Modern Applied Science; Vol. 11, No. 5; 2017
ISSN 1913-1844 E-ISSN 1913-1852
Published by Canadian Center of Science and Education

Vehicular Ad Hoc Networks and Security Issues: Survey

Zaid A. Abdulkader[1,2], Azizol Abdullah[2], Mohd Taufik Abdullah[2] & Zuriati Ahmad Zukarnain[2]

[1] Al Iraqia University, Baghdad, Iraq

[2] Faculty of Computer Sciences and Information Technology Universiti Putra Malaysia 43400 Serdang, Malaysia

Correspondence: Azizol Abdullah, Faculty of Computer Sciences and Information Technology Universiti Putra Malaysia 43400 Serdang, Selangor, Malaysia. E-mail: azizol@upm.edu.my

Received: January 28, 2017 Accepted: February 25, 2017 Online Published: April 8, 2017

doi:10.5539/mas.v11n5p30 URL: https://doi.org/10.5539/mas.v11n5p30

Abstract

Vehicular ad hoc network (VANET) technologies are evolving networked communications advances that incorporate mobile-based routing protocol sets for inter-vehicular exchanges of information in support of smart transportation networks. Privacy and security difficulties are primary concerns in VANET research as a result of the repeated vehicular movements, time-critical responses, and hybrid VANET architectures that differentiate these from other ad hoc networking types. Therefore, the design of secure mechanisms for authenticating and validating message transmissions between vehicles and eliminating adversarial elements from networks are of considerable importance in VANET research. This report offers a review of VANET features and security difficulties. The paper also summarizes certain chief threats to the authentication, confidentiality, and availability of secure services.

Keywords: vehicular ad hoc networks, security, privacy, road side unit, on-board unit, wormhole attack, sybil attack, blackhole attack

1. Introduction

Most people these days use vehicular transports to transit between various places. The increase in vehicular traffic on street networks has also led to rising road queues and fatalities. These can be lessened by affording proper knowledge about street conditions and the neighboring environment to the driving public via secure means. Increases in severe driving problems has led to more street accidents and increased traffic congestion. To resolve these types of problems, vehicles can be equipped with networked communications for exchanging data between vehicles and among vehicles as well as road side units (RSUs). So as to share linked data on important road situations, VANETs provision dual categories of communication exchanges, e.g. vehicle-to-vehicle (V2V) communications and vehicle-to-RSU (V2R) communications (Blum & Eskandarian, 2004). With vehicle-to-vehicle communications, cars directly exchange communications with other cars in order to share situational data. With vehicle-to-RSU communications, cars directly exchange communications with RSUs that are installed alongside the roads. Dedicated short-range communications (DSRC) radio (Jiang and Delgrossi, 2008) is utilized for V2V and V2R communication exchanges in VANETs. The information shared in VANETs is categorized into dual categories, namely safety data and non-safety data. In these dual categories of information, safety data such as curve speed and pedestrian crossing alerts comprise the primary knowledge that is shared to inform drivers about upcoming dangers, so as to reduce the chances of encountering traffic accidents and queues. The objective of provisioning safety data is to protect lives, health, and property (Robinson et al., 2007). Non-safety data is used to improve driving comfort and afford riders value-added service offerings, including pointers to the nearest hospitals and petrol station (Plossl et al., 2006) (Jakubiak & Koucheryavy, 2008). Safety data is not, however, prioritized over non-safety data. Although VANETs offer numerous facilities, malicious users can target VANET wireless media and expose these to different kinds of exploits, including eavesdropping, interference, jamming, etc. (Dhamgaye & Chavhan, 2013). Although numerous exploits exist for compromising the VANET communications security, several researchers have evolved dissimilar strategies (Hao et al., 2011) (Zhang & Lu, 2008) in securing VANET communications. VANET designs must essentially deliver on security for services in terms of information integrity, confidentiality, availability, authentication, and non-repudiation in order to safeguard VANET networks from attack (Raya & Hubaux, 2007). The safeguarding of privacy is an additional major difficulty. To preserve the privacy of users' information, their actual identities (ID) and locational data needs to be protected from undesirable intrusion. User information can be however be transmitted

to a trusted authority (TA) whenever criminal incidents or disputes arise. This survey is further systematized in the following manner. An overview of VANET is described in Section 2, while a brief explanation of VANET difficulties is given in Section 3. Fuller descriptions of security requirements and issues are given in Section 4 and Section 5. Lastly, this research is summarized with its conclusion in Section 6 at the end.

