A Novel Distributed Intrusion Detection System for Vehicular Ad Hoc Networks

Leandros A. Maglaras
School of Computer Science and Informatics
De Montfort University, Leicester, UK

***Abstract*—In the new interconnected world, we need to secure vehicular cyber-physical systems (VCPS) using sophisticated intrusion detection systems. In this article, we present a novel distributed intrusion detection system (DIDS) designed for a vehicular ad hoc network (VANET). By combining static and dynamic detection agents, that can be mounted on central vehicles, and a control center where the alarms about possible attacks on the system are communicated, the proposed DIDS can be used in both urban and highway environments for real time anomaly detection with good accuracy and response time.**

***Index Terms*—VANET; Intrusion Detection; OCSVM**

I. Introduction

Next-generation telematics solutions are being driven by the maturation of recently deployed intelligent transportation systems, assisted by the integration of and rapid collaboration with information communication technology markets and the automotive industry. Inter-vehicle communication (IVC) has emerged as a promising field of research and development [1], [2], [3], [4], [5] , where advances in wireless and mobile ad hoc networks can be applied to real-life problems (traffic jams, fuel consumption, pollutant emissions, and road accidents) and they thus have great market potential.

Vehicular ad hoc network (VANET) applications are based on Car-to-X (C2X) communications and vehicles become smarter with the installation of embedded systems and sensors. Sensors collect crucial data about the situation on the road and this information can be exchanged in order to help the driver make appropriate decisions. The driver receives information about a local anomaly, e.g. a too short inter-distance with the leading vehicle, lane departure etc. and exchange of this information among neighboring vehicles is crucial for VANET applications to be efficient. Communication between vehicles can be used to inform drivers about congested roads ahead, a car accident, parking facilities and so forth. Most of these applications demand frequent data dissemination among vehicles.

As a result, Inter Vehicular Communications may help drivers avoid dangerous situations, decrease driving time, minimise fuel consumption and have overall better driving satisfaction levels.

Vehicular networks have a diverse range of applications that cover both safety to comfort. Safety applications enhance the driving conditions and reduce the chances of accidents such as by providing enough time to the driver and/or applying the brakes automatically (eco-driving). These safety aspects can be further divided into the following:

- Cooperative collision warning.
- Incident management.
- Emergency video streaming.

Due to the scale of a VANET and its decentralized character, full control of each and every node in the network becomes unlikely and hence, the system is vulnerable to attacks [6]. An attacker, on the other hand, is not necessarily a malicious user trying to disrupt the cooperative systems functionality. For, even ordinary drivers might be motivated to misuse vehicular ad hoc communications selfishly in order to free the fast lane on a highway or switch a traffic light to green. As a result, DIDS are needed that constantly observe the system functionality and ensure fairness in the network.

II. Motivation

As with other networks, attacks in VANETs can be classified into the following categories [7]:

Outsider vs. insider attacks: Outside attacks are defined as attacks from nodes which do not belong to a VANET, whilst insider attacks happen when legitimate vehicles or nodes of a VANET behave in unintended or unauthorized ways due to being infected.

Passive vs. active attacks: Passive attacks include eavesdropping or the monitoring of packets exchanged within a VANET. These kinds of attacks target mostly the privacy of the driver rather than the security itself or they can be a preliminary step before an actual attack is initiated on the system. Active attacks involve some modifications of the data stream or the creation of a false one in order to misinform surrounding vehicles about possible danger on the road and thus, raise safety issues.

Malicious vs. rational: Usually, a malicious attacker seeks to gain no personal benefit from the attacks, but rather, just aims to harm the users or the network. By contrast, a rational attacker does pursue personal benefit and hence, is more predictable when compared to a malicious attacker. A typical example of a rational attack is in a situation where a selfish relay node does not retransmit information about a free parking spot in order to take advantage of it.

Local vs. extended: An attacker can be limited in scope, even if he controls several entities (vehicles or base stations), which makes him local , whilst an extended attacker controls

several entities that are scattered across the network, thus widening his scope. This distinction is especially important in privacy-violating and wormhole attacks. A distributed denial-of-service is an example of an extended attack.

