An Intelligent Intrusion Detection Scheme for Self-Driving Vehicles Based On Magnetometer Sensors

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

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

***Abstract*— Both safety and non-safety applications require authentication of messages and vehicles in cooperative vehicular ad hoc networks. Access control can prevent external attackers from achieving their goal of breaking or hacking important information from road side units and self-driving vehicles. However, internal attacks on vehicular systems and networks remain possible. A novel intelligent intrusion detection is proposed to secure the external communication system of self-driving and semi-self-driving vehicles. This system is based on the Integrated Circuit Metric technology, which has the ability to protect systems using features of the system itself. The detection system, called the ICMetric-IDS, is based on novel and unique features, which have been generated from bias values of magnetometer sensors as well as features which have been extracted from a trace file of simulated vehicle network traffic. Practical implementation and testing of the system demonstrate the efficiency in the detection of malicious behaviour.**

***Index Terms*—Intrusion detection, driverless cars, ICMetric, security.**

I. Introduction

Self-driving vehicles are poised to enhance the safety of passengers and drivers by reducing traffic jams and car accidents that are caused by human errors. These vehicles depend heavily on communication systems to exchange control data and sensitive information with Road Side Units (RSUs). Vehicular ad hoc networks (VANETs) represent this external communication system of self-driving and semi-self-driving vehicles [1].

The application of VANETs in autonomous and semi-autonomous vehicles ensures the success of this new generation of technology based on the security of the networks. Moreover, certain characteristics of VANETs have caused vulnerabilities at all their communication layers [2]. In other words, the external communication system has some properties that cause inherent security issues: speed of the car, mobility, high dynamic topology, absence of a fixed security system, open medium wireless communication and the sometimes large number of vehicles on roads [2]. In this case, intruders can launch their attack without physical access. In general, there are two types of communication in VANETs [3]:

- Vehicle-to-Vehicle Communications (V2V): Self-driving vehicles can directly establish communication wirelessly with one another forming V2V communication.
- Vehicle-to-RSUs (V2R): Communication between the self-driving vehicles and their fixed RSUs. It is the formation of V2R communication that is used for the purpose of monitoring traffic and management services.

Figure 1 shows an overview of VANETs for autonomous vehicles.

Traditional systems do not possess the ability to provide protection to sensitive information or control data of communication systems or host computing devices from internal/insider attacks. This means that the role of the intrusion detection system (IDS) is to identify and prevent internal and external attacks on these systems that are seen as the second layer of security systems such as encryption/decryption. The external communication system of self-driving vehicles is affected by many vulnerabilities compared to other types of networks, such as wired networks, since there is no stationary security infrastructure; a high dynamic topology network and the open wireless medium makes them more vulnerable to attacks [2].

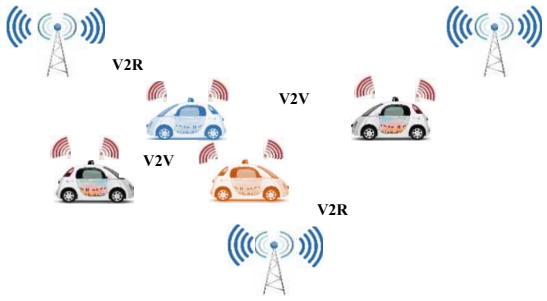


Fig. 1: Communication system of self-driving vehicles.

Integrated Circuit Metrics (ICMetrics) is an emerging technology to create a unique identifier for an electronic systems. Here such a feature has been extracted from the characteristics of magnetometer sensors for self-driving vehicles. ICMetric can be used both for identification and security purposes, akin to the electronic equivalent of a biometric technology [4].

In this paper, implementing ICMetric in IDS leads to the addition of a new dimension to current security systems. An ICMetric basis number is combined with traditional IDS to create a new and robust detection system to secure the external communication of driverless and semi-driverless cars.

An ICMetric-IDS is proposed to establish security for the VANETs of self-driving vehicles. It is based on employing ICMetric technology in identifying external/internal attack and provides two key benefits:

- Improving the authentication communication of driverless vehicles by creating an ICMetric which was extracted from bias readings of the magnetometer sensors.

- Designing an intelligent ICMetric-IDS that relies on the features of driverless vehicles. These features, that indicate either normal or malicious behaviour are extracted from trace files generated using a network simulator.

