AN INTRUSION DETECTION SYSTEM IN A SELF-DRIVING CAR

Security System

Tithal Bhandari
Roosevelt University

DOCUMENT PURPOSE

This document is prepared to provide an abstract of the project that I would be working during the Spring-2016 Semester.

INTRODUCTION

This document covers the scope of the project. It provides a brief overview of what the project on wireless intrusion is all about and how we have used the concept of IDS using VANETs to generate securable information for business purpose.

PROJECT OVERVIEW

Imagine getting in your car, writing or talking an area into your vehicle's interface, then giving it a chance to drive you to your destination while you read a book, surf the web or rest. These things are now possible by huge innovation of artificial intelligence – Self Driving Car. The project is about changing the world for people who are not well-served by transportation today. There is each motivation to trust that self-driving autos will decrease recurrence and seriousness of mishap by 90-95%.

Basically, there are several parts which play a vital role. First, Lidar radar is used to move into appropriate direction but it is very expensive. Second, Global Positioning System (GPS) is used to show the path of their destination based on satellite communication. Finally, Wireless Tire Sensor, is used to move the car as it takes information from Lidar radar and GPS. However, the system is expensive and safety priority concern, the system is very easy to hack for any kind of attack. Generally, GPS and wireless tire sensor are common and easy victim – in short, Wireless Networks. In this presentation, my concern is to show an alert and warning to system for any unauthorized activities. The presentation will describe the key aspects of how to apply VANETs and generate valuable information from it.

Then again it plays out, these vehicles are coming – and quick. Their full selection will take couple of years, yet their accommodation, expense, safety and different components will make them omnipresent and indispensable.

In this project, I will design and develop a network intrusion detection system using Java programming language. We simulate the some attacks to show the effectiveness of the proposed system in which packets in the network are captured online as they come on the network interface.

WHAT DOES THE INTRUSION DETECTION SYSTEM (IDS) DO FOR A SELF DRIVING CAR?

Intrusion is an unauthorized activities by anonymous person in a network. If in a security system, “Intrusion Prevention,” does not prevent intrusions, then “Intrusion Detection,” comes into play. It is the detection of any suspicious behavior in a network performed by the network members.

There are several types of intrusions in a self-driving car that could occur.

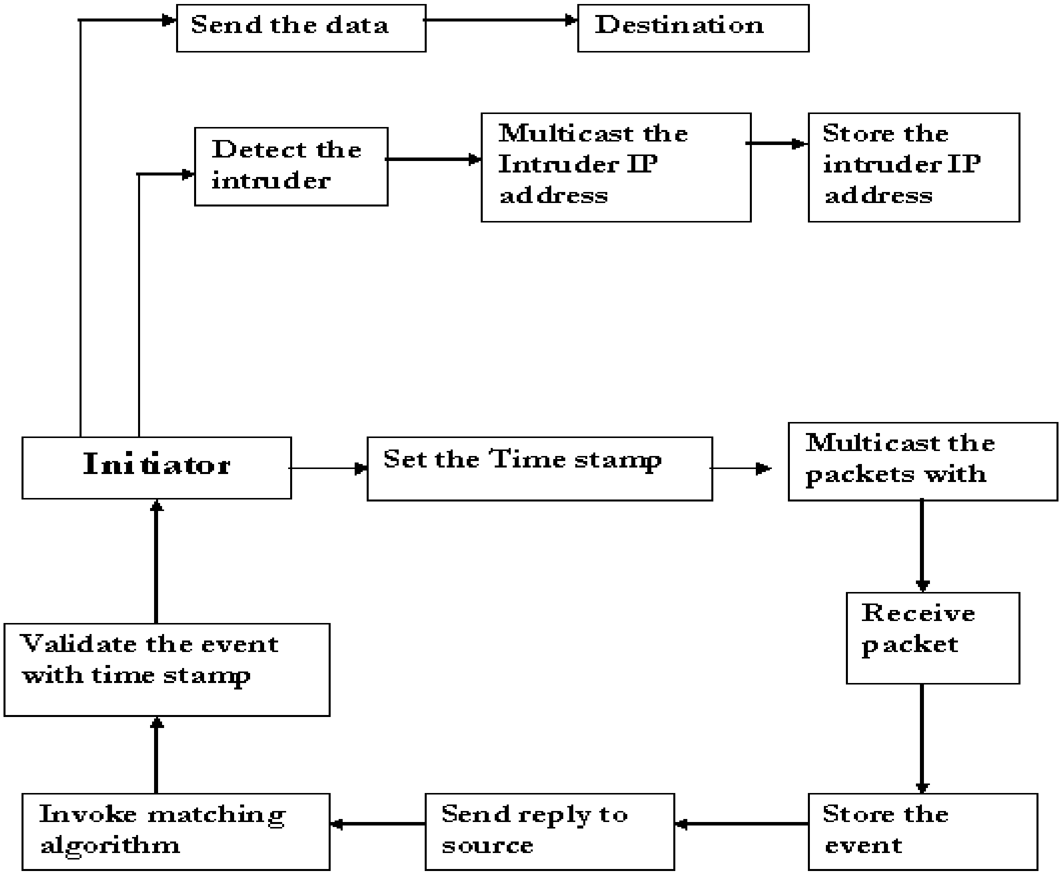
- **Attempted break-in**
- **Masquerade**
- **Penetration**
- **Leakage**
- **Malicious use**

