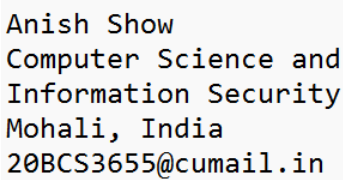
Security Constraints, Solutions and IDS In Vehicular Network



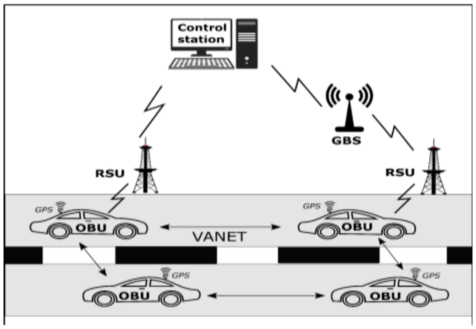
Anish Show
Computer Science and
Information Security
Mohali, India
20BCS3655@cumail.in

Abstract—In-vehicle communication has become an integral part of today’s driving environment considering the growing add-ons of sensor-centric communication and computing devices inside a vehicle for a range of purposes including vehicle monitoring, physical wiring reduction, and driving efficiency. However, related literature on cyber security for in-vehicle communication systems is still lacking potential dedicated solutions for in-vehicle cyber risks. Existing solutions are mainly relying on protocol-specific security techniques and lacking an overall security framework for in-vehicle communication. In this context, this paper critically explores the literature on cyber security for in-vehicle communication focusing on technical architecture, methodologies, challenges, and possible solutions. In-vehicle communication network architecture is presented considering key components, interfaces, and related technologies. The protocols for in-vehicle communication have been classified based on their characteristics, and usage type. Security solutions for in-vehicle communication have been critically reviewed considering machine learning, cryptography, and port-centric techniques. A multi-layer secure framework is also developed as a protocol and use case-independent in-vehicle communication solution. Finally, open challenges and future dimensions of research for in-vehicle communication cyber security are highlighted as observations and recommendations.

Keywords: learning Machine ; cryptography; cyberattacks; cyber security; intrusion detection system; smart intelligent vehicles; in-vehicle network; controller area network (CAN)

INTRODUCTION

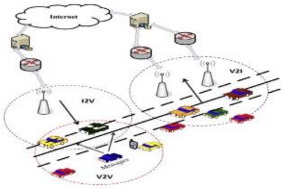
Modern intelligent vehicle can be regarded as cyber- physical system with high connectivity capabilities, and today’s era stands as the testament to this immense progression in the in vehicle automotive technology [1]. Modern intelligent vehicles should not be perceived to work like mechanical systems; rather they have an integrated architecture with millions of line codes to give up-to-date information for vehicle occupants. Advancements of modern communications in-vehicle allow for more precise in-vehicle dash centric communications as well as phone, sensor, headphones, and roadside units. Attention also needs to be given to the inherent short range communication system embedded into vehicle for security reasons due to potential cyber security weaknesses.” Over the recent period there is high attitude on security for vehicle networks studies. This growth is giving rise to researchers to build new protocols, while this culminates in the invention of new smart applications. The auto industry needs to develop efficient protocols that are fully compatible with recent patterns and technologies in order to compete with contemporary requirements. Then, see Figure 1 showing in-vehicle communication security cases and their corresponding threats. The existing protocols of the in-vehicle network have many problems. For example, the unavailability of message authentication and encryption, ID-based arbitration mechanism for contention resolution, etc. There are a lot of reasons to consider the necessity of vehicle’s security. Adversaries In the recent decades, there are improvements in technology of smart intelligent vehicles as well as self-driving vehicles. There have been great innovations in connection to the improved connectivity on the modern automotive industries leading to the development of communication channels and access points. These cyber security vulnerabilities pose a threat to the safety of life because it can be lost. Connected vehicles are modern, equipped with efficient communication capabilities, and sharing safety information to neighboring vehicles and infrastructure in real-time. The dynamic and rapid change in the automotive cyber security environment is attributed to this growth. For solving different in-vehicle domain problems, Artificial Intelligence technology (AI) and Machine Learning technology (ML) have been utilized. These techniques are the most reasonable for today’s complex application domains. The security of in-vehicle networks has to do with one of the complex application domains. In the last few years, research improvements show that ML’s-based schemes could be used to deal with security problems in in-vehicle networks. Modern intelligent vehicle network comprising of wireless communication between vehicles, or infrastructure, has increased vulnerability to multiple attack types, due to its connectivity having widened the security holes. Moreover, many researches have significantly contributed towards this



