Design of an autonomous car essay

PREFACE

“ The beginning of knowledge is the discovery of something we do not understand.” Frank Herbert (1920-1986)

Autonomous systems play a significant role in developing and deploying modern technology [1]. These systems such as driverless vehicles, self-driving vehicles, and Unmanned Aerial Vehicles (UAVs) all have contributed significantly to scientific research, wars, reconnaissance and intelligence [1]. Furthermore, they have had a direct and positive impact in promoting and supporting the scientific revolution.

According to the statistics of many international organisations such as World Health Organisation (WHO) more than 1. 24 million people die and in road accidents every year all over the world, in addition to 20 to 30 million nonfatal injuries [2]. The number of deaths and injuries is expected to increase by 65% in the next two decade [3]. These figure of deaths and injuries are caused by the drivers’ mistakes (human errors) through driving and travelling on the roads [4]. These problems are fixed by one of the applications of the autonomous systems which is autonomous vehicles, sometime called self-driving, driverless or robotic cars [5].

1. 1 Introduction

Autonomous or robotic cars (for example, Google’s robot cars) are considered one of the most significant applications of autonomous systems; that is why we have selected them for our research. These vehicles can promote the safety of road users, whether drivers or passengers, and they

can also have many positive economic impacts on society [6]. They have the ability to reduce the number of accidents and traffic jam on the busy roads. In addition, one economic issue of these self-driving vehicles is the ideal use of the narrow roads through the application of the platoon behaviour [6]. Figure 1. 1 below explains the platoon in self-driving vehicles. Hence, they can establish safety environment for passengers, drivers and vehicles themselves. Primarily, three key technologies are needed to enable autonomous or semi-autonomous vehicles to function: an embedded processor, an array of sensors and a communication system (internal and external) [1].

Figure 1. 1 Platoon in Autonomous Vehicles.

Self-driving and semi self-driving vehicles depend largely on communication systems, whether internal or external, to predict events and sense their external environment used in their moves. The moving/stopping decision of vehicles depends on data and information that have been collected by the sensors and from On-Board Units (OBU).

In addition, these communication systems enable autonomous vehicles to achieve their goals, such as traffic management, reducing the number of deaths and injuries from traffic accidents on the busy roads, reduce human errors and achieve the ideal exploitation of available resources [7]. In other words, the autonomous vehicles can achieve their tasks without human intervention [8]. These vehicles need wireless communication systems to connect vehicles with each other and with their infrastructure on the road side. This network enables the vehicles to exchange necessary information,

warning notification, data control and Cooperative Awareness Messages (CAMs).

All studies have shown that the external communication system used in self-driving or semi self-driving vehicles are vehicular ad hoc networks (VANETs) [9], [10]. The VANETs are mobile nodes that allow vehicles to communicate with each other in a particular zone as well as with RSUs in the absence of a fixed security infrastructure that is used in traditional networks such as a wired network [11]. In addition, VANETs are considered a subclass or subtype of mobile ad hoc networks (MANETs) [12]. They have a direct influence on the Intelligent Transportation Systems (ITS) by providing safety applications and comfort services to drivers and passengers. The goal of VANETs is to provide safety to road users and the vehicles themselves. Hence, VANETs are vital now and in the future because it eliminates time and space constraints and makes information available when it is required for autonomous vehicles [13]. These networks can achieve their goals via an exchange of CAMs, control data, and they provide comfort and emergency notifications to passengers and drivers such as messages regarding emergency braking or accidents [14], [15]. Furthermore, the networks have the most critical role in self-driving and semi self-driving vehicles.

VANETs are exposed for many security and privacy problems because of their unique characteristics that distinguish them from other wireless networks such as: high dynamic topology, the enormous number of vehicles on roads, open medium wireless communication, speed, lack of traditional fixed security stations and high mobility [16]. Unfortunately, the VANET is exposed to many attacks such as network, application and social attacks.

Moreover, these security problems are reflected directly and negatively on the performance of self-driving and semi self-driving vehicles.