Intrusion Detection System is a gadget or software application that screens system or framework exercises for malignant exercises or strategy infringement and produces reports to an administration station.

Network based Intrusion Detection System has two ways to detect the intrusion.

- **Wired based**
- **Wireless based**

However, the way of versatility makes new vulnerabilities that don't exist in an altered wired system, but a hefty portion of the ended up being inadequate. Therefore, the conventional method for securing systems with firewalls and encryption programming is no more adequate in wireless system.


Send the data
Destination
Detect the intruder
Multicast the Intruder IP address
Store the intruder IP address
Initiator
Set the Time stamp
Multicast the packets with
Receive packet
Validate the event with time stamp
Invoke matching algorithm
Send reply to source
Store the event

INTRUSION DETECTION SYSTEM FLOW CHART

Wireless Sensor Networks (WSNs) have engaging elements, because of the absence of a physical line of barrier the security of such systems is a major concern, particularly for the applications like safety concern where classification has prime significance. In this manner, keeping in mind the end goal to work WSNs security, any sort of interruptions ought to be recognized before attacker can hurt the system and/or data destination. Wireless Intrusion Detection Systems can determine advanced checking and reporting capacities to recognize attacks against wireless base, while stopping multiple classes of attack before they are successful against a network. Therefore, we required IDS in a self-driving car project.

WHAT CAN VEHICULAR AD- HOC NETWORKING (VANET) DO?

Nowadays, Vehicular ad hoc networking (VANETs) have turned into an imaginative innovation because of the rising era of self-driving autos, for example, Google self-driving cars. VANETs are working same as Mobile Ad-Hoc networking (MANETs). VANETs have more vulnerabilities compared to other networks such as wired networks, because these systems are an autonomous vehicles and there is no fixed security development, no high element topology and the open wireless medium makes them more vulnerable to attacks. It is essential to design new technics and approaching to rise the security these networks and protect them from attacks. In this paper, we design an intrusion detection mechanism for the VANETs. In this paper, we propose network based detection to detect the attack.

EXISTING SYSTEM

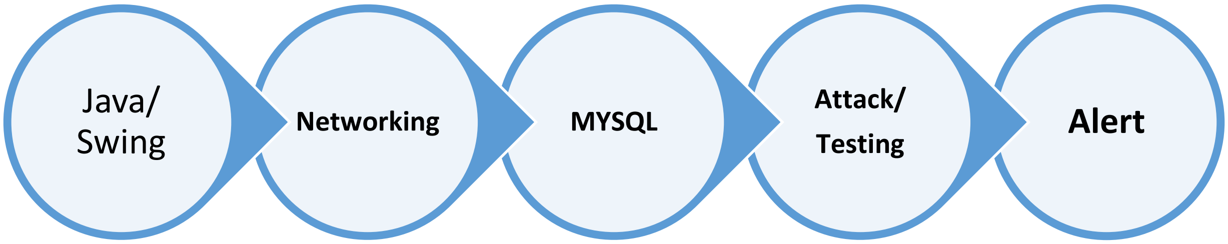
In the existing system, the packet with a new behavior can easily pass without being filtered. The behavior of packets in a network could not able to take decision. So they purely work in the basic method. Moreover, If the any pattern of packets are not given in the record, then it allows the packets to flow without analyzing whether it is an intruder or not.

PROPOSED SYSTEM

In the proposed system, Intrusion Detection Systems (IDSs) that are proposed for WSNs is presented. Firstly, IDSs will detect the intrusion in a wireless network and will not allow to pass any unauthorized packets to receiver. Secondly, IDSs proposed for Vehicular Ad-Hoc Networks (VANETs) is presented and applicability of those systems to WSNs presented. It uses matching algorithm. This is followed by the analysis and comparison of each scheme along with their advantages. Finally, IDSs will take decision in runtime for behavior of the packet.

PROCESS FLOW

The Workflow given below is about how the Project model is going to be built and is subject to change based on the progress of building the queries and any complexities application.



- Create IDS program.
- Create nodes and informative substances.

- Making interface between nodes.

- Connection between database and system
- Send the packets from Sender to Receiver

- Use appropriate module to check the system.

- Throws a notification to System.