direction using machine learning techniques and their variants for security frame work development to detect possible attacks and shield against various security issues in modern vehicular networks. Over time, cryptographic approaches have been proposed as solutions to various security problems. Some of the traditional authentication techniques for in-vehicle networks include biometric authentication security techniques, key-based authentication, and password protection among others. Cryptographic techniques face a major challenge in accurately validating genuine information from a spoofed value. Also, most cryptographic systems are adopted in low-powered vehicle security systems.

LITERATURE REVIEW

One of the relatively new areas for research in today's vehicular networks is known as in-vehicle networks (IVNs). In vehicle's architecture incorporates various elements such as high accuracy sensors that form sensor domain, chassis domain, infotainment domain, telematics domain, powertrain domain among other segments. Therefore, for effective communication of these various domains in in vehicle's network there exist. The increased interoperability between transport facilities coupled with latest advancements like V2X communications has expanded points of entry into the in-car network which are now at the disposal of intruders. Presently, the different technological strands are merging with IOTs projects into ICT. One such important aspect is VANETs. A considerable amount of research has happened in this field. The following new works have recently been discussed. In this study, a new data retrieval scheme was developed giving back to the backbone the robustness. Nodes are less susceptible to denial of service attacks and the length of their request messages is reduced by this proposition. The proposed algorithm is versatile enough to be used with both symmetric and asymmetric cryptographic algorithms. There are many challenges associated with this algorithm, especially on the part of the complexity of the key signature. One of the earliest schemes on a group-key-based protocol for VANEIS has appeared. The algorithm employs a conditional privacy preserving password based approach. The algorithm may offer security features, but it would involve computational complexities and this would cause the delay in the transmission process. It also demonstrates another conditional privacy preserving approach by A key agreement protocol forms the basis of this proposed approach that exploits an identity-based scheme which comprises three phases – the system initialization phase, the anonymous identity generation and message-signing phase as well as the message verification phase.

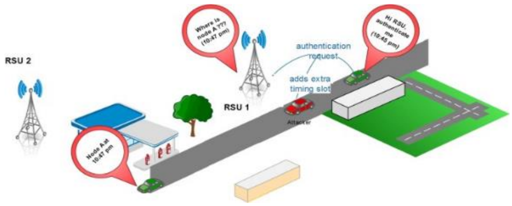


The proposed approach contains off our phases: setup of a system, registration of an individual user, login and authentication phase with password, change of password phase. However, the cost of running the algorithm is way much lower, but it is the packet delay ratio that suffers since it is not optimal for real time purposes. Proposal of a secured multimedia messaging scheme. It employs AES for confidentiality, and SHA-256 for hashing. Even though there is a strong encryption and end device verification process, it lacks an end-to-end authentication process that might result in authentication attack. The description of a key based approach is given by Multiple session keys are employed in the work of the authors, without giving any solution about session hijacking attacks. Reference suggests a secure message delivery approach for VANETs. Group key and symmetric key will be used to authenticate messages in a suggested method. No meaningful evidence that this use of group key should be significant has been found. In the authors employ attribute encryption techniques based on the usage of cryptographic algorithms. The proposed approach also takes into account the access policies. This algorithm ensures the confidentiality of the message dissemination but does not guarantee authentication message, integrity, and non-repudiation.