The VANETs create new threats to self-driving and semi- self-driving cars that contribute to substantial challenges in providing safety environment of autonomous system. These communication systems render driverless vehicles vulnerable to many types of attacks, such as Denial of Service (DoS), black hole, grey hole, dropping and flooding, wormhole and Sybil attacks [17].

Recently, research has revealed that the external communication systems in self-driving and semi self-driving vehicles have experienced problems with these security and privacy systems [18], [19]. Thus, it is anticipated that there will be a gradual increase in the number of security and privacy problems with these vehicles. Hence, the autonomous vehicles will be exposed new security problem unless significant changes to the security design of autonomous cars are made. There is substantial scientific evidence that current security mechanisms are not sufficient or efficient to protect the external communication employed in self-driving vehicles [20].

Employing VANETs in autonomous vehicles makes the success of this new generation of technology dependent on the security of the networks. Today, security in most systems is based on the concept of defence in depth, as is the use of multiple layers of defences to prevent adversaries from violating security policies of these systems. Intrusion Detection Systems (IDS) offer a second layer of defence for the VANETs [21]. Intrusion detection techniques focus on the detection/identification of malignant activity that normally is an

attacker. It is able to penetrate the system and steal sensitive data such as velocity, position and identification (ID).

Despite the application of the security approaches, including access control and authentication services to improve the protection of the networks, these defences mechanisms alone are not sufficient to deter and block all types of attack, especially internal attacks in VANETs. They are still in need of additional protection systems, such as IDS, to increase their security.

In this thesis, a novel intelligent intrusion detection system are proposed which could protect the external communication of self-driving and semi self-driving vehicles from any potential attacks. However, the proposed security systems have the ability to detect and block internal and external attacks that would have a direct and adverse impact on the appearance of these vehicles.

The proposed IDS uses the features extracted from the network as auditable data have been generated from network simulator. An IDS that utilises two types of detection – anomaly based detection and misuse based detection to detect the malicious or aggressive vehicles. A hybrid IDS is designed and implemented to detect differences of attacks on VANETs. The proposed IDSs in this thesis are divided into six parts.

The first part: IDS is based on the features extracted from trace file that has been generated from the network simulator version two (ns-2) to detect the malicious vehicle. It has the ability to identify four types of attack: DoS, black hole, grey hole and rushing. In this proposed IDS, artificial techniques are employed in designing the security system such as: Feed-Forward Neural

Network (FFNN), Support Vector Machine (SVM), k-nearest neighbours (k-NN), Linear Discriminant Analysis (LDA) and Quadratic Discriminant Analysis (QDA).

The second part: The proposed IDS uses the latest Integrated Circuit Metric (ICMetric) technology to detect both internal and external attacks on external communications in self-driving and semi self-driving vehicles. The ICMetric technology uses internal features of a vehicle to generate an identification called an ICMetric. It can be used to provide services related to authentication and attack detection. The ICMetric generation is an automated process and does not need user intervention. It is generated when required and discarded there after thus reducing the chances of identity perversion.

The third part: Fuzzy Petri Net (FPN) is utilised in designing an intelligent IDS to secure the communication system of driverless and semi driverless vehicles. The proposed detection system is based on the interval of beacons (time) that is generated from the vehicles in the platoon behaviour. It is usually considered one of the most important aspects of a new generation of vehicles. In the platoon, the vehicles create a convoy which has many benefits such as reducing cost and enhancing connection performance. FPN-IDS is considered a novel detection system because this is the first time an FPN is employed in designing an intelligent security system for VANETs.

The fourth part: Mobile-IDS is proposed to secure the external communication system for autonomous vehicles. It is based on a virtual layer to sniff or eavesdrop data and information that is sent/transferred between

vehicles and RSUs to detect different types of DoS attack such as flooding and drooping. The proposed IDS was installed on the buses to detect abnormal/ malicious behaviour as well as it introduced in an urban area.