The remainder of our paper is organised as follows: section two discusses related works; section three provides an overview of vehicular ad hoc networks; section four discusses the proposed ICMetric intelligent intrusion detection system; the methodology of the proposed security system is presented in section five, and simulation results are discussed in section six. The discussion of the results is presented in section seven. The final section is the conclusion.

II. Related Works

The emergence of driverless and semi-driverless cars which utilise vehicular ad hoc networks has attracted significant interest due to its direct and positive impact on society. These vehicles, for the most part, depend on the sensitive external communication with their environment in order to move and exchange warning messages. The external communication system that is used in these vehicles has characteristics that make it susceptible to various attacks [2]. The security problem in VANETs of self-driving and semi-self-driving vehicles has been widely researched.

Chaudhary et al. in [5] suggested a malicious intrusion detection that utilises fuzzy logic to secure mobile ad hoc networks MANETs. It can identify dropping attacks as well as isolated malicious vehicles from their Internet Protocol (IP) exchanges. The authors [3] propose an intelligent IDS to secure the external communication of self-driving vehicles and semi-self-driving vehicles from any attacks. It possesses the ability to identify and prevent the grey hole and rushing attacks that have a direct and negative impact on lives of passengers, drivers and the vehicles themselves. This system depends on the characteristics of vehicles which have been extracted from the trace file. Zaidi et al. in [6] presented different aspects of security and privacy of vehicular internet that plays an important role in bridging all of the security holes. In [7], the researchers create an IDS to provide sufficient security to the routing protocol of self-driving and semi-self-driving vehicles. The system is deployed on the network layer for every RSU and car to provide sufficient protection for data and information from black hole attacks.

Our research seeks to protect the external network of such vehicles from some types of attacks, such as Black hoke, Grey hole, Denial of Service (DoS) and Sybil attacks. It depends on the features of the trace file which have been generated from network simulator as well as a new ICMetric feature that was determined from the bias reading of magnetometer sensors on self-driving vehicles.

III. Overview Of Vehicular Ad Hoc Networks

The arrival of self-driving vehicles means that privacy and security are vital issues for VANETs, and these are of concern to many researchers. Autonomous vehicles send warning messages and Cooperative Awareness Messages (CAMs) via wireless channels to communicate their status to other nodes in the radio coverage area. These messages are sent to determine the status of these vehicles to mitigate any risks.

Self-driving vehicles' communication configurations are heavily based on the acquisition of accurate broadcast data and control data of both, vehicles and the surrounding environment. In other words, these vehicles require up-to-date kinematic data, communication protocols and the aid of positioning systems for the efficient and reliable information exchange between them.

Self-driving vehicles in VANETs are equipped with sensors, communication systems and On Board Units (OBUs) that work together for the provision of a wide range of services required by the vehicles and the infrastructure [8]. The communication system allows OBUs-enabled vehicles to send and receive messages to and from other vehicles or RSUs in that radio coverage area. These devices play a vital role in providing short-range wireless ad hoc networks for the transmission of needed kinematic data and control data to the vehicular networks, thus facilitating traffic efficiency and safety on the roads indicated above [9]. In addition, self-driving vehicles are fitted with Global Positioning System (GPS) or Differential Global Positioning System (DGPS) receivers to process their position [10].

Fixed infrastructure such as the RSUs are connected to the backbone network, and are installed at strategic positions across the roads for reliability effectiveness and timely VANETs. Network devices are connected to the RSUs to support Dedicated Short-Range Communications (DSRC) using IEEE 802.11p radio technology.

IV. Intrusion Detection Systems

IDS are considered the second layer in any security system which has the ability to detect malicious behaviour [11]. These security systems have a significant role in the detection of many potential attacks on autonomous and semi-autonomous systems. The major concern in traditional security systems for example is that encryption/decryption alone does not have the ability to detect internal attacks [11].

The detection systems have been utilised to secure sensitive data using prevention mechanisms such as authentication and access control mechanisms. It can be classified as network-based (NID) and host-based (HID), according to the collected data set. In other words, the classification is based on the source of information detection. HIDs are configured on computers or hosts and they monitor an audit trail, while NID is based on the data that has been collected from network traffic.