SECURITY CHALLENGES OF SECURITY VANET

High level of mobility and density combined with fix resources create the problem is difficult issues in VANET. The uniqueness of VANET is what contributes to the problems. These The features of this design are hard, which makes it difficult to create. Access for attackers is easy. These specific features of VANET are responsible for the following challenging issues:

Privacy: This involves offering an appropriate security model and the privacy model in VANET. Most drivers often want to safeguard their location and history data. As a hence, a control center can never know what happened on the road before the point of result. Here, providing privacy is It is the main constraints of a security model. One model is required for handling all these vehicles. however, not all information will be required to be shared as most of the drivers do not like sharing.



Mobility: The nodes of VANET moves very fast and change their location frequently. While moving with over 20m/s speed, it is not easy to stay connected with the network for the nodes. As a result, packet loss and link breakage happen. In this position, it is not easy to provide a proper security model for VANET.

Scalability: VANET has high density. VANET connects more than 250 million vehicles worldwide. There is no commonplace, appropriate security policy for so many nodes. Usually various local or private authorities seek to keep order within a small territory. As a result, due to this, drivers are unable to receive traffic information concerning exterior of the area and drivers cannot get made aware of every incidence happening therein while in the car. However, VANET have some few different reasons except those listed below that hinder its security. In general, a VANET is protected by an intrusion detection system (IDS). However, if any attack incident occurs in the network there is an urgent need for systems to make quick decisions to address the situation. Network IDS sends informs or warns the drivers of the incident enabling them to manually take required measures. There, drivers can go about business without having this would entail having the right information on what should be done during the incident. Such a loss can have adverse implications for the network this makes it possible for an attacker to have a greater period of time to contaminate the network's information. The idea behind attackers is also advancing along with advances in wireless networks. When attackers look for any leak in the network and try to attack the network using multiple kinds of attacks. So, Security is an important issue on any network. In VANET, the special attacks are conducted by the attacker network. They use the network for its convenience as a means of travelling and at ease by attackers. They also attack the accidents and roadblocks will be used by the network.

Sybil attack:

One of the deadliest attacks in VANET is that it is a Sybil attack. Specifically, Sybil attack involves the creation of a similar situation nodes get multiple identities. As a result, attackers attack any nodes and obtain info about them announce it in many areas. Therefore, they normally assume it is another node go up and down, changing directions, in order to navigate easily. An example would be when an attacker gives false information the network about the road congestion and blockage such that the other nodes change. direction to other routes. The nodes that impersonate their identities are called Sybil nodes and they include: Sybil is one term used to describe a certain type of attacker, where the attacker makes use of multiple nodes and identifies itself as an attacker node Sybil attacker. This type of Sybil attack may cause a big accident. cannot be detected easily. Unlike other attacks, Sybil is challenging and cumbersome to detect thus Sybil. This is truly one of the most dangerous attack. An identity spoofing attack is another name for Sybil attack. The attacker tricks the network into believing that the nodes have different identities. After that, attackers are able to insert false data into the VANET cloud. It could be a huge misfortune that will cause an accident on the road. For instance, in case of an accident, the neighboring car will deliver the note to other nodes and these others to the network as a whole. An assault case occurs where there is another attacker at the same time who receives the message before he can deliver it elsewhere and he also changes the message to read big accident. Sybil attack has three types.

a) Identity theft category: The Sybil attack involves an attacker taking on identities of neighboring nodes. Afterwards, they employ these identities and then make phony images of congested traffic jam on a road to mane. Random identity theft or attackers impersonating neighboring honest nodes.