The fifth part: The distributed IDS is based on Trust Third Party (TTP) as like central dataset to register the position, time and ID for each vehicle on roads to detect Sybil attacks. In addition, Sybil attack is a leading cause of many types of other attacks such as node Impersonation and Fabrication Attacks. In other words, the distributed IDS can detect/identify Sybil, Impersonation and Fabrication attacks.

The sixth part: Integrated-IDS has the ability to detect various types of attacks on the external communication system of self-driving and semi self-driving vehicles such as: black hole, grey hole, rushing, flooding, dropping and Sybil attacks. It is based on the position of vehicles and interval beacons that are generated from the vehicles to detect impersonation, Sybil and DoS attacks. To increase the power defensive to the proposed IDS, it was installed on RSUs.

All the proposed intelligent security systems have demonstrated good performance in detecting and blocking the malicious vehicle in VANETs of self-driving vehicles and semi self-driving vehicles. Almost, at least one research paper for each part was published in international conferences and journals. We have formulated a clear research question:

How can we detect an intruder quickly and effectively in the communication networks of self-driving and semi self-driving cars?

A novel quick reaction mechanism, programmed inside the data link layer of the network that enters the victim vehicle in the safe mode, is designed for infected self-driving and semi self-driving vehicles. The mechanism will allow the infected car to communicate directly with the nearby RSU without any intermediary at a suitable time without delay. In other words, when the infected vehicle is unable to connect with neighbouring vehicles in any situation, the car will directly connect to the closest infrastructure on the roadside, for example, the RSU. The safe mode response provides superior response capabilities with improved performance.

Finally, routing protocols influence the efficiency of detection and the selection of stable routers in VANETs. AODV is used in the proposed schemes because it is considered one of the most important protocol in MANETs [28]. The basic AODV has been adapted to reduce communication overhead and enhance the stability of select route between source to destination vehicle. The proposed AODV protocol formally called Vehicle AODV (VAODV) is an effort to improve the network performance by incorporating new routing selection algorithm.

1. 2 Motivations

The designing of self-driving and semi self-driving vehicles is, of course, a great addition to ITS in modern technology. These vehicles try to improve traffic management and provide safety environment to the passengers/drivers. In other words, the target of the autonomous vehicles is to improve security’s passengers and drivers by reducing the number of road accidents and traffic jams caused by human error [20]. Current research

shows that the communication systems in self-driving vehicles have encountered problems with the security and privacy systems [1], [2], [8]. The external communication system of self-driving vehicles inherits security weakness of ad hoc networks. In addition, new security challenges are added to self-driving vehicles because of their unique features of the external communication system such as, fast change topology and an enormous number of vehicles. The proposed IDSs in this thesis address security and privacy issues for the communication system of self-driving vehicles. To sum up, without significant changes to the security design of the autonomous car, we will see a gradual increase in the number of security attacks on these vehicles. There is abundant proof that the current security measures are in sufficient to protect the external communication systems for self-driving and semi self-driving vehicles [21]. The security system, economic impact, safety and privacy are considered key motivations in this thesis. The motivations in this thesis are based on the four following factors:

The Security Factor . The application of VANETs in autonomous vehicles makes the success of this new generation of technology dependent on the security of the networks. Despite the use of the protection approach, including access control and authentication services to improve the security of the networks, these defence mechanisms alone are not sufficient to deter all types of attacks. The security system of self-driving vehicles needs to have some properties such as begin lightweight, robust, fast and efficient and capable of online-detection.

The Economic Factor . Driverless vehicles are considered one of the most significant applications of autonomous systems. Platoon behaviour of these

vehicles plays a vital role in reducing costs through the ideal use of narrow roads. In this case, these vehicles enable the largest number of vehicles on the narrow roads, and this will have an significant economic reflection on the expansion of the road [22].

The Attacks Type Factor. Traditional security systems such as encryption mechanisms are unable to detect all types of attacks on the external communication of autonomous vehicles, especially internal attacks in VANETs. They are still in need of backup protection systems, such as IDS, to increase their security.