2. Summary of VANET Schemes

A vehicular ad-hoc network (VANET) comprises a specific case of ad hoc networking wherein the communicating nodes comprise vehicles that have unfixed or non-existent infrastructure. These have arisen to supply comforting and flexible services to drivers and passengers and provision communications on the way, such as providing alerts on emergencies some kilometers from their current position. Various VANET implementations can be implemented via Peer-to-Peer (P2P) communications or otherwise multi-hop communications (Blum & Eskandarian, 2004). VANETs continue to supply new application types as they confront numerous challenges. Networks are responsible for communications among moving vehicles. There are different VANET application types, including Road Traffic Safety, Traffic Efficiency or Engineering, Quality and Comfort of Road Travel, Dynamic Topologies, Frequent Disconnection, Mobility Models, Predictive Mobility Patterns, Uses of Other Technologies, Stringent Delays and No Power Constraints. VANETs account for communications among moving vehicles in some environments. Such exchanges can be categorized as (a) Vehicle-to-Vehicle Communications and (b) Vehicle-to-Infrastructure Communications (Road Side Unit) (Abdulkader et al., 2017). The range of application types has led many to term such a network as an Intelligent Transportation System (ITS) (Jiang & Delgrossi, 2008). Certain problems in ad hoc networking that appear in VANET communications such as interferences can be generated with multiple nodes communicating with a single node via direct connections. Thus, multi-hop connections are utilized with certain technologies, including Bluetooth and frequency-hopping schemes (Robinson et al., 2007). Nonetheless, due to VANET multi-hop transmissions, routing problems still remain as no there are no figures for networking infrastructure involving vehicular nodes. A VANET is considered to be a mobile ad hoc network (MANET) subclass. There are particular differences such as recurrent topology changes with increased speeds, increased likelihood of network fragmentation given the vehicle speeds, less rigorous limits on power draw, large-scale operation inside cities and their boundaries and motorways, based on vehicular behaviors in response to delivered messaging (Jiang and Delgrossi, 2008). Vehicles have particular components that allow them to communicate with others. These components are termed On-Board Units (OBUs). Additionally, VANET architectures can represent dissimilar schemes, including wireless local area network or cellular (WLAN), ad hoc, and hybrids. With the first type, vehicles communicate information with base stations termed road side units (RSUs) or fixed remote nodes (V2R). With the second architecture, vehicles communicate directly with no need for intermediate nodes (V2V communications). The third, hybrid-type architecture blends the previous types. As well, vehicles in a VANET send self-information to fixed remote nodes, including their speeds, directions, accelerations, and traffic condition. Dedicated short range communications (DSRC) are standards that have risen to support IEEE 802.11 in communication exchanges among vehicles. An IEEE P1609 working group also suggested DSRC for the IEEE 802.11p standards that provide specifications for wireless media access control (MAC) and physical layers for wireless access in vehicular environments (WAVE) (Jakubiak & Koucheryavy, 2008).

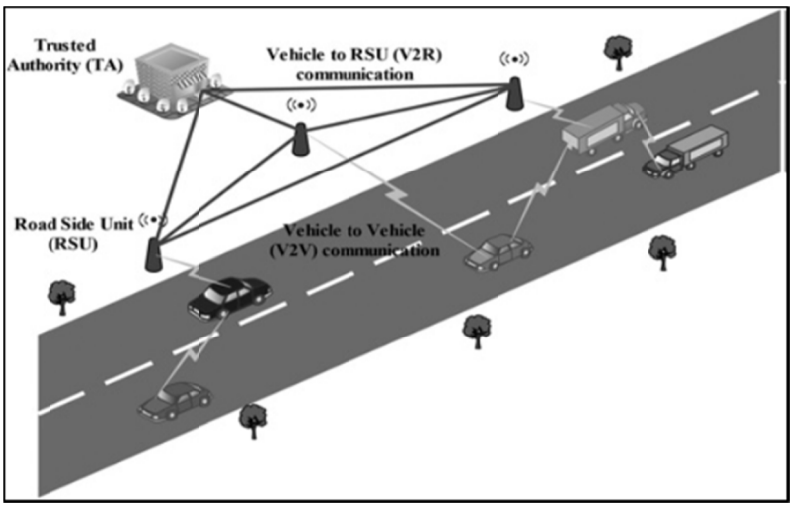

Figure 1. VANET Scheme

2.1 VANET Schematic Model

A VANET scheme is depicted in Fig. 1, comprising a trio of key components to include trusted authority (TA), fixed RSU, and an on-board unit (OBU) installed in moving vehicles (Ghosh et al., 2009). Every vehicular OBU is linked with groups of sensors that collect the observations such as velocity, compromising data and so on. These collected observations are transmitted as messages to neighboring vehicles via wireless mediums. Every RSU is interlinked with one another, and in turn are linked to TAs via wired connections. The TA serves to maintain the entirety of the VANET system.

1) Trusted authority: TA accounts for registrations of RSUs, vehicular OBUs, and vehicle users. Furthermore, it also serves to verify authorizations of actual vehicular OBU or user IDs, so as to prevent adversarial vehicles (Ghosh et al.,2009) from accessing VANET systems. The TA is established with powerful computational infrastructure and enough storage capacity. A TA can reveal the actual ID of OBUs in the event of malicious messaging broadcasts or other behaviors.
2) Road side unit: RSUs are typically stationary units that are installed alongside streets or in fixed sites to include parking or street intersection locations. RSUs resemble OBUs in that they contain transceivers, antennae, processors, and sensor clusters. Each RSU is intended to provision wireless services to vehicle users. For instance, an RSU may be located near a street intersection in order to regulate the traffic as well as to reduce accident incidence. Each RSU utilises DSRC radios according to IEEE 802.11p radiofrequency technology to retrieve radio channels utilising omnidirectional or directional antennae. For RSU to send messages to a particular location, directional antennae may have to be installed. Furthermore, it may be further equipped with various networking equipment to communicate with TAs and farther RSUs. Each RSU possesses the storage capacity to store the data from vehicular OBUs as well as the TA.
3) On board unit: OBUs are transceivers installed in vehicles for exchanging data with RSUs as well as the other vehicular OBUs in collaboration with computing devices. The components of an OBU comprise a resource-commanding processor for computational capacity, read/write capacity for data storage and retrieval, a user interface, and a DSRC radio that works according to IEEE 802.11p radio technology in order to retrieve wireless channels (Dhamgaye and Chavhan, 2013). OBUs draw power from the vehicular batteries. All such vehicles additionally feature sensors such as global positioning systems (GPS) receivers, tamper-proof devices (TPD), event data recorders (EDR), and velocity as well as forward- and rear-facing sensors that provide inputs to OBUs. The sensors gather data about surrounding conditions. Of this equipment, the GPS receiver is utilised to supply geographic data in terms of the location of vehicles. The TPD is utilised to record sensitive information such as the private and group keys and IDs of vehicles. EDRs are utilised to record data associated with accidents or vehicular crashes. Speed sensors are utilised to gather the recordings such as velocity and compromising data. Forward- and rear-facing sensors are utilised to monitor events occurring to the front and rear of vehicles. These monitored and collected recordings are transmitted as messages to neighbouring vehicles via wireless media.

