An Intelligent Security System for Autonomous Cars based on Infrared Sensors

Khattab M Ali Alheeti, *Member, IEEE*
School of Computer Sciences and Electronic Engineering
University of Essex, Colchester, UK, kmali@essex.ac.uk
University of Anbar, College of Computers-Anbar, Iraq

Klaus McDonald-Maier, *Senior Member, IEEE*
School of Computer Sciences and Electronic Engineering
University of Essex, Colchester, UK
kdm@essex.ac.uk

***Abstract*— Safety and non-safety applications in the external communication systems of self-driving vehicles require authentication of control data, cooperative awareness messages and notification messages. Traditional security systems can prevent attackers from hacking or breaking important system functionality in autonomous vehicles. This paper presents a novel security system designed to protect vehicular ad hoc networks in self-driving and semi-autonomous vehicles that is based on Integrated Circuit Metric technology (ICMetrics). ICMetrics has the ability to secure communication systems in autonomous vehicles using features of the autonomous vehicle system itself. This security system is based on unique extracted features from vehicles behaviour and its sensors. Specifically, features have been extracted from bias values of infrared sensors which are used alongside semantically extracted information from a trace file of a simulated vehicular ad hoc network. The practical experimental implementation and evaluation of this system demonstrates the efficiency in identifying of abnormal/malicious behaviour typical for an attack.**

***Index Terms*— security system, Intrusion detection, autonomous vehicles, ICMetric technology.**

I. Introduction

Self-driving and semi-autonomous vehicles have the potential of improving the safety of passengers. They achieve this by reducing the traffic jams and car accidents which are often a result of human error. Autonomous vehicles exchange Cooperative Awareness Messages (CAMs), warning messages, caution messages, control data and sensitive information with Road Side Units (RSUs) by utilising the communication systems. Vehicular ad hoc networks (VANETs) are the typical external communication system employed in self-driving and semi-autonomous vehicles [1].

The success of this new technology relies on the security of VANETs in driverless vehicles. There are however, some features in VANET which have caused vulnerabilities to the entire communication layers [2]. The external communication system is inherently a complex system due to the highly dynamic topology, speed of the vehicle, mobility, open medium wireless communication, absence of a fixed security system and in some cases, large number of vehicles on roads [2]. In the presence of these complexities, attackers can launch an attack remotely. Overall, the communications in VANET are placed in two types [3]:

- Vehicle to Vehicle Communication (V2V) – when autonomous vehicles create direct wireless communication with one another to form V2V.
- Vehicle to RSUs (V2R) - This represents how information is shared between the self-driving vehicles and their fixed RSUs. This communication is made possible by formation of V2R and is used in monitoring of traffic and management services.

Figure 1 shows an overview of VANETs for autonomous vehicles. The implication of this is that the Intrusion Detection System (IDS) performs the function of identifying and preventing both internal and external attacks on these systems. External communication systems of self-driving vehicles are more prone to attack as compared to other types of networks, for example wired local area networks. This is as a result of lack of stationary security infrastructure; the open wireless medium, and a highly dynamic network topology which exposes this vulnerability to attack [2].

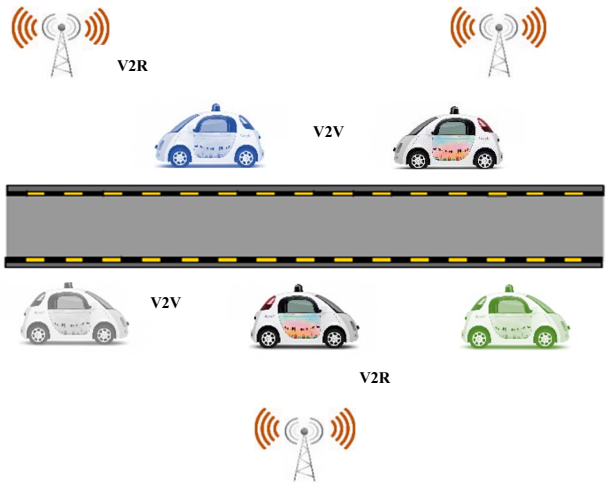

Fig. 1: The External Communication system of Autonomous Vehicles.

An emerging technology known as the Integrated Circuit Metrics (ICMetrics) can be utilised to create a unique identifier for an electronic system [4]. The technology uses measurable features of a device to create an identity (basis number). This paper studies features obtained from infrared sensors' characteristics for driverless vehicles to create a unique identification. ICMetrics can be deployed for the purposes of identification and security, similar to the electronic equivalent of a biometric technology [5].