A substantial amount of research on intrusion detection systems ($IDSs$) has targeted the CAN protocol [8]. For the detection of these attacks, both specification-based and anomaly-based detection methods have been proposed. Hoppe et al. [9] has demonstrated an anomaly-based IDS for the CAN protocol, which detects deviations on the number of transmitted messages by considering the rate of how often specific messages are transmitted on the CAN bus, and comparing this with ewhat is deemed to be normal. When the anti-theft alarm is activated, the system sends messages to the lights of the vehicle to turn them on and off, such that they flash. Furthermore, several approaches to introducing IDSs into vehicles have been suggested. Regarding which, both specification-based [10] and anomaly-based treatments [11], [12] have been investigated. Moreover, an attempt to deflect attacks using honeypots has been described in [13].

In detecting security threats in VANETs, along with the common signature based and anomaly based detections, we can exploit the context of a VANET and its application to detect attacks upon it.

Signature-Based Detection: In signature-based detection, attacks can be detected by comparing network traffic with known signatures of attacks and as soon as an attack is detected appropriate countermeasures can be initiated. The primary concern of this approach is to realize a mechanism that is capable of detecting known attacks on a communication system and the advantages of this detection technique are that it is simple and usually provides reliable detection of known attacks. However, the frequent updates of the attack signature database, the slow reaction to new attacks and of course, the difficulty in defining attack signatures are the shortcomings of this detection technique.

Anomaly Detection: This approach is based on a statistical approach that defines normal communication system behavior. Any deviation from that behavior is statistically analyzed and as soon as a defined level is reached, the security system concludes that there is an attack on going. The advantage of this detection technique is that it enables the detection of previously unknown attacks without requiring an database that contains the different kinds of attacks to be updated. However, there are also some disadvantages, in particular, the definition of normal system behavior is pretty complex and anomaly detection is known to produce many false positives.

Context Verification: Context verification is an approach that specifically considers the properties of VANETs and applications within them. The underpinning idea is the collection of as much information from any source available (e.g. the warning system, data from telemetric monitoring, etc.) by each vehicle so as to create an independent view of its current status, its current surrounding (physical) environment and current or previously neighboring vehicles. Situation evaluation mechanisms can be either application independent or dependent. In the former case, the position can be exploited as well as time related information, whilst in the latter circumstance evaluation mechanisms exploit parameters specific to a certain application.

A. Contributions

The present work presents a DIDS for VANETs and several scenarios are investigated in a highway environment with several routing distributions of vehicles.

The article makes the following contributions:

- Discusses security and privacy issues in vehicular ad hoc networks (VANETs)
- Proposes a Distributed Intrusion Detection System (DIDS), which can be mounted both on RSUs (Static DIDS) or on vehicles that have a central role in the network (Dynamic DIDS).
- The system is based on a Support Vector Machine module (k-OCSVM). The information about any detected attacks is communicated to the security center with the use of dedicated messages.
- A performance evaluation of the proposed method is conducted.

III. Intrusion Detection

In the new interconnected world, we need to secure the IP based Ethernet Channel using sophisticated intrusion detection approaches. In the next subsection we present our integrated intrusion detection mechanism [14] and how it could be used in a Vanet environment by using the social characteristics of the vehicles.

A. K-OCSVM module

The K-OCSVM module, which is used as the main detection module of our IDS, combines the well known OCSVM classifier with the RBF kernel and a recursive K-means clustering module. Figure 1 illustrates the procedure of intrusion detection for the K-OCSVM module.

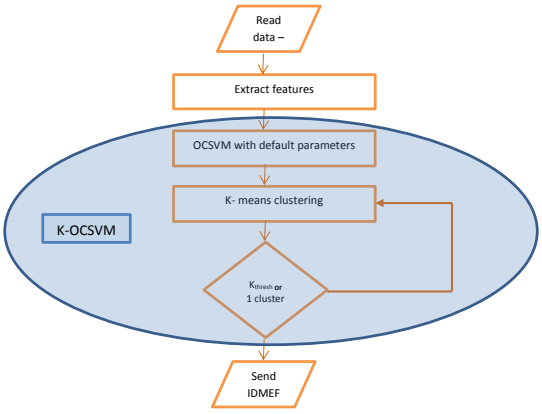

Fig. 1: K-OCSVM module

The OCSVM classifier runs with default parameters and the outcome consists of all possible outliers. These outliers are

clustered using the k-means clustering method with *2* clusters, where the initial means of the clusters are the maximum and the minimum negative values returned by the OCSVM module. From the two clusters that are created from the K-means clustering, the one that is closer to the maximum negative value (severe alerts) is used as the input in the next call of the K-means clustering. This procedure is repeated until all outcomes are put in the same cluster or the divided set is big enough compared to the initial one, according to the threshold parameter k_{thres}.

