Chapter 11
Traffic Analysis of UAV Networks Using Enhanced Deep Feed Forward Neural Networks (EDFFNN)

Vanitha N.
Avinashilingam Institute for Home Science and Higher Education for Women, India & Dr. N. G. P. Arts and Science College, India

Padmavathi Ganapathi
Avinashilingam Institute for Home Science and Higher Education for Women, India

ABSTRACT

The world is moving to an autonomous era. Autonomous vehicles take a major role in day-to-day activity, helping human personnel do work quickly and independently. Unmanned aerial vehicles (UAVs) are autonomous vehicles controlled using remotes in ground station by human personnel. These UAVs act as a network that plays a vital role in the digital era. There are different architectures of UAV networks available. This chapter concentrates on centralized UAV network. Because of wireless and autonomy characteristics, these networks are prone to various security issues, so it's very important to monitor and analyze the traffic of the UAV network in order to identify the intrusions. This chapter proposes enhanced deep feed forward neural network (EDFFNN) in order to monitor and analyze the traffic of the UAV network to detect the intrusions with maximum detection rate of 94.4%. The results have been compared with the previous method of intrusion detection.

INTRODUCTION

Unmanned Aerial Vehicles (UAV) systems or drones plays a vital role in recent days, which can fly autonomously or it can be functioned remotely. Due to the high mobility of drones they have been widely used for a lot of applications like military, search and rescue operations, health care, delivery, monitoring etc. Ad-hoc networking between UAVs or drones (FANET- Flying Ad-hoc Networks) can solve the

DOI: 10.4018/978-1-5225-9611-0.ch011

problems that arising from the infrastructure-based UAV network. Because of lot of applications the communication between UAVs are very important, so it is vital to have the communication architecture for creating a UAV networks. These Communication architectures prone to various cyber-attacks, it is mandatory to have an Intrusion detection systems (IDS) to detect the cyber- attacks on those architectures. IDS performances are essential in cyber security. This paper aims to introduce the Intrusion detection systems (IDS) for centralized Unmanned Arial Vehicle (UAV) assisted Vehicular ad-hoc network (VANET) architecture having U2V/V2U communication. This chapter concentrates on the Centralized UAV networks assisted VANET architecture. Network Intrusion Detection System (NIDS) shields a network from nasty software attacks. Traditionally, there are two forms of NIDS according to the strategies to detect network attacks. At first, signature-based detection, compares new data with a knowledge base of known intrusions. Regardless of the state of affairs that, this method cannot spot new attacks, this ruins the most widespread tactic in commercial intrusion detection systems. Latter, anomaly-based detection, compares new data with a model of standard user behavior and marks a significant deviation from this model as an anomaly using machine learning. As a result, this approach can detect anomaly-based attacks that have never been seen before. The anomaly-based detection approach is usually combined with flow-based traffic monitoring in NIDS. Flow based monitoring is based on the information which is existing in the packet headers, so flow-based NIDS have to handle a lower amount of data compared to a payload-based NIDS. This exertion builds a Deep Neural Network (DNN) model for an Intrusion detection system and train the model with simulated dataset. (Hichem Sedjelmaci, 2017)

Applications

UAVs or drones have a countless imminent to build abundant applications in military and civilian domains. Applications include,

Military

- Military men and women are protected by drone anytime; they will be armed with live video remote communications to ground troops, essential gear, or weapons.
- The main drone use overseas in war zones is reconnaissance of unknown areas/buildings, adversary tracing, and force defense (making sure our crowds are safe and no one is approaching them).
- Drones are a very good searching tool for lost or injured soldiers as well as a real-time view of various situations and missions, allowing for commanders to make better decisions in resource allocations.

Civilian

Applications of Civilian contains, Healthcare, Filmmaking, Archaeology, Cargo transport, Conservation, Hobby and recreational use, Journalism, Law enforcement, Scientific research, Search and rescue and Surveillance.