ICMetric is integrated with IDS in this research and the result shows that it leads to the addition of a new dimension to the current security systems. The ICMetric basis number that is determined from infrared sensors is combined with a traditional IDS to create a new and robust detection system which can be used to secure the external communication of driverless and semi-autonomous cars.

This ICMetric-IDS is proposed to create security system for the external communication system in self-driving vehicles and utilised ICMetric technology to identify outsider and insider attacks and has two advantages:

- It enhances the authentication aspect of autonomous vehicles by establishing an ICMetric generated from bias readings of the infrared sensors.
- Creation of intelligent ICMetric-IDS which depends on the characteristics of self-driving vehicles. The characteristics which show normal or malicious behaviours are extracted from trace files that are generated utilising network simulator version two (ns-2).

The remainder of the paper is organized as follows: related works are discussed in section II, and overview of the VANET in section III. Section IV studies the proposed ICMetric intelligent intrusion detection system whereas section V focuses on the methodology of the proposed security system. The results of the simulation are discussed in section VI. A discussion on the proposed ICMetric-IDS is presented in section VII while the conclusion and future work are presented in the last section.

II. Related Works

There has been a significant interest in the emergence of driverless and semi-autonomous cars which made use of VANETs due to its direct and positive effect on the society. To move and exchange important information among vehicles and RSUs, these vehicles rely extensively on sensing their surrounding environment. The external communication system which is being utilised in these vehicles possess some features that make it vulnerable to different attacks [2].

Chaudhary et al. in [6] proposed a novel intrusion detection which makes use of fuzzy logic to provide security to mobile ad hoc network (MANET). The security system can detect dropping attacks and blocked malicious vehicles from their Internet Protocol (IP) exchanges.

A recent by [3] suggested an intelligent security to protect the external communication of self-driving vehicles from internal or external attacks. It has the ability to detect and prevent grey hole and rushing attacks which could have a negative impact on the safety of passengers. The IDS is based on the extracted features that have been generated from the trace file of ns-2.

In [7], the researchers presented various aspects of the current protection and privacy systems of vehicular internet which performs a vital role in bridging all of the security holes.

In [8], an IDS is presented to provide adequate security to the routing protocol of self-driving vehicles. The system is designed on the network layer for deployment on RSUs and vehicles. It has the ability to provide adequate security to protect data and information from black hole attacks.

The aim of this research is to design an intelligent IDS for external network of vehicles from attacks such as Sybil and two types of Denial of Service (DoS) attacks: 1) grey hole and 2) black hole.

III. Overview Of Vehicular Ad Hoc Networks

Security and privacy are serious issues for VANETs. These vehicles are responsible for sending warning messages and CAMs through open wireless channels to inform other nodes of their status within the radio coverage area. The purpose of sending these messages is to determine the status of the vehicles thus.

The communication configurations of self-driving vehicles are heavily dependent on the correct acquisition of control data and information of both vehicles and the surrounding environment. In more details, they need up-to-date communication protocols, kinematic data, and the help of positioning systems for the reliable and efficient information exchange between them. Sensors, communication systems and On Board Units (OBUs) that work together are placed in self-driving vehicles to provide a wide range of services that is needed by the vehicles and the infrastructure [9].

The communication system permits OBUs-enabled vehicles to send and receive messages to and from other vehicles or RSUs in the same communication zone. There are important roles these devices play in providing short-range wireless ad hoc networks for transmission of the required kinematic data and control data to the vehicular networks. These functions help in facilitating efficiency of traffic and safety on the roads mentioned above [10]. Additionally, Global Positioning System (GPS) or Differential Global Positioning System (DGPS) receivers are fitted into self-driving vehicles to process their position [11].

Other fixed infrastructures such as the Road Side Units are connected to the network backbone and they are installed at vital positions across the roads for reliability effectiveness and efficiency in vehicular ad hoc network. Finally, the network devices are connected to the RSUs to provide support to Dedicated Short-Range Communication (DSRC) utilising IEEE 802.11p radio technology.

IV. Intrusion Detection Systems

Intrusion detection systems are seen as an essential second layer in any security system designed to identify malicious behaviour [12]. These systems play a very important role in the identification of various attacks on autonomous systems. In the traditional security systems, the main concern for instance is that the encryption/decryption does not possess the capacity to identify insider/internal attacks [12].

