Chapter 8
Security in Mission Critical Communication Systems:
Approach for Intrusion Detection

Karen Medhat
Cairo University, Egypt

Rabie A. Ramadan
Cairo University, Egypt

Ihab Talkhan
Cairo University, Egypt

ABSTRACT

This chapter introduces two different algorithms to detect intrusions in mission critical communication systems to guarantee their security. The first algorithm is a classification algorithm which applies the concept of supervised learning. The second algorithm is a clustering algorithm which applies the concept of unsupervised learning. The algorithms detect intrusions using a set of detection rules that are structured in the form of decision trees. The algorithms are described in details and their results on well-known dataset are introduced. An enhancement for the J48algorithm is also introduced, where the decision tree for the algorithm is changed to a binary tree. The change enhances the complexity to reach a decision. The chapter includes a brief introduction about the security in Mission critical systems and the reason behind securing such systems. It introduces different methodologies that were introduced to detect intrusions in wireless communications.

INTRODUCTION

A mission critical system is essential to the survival of a business or organization. When a mission critical system is attacked or failed, business operations and organizations are significantly impacted. For some governmental organizations and some IT sectors, databases are considered as Mission Critical systems. For the internet applications, servers are considered as Mission Critical systems. For public

DOI: 10.4018/978-1-5225-9866-4.ch008

safety organizations, the systems must be reliable and available around the clock to guarantee instant responses in order to save lives. The security in mission-critical systems and wireless communications has attracted a great attention, especially with its rapid development. Security considerations in mission critical systems and wireless communications act as a challenging research area due to the increase of security-critical applications in which a reliable intrusion detection mechanism is needed. Mission-critical communications are extensively used by public safety responders and organizations where connections and communications have to be done reliably and instantly. Public safety organizations also use the Mission Critical systems to monitor major crime and large scale disasters. The mission Critical systems have three main elements:

1. Interoperability where the communications can be taken instantaneously with different organizations.
2. Critical Networks which offers security to the users of the system.
3. Mission Critical data where the important data needed to secure the network can be easily accessed.

The reliability in Mission Critical Systems is highly needed for the survival of the purpose that they are built for. Securing these systems from attacks increases their reliability greatly. Thus, the security in Mission Critical Systems is one of the important concerns to be addressed in those systems. One of the security issues to be addressed is to detect the intrusions that may attack the devices used in the communications as intrusions can greatly affect the performance of the Mission critical systems or may do unwanted manipulation with the critical data sent over the network. The real-time security monitoring for the Mission-critical systems is highly recommended to protect these systems.

In this chapter, an intrusion detection paradigm is introduced. This paradigm introduces an unsupervised learning algorithm and a supervised learning algorithm to detect intrusions. The algorithms can be embedded in the devices used in the Mission critical systems to detect intrusions. Each one of the algorithms builds a set of the intrusion detection rules. The intrusion detection rules generated from both algorithms are structured in the form of a binary tree which decreases the complexity of reaching a decision. The proposed algorithms provided a high detection accuracy using only 10% of the data for training in addition to less number of features, compared to previous work for intrusion detection, which decreased the complexity and the processing time. An enhancement for J48 classification algorithm is also proposed which decreases the size of the algorithm's decision tree and makes it suitable to be used for intrusion detection in memory constrained devices that are used in mission critical systems.

Background

In order to protect the Mission-Critical systems, there must be a real-time security monitoring systems as these systems can't tolerate any faults. An example of the real-time monitoring services is the one offered by Motorola (MOTOROLA, 2015). Motorola's Security Monitoring service depends on five main concepts. The first is to identify the parts of the system to be monitored. The second one is to protect the system with continuous monitoring of the system's activity. The third one is to detect all the anomalies or the attacks that can threaten the system. The fourth one is to respond by taking corrective actions for the detected threats. The fifth is to recover the system from the attack to a restoration point. Alcatel-Lucent (Alcatel-Lucent, 2013) delivers a Mission-critical communications networks for public safety. They introduced IP/Multiprotocol Label Switching (MPLS)-based communications network for public safety using next-generation products and advanced management tools.