The Safety Factor . To save passengers and drivers' lives, self-driving vehicles need to have an intelligent reaction response system which has the ability to introduce an infected vehicle into a safe mode immediately and without delay.

1. 3 Thesis Challenges

A wide range of safety, non-safety applications, traffic management, security and privacy systems have been established for future deployment in external communication of self-driving and semi self-driving vehicles [23]. However, these security systems and services applications faced many challenges that were considered obstacles to developing the VANETs. The high mobility, dynamic change in network topology are considered the most challenging issue in developing and deploying communication systems of autonomous vehicles [11], [24].

Communication System Challenges

The external communication system of self-driving vehicles has characteristics that can distinguish it from others. Unfortunately, these characteristics establish technical and security challenges to deploy the self-driving vehicles. These challenges can be classified into the following categories [24]:

Network Management . The high dynamic change topology, high mobility, velocities make network management a very difficult task in VANETs. In addition, the enormous number of vehicles and the rapid channel changing added extra challenges to VANETs management.

Communication Environment. The wireless medium communication in VANETs creates new threats to security systems in the external communication of autonomous vehicles. Hence, attackers can launch attacks from anywhere and anytime without physical access. This communication environment makes designing and building security systems in the external communication od self-driving vehicles a challenging and complicated task.

Environmental Impact. Electromagnetic waves are utilised in the principle communication system of vehicles. The external environmental factors play an important and direct role in the performance of VANETs. In addition, buildings and mountains have a substantial impact on the quality and strength of the broadcast signal.

Congestion and Collision Control. The congestion and collision occur in VANETs when the traffic load is very high that made communication difficult between vehicles and vehicles with RSUs in that radio coverage area. This challenge has a direct and adverse impact on the performance metrics of

VANETs such as decreasing the amount of Packet Delivery Ratio (PDR) and increasing the amount of dropping packets.

Security Challenges

The distinguishing process between normal and abnormal/malicious behaviour is one of the most complicated issues in VANETs because of the dynamically changing topology and the volatile physical environment. The security challenges can be classified into following categories [13]:

Online Detection . The real-time detection is one of the critical issues in designing security systems. In safety applications, CAMs and data control should arrive at the destination node with 100 *ms* transmission delay. In this point, the intelligent detection system should have the ability to identify and allow sent/received packets between source and target at the suitable time without delay. Any delay will have a direct impact on the life’s passengers and drivers.

High Mobility . The detection system is based heavily on features that have been collected from network behaviour. Moreover, the high mobility in VANETs makes the collection process for type and number of features very difficult. As a result, the designers of security systems need to some technologies to fill the gap that was created by high mobility in VANETs such as fuzzification.

Traditional Security Systems. The conventional security systems are unable to provide sufficient security to the communication system of self-driving

vehicles. In this case, VANETs need to design and build a new security system or modify existing protection systems.

Internal Attacks. All encryption algorithms can detect and prevent the external attacks. Unfortunately, these algorithms are unable to prevent internal attacks that have a negative effect on VANETs. This encourages researchers to create and find security systems which can detect and prevent attacks on VANETs such as intelligent IDS.

These challenges should be taken into account of designers to avoid problems that were caused in creating security obstacles. In this thesis, a novel intrusion detection system is proposed to overcome these key challenges.

1. 4 Problem Statement

Communication systems are considered one of the fundamental components in the development and existence of autonomous systems such as driverless cars. Research has shown that autonomous vehicles have encountered problems with the security of their communication systems [1]. Moreover, the use of ad hoc wireless networks for these vehicles has added new threats as they have increased the vulnerability of the communication systems [25]. Vehicular communication differs from other wireless communication networks because of the high mobility involved and the rapidly changing topology that makes security a huge challenge in self-driving vehicles. Protection of these networks and the creation of new security mechanics will increase the development and promotion of autonomous vehicles [26].

VANETs have incorporated some of the characteristics that have made them susceptible to many security attacks. These properties are [27]:

An open communication medium.