The IDSs were used in securing sensitive data by making use of prevention mechanisms through access control and authentication methods. This can be categorized as the network-based Intrusion Detection (NID) and host-based Intrusion Detection (HID), according to the source date set collected. HIDs are integrated on computers so that they can monitor an audit trail. Whereas, the NID is based on the data that has been collected from network traffic.

Detection approaches, which include anomaly and misuse detection systems, are employed in the classification of IDS [13]. The detection process of anomaly or behavioural method is based on identifying normal traffic behaviour of driverless vehicles in VANETs. Hence, it has the ability to detect attacks that are active. This is achieved by establishing that the system has significantly deviated from its normal behaviour. When this happens, such behaviour is considered to be abnormal.

The other detection system, known as the misuse or signature detection system is based on predefined data or system vulnerabilities. This detection system simply matches the traffic

pattern with signatures from abnormal behaviour, to detect malicious behaviour in VANETs. The only problem with these systems is that they do not have the capacity to detect novel types of attacks.

On the contrary, with anomaly-based detection system, novel attacks can be detected that have not previously been encountered. The implication of this is that the misuse detection is based on rules instead of patterns and therefore can detect any type of abnormal behaviour in the external communication of autonomous vehicles. With this approach, malicious behavior can not only be detected but it is also capable to detect unknown/new malicious behaviour. Additionally, with anomaly detection system, intrusions can be identified through the misapplication of legitimate users, without breaking security policies [14], [15].

Limitation in anomaly detections systems are a high-false positive detection errors combined with expensive computation load and the difficulty of handling gradual misbehavior [16]. There are many limitations in the misuse detection approach such as inflexibility and the difficulty of updating intrusion signatures rules [15]. The strengths and limitations inherent in both systems mean that an effective IDS should use both signature and behaviour detection simultaneously [16].

The protection system presented here is an anomaly detection system to secure the external communication of self-driving and semi-autonomous vehicles.

V. ICMetric Intelligent Intrusion Detection System

An issue with current defensive mechanisms is that they lack features required for effectively preventing internal attacks in VANET. The purpose of employing ICMetric technology in the design of the proposed system is that it has the ability of using measurable features which have been extracted from the characteristics of a specific embedded system [17]. These features can generate a unique identifier for a specific system. These features are extracted and then normalised to verify their uniqueness and deterministic characteristics. In this paper, the focus in on utilising infrared sensors which are typically found in modern autonomous systems as a basis for device identification.

Infrared sensor bias readings are utilised in designing the proposed IDS. These readings are employed in creating an ICMetric basis number.

The proposed ICMetric-IDS is composed of six stages; Figure 3 shows the overall architecture of the proposed ICMetric-IDS.

- 1st Stage (Generate ICMetric number) – The offset reading is extracted in this stage from the infrared sensors in the autonomous vehicle. Statistical functions are employed in calculating the ICMetric basis number from the extracted reading from the sensor. In addition to this, the hash value is generated from the ICMetric number which will be used in the ICMetric-IDS. Figure 2 below shows the setup hardware which is made up of Infra-Red (IR) sensor infrared module Arduino raspberry PI sensor that is embedded with the infrared sensor.

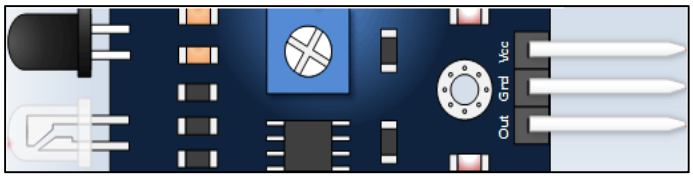

Fig. 2: Infra-Red Sensor.

- 2nd Stage (real-world) – Two software tools are utilised in creating the real-world simulation. These tools are Simulation Urban Mobility (SUMO) and Mobility Vehicles (MOVE) which reflect mobility of vehicles.

- 3rd Stage (feature extraction) – The suggested ICMetric-IDS makes use of just 16 significant features from the whole extracted features space [8]. We also discovered that decreasing the number of features can play an important role to improve the detection rate, decreasing error rate and false alarms.
- 4th Stage (Pre-processing): The important features in this stage performs pre-processing like: a) transmission of some symbols and letters to numbers, b) uniform distribution done to balance both normal and abnormal records to increase the IDS efficiency, c) Values of features that were generated from the trace file are normalised in this stage to make the ICMetric-IDS performance more efficient in detecting and blocking malicious behaviour.
- 5th Stage (Training phase- k-Nearest Neighbours (k-NN)): The employment of k-NN in designing the ICMetric-IDS. The dataset that are extracted in stage three are used in the training phase of the proposed IDS.
- 6th Stage (Testing phase-k-NN): This stage involved the testing of ICMetric-IDS with the extracted features. The detection accuracy rate and four kinds of alarms are also calculated in the test phase. Some criteria are used for measuring the efficiency of k-NN. These criteria include the detection rate, Packet Delivery Rate (PDR), the number of false alarms, and End-to-End delay.