Detection schemes, such as anomaly detection and misuse detection systems, are utilised in the classification of IDS [12]. Anomaly or behaviour detection is based on normal traffic behaviour of self-driving vehicles in VANETs. Thus, it detects any active attacks by identifying that the system significantly deviates from its' normal behaviour. Such behaviour is thus considered abnormal.

Misuse or signature detection is based on predefined data or system vulnerabilities. It matches the traffic pattern with these signatures of abnormal behaviour and generates an alarm when it detects malicious behaviour in VANETs. The main drawback of misuse detection systems is that they cannot detect novel types of attacks; however, anomaly-based detection can detect a novel, not previously encountered attacks. In other words, it is based on rules instead of patterns, and can detect any type of abnormal behaviour in the external communication of self-driving vehicles.

Thus, this approach is able to identify not only known malicious behaviours, but also the unknown malicious behaviours. In addition, anomaly detection can detect intrusions that are achieved through the misapplication of legitimate users, without breaking security policies [13], [14].

A high-false positive detection error is considered one of the limitations in anomaly detection system in addition to expensive computation and the difficulty of handling gradual misbehaviour [15]. In contrast, the misuse detection approach has many limitations such as inflexibility and difficulty of updating intrusion signature rules [14]. These strengths and limitations of the two approaches imply that effective IDS should employ a behaviour detector and a signature detector simultaneously [15]. In this paper, an anomaly detection system is proposed to secure the external communication of self-driving vehicles.

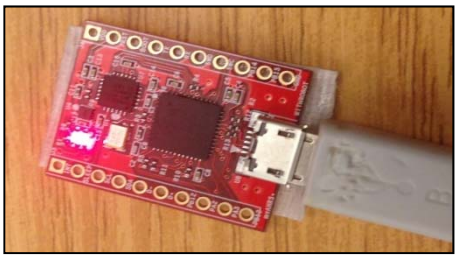
V. ICMetric Intelligent Intrusion Detection System

The key problem with existing defensive mechanisms is that they are not sufficient for preventing the internal attacks in VANETs ,since they require additional protection systems like IDS to increase their security. The idea of the ICMetrics technology depends significantly on potential features, which have been extracted from the characteristics of a specific embedded system [16]. These features are viewed as a unique identifier, which is unique to the specific system it is generated for. Features are extracted and normalised to determine if they are truly unique and deterministic. Here, the focus is on utilising a magnetometer sensor that is typically found in modern navigation systems.

In this paper, the bias reading that has been extracted from magnetometer sensor devices is utilised in the presented IDS. These bias readings were used to generate an ICMetric basis that was employed as identifications for driverless vehicles.

There are six stages of the proposed detection system; the overall architecture of the proposed security system is illustrated in the figure 3.

- 1st Stage (Generate ICMetric number) – The offset reading is extracted from the magnetometer sensors on autonomous vehicles. Mathematical and statistical functions are utilised to generate the ICMetric number from the extracted reading of the sensors. Additionally, the hash value is generated from the ICMetric number which will be employed in the ICMetric-IDS. Figure 2 shows the hardware setup composed of a myAHRS sensor which contains the magnetometer.



- Fig. 2: myAHRS_plus sensor.

- 2nd Stage (real-world) – Two tools are used in creating the real world simulation, which are Simulation Urban Mobility (SUMO) and Mobility Vehicles (MOVE) that reflect mobility of vehicles. The output files from SUMO and MOVE are used as input to generate a trace file.
- 3rd Stage (feature extraction) – The proposed ICMetric-IDS utilises only 16 significant features from the entire extracted features space [7]. Reducing the number of features plays an important role in enhancing the detection rate, decreasing error rate and false alarms.
- 4th Stage (pre-processing): the significant features require pre-processing, such as: 1) transfer some symbols and letters to numbers, 2) uniform distribution to balance abnormal and normal records to increase the efficiency of IDS, 3) normalisation values of extracted features that are generated from the trace file to make the performance of ICMetric-IDS more efficient in identifying and blocking malicious behaviour.
- 5th Stage (training phase- k-nearest neighbours (k-NN)): The k-NN is employed in designing the ICMetric-IDS. It is trained with extracted dataset which was produced in the third stage.
- 6th Stage (testing phase-k-NN): The ICMetric-IDS is tested with the extracted features. The accuracy rate of detection and four types of alarms are calculated in the test phase. There are some criteria for measuring the efficiency of k-NN, such as, detection rate, throughput, the number of false alarms, Packet Delivery Rate (PDR) and End-to-End delay.

