more severe than triggering a false alarm. In *cost-sensitive* classification, decisions are made in order to minimise the expected cost, rather than the probability of error. The concept of

* Corresponding author.
E-mail addresses: katerina.mitrokotsa@epfl.ch (A. Mitrokotsa), christos.dimitrakakis@epfl.ch (C. Dimitrakakis).

1570-8705/$ - see front matter © 2012 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.adhoc.2012.05.006

cost-sensitive classification has been already investigated in wired networks [26].

This paper examines how to properly use classification methods in intrusion detection for MANETs. We perform a comparison of the performance of four well known classifiers. We extend our previous approach [25] in wireless ad hoc networks, where we only investigated simple classification, to cost-sensitive classification, i.e. making classification decisions that minimise the expected cost, rather than the probability of misclassification, and measure its effectiveness for each classifier under consideration. We also address a common problem in intrusion detection applications: the fact that in real world deployment, the data distribution can be very different from that in the training set. This will for example be the case if new attacks are seen which were not present in the training data. In order to do this, we use a variant of the well-known k-fold cross validation method. This method partitions the training dataset in k parts, and iteratively trains the classifier on $k-1$ parts, while keeping the remainder for validation. This can be used to select classifier parameters that will also have good performance in unseen data. While normally the partition is random, in this paper we also examine a *sequential* partition. Due to our method of data collection, this guarantees that most attacks will only be present in some folds. Consequently, this mimics real-world conditions more accurately, since some attacks will never be present during training. Ultimately, this enables us to make a less optimistic tuning of the classifiers' hyper-parameters and hopefully to a more robust performance. The cross-validation and hyper-parameter selection method is described in detail in Section 4.2. We compare this *sequential* cross-validation method with standard *random* cross-validation both in terms of classification error and in terms of expected cost.

More precisely, the contributions of this paper are the following: (a) Firstly, we perform a thorough comparison of four well-known classification algorithms for intrusion detection in Mobile Ad hoc Networks (MANETs), for both simple and cost-sensitive classification. (b) Secondly, we investigate how the performance of the classifiers is affected if the tuning of the hyper-parameters has been performed with random or sequential cross-validation.

All experiments are reported on datasets produced via extended simulations; consequently the ground truth is always known. We perform an unbiased comparison, whereby we tune the hyperparameters of all five models, using a proper experimental protocol, where the algorithms are tuned before seeing any actual test data.

In all cases, we compare the performance of the classification models under different traffic conditions, including: the mobility of the network, the number of malicious nodes, the sampling interval time (i.e. the amount of time statistics are collected before the classifier makes a decision) and the type of attacks. For the performance comparison we use five well-known and efficient classification algorithms (i.e. MultiLayer Perceptron (MLP), Linear classifier, Naïve Bayes classifier, Gaussian Mixture Model (GMM), Support Vector Machines (SVMs)). For the performance comparison with and without cost-sensitive classification we use four of them since the employment of cost-sensitive classification in Support Vector Machines (SVMs) is not a proper probabilistic model. We have selected features from the network layer for MANET and we investigate the performance of the classification algorithms for four types of attacks (i.e. Black Hole, Forging, Packet Dropping and Flooding attacks).

The remainder of the paper is organised as follows. Section 2 describes the related work while Section 3 describes the quality metrics used for the comparison of the employed classification models. Section 4 describes the simulation environment and the experimental results, while Section 5 concludes the paper.

2. Related work

Intrusion detection is a mature field in network security. While there are many possible approaches, such as rule-based systems [37] and anomaly detection systems [28], this paper focuses particularly on systems based on classification algorithms. In particular, we investigate how these algorithms can be employed most appropriately.

Classification algorithms have been extensively used for intrusion detection, and especially for wired networks. The amount of work reported on for classification-based intrusion detection in wireless ad hoc networks is more limited.

More specifically, Zhang and Lee [39] proposed the first (high-level) Intrusion Detection System (IDS) approach specific for ad hoc networks. They proposed a distributed and cooperative anomaly-based IDS, which provides an efficient guide for the design of IDS in wireless ad hoc networks. They focused on an anomaly detection approach based on routing updates on the Media Access Control (MAC) layer and on the mobile application layer.

Huang and Lee [15] extended their previous work by proposing a cluster-based IDS, in order to combat the resource constraints that MANETs face. They use a set of statistical features that can be derived from routing tables and they apply the classification decision tree induction algorithm C 4.5 in order to detect "normal" versus "abnormal" behaviour. The proposed system is able to identify the source of the attack, if the identified attack occurs within one-hop.

Deng et al. [7] proposed two distributed intrusion detection approaches, based on a hierarchical and a completely distributed architecture respectively. The intrusion detection approach used in both of these architectures focuses on the network layer and it is based on a Support Vector Machine (SVM) classification algorithm. They use a set of parameters derived from the network layer and suggest that a hierarchically distributed approach may be a more promising solution versus a completely distributed intrusion detection approach. Liu et al. [19] proposed a completely distributed anomaly detection approach. They used MAC layer data to profile the behaviour of mobile nodes and then applied cross-feature analysis [14] on feature vectors constructed from the training data. Bose et al. [2] proposed a cooperative and distributed intrusion detection system that uses data from the MAC, routing and application layers, coupled with a Bayesian classifier.