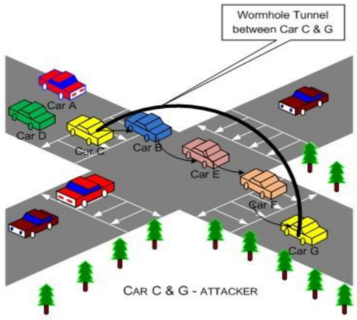
b) Communication category: during a Sybil attacker in a network, any normal node can send a message to that Sybil nodes. The first step is when the messages that Massage sends are sent to the Sybil attacker via the Sybil nodes. Second, the attacker changes or modifies the massages' data. When Sybil nodes communicate with normal nodes without involving any middle node, then we refer it as direct communication. Lastly, when SYL nodes receive information via normal node through Sybil attacker, we term this direct communication.

c) Participation category: This spoofs its identity and creates one or more fake identities to cause congestion in the road. This causes confusion to the other normal node, which in turn leads to traffic jam.

DoS attack: Every network is faced with DoS attack being one of them. The network freezes for some moments with DoS attack. This consequently means that other nodes cannot use the network. Attacker sends so many requests that the network system cannot manage all of them. Consequently, attacker renders system inactive for certain duration. During this period, no data be shared either by other nodes nor could it be received. network. There are various types of DoS attack such as flooding attack, Jelly Fish attack, and intelligent cheater attack. When a flood of worthless information is continuously shared by attackers in the network as part of another attack known as data flooding, the networks gets occupied with worthless requests. Jelly Fish generally interferes with the networking protocols and causes disorder within the system and delays on the network. Intelligent cheater attack likewise attacks the security procedures and incessantly attempts to give wrong impression about the other nodes which could be the case for intelligent cheater attack as well. The two attacks are also undetectable.

Black hole attack: The special case of black hole attack can be seen as when a specific node does not respond to the rest of the network, therefore it creates a black hole. The data for the node does not reach any one because it is not disclosed thus the other nodes are unaware of the same. Then, the attacking node floods the network with false routing information such that all the packets end at the attacking node. The attackers do not respond to their requests when they get the packets and send them into the network.

Wormhole attack: Attackers in a wormhole attack intend to manipulate the traffic by altering the network topology. Attacker node in this case catches the packet, edits that packet and sends to other victim's node. The packet is thereafter sent across the network. Hence, the attacker creates an artificial routing route while the shortest path proves the optimal way through the intruder node. In the first case when there is only one attacker, the attacker receives a packet at some part of an instance and afterwards modifies this packet on other part of this instance. As a result, many of the packet points at this period will not transmit in order.



Fake Information attack: However, one of the important considerations associated with VANET relates to sending out fake messages. This renders the network unfit for the subscribers, resulting in misguidedness. Such erroneous locations could prevent many crucial and emergency messages being received Fake information in a VANET can lead to serious damage and collisions.

