Chapter 6
Artificial Intelligence Based Intrusion Detection System to Detect Flooding Attack in VANETs

Mannat Jot Singh Aneja
Thapar University, India

Tarunpreet Bhatia
Thapar University, India

Gaurav Sharma
Université libre de Bruxelles, Belgium

Gulshan Shrivastava
National Institute of Technology Patna, India

ABSTRACT

This chapter describes how Vehicular Ad hoc Networks (VANETs) are classes of ad hoc networks that provides communication among various vehicles and roadside units. VANETs being decentralized are susceptible to many security attacks. A flooding attack is one of the major security threats to the VANET environment. This chapter proposes a hybrid Intrusion Detection System which improves accuracy and other performance metrics using Artificial Neural Networks as a classification engine and a genetic algorithm as an optimization engine for feature subset selection. These performance metrics have been calculated in two scenarios, namely misuse and anomaly. Various performance metrics are calculated and compared with other researchers' work. The results obtained indicate a high accuracy and precision and negligible false alarm rate. These performance metrics are used to evaluate the intrusion system and compare with other existing algorithms. The classifier works well for multiple malicious nodes. Apart from machine learning techniques, the effect of the network parameters like throughput and packet delivery ratio is observed.

DOI: 10.4018/978-1-5225-4100-4.ch006

INTRODUCTION

Vehicular ad hoc networks (VANETs) are the special category of Mobile Adhoc Networks (MANETs). In MANETs the node can move randomly whereas in VANETs the node does not follow the random movement. The nodes simulate like vehicle and move along the direction of roads. Due to increase in population, there has been the exponential increase in the number of vehicles. This increase in vehicles tends to increase the chance of road accidents. According to the survey, there have been 12 lakhs life are lost daily worldwide (Raw et al., 2013). We need to have a mechanism by virtue of which the vehicles can be made smart enough so that they are able to handle the road safety on their own. This concept was the laid under VANETs to provide secure and reliable driving environment. VANETs allow mainly two types of interactions-V2V (vehicle to vehicle) and V2I (vehicle to infrastructure) (Al-Sultan et al., 2014). Apart from these basic interactions, there is yet another interaction that takes care of crucial information like fatigue detection of the driver. This type of interaction is known as intra-vehicular interaction. VANETs have complied with IEEE 802.11p dedicated short range communication (DSRC). The vehicles have the On-Board Units (OBU) which consists of sensors. The communication has to be sent in form of cooperative awareness message (CAM) and has to pass through Road Side Units (RSU) (Alheeti et al., 2015). In VANETs, the OBU is responsible for interacting with outside network which includes other vehicles and roadside unit infrastructure.

VANETs have the huge number of applications. These are safety applications which let other vehicle know about the status of road and can protect some mishap. There is also the user based application which lets the user be entertained on the go where the driver can download some media file or access the weather conditions etc. (Kabir, 2013). VANETs are highly mobile and lack a fixed infrastructure. There is no guarantee of the end to end connection. The auto-configuration adds to its demerits. With the huge number of applications some involving life-saving applications; there are few challenges associated with VANETs such as high mobility, scalability and fault tolerance. Among these challenges, the most crucial is the security. There are two types of solutions to tackle these attacks- cryptography-based solutions and Intrusion Detection Systems (IDS). In this chapter, we have used IDS based solutions as cryptographic solutions do not prove to be robust while determining the new type of attacks and are also resource intensive. There are various types of attacks that can arise due to vulnerabilities in VANETs. We have focused on RREQ Flooding attack as it forms basis of various other attacks like distributed denial of service (DDoS) (Shrivastava et al., 2010) in which an intruder node tries to send multiple numbers of route request messages to a node which does not exist thereby consuming the channel that was supposed to be dedicated to a legitimate node for service. Security is the indispensable component in any industry or in any field. We need security as it gives the sense of surety of wellness. The vehicular networks also need to be secured. The ill effects could also lead to loss of life. There has been a lot of research in the field of security but still, there are lots of demerits, so there is a need to have the research go on in the field of network security especially vehicular networks as driverless cars are trending to become the hot topic in near future.

The remainder of the paper is organized as follows. Section 2 discusses the work done in the related field by various researchers. Section 3 gives an outline of Intrusion Detection System. Section 4 gives an overview of Artificial Intelligence techniques. Section 5 explains the proposed work. The results and conclusion part is covered in Section 6 and 7 respectively.