Computer Engineering and Intelligent Systems
ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online)
Vol.9, No.1, 2018

A Survey on Attacks and Preservation Analysis of IDS in Vanet

Pooja Kourav*
PG Scholar, CSE, VITS, Bhopal, India

Prof. Sumit Sharma
HOD CSE, VITS, Bhopal, India

Abstract
Vehicular Ad-hoc Networks (VANETs) are the extremely famous enabling network expertise for Smart Transportation Systems. VANETs serve numerous pioneering impressive operations and prospects although transportation preservation and facilitation functions are their basic drivers. Numerous preservation allied VANETs functions are immediate and task imperative, which would entail meticulous assurance of preservation and authenticity. Yet non preservation associated multimedia operations, which would assist an imperative task in the future, would entail preservation assistance. Short of such preservation and secrecy in VANETs is one of the fundamental barriers to the extensive extended implementations of it. An anxious and untrustworthy VANET could be more hazardous than the structure without VANET assistance. So it is imperative to build specific that "life-critical preservation" data is protected adequate to rely on. Securing the VANETs including proper shield of the secrecy drivers or vehicle possessors is an extremely challenging assignment. In this research paper we review the assaults, equivalent preservation entails and objections in VANETs. We as well present the enormously admired common preservation guidelines which are based on avoidance as well recognition methods. Many VANETs operations entail system wide preservation support rather than individual layer from the VANETs' protocol heap. This paper will also appraise the existing researches in the perception of holistic method of protection. Finally, we serve some potential future trends to attain system-wide preservation with secrecy pleasant preservation in VANETs.
Keywords: VANET (Vehicular Ad-hoc Network), Routing algorithm, Vehicle preservation, IDS, attack, Secrecy

1 INTRODUCTION

It is now widely accepted by academician and industry that VANETs can significantly improve traffic preservation, road efficiency and reduce environmental impact [1]. Studies [2] show that about 60% roadway collisions could be avoided if the driver of the vehicle was served warning at least one-half second prior to a collision.

VANETs allow vehicles to communicate with each other (V2V) and/or with roadside infrastructure (V2R). Based on these communications VANETs can offer a wide range of services. In a report [3], US Dept. of Transport has already listed more than75 different operation scenarios where it can be useful. These can be broadly categorized in two: preservation and non-preservation associated services/operations. Many safeties associated ITS operations are real-time and mission critical, which would entail meticulously assurance of quality of service (QoS), in terms of latency, error rate, and preservation. For instance, a preservation message to prevent a probable accident has to reach interested vehicles within a fraction of a second (e.g. 100ms [3]) so that the vehicles and their drivers can take necessary actions to prevent the accident. Preservation is fundamental interest for future VANETs implementations. In VANET a road user will relay on it and does action accordingly whereas on typical systems user takes actions by his/her observation and knowledge. An insecure and unreliable VANET can be more hazardous than the system without it. So, secure VANETs system is more than necessary. Potential preservation measures could include a method of assuring that the packet/data was generated by a trusted source (neighbor vehicle, sensors, etc.), as well as a method of assuring that the packet/data was not tampered with or altered after it was generated. Any operation that involves a financial transaction (such as tolling) entails s the capability to perform a secure transaction.

Securing the VANETs including appropriate protection of the secrecy drivers or vehicle holders is an extremely challenging assignment. As the operations of VANETs are diverse, their communications and/or system-level preservation entails could be diverse too. There are some extremely good works on VANETs' preservation and secrecy [4, 5], which review preservation associated issues attacks, entails, objections, and preservation solutions. But none of these comprehensively covers all of these issues associated VANETs' preservation and secrecy except [5]. In [5] preservation and secrecy implementation associated issues are missing, precisely communication perspective. In this work we summarize the attacks, corresponding preservation entails and objections in VANETs. We also present the extremely popular generic preservation guidelines which are based on prevention as well detective methods. Many VANETs operations entail system wide preservation assistance rather than individual layer from the VANETs' protocol stack. In this work we will review the existing works in the perspective of holistic method of preservation. Finally, we will serve some

possible future directions to achieve system-wide preservation as well as secrecy-friendly preservation in VANETs.