SOLUTION FOR SECUIRTY ISSUES

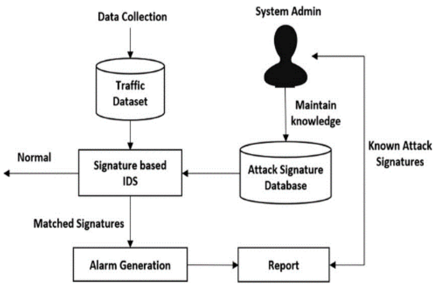
A sophisticated network designed for vehicular nodes in VANET. Therefore, it is necessary to ensure that.
appropriate network operating model for security. Various researchers offered various means of ensuring a viable security model for VANET. However, not every type of attack can be handled by one specific model. But some the models may be able to mitigate effects of these attacks. Researchers are working hard to establish that Sybil attack is dangerous. right way of identifying the breach. Therefore, one has to identify the fraud in the information. network. The performance of all nodes should include enhanced sensor capabilities. How data should be shared need to be pinpointed like other neighbor nodes, should be as correct. The need to analyze the signal strength of one packet in a network detect the fake packets. Similarly, frequent node authentication will be also able to expose the malicious nodes and subsequently block them. The impact of DoS attacks on the VANET is huge. As such, a suitable remedy is required. The request detector ensures that the correct request reaches the source and the destination in the network. Any specific authorized node can serve as this. RSU. The detector collects the information on the source and destination and synchronized here. acknowledgment of the transmission. The response packets are protected here by a response detector. A threshold value must be kept constant in the network, at which the transmission has been limited time. The watchdog technique prevents black hole attacks. This technique involves nodes.it will then send and share the packet to others and verify if the other node is sharing the same packet and so on. For this, for sharing with the transmission information, all nodes must have a high trust degree. Again, using the Minimizing of black hole attack may also be achieved using clustering technique. In this case, however, only the cluster heads are liable. The main communication. There are different routing protocols against for worm hole attacks. The protocols are meant to get details on correct placement of each node using various sensors. This information is propagated through the network. Consequently, every node will have identical coordinates associated with it. Message filtering solutions play a crucial role in mitigating fake communication issues. Here, verified RSUs receive data from nodes. Therefore, whenever any node gives its location (face) data to other nodes, each RSU can perform such computations take hold of the data and compare with all other data. Only when RSUs are certain about the appropriateness of the data. the data gets shared in the network. The position information attack can be countered via a proper verification process. The attack node should not be able to spoof false position information to multiple RSUs at once. information in the network. Checking sensors frequently will help prevent such attack types as illusion and GPS spoofing. This process needs to repeated at specified intervals after it is being implemented.

IDS IN VANET

Therefore, when it comes to VANET security, IDS is the most suitable answer from the beginning. Different types of IDS provide the diversity of VANET detection strategies. However, it's indispensable that we use IDS in designing VANET. one should have at mind that IDS are not a complete security assurance from any kind of attack. Therefore, it is required to find a group a large majority of area in security can be covered by IDS.

Signature based IDS:

Signature-based intrusion detection system relies on previous records and compares them with new data collected malicious events. The unsuitable pattern is retrieved by this IDS through pattern matching process. Here, the false positive(FP) is low. Therefore, it is challenging to implement signature-based IDS in VANET. Controller management should be able to collect and save all of the logs of previous detection in order to have appropriate outcomes. New attacks can go unnoticed in signature-based IDS, as there aren't any logs of the new attacks. Thus, it gives an opportunity for new malicious attack which can bring down the whole network.

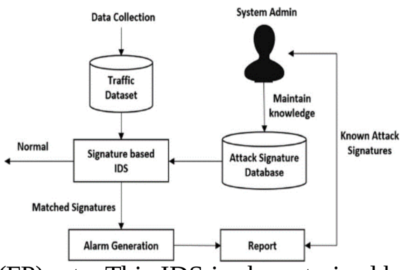


Watch-dog based IDS:

This kind of IDS, particular nodes are assigned to observe other neighboring nodes to ascertain how much they behave those nodes. In this case, an intermediate point that transmits information from the source node towards the target is considered. But the sourcing watches what happens in the nearest nodes and when they send their data to the local nodes. The actual data sent to the destination node is monitored by a source node. If there seems any The server receives an alarm regarding the type of disturbance from the originating point.

Anomaly based IDS:

The nodes' behavior defines the attack modes used by anomaly-based or node-based IDS. This IDS makes different It maintains the latest profiles of various nodes and frequently updates the details.. This is achieved by employing different statistical methods update the profiles. The profile updates are done by clustering in this IDS as well. However, it has got a very high false positive (FP) rate. This IDS is characterized by large delay/overhead and it consumes significant amount of computation resources.



Cross layer based IDS:

Generally speaking, IDS is installed in application layers and it can only find the attacks of the application alone layer. However, the attacker can hit other layers as well. Cross-layer IDS involves deploying IDS into different levels of network operations. To this end, it has different security detection mechanisms that ensure the layers have not failed. This IDS also use improving detection accuracy via a watchdog-based IDS. The second one is considered as being a more deferred and heavier IDS.

a efficient way.