The K-means clustering method divides the outcomes according to their values and those outcomes with the most negative values are kept. This way, after the completion of this recursive procedure only the most severe alerts are communicated from the K-OCSVM. The division of the data requires no previous knowledge about the range of the outcomes, which may vary from *-0.1* to *-160* depending of the assigned values to configuration parameters σ and ν. The method can find the most important/possible outliers for any given values to the parameters σ and ν.

B. OCSVM based intrusion detection system

The main purpose of the intrusion detection mechanism is to perform anomaly detection in a time-efficient way, with good accuracy and low overhead, within a temporal window. In order to achieve the aforementioned goals, several operation stages need to be carried out: Pre-processing of raw input data, feature selection, creation of detection modules, fusion of initial alarms and the reporting of an alarm to the system. Pre-processing is used so as to transform the data of incoming packets into a convenient format for the classification modules. After this step, the most appropriate features are selected and the intrusion detection modules created, which produce initial alarms indicating a variation in network traffic from that which is is normal. Since the initial alarms may be too many, a fusion method that includes k-means clustering is used. The final alarms that may be produced are communicated from the system to the management authority in order to report the attack and to decide upon the counter measures to be taken.

The intrusion detection mechanism (see Figure 2) can run in the cloud by analyzing the network traffic that is sent from the RSUs that are scattered along the road network. A dynamic DIDS(distributed detection agents) can operate in some central vehicles by analyzing the packets sent in the vehicles neighborhood, and these central vehicles can be chosen by using a clustering method [15], which is based on the mobility of the vehicles. Each vehicle that detects a possible attacker may communicate this information to the system through a dedicated message. The central system gathers the information received from the distributed agents and takes final decisions about the severity of the alarm.

C. Dynamic detection agents

In the DIDS the K-OCSVM is mounted on vehicles that have a central role in the VANET and in order to choose the central roles, the spring clustering methods is used. The

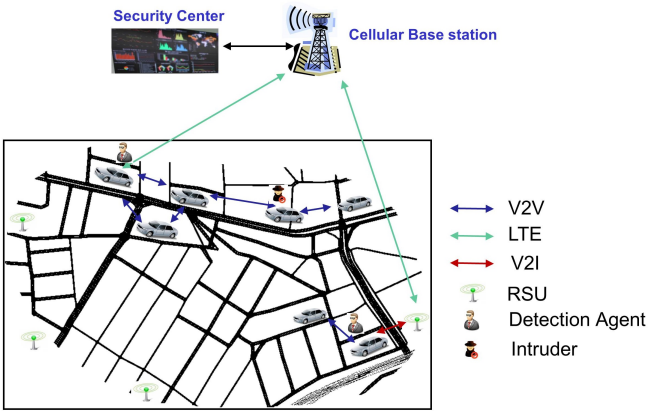

Fig. 2: Intrusion detection mechanism

idea behind the spring clustering method is based on force-directed algorithms. The force-directed assign forces among the set of edges and the set of nodes in a network. The most straightforward method is to assign forces as if the edges were springs and the nodes electrically charged particles. The entire graph is then simulated as if it were a physical system. The forces are applied to the nodes, pulling them closer together or pushing them further apart.

Every node applies to its neighbors a force F_{rel} according to their distance and their velocities. Vehicles that move in the same direction or towards each other apply positive forces, while those moving away apply negative ones. The components of the vector F_{rel} along the east-west F_x and north-south F_y axes are then calculated. In order to form stable clusters, only vehicles that move in the same direction or towards each other are considered as candidate cluster members. For a specific vehicle where the total magnitude of forces applied to it is negative, no clustering procedure is triggered since all the surrounding nodes tend to be moving away from it. Calculating the total force F helps to avoid re-clustering in many situations when groups of vehicles move away from each other.