2.2 Features of VANETs

VANETs comprise a wireless network where nodes entities comprise either fixed street components or highly-mobile vehicles. Entities transmit messages to others as ad hoc nodes, exchanging information with the equipment operating along the streets in infrastructure modes. Thus, the features of VANETs essentially blend the properties of wireless media and the features of various topologies in infrastructure and ad hoc modes. These features include:

1) Increased mobility: The increased nodes mobility of VANETs is among their most salient features. In normal network operations, nodes move about continually, with varying directions and velocities. Based on (Zeadally et al., 2012), the increased nodes mobility degrades the networking mesh with fewer routes across nodes. In contrast to MANETs, VANET mobility can be comparatively high. In the literature, research (Hossain and Atiquzzaman, 2009) has been particularly dedicated to studying the influence of mobility factors on ad hoc networks, particularly with vehicular networking.

2) Dynamic topologies: With increased mobility, VANET topologies change rapidly and as a result are dynamically non-predictable. Connection times are brief, particularly across nodes that move in opposite directions. The topology enables the exploitation of entire networks, making it a challenge to detect malfunctions.

3) Recurrent disconnections: The dynamic topologies involved and the high nodes mobility as much as the other conditions including weather and traffic densities can result in recurrent disconnections of vehicle users from networks.

4) Availabilities of transmitting mediums: The air is the transmitting medium of a VANET. Even though the universal accessibility of this wireless transmitting media is among its greatest advantages in IVC, its properties also lead to particular security issues associated with the nature of transmissions in wireless environments as well communication security with open support.

5) Anonymous support: Data transmissions that rely on wireless media are typically anonymous in nature. Leaving aside the constraints and usage limits, any user with a transceiver that operates in the same frequencies can send and hold those bands (Blum and Eskandarian, 2004).

6) Constrained bandwidth: The standardized DSRC band (5.850–5.925 GHz) for VANET can be regarded as constrained as the breadth of the entire band spans just 75 MHz. Usage constraints in certain nations imply that this range is not always accessible. Maximum theoretical throughputs can reach 27 Mbps.

7) Attenuation: DSRC bands are also subject to problems with transmissions that are associated with digital transmissions on these frequency bands, including diffraction, reflection, dispersion, various classes of fading, Doppler effects, propagation delays and losses as a result of multi-pathing reflections.

8) Constrained transmission power: Transmitting power is constrained in WAVE architectures, limiting the distances that information can traverse to around 1000 meters. Nevertheless, in particular instances such as public emergencies and safety alerts, transmissions of higher power are usually allowed.

9) Power draw and computing: Compared to other mobile network types, VANET operation are not subject to power draw or computing capacity problems as well as storage failures. Nevertheless, meeting the concurrent processing requirements for large quantities of data can be challenging.

2.3 VANET Applications

VANETs facilitate communication exchanges between neighboring vehicles and among the vehicles and neighboring fixed equipment. Every vehicle type can take advantage of VANETs. Road side units are typically maintained by government agencies. However, the operations are privatized in certain nations. The various categories of VANET application types are categorized as follows:

1) Street safety applications: For the purpose of improving travel safety and reducing street incidents, VANET applications can offer collision and street work avoidance, detections of fixed and moving obstacles, and distribution of weather alerts. Among this class of implementations are Slow/Stop Vehicle Advisors, Emergency Electronic Brake Lights (Mishra et al., 2011), Post-Crash Notifications, Road Hazard Control Notifications, and Cooperative Collision Warnings.

2) Driver assist applications: The objective is to enhance driving and help drivers in particular situations, i.e. in the overtaking of cars, avoidance of channel outputs, discovery and alerts of congestions, alerts of potential traffic queues, etc. Among this class are congested road notifications, parking availability notifications, and toll booth collection information.

3) Passenger comfort applications: These types are meant to comfort drivers and riders, as they basically provision services including mobile Internet messaging, discussion, and access among vehicles, collaborative networked gaming, and so on. In the remaining part of this section, we shall limit discussion to the explanation of certain services, with implementation examples of vehicle-to-vehicle communication systems.

3. Challenges with VANETs

In spite of the advantages of VANETs, several difficulties must still be tackled by the industry and researchers. Certain of these problems are listed as timing constraints, networking scales, nodes volatility and mobility (Issac et al., 2010).

3.1 Timing Constraints

One critical prerequisite of VANET operation is associated with each node's capability for transmitting messages within standard timings. A few implementations, including those pertaining to safety, entail rigorous deadlines (Yang et al., 2004). Nevertheless, it can be challenging to validate messaging authenticity, thus increasing the delivery times with respect to messaging delivery deadlines. It is quite critical to meet important deadlines in particular instances with some application types (Torrent et al., 2005). As an example, all the implementations employed by emergency services necessitate timing constraints for message delivery. Drivers who receive alert messages require enough time to respond. If arrival deadlines are not respected, it may be too late for the consequences not to be disastrous.