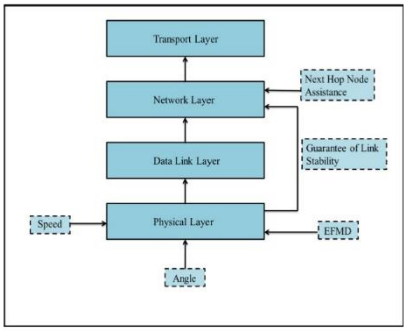


Fig. 4. Proposed Cross Layer Architecture in CL-RVR.

Hybrid IDS:

Hybrid IDS refers to combining the signature and anomaly-based IDS. These types of IDSs use historic logs and frequently updates the profiles. This IDS is configured based on the information provided in its profiles. This IDS is capable of detecting known and new attacks on the network. It is not cost effective as combining the multiple IDS is difficult . Though the detection rate is This IDS has a great delay, thus making it high in this IDS.

Honeypot based IDS:

Selfish Nodes Detecting System based on Honey Pot IDS. In order to watch the movement of vehicles, it has a selfishness detection system activity. Each time it receives such a behavior, it cuts its connections with those nodes. This process reduces packet loss rate and enhances throughput while minimizing average end-to-end latency. But this process provides extra however, this IDS will require additional module aimed at improving the accuracy of its detections.

IDS types	**Comparison Different Attacks**		
	Security attacks	***features***	***Limitations***
Signature based	DoS, false atert, fake congestion	This IDS verifies the identities of all nodes and monitoring the behaviors of the nodes, detects the malicious nodes. Fake messages can be easily detected by this IDS.	Cannot detect zero-day attacks. ●New types of attacks cannot be detected easily. • Depends on the previous records.
Watch-dog based	Blackhole, false alert	It employs various statistical techniques. identify the corrupt nodes that offer support. false alerts. It provides a threshold to detect attacks. This IDS has low FP rate.	It only detects particular attacks. selfish, greedy and misbehaving nodes. Extra delay and overhead. in the network.
Cross layer based	Blackhole	Compares differently. normal and abnormal behaviors.	Not energy efficient. Extra delay and overhead.
Honeypot based	DoS, Blackhole	A lot of famous assaults are very easy for it to discern. zero-hour attack as well as zero-day attack. generalized framework	It requires additional components to be efficient. detection rate. High overhead.

CONCLUTION

Therefore, VANET becomes a promising technology in wireless environment. A large amount of users wants too safe as much as possible safety on this path, with plenty of people around getting hurt by others' harassment and ill-will. In the in order to have a secure VANET's environment one need to put in more efforts on overcome future problems. This paper Most VANET security challenges and their solutions will be introduced, summarily. causes and solutions. In this section, we discuss various attacks on VANET. We explain different IDS in Comparison of the solution for various attacks in VANET. Challenges in security and their solutions at different levels. It also addresses attack or any detection for fake information in VANET. difficult problem. Various effective procedures as well as adaptable discovery methods can be used on the basis of computer. other promising research direction relates to VANET safety, for instance using intelligence designs in future studies.

FUTURE SCOPE

"The sky for healthcare innovation is the limit", with respect to the recent advances in sensor tech, AI, and ML. The introduction of the IOT also brings forth not only new opportunities but the obligation for their utilization in patients, hospitals and doctors, and medical device manufacturers. It is clear that hurdles as well as major risks must be overcome. For health infrastructures, artificial intelligence, and block chain technology drive improvement of user experiences within the reviewed literatures. With regard to intelligent systems in smart cities, despite the fact that these solutions may be risky in general, their application can change the perception of the existing model of health care and smart cities in general.

REFERENCES

C. R. Dow, M. H. Ho, Y. H. Lee, and S. F. Hwang, "Design and Implementation of a DSRC Based Vehicular Warning and Notification System," 2011 IEEE International Conference on High Performance Computing and Communications, pp. 960–965, 2011.