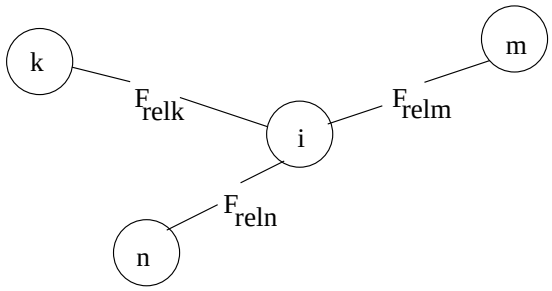

Fig. 3: Relative forces applied to vehicle i.

D. Privacy

Privacy preservation is critical for vehicles and in this context it is achieved when two related goals are satisfied:

untraceability and unlinkability [16], [17], [18]. The first property refers to a vehicle's actions not being able to be traced and the second, that it must be impossible for an unauthorized entity to link its identity with that of its driver/owner. On the other hand, no traffic regulation or congestion avoidance can be achieved if this privacy protection is not removed. That is, access to the data concerning owner identity for a given vehicle and the path followed along a period of time are crucial for building its social profile. Therefore, security mechanisms should prevent unauthorized disclosures of information, whilst at the same time allowing for an appropriate amount of data to be fed to the applications in order to work properly [19].

IV. Simulation and performance evaluation

A simulation study was conducted to evaluate the performance of our IDS using a custom simulator with different mobility scenarios. In our simulation, we consider various road traffic and network data parameters. The simulation environment (Figure 4) is a two direction, 3-lane per direction, 2km long highway in order to evaluate the performance of the scheme. The system is set to split network traffic datasets into distinct parts of 2 second periods and use them in order to detect malicious traffic.

In all the simulated scenarios a malicious node is performing a DOS attack and the proposed K-OCSVM module is used in order to detect it. With a DOS, the main objective is to prevent the legitimate user from accessing the network services and network resources. Such an attack can occur by jamming the channel system so that no authentic vehicle can access it. In a VANET it is a very serious problem as the user cannot communicate in the network and pass information to other vehicles, which could have devastating results in life critical applications like cooperative collision warning or intersection warning assist.

In order to evaluate the performance of the proposed IDS, we measure both the accuracy of the K-OCSVM module and the total time that the system needs in order to detect the attack. The first characteristic is mainly affected by the correct calibration of the K-OCSVM module and the driving behavior of the intruder, while the second is more influenced by the correct placement of the detection agents both in the static and DIDSs.

During the simulation period, all normal nodes periodically broadcast beacon messages (cooperative awareness messages (CAM)) with a frequency of 10 Hz in order to inform surrounding vehicles about their presence and decentralized environment notification messages (DENM) With a frequency of 1 Hz, which are used for creating clusters, sending warnings to neighboring vehicles and announcing the detection of an intruder. The intruder, on the other hand. floods the channel by sending CAM messages with high frequency (200 Hz), thereby blocking communication among neighboring vehicles.

In the first set of simulations the static IDS system is used, where the RSUs collect the network data and detect the malicious behavior of an intruder. In the second set of simulations the dynamic IDS is used, where the detection agents are

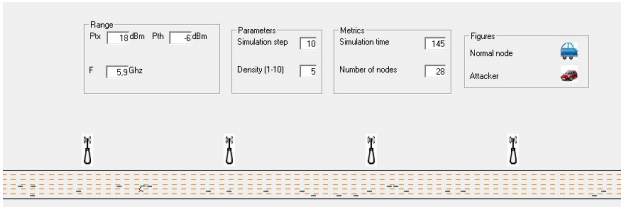

Fig. 4: Simulation environment

selected according to the spring clustering method [15]. All nodes are equipped with GPS receivers and On Board Units (OBU). Location information of all vehicles/nodes needed for the clustering algorithm is collected with the help of GPS receivers. The only communications paths available are via the ad-hoc network and there is no other communication infrastructure. The power of the antenna is $P_{tx} = 18dBm$ and the communication frequency f is 5.9 Ghz.

The communication range of the vehicles is calculated according to Table I. In our simulations, we use a minimum sensitivity (P_{th}) of -69 dBm, which gives a transmission range of 130 meters.

Data Rate (Mb/sec)	*Minimum Sensitivity(dBm)*
3	-85
4.5	-84
6	-82
9	-80
12	-77
18	-70
24	-69
27	-67

TABLE I: Minimum sensitivity in receiver antenna according to data rate.