3.2 Network Scale

VANET is poised to emerge as the most widespread ad hoc networking worldwide. Node counts of such networks can exceed 750 million and are still rising (Samara et al., 2010). Nevertheless, numerous issues remain about the applications and deployments involving such networks. Global authorities that can regulate such a networking are yet to be established. Security and privacy issues for users can vary across different regions of the world. Thus, it will be difficult to standardize on rule sets in terms of the deployments and utilization of such networks. Another issue is which authorities will be regulating the management of identifications and allocating private and public keys. Such collaboration with respect to key installations is required by manufacturing concerns the world over (Raya et al., 2006).

3.3 High Nodes Mobility

High nodes mobility in VANETs has led to considerable difficulty in research. It is not possible to apply conventional authenticating methods for messages and nodes as a result of the high levels of nodes mobility. It is not feasible to recommend protocols that utilize handshakes in VANET schemes, since certain nodes will exchange communications only once and insufficient time hampers checks of the authenticity of every message receipted from all nodes. Addressing mobility issues is a key problem area and even though several research efforts have covered these difficulties, many issues remain (Karnadi et al., 2007). Security protocols lead to mobility limitations. Messages can be transmitted without consideration of the mobility of secure vehicles via unicast or broadcast strategies. These approaches do not impose either specialized routes or particular speeds on drivers (Gosman et al., 2010). As vehicles continually change their network attachment points whenever Internet services are accessed, there is a need for mobility management systems that offer seamless communications. Such capabilities must meet prerequisites that involve seamless mobility, scalable overhead, support for IPV6, and low-latency handoffs. All VANET nodes are highly mobile and vehicles interconnect with each other in sessions of only a few seconds. Therefore, secure protocols necessitate significant interaction among senders and receivers (Parno and Perrig, 2005). Any two vehicles that have never come across each other may never interact in the future (Samara et al., 2010).

3.4 Volatility

Connection timespans across two nodes may vary and such events may transpire just once. All vehicles have a high mobility level, so links among the vehicles can be lost and stay so after a few wireless hops in a narrow interval of time. Moreover, the linked autos could be even travelling in opposing directions (Raya et al., 2006). As a result of the insufficiently long-lived contexts in VANET schemes, it would be challenging or impossible to attain the long-lived passphrases needed to ensure high security for personal contacts channeled by user devices. The contacts in these secure channels would need long-lived passphrases, which is not practical for safety in vehicular communications as a result of the brief lifetimes of such contexts (Samara et al., 2010).

4. Security prerequisites

Prior to reviewing VANET security issues, it is important to review the prerequisites that such schemes have to meet to maintain proper network operation. Any failures in meeting conditions may invite probable security attack. The main prerequisites described in (Biswas and Misic, 2010) are: availability, access control, integrity, confidentiality, authentications, non-repudiation, privacy protections, and real-time constraints. The majority of these conditions are associated with generalized security issues, while others are particular to VANET. The section following this discusses the details related to these needs.

4.1 Authentication

This is among the main prerequisites for any scheme. With a VANET, it is rather critical to obtain some information about transmitting nodes, including their identifications, as well as that of message senders and their properties and locations. It is critical to authenticate every user and message that transit through these networks. Authentications control the authorization levels of vehicle users. With VANETs, authenticating processes prevent Sybil exploits by assigning particular identities to every vehicle. For example, congestion avoidance can prevent single vehicles from presenting themselves as a group comprising a hundred cars for the purpose of providing the illusion of a congested street. Effective authentication can supply legal evidence through the use of external mechanisms, including traditional law enforcement, in order to detect exploits (Parno & Perrig, 2005). There are numerous means of authenticating users and messages (Kargl et al., 2006): ID authentications permit nodes to identify the transmitters of messages via a unique means. This authenticating method also enables nodes to join networks. Once the ID authenticating method is set, it is readily easy to prevent some exploits, including the impersonation or faking of nodes. Proper authentication assist in determining what type of entity is transmitting,

such as a car, an RSU, or else other equipment types. Location authentications help to verify nodes positions whenever location applications are involved.

4.2 Integrity

Integrity makes sure that messages are not modified between the times they were transmitted and received, as the information received needs to match the information transmitted. The receivers will then corroborate sender identities during transactions (Biswas & Misic, 2010). Integrity safeguards against unauthorized creation, erasure, or modification of information. If corrupt information is accepted, integrity property violations occur and protocol flaws would be recognized. To attain integrity, systems have to stop attackers from modifying messages, as message contents have to remain trustworthy (Papadimitratos et al., 2008). Outside agents will be prevented from interpolating messages via authentications (Issac et al., 2010). Security protocols work to ensure that information is not compromised whenever it is forwarded between secure vehicles onto its final destination, as a result of messaging-appended signatures from secured traffic light installations. Messages can also be validated with comparable transmissions produced in the immediate neighborhood within small time intervals (Stampoulis & Chai, 2007).

4.3 Confidentiality

In exchanges among nodes (vehicles or infrastructure), outside agents should not be able to discern confidential knowledge that is associated with any entity. This can be attained as a result of data encryption that works to protect confidential information for all users (Papadimitratos et al., 2008) including user identities and usage profiles (Issac et al., 2010). Messaging confidentiality in VANETs depends on the particular implementation scenario. Safety-related messages as an example do not normally comprise sensitive knowledge, and encryption is therefore not necessary in this case. Nevertheless, a few messages from applications, including those employed for toll payments wherein vehicles require Internet services from RSUs, need to be communicated confidentially via encryption systems. Confidentiality is attained through the use of symmetric or public key encryption, in order to ensure communication security. With V2I communications, both RSUs and vehicles share session keys that are produced after mutual authentications. Every message is successively encrypted for confidentiality using these session keys, which are also affixed to the Message Authentication Code (MAC) for information authentication (Kim et al., 2011). Non-repudiation is described as the unfeasibility for any one node involved in exchanges of communications to deny prior participation in part or whole of particular communication event. These safeguards against false denials involving communications. Non-repudiation supplies receivers with proof that senders are responsible for the messages produced (Armknecht et al., 2007). The primary objective of non-repudiation comprises the gathering, maintenance, availability, and validation of undeniable evidence regarding a particular action or event, for the purpose of resolving disputes on the occurrence or absence of such action or event. Non-repudiation is dependent on authentication; however, it produces strong evidence since the scheme can recognize an attacker who cannot then deny his violation. Violators or misbehaved users cannot deny such actions under such a system. All vehicle recordings including speeds, times, trip routings, and violations are recorded in a tamper proof device (TPD), from which an authorized official can retrieve the information (Papadimitratos et al., 2008).