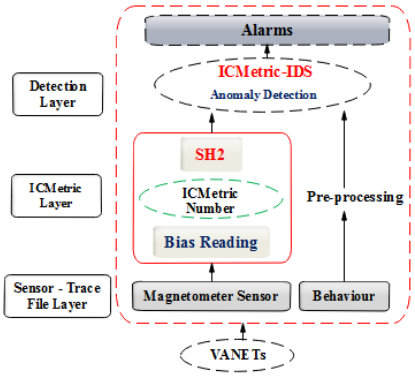


Fig. 3: Overall ICMetric-IDS architectural.

The proposed system first determines the ICMetric basis from the magnetometer sensors. They are then integrated with CAMs from source node to the destination node. The behaviour features require a pre-processing phase and are then considered the input to the IDS. The IDS outputs are then considered normal or malicious.

VI. Simulation Results

In this experiment, the bias readings that were generated from the magnetometer (myAHRS_plus) sensors are employed in designing a novel IDS to identify internal/external attacks. The bias readings are extracted from the three identical sensors to generate the ICMetric, and 1000 readings were recorded for three different axes. In the testing phase, the extracted data is used to evaluate the anomaly detection in the VANETs.

The detection accuracy rate and four types of alarms, true positive, false positive, true negative and false negative are calculated to evaluate the performance of the ICMetric-IDS.

Table 1 shows the detection rate and false alarm of the proposed ICMetric-IDS with the traditional IDS.

Table 1. Detection Rate and False Alarm

Performance Metrics	Detection rate		False Alarm
	Normal	Abnormal	
VANETs with Normal-IDS	98.45%	85.02%	12.24%
VANETs with ICMetric-IDS	99.77%	98.78%	1.21%

The significant improvement the proposed ICMetric-IDS can achieve is shown in Table 1 on the external communication of self-driving vehicles under various kinds of attacks with average error rate 0.72%. Table 2 shows the performance metrics of ICMetric-IDS.

Table 2. Performance Metrics

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	80.22%	99.64%	28.71*ms*

All these IDSs are evaluated under abnormal conditions to calculate their performance metric.

VII. Discussion

The success and development of self-driving vehicles depends enormously on suitable security systems which provide a safe environment for external communication systems/VANETs.

The average error rate of the IDS which utilises ICMetrics is 0.72%. The rate of detection fluctuated between 98.78% and 99.77% with efficient and excellent accuracy. The average false rate of alarm was very low, at about 1.21%, a further strong indicator for the good results.

Meanwhile, the detection rate of the normal IDS fluctuated between 85.02% and 98.45% whereas the false alarm was 12.24%. The detection rate is improved by using ICMetric technology with k-NN. Table 2 shows the significant role of ICMetric-IDS by calculating performance metrics: throughput, PDR and End-to-End delay.

Comparing these results with the previous works of the authors [2], the here proposed ICMetric-IDS obtains a higher accuracy rate of detection with low rate of false alarms and errors in identifying malicious behaviour of autonomous vehicle.

VIII. Conclusion

An ICMetric-based vehicle sensing scheme which utilises the MEMS magnetometer sensor is proposed to protect the external communication of self-driving cars. In this paper, a novel car identification known as the vehicle ICMetric basis was utilised to idenfity the vehicle and designed for training and testing abnormal and normal behaviours which were built on the network simulator. The proposed scheme has the ability to detect external and internal attacks. The ICMetric-IDS is seen as a novel IDS which provides protection to the VANETs because this is the first time an ICMetric is utilised in the external communication of self-driving vehicles. The anomaly ICMetric-IDS has shown acceptable performance in detecting malicious vehicles in the external communication of autonomous vehicles. Our proposed work can be extracted to design intelligent IDS that can detect and block other types 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] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

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

[12] 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.

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

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

[15] B. Mukherjee, L. T. Heberlein, and K. N. Levitt, "Network intrusion detection," *IEEE Netw.*, Vol. 8, no. 3, pp.26–4, 1994.

[16] X. Zhai, K. Appiah, S. Ehsan, H. Hu, D. Gu, K. McDonald-Maier, W. M. Cheung, and G. Howells, "Application of ICmetrics for Embedded System Security," in *2013 Fourth International Conference on Emerging Security Technologies*, 2013, pp. 89–92.