The arrival rate of the vehicles follows the Poison process with parameter λ. The speed assigned to the vehicles is according to the speed limit of the road lane that it chooses to follow according to Table II. The malicious node, in contrast to the normal ones, follows its own mobility pattern as discussed in following subsections.

Lane	*Speed km/h*
1	80
2	100
3	120

TABLE II: Speed per lane for both directions.

The density of the vehicles depends on the parameter λ. The number of vehicles per lane is between (2 -15 v/km/Lane), which determined by the speed being used and the value of parameter λ, according to Table III.

A. Static intrusion detection system

In these scenarios we have placed RSUs along the highway that collect the data and run the proposed K-OCSVM module. Once a malicious node is detected, the information is passed

Parameter λ	*v/km/lane*
3	8-15
5	5-9
7	3-6

TABLE III: Density per lane.

to the central control system and counter measures are taken according to the severity of the event. We carried out 50 different runs for each scenario with different velocities and RSU placements. The attacker and the start time of the attack in each scenario were selected randomly.

Figure 5 illustrates how the accuracy of the K-OCSVM module is affected by the speed of the intruder. Regarding which, when a malicious node moves at a high speed in the system, the RSUs that are placed along the highway do not have sufficient time to collect enough data and thus, produce inaccurate results.

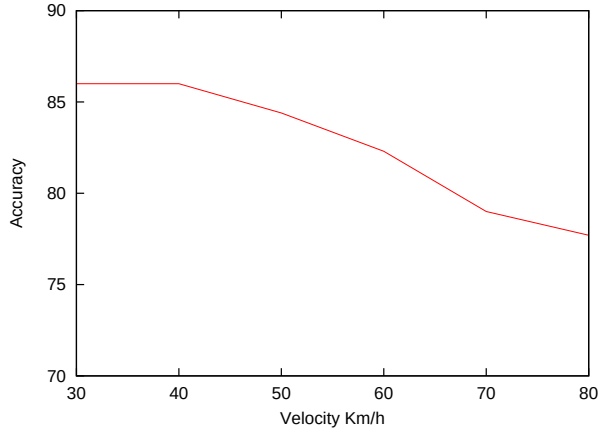

Fig. 5: Accuracy of the static IDS is affected by the velocity of the intruder (Distance among RSUs: 200 m)

In Figure 6, we can observe that the response time of the system is highly affected by the distance between the RSUs, since by placing the RSUs far enough from each other we leave some parts of the road network unprotected. Denser networks of RSUs come with increased response times and with higher infrastructure costs. The response time is also affected by the time slots that the system chooses to collect, process and analyze the network traffic. Smaller time slots would lead to better response times, but at the cost of lower accuracy, since the collected network traces would not be enough to identify possible malicious traffic on the channel.

B. Dynamic intrusion detection system

In the second group of simulated scenarios, clustrheads play the role of RSUs that collect the data and run the proposed K-OCSVM module. Once a malicious node is detected, the information is passed to the central control system and counter measures are taken according to the severity of the event. We executed 50 different runs for each scenario of different

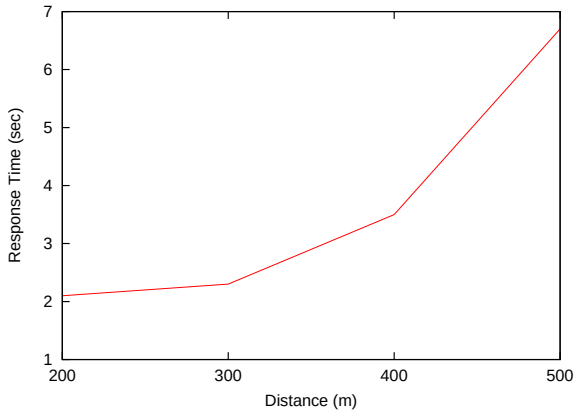

Fig. 6: Response time of the system is affected by the placement of the RSUs (Attacker velocity: 40 Km/h)

velocities and vehicle densities. The attacker and the start time of the attack in each scenario were selected randomly.