4.4 Availability

Networks and their applications must stay operational even when faults or malevolent conditions are present. This entails not just secure but fault-tolerant designs, resilience to depletion exploits, and survivable protocol sets, all of which should return to normal once fault-inducing agents are removed (Yi & Moayeri, 2008). Proper routing protocols are needed to reach every involved recipient that may remain unknown to senders. Some messages such as icy street alerts must also be maintained in specified locations for a certain interval of time (Plossl et al., 2006). This addresses the availability of some resources that are handled by the associated protocol. In the example of key-exchange protocols, it must be ensured that sessions will be actually established. Thus, if a user x1 requests a server to initiate session key set up, the system must consequently attain a state wherein both x1 and the server retain information about the new session key (Li et al., 2008). Several implementations need more immediate responses from sensor or ad hoc network components, as delays can render some messages meaningless, with harmful consequences. Particularly, in instances where application layers become unreliable, partial messages can be recorded for future transmission completion, in order to ensure the future availability of recordings. Therefore, a real-time or a near-real-time approach is needed for several VANET implementations.

4.5 Access Control

This prerequisite has the function of determining network rights and privileges. Particularly sensitive communication exchanges, including those from police vehicles or other law enforcement, should not be

receivable by other unauthorized network nodes. The retrieval of particular services provisioned by the infrastructure and other nodes is established via local policies. Within access controls, authorizations establish the rights of all networked nodes (Yi & Moayeri, 2008). In (Moustafa et al, 2006), Moustafa et al. presented a Kerberos modelled scheme wherein all services demand particular credentials from clients in the form of tickets. Of the dual ticket categories, Ticket Granting Tickets (TGT) and Ticket Granting Services (TGS), TGT permit clients to obtain TGSs, whereas TGS grant service requests to each client. Clients should therefore initially obtain TGTs before requesting TGS for all the services desired. These access control provisions therefore represent a further warrant that stops unauthorized users from inadvertently or maliciously accessing services where they have no retrieval rights.

5. VANET Security Attacks

In this part, we discuss numerous security attacks on VANETs.

5.1 Sybil Attacks

In Sybil attacks, attackers transmit multiple messages to other vehicles, with all containing various spoofed source identities (ID). It pushes illusions to other vehicles via a few false messages such as traffic queue messages (Manik et al., 2006). Fig 2 describes Sybil exploits whereby adversaries create multiple vehicles on the streets using the same ID. They aim to compel other users to exit the road and open a path that advantages the attackers.

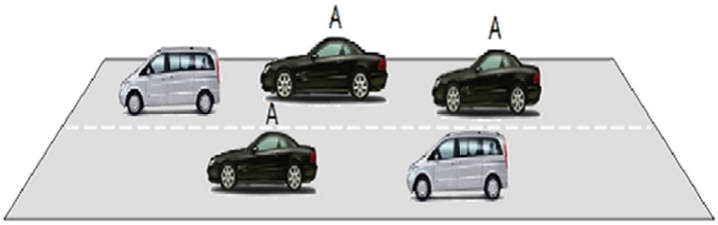

Figure 2. Sybil attack

5.2 Node Impersonation Attacks

In VANETs, every vehicle is assigned a unique ID based on how each is recognized within the network. This becomes more significant whenever accidents happen. In nodes impersonation attacks, attackers can change their identities to act as actual originators of the messages. Such adversaries receive the messages from the real originators of these messages, altering the contents for their own respective advantages and then resending these false messages to surrounding vehicles (Churn et al., 2008).

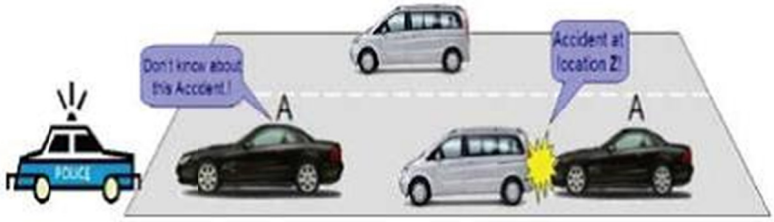

Figure 3. Node Impersonation Attacks

5.3 Messaging Suppression

Attackers can selectively cast out network packets that may contain important data that is needed by their intended recipients (Yi-Wei & Wu, 2003). Adversaries can suppress such received congestion warnings so as to stop other nodes from seeking alternative paths to their respective routing destinations, compelling other vehicular users to wait in traffic. This may later prove profitable for such attackers, for they may re-utilize these same packets in order to get ahead. The primary aim of such attacks would be to thwart the authorities from learning about collisions and other road events via RSU alerts.

5.4 Black Hole Attacks

With this attack, attacking vehicles refuse to participate in networks, or established vehicles drop connections in order to form black holes. In this exploit, all informational packets are forwarded to a specific vehicle, whose

existence is not made publicly available. Attack vehicles may select malicious code that forces packet loss in performing denial-of-service attacks or exploit its location along the route as the initial phase for man-in-the-middle exploits.