A highly changeable topology.

Cooperative communication algorithms.

The absence of fixed security infrastructures.

Lack of centralised point whether management, defence and monitoring.

High mobility.

Unfortunately, such characteristics represent the vulnerabilities of the VANETs which make them easy to penetrate by the attacker. The security of these networks is vital as, in the case of malicious behaviour involving just one vehicle, the entire system will be paralysed which will affect all other vehicles in that particular zone, for example via DoS attacks. These attacks will prevent communication between all the vehicles in that radio coverage area. The deployment and evolution of self-driving vehicles are dependent on providing security for all the system components. One such component is the communications system. 1. 5 Thesis Aim and ObjectivesThe aim of the invention of self-driving cars is to reduce the number of accidents and traffic jams caused by human errors on busy traffic roads. These vehicles cannot predict the road conditions so they need to be able to exchange data and CAMs with other vehicles and with RSUs. In other words, the movements and actions of self-driving cars depend heavily on the data control and sensitive

information that are collected from the external environment (gained information). In this scenario, the accuracy of the data exchanged between vehicles and RSUs has a significant role and will directly influence the lives of passengers, drivers and the vehicles themselves [26]. One of the most critical issues is the protection of the data control and the data transferred between these vehicles. In this thesis, the aim is to provide intelligent security mechanisms to reduce the number of attacks on the external communication systems (VANETs) to be used in self-driving and semi self-driving vehicles. In addition, the proposed intrusion detection has the ability to protect data and warning messages that were exchanged between vehicles and RSUs. For this purpose, we introduced more than one intelligent IDS to secure the external communication system of these vehicles from the potential attacks. It aims to secure sent/transferred data and CAMs between the source and the destination from any expected attacks. The proposed security system must be able to detect and block various attacks such as DoS, Sybil, flooding, black hole, grey hole, dropping, wormhole and rushing attacks in self-driving and semi self-driving vehicles. In this thesis, the objectives are as follows: Designing an intelligent IDS to secure the external communication system of autonomous and semi-autonomous vehicles. Training and testing the proposed IDS using optimised FFNN, SVM, k-NN, LDA and QDA. Designing an IDS with different detection schemes and architectures. Employing some of the techniques that are used for the first time in building IDS such as FPN and POS in selecting significant features. Detecting and blocking a range of external and internal attacks on self-driving and semi self-driving vehicles and network. Developing a time-efficient system so that the safe mode can be induced in a compromised

vehicle without delay. In other words, designing and implementing a quick response for abnormal scenarios in VANETs. Implementing the detection system using various routing protocols. Creating mobility and traffic model to generate trace file to detect abnormal scenarios. Enhancing performance detection which is increasing detection rate and reducing the number of false alarms by declining the number of features that have been extracted from trace file and Kyoto dataset. Fuzzification, normalisation and uniform distribution of significant features extracted from trace file by using Proportional Overlapping Score (POS) method. Comparison and analysis of the results to show improved detection rates in false alarms. 1. 6 Thesis ContributionsIn this thesis, various intelligent IDSs are proposed to secure the external communication of self-driving and semi self-driving vehicles. The proposed security system has the ability to protect the data control and sensitive information that are sent/transferred between vehicles and RSUs in that radio coverage area. A theoretical basis is incorporated into this thesis to detect and block different types of potential attacks on the communication system. In addition, artificial intelligence techniques are utilised in building and improving the performance of IDS. The major contributions are outlined below: 1. 6. 1 Designing Intrusion Detection SystemDesigning various intelligent IDSs to secure the external communication system for self-driving and semi self-driving vehicles such as FFNN-IDS, SVM-IDS, LDA-IDS, QDA-IDS, k-NN-IDS, BusNet-IDS and Distributed-IDS. Designing IDSs with different detection algorithms, architectural model and artificial intelligence techniques to get a different detection mechanism with different performance metrics values. ICMetric technology is employed in designing novel ICMetric-IDS to secure vehicles communication systems. It is based on