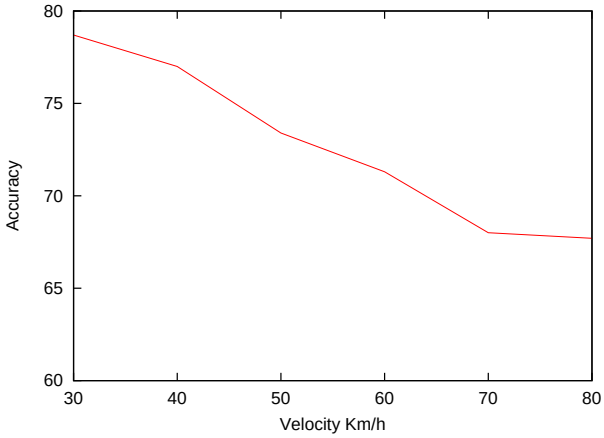

Fig. 7: Accuracy of the dynamic IDS is affected by the velocity of the intruder

Figure 7 presents how the accuracy of the K-OCSVM module is affected by the speed of the intruder. Regarding which, when the malicious node moves in a high speed in the system the clusterheads do not have sufficient time to collect enough data and hence, produce inaccurate results. This problem could be solved if the mobile detection agents are combined with RSUs that are placed on critical points in the road network (e.g. intersections), thus creating a hybrid detection system.

In Figure 8, we can observe that the response time of the system is highly affected by the vehicle density. More dense network of vehicles reassures that the intruder is near a clusterhead for a sufficient time in order to be detected by the IDS. When the network is sparse, the intruder may be near a vehicle blocking its communication, but with no clusterhead in its vicinity can stay undetected for a long period of time.

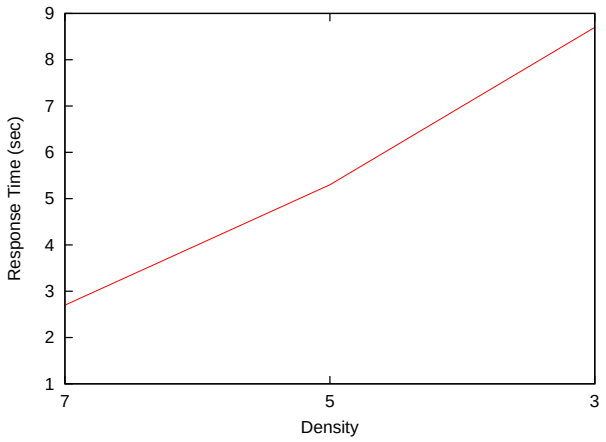

Fig. 8: Response time of the system is affected by the density of the vehicles

C. Counter measures

To mitigate these attacks, switching between different channels or even communication technologies (e.g. DSRC, LTE), when one of them (typically DSRC) is brought down, is a typical counter measure [20]. In the worst-case scenario (i.e. when no means of communication between vehicles exist), the VANET safety features (e.g. collision avoidance, intersection warning) should automatically be turned off until the network is re-established.

Automatic reaction techniques can also be used on the malicious node itself. An example would be automatic braking of the vehicle under attack, in case of a detected problem by the IDS. If it incorrectly detects a malicious activity and independently decides to stop the car in the middle of a highway, this may result in terrible consequences. A more simple technique would be the automatic switching off of all the network cards of the malicious node with concurrent notification to the driver that the vehicle is under attack.

V. Conclusions - Future work

In order to secure vehicular communications, we propose a DIDS that is based on machine learning techniques. That is, the system is based on a machine learning module that can achieve high accuracy and a low false alarm rate. Both a static detection system that operates on the RSUs, and a dynamic system that uses mobile agents which are mounted on central vehicles collect are presented. The proposed DIDS analyze network traffic and report malicious activity to the security center in real time. The proposed systems are capable of detecting the attacker in a relative short period of time with good accuracy and rapidly report the attack in the central security system.

In future work, the proposed mechanism will be evaluated against other attack scenarios and will be enhanced in order to improve accuracy as well as response times. As the system is highly affected by the correct placement of the RSUs and the position of the clusterheads, which play the role of detectors, optimization techniques must be developed in order to choose the best allocation strategy of the detection agents. In order to get realistic evaluation results, future enhancements should also be based on the automotive hardware and software components being already used in field operational tests.

References

[1] H. Hartenstein and K. P. Laberteaux, "A tutorial survey on vehicular ad hoc networks," *IEEE Communications magazine*, vol. 46, no. 6, pp. 164–171, 2008.