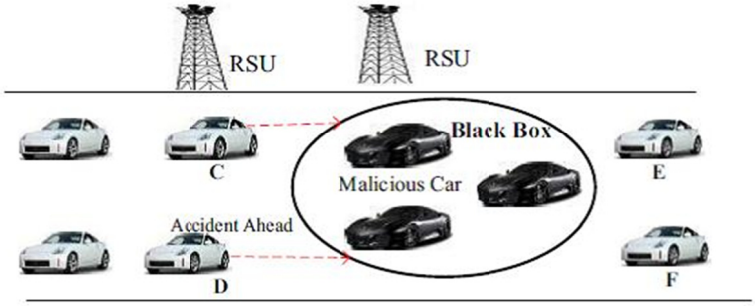

Figure 4. Black Hole Attack

5.5 Malware Attack

Malware exploits are much like viruses in that they can degrade normal network operations. VANETs normally become infected by such exploits whenever software updates are applied to VANET or RSU units (Carlos et al., 2007).

5.6 Eavesdropping

This is among the more significant attacks against confidentiality over VANETs. To perform such attacks, adversaries can either be in a car that is stopped or moving, or else in false RSUs, in order to demonstrate that they form parts of the main network. The illegal aim is to retrieve confidential information.

5.7 Man-in-the-Middle Attacks

As implied, adversaries sit in the middle between two vehicles that are in communication, ready to launch such attacks. With this approach, attackers manipulate all communications among senders and receivers, although the vehicles assume that they are in direct communication with one another (Moustafa et al, 2006). Mime attacks listen to communications among the vehicles in order to introduce false or else modified data.

5.8 Misleading Information

In such forms of attack, the adversary belongs to an outsider/intruder or else insider/legitimate node. Attackers broadcast incorrect data on vehicular networks so as to influence the algorithms of other cards, by disseminating false data around the network (Raya et al., 2006).

5.9 Denial of services (DOS) Attacks

In DOS, the primary aim is to thwart legitimate users from retrieving access to and from the networked services and resource materials (Kumar and Sinha, 2014). VANETs comprise many key components, the more vital of which are the road side units (RSUs) that are positioned alongside roads, as well as the on-board units (OBUs) that newer vehicles tend to have as standard equipment. The distribution of safety-related alerts, including turn alerts, speed limit alerts and so on, is one of the more useful VANET applications. As safety alerts can contribute to the survival of persons who are driving while participating in the VANET, security is of less importance to this particular application.

5.10 Distributed Denial of Services (DDOS) Attacks

DDOS exploits are more severe than DOS exploits for these are distributable according to the means for launching attacks. In this, attackers launch attacks from other locations and may introduce varying time slots when initiating their exploits. The time slots and attacking natures of the adversarial vehicles may vary. In total, the exploit scheme relies on vehicles whose primary aim is to take down the network, so that it will not be operationally available for continued use.

5.11 Wormhole Attacks (Tunneling)

ormhole poses a severe threat in VANETS and various other ad hoc networking schemes. With such attacks, multiple malicious nodes set up tunnels to send informational packets to further malicious nodes at the other end, which are then broadcast back to the network (Al-Kahtani, 2012). The adversarial nodes can take control of such

briefly networked connections or links, threatening the security of informational packets in transmission by deleting these.

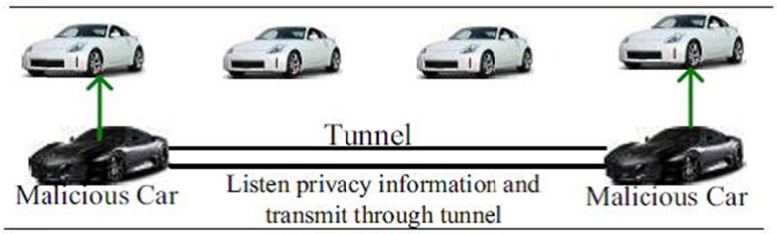

Figure 5. Wormhole Attack

5.12 Timing Attacks

Transmitting information at the right times between vehicles is vital to attaining information integrity and security (Mejri, 2014). In timing exploits, when adversaries receive emergency messages, they will not forward these to the neighboring vehicles at the right times, adding a few timeslots to the original messaging so as to inject delays. Neighboring vehicles will therefore receive the messages long after these were actually needed. Figure 6 shows that when an adversarial black vehicle receives an "Accident Ahead" alert, it transmits the message to the next vehicle once it reaches the proper position F. However, it transmits the message after adding a few timeslots, such that when other vehicles receive the alert, they will already be late at the site F1 where the accident occurred.

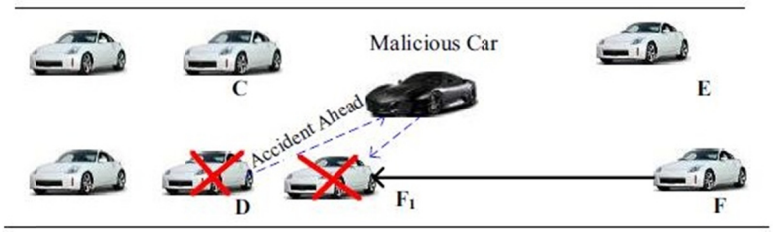

Figure 6. Timing Attacks

5.13 Masquerades

Malicious vehicles can fake their identities and pretend to be other vehicles for their own respective advantages. This is attained by using messaging fabrication, modification, and replay. As an example, adversarial vehicles or other attackers can fake being ambulances in order to mislead other vehicle users into slowing down and yielding to their passage

5.14 Global Positioning Systems (GPS) Spoofing

GPS satellites maintain location tables containing the geographic locations and vehicular identities within the networks (Al-Kahtani, 2012). Attackers can generate false readings in these positioning systems so as to mislead vehicle users into thinking that they are at other locations. Such attacks exploit GPS satellite simulations in order to produce GPS signals that are more powerful than those transmitted by the real satellites.