readings bias collected from different sensors, such as accelerometer, gyroscope, magnetometer and ultrasound sensors, which are utilised in designing IDS. Proposing a novel IDS based on FPN. This is the first time FPN was utilised in building IDS for VANETs. It is based on features that are calculated from trace file such as PDR and Drop Packet Rate (DPR). Designing hybrid “ anomaly and misuse” base-detection methods to overcome their limitations. In other words, we make use of the benefits of both types of detection systems by designing hybrid IDS. Designing integrated-IDS to identify various attacks such as: black hole, grey hole, wormhole, Sybil. These attacks are very influential on the performance of IDS. IDS is installed on vehicles and RSUs to provide full safety environment for self-driving and semi self-driving vehicles. The proposed IDS is designed with three architectural of IDS, which are: alone, cooperative and hierarchical. Finally, external and internal attacks are detected and blocked by the proposed intelligent IDS. 1. 6. 2 Improving the Performance of the Detection SystemEnhancing detection rate and reducing the amount of false alarms that was generated from the proposed IDS. In this thesis, we tried to get the best results by using some techniques such as fuzzification, normalisation, uniform distribution, sub validation dataset and POS to select significant features. Creating a new dataset to evaluate performance for the proposed IDS from the trace file that has been generated by ns-2. The network simulator need to traffic and mobility model to generate a trace file that reflects the real communication between vehicles and RSUs. Reducing the number of extracted features to improve detection performance. The elimination of useless features improves the detection rate, decreasing the computation time and memory, hence enhancing the overall performance of

an IDSThe Kyoto data set is used to validate performance detection for the proposed IDS. Significant features are selected from Kyoto dataset to enhance the computation time and memory. 1. 6. 3 Designing a Novel Response SystemDesigning a novel response system to introduce infected vehicles in safe mode at a suitable time without delay to save passenger and drivers live's. Improving the authentication aspect of self-driving and semi self-driving vehicles by generating an ICMetric basis number, which was generated from bias reading of typical automotive sensors. 1. 7 Thesis OutlineThe remainder of this thesis is organised as follows: Chapter Two presents the literature review associated with security in self driving vehicles. The chapter particularly focuses on intrusion detection algorithms and methods being utilised in VANETs. In Chapter two, we will provide an overview of communication systems for self-driving vehicles as well as threats and vulnerability in the external communication system for autonomous vehicles. In addition, the relevant artificial intelligence techniques, detection types and routing protocol employed are reviewed in this thesis. Moreover, the security goals are discussed that should be taken into account when build intrusion detection system. Chapter Three presents our novel intrusion detection system based on readings bias that have been extracted from various sensors in self-driving vehicles. The intrusion detection system uses the latest ICMetric technology to secure data control and sensitive information from the potential attacks. Then, it detects both internal and external attacks on an external communication system of autonomous vehicles. Chapter Four introduces more than one IDS to detect and block various attacks such as, DoS, black hole, grey hole, rushing, wormhole and Sybil attacks. In addition, we will review methodologies,

artificial intelligent technologies, mobility and traffic models that employed in the design intrusion detection. In Chapter Five, a new response reaction mechanism is proposed to introduce the infected vehicle in safe mode at a suitable time to save passenger and drivers life’s as well as vehicles themselves. The safety model integrated with a novel intrusion detection system that based on FPN. This is the first time FPN was utilised in building IDS for VANETs. In Chapter Six, a new integrated intrusion detection system is proposed for detecting various attacks. This system has the ability to detect and block different attacks such as, black hole, grey hole, rushing, flooding, drooping and Sybil attacks. In addition, a novel mobility detection system is proposed that was installed on bus truck to eavesdrop and sniff the information between vehicles and RSUs in that radio coverage area. This IDS represent as like BusNet layer or virtual layer to listen for important messages and sent it to the closest RSUs. Finally, the conclusion is presented in Chapter Seven and discusses some ideas for future work.