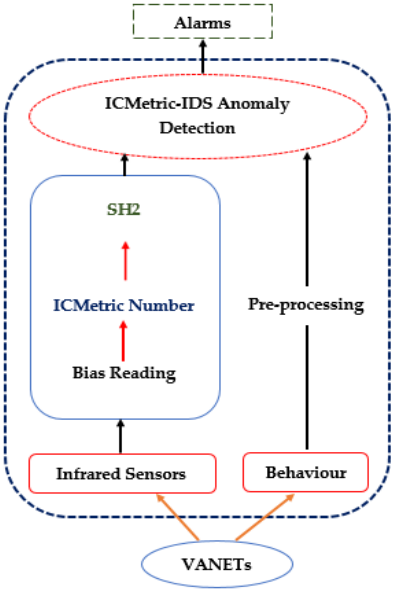

Fig. 3: Overall ICMetric-IDS architectural.

The security system initially assesses the ICMetric basis number from the infrared sensors. The ICMetric basis number is integrated with CAMs that beacon from source vehicle to the destination vehicles in the radio coverage area. The extracted features of the normal / abnormal behaviour require a pre-processing phase to enable easy adaptability with the proposed system. They are then considered as the input to the ICMetric-IDS. Finally, the IDS outputs are then classified as normal or malicious.

VI. Simulation Results

The bias readings which were obtained from the infrared sensors in this experiment are used in the creation of a novel ICMetric-IDS to detect internal/external attacks. To generate the ICMetric number, the bias readings were extracted from three identical sensors and 1000 readings were recorded for three different axes. In the testing phase, the generated readings are utilised to evaluate the anomaly detection for the external communication systems of autonomous vehicles.

To evaluate the performance of ICMetric-IDS, the detection accuracy rate and four kinds of alarms are used. The alarms used for evaluating the proposed IDS are 1) false positive, 2) true positive, 3) false negative and 4) true negative. The detection rate and also the false alarm of the ICMetric-IDS with the traditional IDS are illustrated in Table 1.

Table 1. Detection Rate and False Alarm.

Performance Metrics	Throughput	PDR	Delay
VANETs without-IDS	1.02%	0.05%	23.33*ms*
VANETs with Normal-IDS	78.57%	97.86%	1.47*ms*
VANETs with ICMetric-IDS	79.23%	99.54%	30.56*ms*

Table 1 shows the significant improvement of the ICMetric-IDS in VANETs of autonomous vehicles under different types of attack which possess an average error rate of 6.01%. In Table 2 below, we show the performance metrics of ICMetric-IDS.

Table 2. Performance Metrics.

Performance Metrics	Detection rate		False Alarm
	Normal	Abnormal	
VANETs with Normal-IDS	98.45%	85.02%	12.24%
VANETs with ICMetric-IDS	95.23%	92.74%	3.69%

The proposed ICMetric-IDS and traditional IDS are evaluated under abnormal conditions to evaluate their performance metrics.

VII. Discussion

Self-driving vehicles heavily depend on appropriate security systems for their successful deployment.

Simulation results show that 6.01% is the average error rate of the IDS that uses ICMetric, while the rate of detection varied between 95.23% and 92.74% with efficient accuracy. Furthermore, the result revealed that the average false rate of alarm was about 3.69% which is very low and this is also another indicator that the result is promising.

On the other hand, the rate of detection of the normal IDS ranges between 85.02% and 98.45% while the false alarm remained at 12.24%. The rate of detection was improved by making use of ICMetric technology with k-NN. The importance of ICMetric-IDS has been presented in Table 2 by calculating performance metrics, PDR, throughput and End-to-End delay.

The simulation results are compared with previous works [2]. Result of the proposed ICMetric-IDS showed a higher accuracy rate of detection with low false alarms rate and some errors in detection of malicious behaviour in autonomous vehicles.

VIII. Conclusion and Future Work

An ICMetric-based vehicle sensing approach that uses the specific bias characteristics of infrared sensors is proposed to provide protection to the external communication of autonomous vehicles. In this paper, a novel vehicle identification known as the vehicle ICMetric basis number derived from the infrared sensors is employed to idenfity self-driving vehicles. The ICMetric-IDS is designed for training and testing both abnormal and normal behaviours which were built on the ns-2. It has the capacity to identify external and internal attacks.