5.15 Illusion Attacks

This is a novel VANET security threat wherein adversaries broadcast traffic alert messages according to current street conditions, producing illusory maps to mislead other vehicular users within their neighborhood (Mejri, 2014). This method is capable of spreading such illusions based mainly on the responsive behaviors of other drivers, which can induce increased traffic queues and vehicular accidents as well as overall decreased VANET performance. Current message authentication strategies are incapable of securing networks against such illusion-based attacks due to the adversaries' direct control of their own cars' sensors, which allows them to maliciously generate and broadcast misleading traffic data.

6. Conclusion

Vehicular ad hoc networks (VANETs) are gaining popularity in transportation systems as they facilitate traffic

management, offer road safety, and provide access to the Internet on highways; besides distribute safety information to passengers as well as drivers. However, deploying VANETs in value-added services is a major challenge because of the intruder vehicles and multiple security attacks. Therefore, offering privacy and security in VANETs is termed as a major research concern. Furthermore, vehicle movement and the network's dynamic nature present a significant challenge to eradicate malicious vehicles and devise safe data transmission protocols. Although lot of research is being carried out to offer privacy and security in VANETs, the majority of these approaches seek to decrease computational and communication outlay, and processing delay with regards to authentication between the source and destination vehicles. The protocols for applications with high priority are still in investigative stage when it comes to security measures.

References

Abdulkader, Z. A., Abdullah, A., Abdullah, M. T., & Zukarnain, Z. A. (2017). LI-AODV: Lifetime Improving AODV Routing for Detecting and Removing Black-Hole Attack from VANET. *Journal of Theoretical and Applied Information Technology, 95*(1).

Al-Kahtani, M. S. (2012). *Survey on security attacks in Vehicular Ad hoc Networks (VANETs)*. In Signal Processing and Communication Systems (ICSPCS), 6th International Conference on (pp. 1-9). IEEE. https://doi.org/10.1109/icspcs.2012.6507953

Armknecht, F., Festag, A., Westhoff, D., & Zeng, K. (2007). *Cross-layer privacy enhancement and non-repudiation in vehicular communication*, in: Communication in Distributed Systems (KiVS), ITG-GI Conference, 1–12.

Biswas, S., & Mišic´, J. (2010). *Proxy signature-based RSU message broadcasting in VANETs*, in: 25th Biennial Symposium on Communications (QBSC), 5–9. https://doi.org/10.1109/BSC.2010.5473015

Blum, J., & Eskandarian, A. (2004). The threat of intelligent collisions. *IT Prof., 6*(1), 24–29. https://doi.org/10.1109/MITP.2004.1265539

Carlos, J. B., Ignacio, S., & Maria, C. (2007). *VARON: Vehicular Ad hoc Route Optimisation for NEMO, Computer Communication, 30*, 1765- 1784. https://doi.org/10.1016/j.comcom.2007.02.011

Churn-Ta, L., Min-Shiang, H., & Yen-Ping, C. (2008). A Secure and Efficient Communication Scheme with Authenticated Key Establishment and Privacy Preserving for Vehicular Ad Hoc Networks. *Computer Communications, 31*, 2803-2814. https://doi.org/10.1016/j.comcom.2007.12.005

Dhamgaye, A., & Chavhan, N. (2013). *Survey on security challenges in VANET*, Int. J. Comput. Sci. 2,88–96, ISSN 2277-5420.

Dhamgaye, A., & Chavhan, N. (2013). *Survey on security challenges in VANET. Int. J. Comput. Sci., 2*, 88–96.

Ghosh, M., Varghese, A., & Kherani, A. A. (2009). *Distributed misbehavior detection in VANETs.* IEEE Wireless Communication and Networking Conf., WCNC 2009, Budapest, Hungary. https://doi.org/10.1109/WCNC.2009.4917675

Gosman, C., Dobre, C., & Cristea, V. (2010). *A security protocol for vehicular distributed systems*, in: 12th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC), pp. 321–327. https://doi.org/10.1109/SYNASC.2010.9

Hao, Y., Cheng, Y., Zhou, C., et al. (2011). '*A distributed key management framework with cooperative message authentication* in VANETs', IEEE J. Sel. Areas Commun., 29(3), pp. 616–629. https://doi.org/10.1109/JSAC.2011.110311

Hossain, M. S., & Atiquzzaman, M. (2009). *Stochastic properties and application of city section mobility model*, in: Global Telecommunications Conference, GLOBE-COM, IEEE, pp. 1–6. https://doi.org/10.1109/GLOCOM.2009.5425473

Issac, J. T., Zeadally, S., & Camara, J. S. (2010) *Security attacks and solutions for vehicular ad hoc networks*, IET Commun, (4), 894–903. 2010-04-30. https://doi.org/10.1049/iet-com.2009.0191

Jakubiak, J., & Koucheryavy, Y. (2008). *State of the art and research challenges for VANETs.* Fifth IEEE Consumer Communications and Networking Conf., 10–12 January 2008, pp. 912–916. https://doi.org/10.1109/ccnc08.2007.212

Jiang, D., & Delgrossi, L. (2008). *IEEE 802.11p: towards an international standard for wireless access in vehicular environments.* Proc. IEEE 68th Vehicular Technology Conf (VTC 2008-Spring), pp. 2036–2040. https://doi.org/10.1109/VETECS.2008.458

Kargl, F., Ma, Z., & Schoch, E. (2006). *Security engineering for VANETs*, in: 4th Workshop on Embedded Security in Cars.