F. Bai and H. Krishnan, "Reliability Analysis of DSRC Wireless Communication for Vehicle Safety Applications," 2006 IEEE Intelligent Transportation Systems Conference, pp. 355–362, 2006.

K. Indira and E. C. Joy, “Energy Efficient IDS for Cluster-Based VANETS,” Asian Journal of Information Technology, 14(1), 37-41, 2015.

G. Loukas, T. Vuong, R. Heartfield, G. Sakellari, Y. Yoon, & D. Gan, “Cloud-based cyber-physical intrusion detection for vehicles using deep learning,” Ieee Access, 6, 3491-3508, 2017.

K. A. 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, 2016.

O. Y. Al-Jarrah, C. Maple, M. Dianati, D. Oxtoby, and A. Mouzakitis, “Intrusion Detection Systems

K. Zaidi, M. B. Milojevic, V. Rakocevic, A. Nallanathan, and M. Rajarajan, “Host-Based Intrusion Detection for VANETs: A Statistical Approach to Rogue Node Detection,” IEEE Transactions on Vehicular Technology, vol. 65, no. 8, pp. 6703–6714, 2016.

S. M. Sangve, R. Bhati, and V. N. Gavali, “Intrusion detection system for detecting rogue nodes in vehicular ad-hoc network,” 2017 International Conference on Data Management, Analytics and Innovation (ICDMAI), pp. 127–131, 2017.

F. Sakiz and S. Sen, “A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV,” Ad Hoc Networks, vol. 61, pp. 33–50, 2017.

A. Kapadia, N. Triandopoulos, C. Cornelius, D. Peebles, and D. Kotz, “AnonySense: Opportunistic and Privacy-Preserving Context Collection,” Lecture Notes in Computer Science Pervasive Computing, pp. 280–297, 2008.

S. Marti, T. J. Giuli, K. Lai, and M. Baker, “Mitigating routing misbehavior in mobile ad hoc networks,” Proceedings of the 6th annual international conference on Mobile computing and networking - MobiCom 00, pp. 255–265, 2000.

R. V. der Meulen and J. Rivera, “Gartner says by 2020, a quarter billion connected vehicles will enable new in-vehicle services and automated driving capabilities,” Gartner) Retrieved September, 18, 2015.

I. A. Sumra, I. Ahmad, H. Hasbullah, and J.-L. B. A. Manan, “Classes of attacks in VANET,” 2011 Saudi International Electronics, Communications and Photonics Conference (SIECPC), pp. 1–5,2011.

J. Grover, M. S. Gaur and V. Laxmi, “Sybil Attack in I. Aad, J.-P. Hubaux, and E. W. Knightly, “Denial of service resilience in ad hoc networks,” Proceedings of the 10th annual international conference on Mobile computing and networking MobiCom 04, pp. 202–215, 2004.

A. S. K. Pathan (Ed.), “Security of self-organizing networks: MANET, WSN, WMN, VANET,” CRC press, 2016.

Y. C. Hu, A. Perrig, and D. B. Johnson, “Packet leashes: a defense against wormhole attacks in wireless networks,” IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE Cat. No.03CH37428), vol. 3, pp. 1976–1986.

K. Verma, H. Hasbullah, and A. Kumar, “Prevention of DoS Attacks in VANET,” Wireless Personal Communications, vol. 73, no. 1, pp. 95–126, Nov. 2013.

J. Hortelano, J. C. Ruiz, and P. Manzoni, “Evaluating the Usefulness of Watchdogs for Intrusion Detection in VANETs,” 2010 IEEE International Conference on Communications Workshops, pp. 1–5, 2010.

P. Patel and R. Jhaveri, “A Honeypot Scheme to Detect Selfish Vehicles in Vehicular Ad-hoc Network,” Lecture Notes in Networks and Systems Computing and Network Sustainability, pp. 389– 401, 2017.