This ICMetric-IDS is a novel intrusion detection system that offers protection to VANETs with the first use of ICMetrics in protecting the external communication of autonomous vehicles. The anomaly ICMetric-IDS reveal some satisfactory performance in identifying malicious vehicles for the external communication in self-driving and semi-autonomous vehicles. The ICMetric-IDS is an intelligent IDS which will has the ability to detect and even block other kinds of attacks such as Sybil and wormhole attacks.

References

[1] K. Ali Alheeti, A. Gruebler, and K. McDonald-Maier, "Intelligent Intrusion Detection of Grey Hole and Rushing Attacks in Self-Driving Vehicular Networks," *Computers*, vol. 5, no. 3, p. 16, Jul. 2016.

[2] K. M. A. Alheeti, A. Gruebler, and K. D. McDonald-Maier, "An intrusion detection system against malicious attacks on the communication network of driverless cars," in *2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC)*, 2015, pp. 916–921.

[3] K. M. A. Alheeti, A. Gruebler, and K. D. McDonald-Maier, "On the detection of grey hole and rushing attacks in self-driving vehicular networks," in *2015 7th Computer Science and Electronic Engineering Conference (CEEC)*, 2015, pp. 231–236.

[4] X. Zhai *et al.*, "Application of ICmetrics for Embedded System Security," in *2013 Fourth International Conference on Emerging Security Technologies*, 2013, pp. 89–92.

[5] R. Tahir, H. Tahir, and K. McDonald-Maier, "Securing Health Sensing Using Integrated Circuit Metric," *Sensors*, vol. 15, no. 10, pp. 26621–26642, Oct. 2015.

[6] A. Chaudhary, V. N. Tiwari, and A. Kumar, "Design an anomaly based fuzzy intrusion detection system for packet dropping attack in mobile ad hoc networks," *Souvenir 2014 IEEE Int. Adv. Comput. Conf. IACC 2014*, pp. 256–261, 2014.

[7] K. Zaidi, M. Rajarajan, S. Furnell, and A. Hudson-Smith, "Vehicular Internet: Security & Privacy Challenges and Opportunities," *Futur. Internet*, vol. 7, pp. 257–275, 2015.

[8] K. M. A. Alheeti, A. Gruebler, and K. D. McDonald-Maier, "An Intrusion Detection System against Black Hole Attacks on the Communication Network of Self-Driving Cars," in *2015 Sixth*

International Conference on Emerging Security Technologies (EST), 2015, pp. 86–91.

[9] E. C. Eze, S. Zhang, and E. Liu, "Vehicular ad hoc networks (VANETs): Current state, challenges, potentials and way forward," in *2014 20th International Conference on Automation and Computing*, 2014, pp. 176–181.

[10] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETS): status, results, and challenges," *Telecommun. Syst.*, vol. 50, no. 4, pp. 217–241, Aug. 2012.

[11] J. Jakubiak and Y. Koucheryavy, "State of the Art and Research Challenges for VANETs," in *2008 5th IEEE Consumer Communications and Networking Conference*, 2008, pp. 912–916.

[12] D. Tian, Y. Wang, G. Lu, and G. Yu, "A vehicular ad hoc networks intrusion detection system based on BUSNet," *2010 2nd Int. Conf. Futur. Comput. Commun.*, pp. V1-225-V1-229, 2010.

[13] K. M. Ali, W. Venus, and M. S. Al Rababaa, "The affect of fuzzification on neural networks intrusion detection system," *2009 4th IEEE Conf. Ind. Electron. Appl. ICIEA 2009*, pp. 1236–1241, 2009.

[14] D. E. Denning, "An Intrusion-Detection Model," *IEEE Trans. Softw. Eng.*, vol. SE-13, no. 2, pp. 222–232, Feb. 1987.

[15] P. Porras, "STAT -- A State Transition Analysis Tool For Intrusion Detection." University of California at Santa Barbara, 1993.

[16] B. Mukherjee, L. T. Heberlein, and K. N. Levitt, "Network intrusion detection," *IEEE Netw.*, vol. 8, no. 3, pp. 26–41, May 1994.

[17] X. Zhai *et al.*, "Application of ICmetrics for Embedded System Security," in *2013 Fourth International Conference on Emerging Security Technologies*, 2013, pp. 89–92.