Karnadi, F. K., Zhi, H. M., & Kun-Chan, L. (2007). *Rapid generation of realistic mobility models for VANET*, in: Wireless Communications and Networking Conference, WCNC IEEE, pp. 2506–2511. https://doi.org/10.1109/WCNC.2007.467

Kim, I. H., Hyoung-Kee, C., & Jae-Chern, Y. (2011). *Secure and efficient protocol for vehicular ad hoc network with privacy preservation*, EURASIP J. Wirel. Commun. Networking. https://doi.org/10.1155/2011/716794

Kumar, A., & Sinha, M. (2014). *Overview on vehicular ad hoc network and its security issues*. In Computing for Sustainable Global Development (INDIACom), International Conference on (pp. 792-797). IEEE. https://doi.org/10.1109/IndiaCom.2014.6828071

Manik, L. D., Ashutosh, S., Ved, P. G., & Deepak, B. P. (2006). A novel remote user authentication scheme using bilinear pairings. *Computers & Security, 25*, 184-189. https://doi.org/10.1016/j.cose.2005.09.002

Mejri, M. N., Ben-Othman, J., & Hamdi, M. (2014). Survey on VANET security challenges and possible cryptographic solutions. *Vehicular Communications, 1*(2), 53-66. https://doi.org/10.1016/j.vehcom.2014.05.001

Mishra, B., Nayak, P., Behera, S., & Jena, D. (2011). *Security in vehicular adhoc networks: a survey*, in: Proceedings of the International Conference on Communication, Computing & Security, ACM, pp. 590–595.

Moustafa, H., Bourdon, G., & Gourhant, Y. (2006). *Providing authentication and access control in vehicular network environment*, in: Security and Privacy in Dynamic Environments, 201, Springer, New York, 62–73. https://doi.org/10.1007/0-387-33406-8_6

Papadimitratos, P., Buttyan, L., Holczer, T., Schoch, E., Freudiger, J., & Raya, M. (2008). *Secure vehicular communication systems: Design and architecture*, IEEE Commun. Mag. (46), 100–109. https://doi.org/10.1109/MCOM.2008.4689252

Parno, B., & Perrig, A. (2005). *Challenges in securing vehicular networks*, in: Workshop on Hot Topics in Networks (HotNets-IV). https://doi.org/10.1145/1947940.1948063

Plossl, K., Nowey, T., & Mletzko, C. (2006). *Towards a security architecture for vehicular ad hoc networks*, in: The First International Conference on Availability, Reliability and Security, ARES, p. 8. https://doi.org/10.1109/ARES.2006.136

Raya, M., & Hubaux, J. P. (2007). Securing vehicular ad hoc networks. J. Comput. Secrity, Special Issue on Security of Ad Hoc Sensor Netw., 15(1), 39–68. https://doi.org/10.3233/JCS-2007-15103

Raya, M., Jungels, D., Papadimitratos, P., & Add, I. J. P. (2006). *Certificate Revocation in Vehicular Networks,* Laboratory for Computer Communications and Applications (LCA), School of Computer and Communication Sciences, EPFL, Switzerland, LCAReport-006.

Raya, M., Papadimitratos, P., & Hubaux, J. P. (2006). *Securing vehicular communications*, IEEE Wirel. Commun, (13), 8–15. https://doi.org/10.1109/WC-M.2006.250352

Robinson, C., Caveney, D., Caminiti, L., et al. (2007). *Efficient message composition and coding for cooperative vehicular safety applications.* IEEE Trans. Veh. Technol., 56(6), 3244–3255. https://doi.org/10.1109/TVT.2007.907325

Samara, G., Al-Salihy, W. A. H., & Sures, R. (2010). *Security analysis of vehicular ad hoc networks (VANET)*, in: Network Applications Protocols and Services (NETAPPS), pp. 55–60. https://doi.org/10.1109/NETAPPS.2010.17

Stampoulis, A., & Chai, Z. (2007). *A Survey of Security in Vehicular Networks*, Project CPSC 534.

Torrent-Moreno, M., Santi, P., & Hartenstein, H. (2005). *Fair sharing of bandwidth in VANETs*, in: Presented at the Proceedings of the 2nd ACM international workshop on Vehicular ad hoc networks, Cologne, Germany. https://doi.org/10.1145/1080754.1080762

Yang, X., Liu, L., Vaidya, N. H., & Zhao, F. (2004). *A vehicle-to-vehicle communication protocol for cooperative collision warning,* in: The First Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services, 114–123. https://doi.org/10.1109/MOBIQ.2004.1331717

Yi, Q., & Moayeri, N. (2008). *Design of secure and application-oriented VANETs*, in: Vehicular Technology

Conference. VTC Spring IEEE, pp. 2794–2799. https://doi.org/10.1109/VETECS.2008.610

Yi-Wei Lu, L. W. (2003). *Electronic payment systems by group blind signatures.* Retrieved from http://ethesys.yuntech.edu.tw

Zeadally, S., Hunt, R., Chen, Y. S., Irwin, A., & Hassan, A. (2012). Vehicular ad hoc networks (VANETs): Status, results, and challenges. *Telecommun. Syst, 50*(4), 217–241. https://doi.org/10.1007/s11235-010-9400-5

Zhang, C., & Lu, R. (2008). '*An efficient identity based batch verification scheme for vehicular sensor networks'*. Proc. 27th IEEE INFOCOM, Phoenix, AZ, USA, 246–250. https://doi.org/10.1109/INFOCOM.2008.58