[2] G. Karagiannis, O. Altintas, E. Ekici, G. Heijenk, B. Jarupan, K. Lin, and T. Weil, "Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions," *IEEE Communications Surveys & Tutorials*, vol. 13, no. 4, pp. 584–616, 2011.

[3] M. L. Sichitiu and M. Kihl, "Inter-vehicle communication systems: A survey," *IEEE Communications Surveys & Tutorials*, vol. 10, no. 2, pp. 88–105, 2008.

[4] Y. Toor, P. Mühlethaler, A. Laouiti, and A. De La Fortelle, "Vehicle ad hoc networks: Applications and and related technical issues," *IEEE Communications Surveys & Tutorials*, vol. 10, no. 3, pp. 74–88, 2008.

[5] T. L. Willke, P. Tientrakool, and N. F. Maxemchuk, "A survey of inter-vehicle communication protocols and their applications," *IEEE Communications Surveys & Tutorials*, vol. 11, no. 2, pp. 3–20, 2009.

[6] N. Bißmeyer, "Misbehavior detection and attacker identification in vehicular ad-hoc networks," 2014.

[7] S. Khan and A.-S. K. Pathan, *Wireless Networks and Security: Issues, Challenges and Research Trends*. Springer, 2013.

[8] P. Kleberger, T. Olovsson, and E. Jonsson, "Security aspects of the in-vehicle network in the connected car," in *Intelligent Vehicles Symposium (IV), 2011 IEEE*. IEEE, 2011, pp. 528–533.

[9] T. Hoppe, S. Kiltz, and J. Dittmann, "Applying intrusion detection to automotive it-early insights and remaining challenges," *Journal of Information Assurance and Security (JIAS)*, vol. 4, no. 6, pp. 226–235, 2009.

[10] U. E. Larson, D. K. Nilsson, and E. Jonsson, "An approach to specification-based attack detection for in-vehicle networks," in *Intelligent Vehicles Symposium, 2008 IEEE*. IEEE, 2008, pp. 220–225.

[11] T. Hoppe, S. Kiltz, and J. Dittmann, "Adaptive dynamic reaction to automotive it security incidents using multimedia car environment," in *Information Assurance and Security, 2008. ISIAS'08. Fourth International Conference on*. IEEE, 2008, pp. 295–298.

[12] M. Muter, A. Groll, and F. C. Freiling, "A structured approach to anomaly detection for in-vehicle networks," in *Information Assurance and Security (IAS), 2010 Sixth International Conference on*. IEEE, 2010, pp. 92–98.

[13] V. Verendel, D. K. Nilsson, U. E. Larson, and E. Jonsson, "An approach to using honeypots in in-vehicle networks," in *Vehicular Technology Conference, 2008. VTC 2008-Fall. IEEE 68th*. IEEE, 2008, pp. 1–5.

[14] L. A. Maglaras and J. Jiang, "A real time ocsvm intrusion detection module with low overhead for scada systems," *International Journal of Advanced Research in Artificial Intelligence(IJARAI)*, vol. 3(10), 2014.

[15] L. A. Maglaras and D. Katsaros, "Distributed clustering in vehicular networks," in *Wireless and Mobile Computing, Networking and Communications (WiMob), 2012 IEEE 8th International Conference on*. IEEE, 2012, pp. 593–599.

[16] M. Gerlach, "VaNeSe – An approach to VANET security," in *Proceedings of the International Workshop on Vehicle-to-Vehicle Communications (V2VCOM)*, 2005.

[17] M. Whaiduzzaman, M. Sookhak, A. Gani, and R. Buyya, "A survey on vehicular cloud computing," *Journal of Network and Computer Applications*, vol. 40, pp. 325–344, 2014.

[18] G. Yan, S. Olariu, and M. C. Weigle, "Providing {VANET} security through active position detection," *Computer Communications*, vol. 31, no. 12, pp. 2883 – 2897, 2008, mobility Protocols for ITS/VANET.

[19] J. M. De Fuentes, A. I. Gonzalez-Tablas, and A. Ribagorda, "Overview of security issues in vehicular ad-hoc networks," in *Handbook of Research on Mobility and Computing: Evolving Technologies and Ubiquitous Impacts*, 2011.

[20] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security*, vol. 15, no. 1, pp. 39–68, 2007.