Chapter 13

BANBAD: A Centralized Anomaly Detection Technique for Ad Hoc Networks

Rajeev Agrawal
North Carolina A & T State University, USA

Chaoli Cai
Western Michigan University, USA

Ajay Gupta
Western Michigan University, USA

Rajib Paul
Western Michigan University, USA

Raed Salih
Western Michigan University, USA

ABSTRACT

Anomaly detection is an important aspect of any security mechanism. We present an efficient anomaly detection algorithm, named BANBAD. Using Belief Networks (BNs), the algorithm identifies abnormal behavior of a feature, like inappropriate energy consumption of a node in a network. By applying structure learning techniques to training dataset, BANBAD establishes a joint probability distribution among relevant features, such as average velocity, displacement, local computation and communication time, energy consumption, and response time of a node of the network. A directed acyclic graph (DAG) is used to represent the features and their dependencies. Using a training process, BANBAD maintains dynamic, updated profiles of network node behaviors and uses specific Bayesian inference algorithm to distinguish abnormal behavior during testing. BANBAD works especially well in ad hoc networks. Extensive simulation results demonstrate that a centralized BANBAD achieves low false alarm rates, below 5%, and high detection rates, greater than 95%. We also show that BANBAD detects anomaly efficiently and accurately in two real datasets. The key for achieving such high performance is bounding the false alarm rate at certain predefined threshold value. By fine-tuning at the threshold, we can achieve high detection rate as well.

DOI: 10.4018/978-1-60960-777-7.ch013
INTRODUCTION

Ad hoc network consists of a number of peer mobile nodes that are capable of communicating with each other without a priori fixed infrastructure. However, arbitrary node movements and lack of centralized control make ad hoc networks vulnerable to a wide variety of attacks from inside as well as from outside. It is very difficult to narrow down a single node that has been attacked in a large ad hoc network. Therefore, providing effective security protection is important to ensure the continued viability of these networks in a variety of pursuits.

In general, two complementary approaches exist to protect a system: prevention and detection. Intrusion prevention techniques, such as encryption and authentication, attempt to deter and block attackers. Unfortunately, prevention techniques can only reduce intrusions, not completely eliminate them (Gollmann 1999; Schneier, 2000). Despite the amount or quality of intrusion prevention measures, an intelligent attacker can exploit a single security hole to break into a system. Nothing is absolutely secure. Therefore, intrusion detection systems (IDSs) are indispensable for a reliable system. They serve as the important secondary line of defense.

Intrusion detection can be based either on detecting misuses or detecting anomalies. A misuse-based detection technique checks potential security breaches against known attack signatures and system vulnerabilities. If it finds a match, an alarm is generated. Since it is impossible to know all future attacks-or attack patterns in advance, misuse detection techniques are not effective in detecting new or unknown attacks. Given the constantly evolving nature of security breaches, anomaly-based techniques are needed. An anomaly-based detection technique models normal behavior by creating profiles of system and node states during the training process. During the testing process, it compares deviations from the normal profiles to determine whether a deviation is significant. If so, an alarm is triggered. Therefore, anomaly detection can check a whole host of different and new types of attacks. While misuse detection may be more efficient, anomaly detection is more comprehensive. In a dynamic security environment, a comprehensive technique is highly desirable and considered best. Anything less leaves systems open for attack. Unfortunately, the mobility of nodes inherent in ad hoc network makes profile generation difficult. Therefore, efficiently establishing and maintaining profiles for mobile nodes is crucial. Because of the ad hoc nature of the network, often availability of complete data is not possible; therefore a technique handling incomplete data is desired. The proposed BANBAD technique addresses these issues.

Intrusion Prevention Systems

Data encryption and authentication are two primary methods, and play an important role for intrusion prevention techniques. The basic idea behind such techniques relies on key management. Li, He, & Fu (2006) propose a static key management strategy, in which a key pre-distribution scheme is designed using the bivariate t-degree polynomial in a hexagonal coordinate system for the expected locations of the sensor nodes. By comparing with the square-based polynomial pre-distribution scheme, Liu & Ning, (2003) show that their scheme can improve the effectiveness of key management in terms of the probability of key establishment, and can extract appropriate security threshold with different polynomial degrees in sensor networks. In addition to static key management scheme (KMS), another type of KMS is the dynamic KMS in which keys can be updated periodically or on demand as a response to node capture. By performing key update, the compromised nodes are segregated and the network security can be enhanced. Li, He, & Fu (2007) propose a group-based dynamic key management scheme in wireless sensor networks without the requirement for a fixed infrastructure such as...