2 OVERVIEW OF VANET

A modern vehicle can be considered as a network of sensors/actuators on wheels. VANET is a special kind of Mobile Ad-hoc Network (MANET) where vehicles equipped with the technologies are the fundamental constituents. Generally, a VANET differs from MANET in the following aspects:

- Large scale – potentially billion
- Fleeting contact with other vehicles
- Nodes not as constrained in terms of energy, storage and computation.
- Higher mobility
- Secrecy entail

The single extremely important objective of a VANET is to serve communications between different vehicles on the roads and roads' environments (e.g. roads' condition, weather, traffic, etc.), to improve the driving experience and make driving safer. In doing so, in VANET each vehicle needs to have an OBU (On-Board Units) – communication devices mounted on vehicles and also a WSNs assistance roadside unit (RSU) as shown in figure 1. By using OBUs, vehicles can communicate with each other as well as with RSUs. A VANET is a self-organized network that enables communications between vehicles and RSUs, and the RSUs can be connected to a backbone network, so that many other network operations and services, including Internet access, can be served to the vehicles.

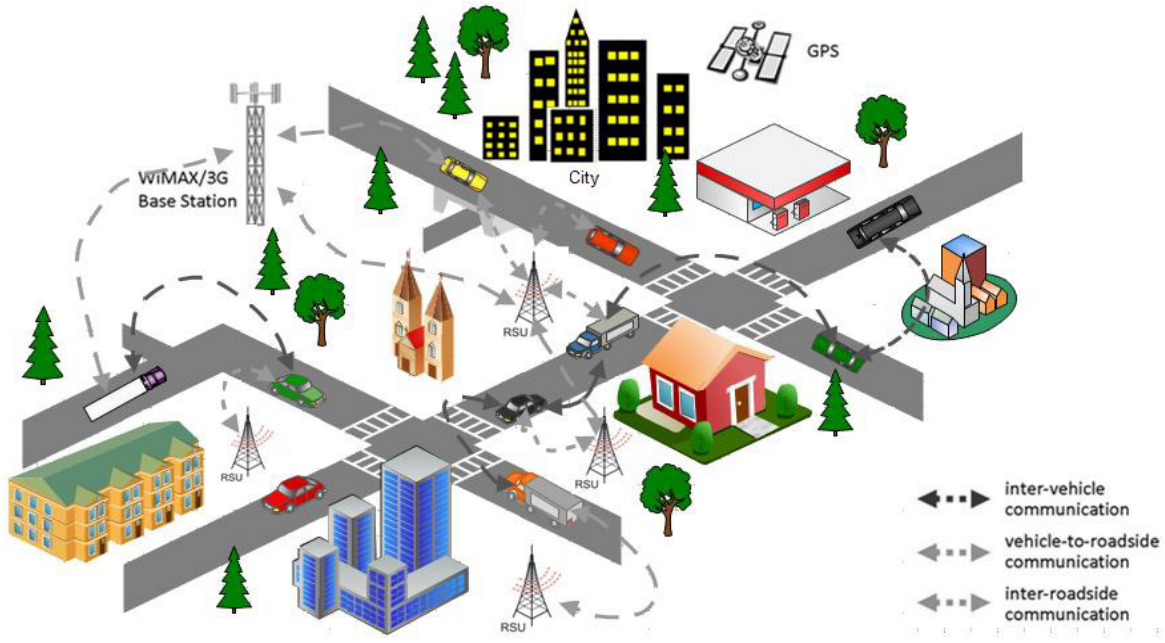

Fig. 1. An example of VANET

So in VANET communications can be Vehicle to Vehicle (V2V)/inter vehicle and/or with roadside infrastructure (V2R) [10]. Figure 1 presents an example VANET, which shows possible communications within a VANET.

To make VANETs Smart, it integrates multiple ad-hoc networking technologies such as Wi-Fi IEEE 802.11p, WAVE IEEE 1609, WiMAX IEEE 802.16, Bluetooth, IRA, and ZigBee for easy, accurate, effective and simple communication between vehicles on dynamic mobility. One of the IEEE1609 (P1609.2) explicitly defines preservation, secure message formatting, processing, and message exchange. Use of these technologies in VANETs helps in defining preservation measures in vehicles, streaming communication between vehicles, infotainment and telematics. VANETs are expected to implement a variety of wireless technologies such as Dedicated Short Range Communications (DSRC), are one or two way short- to medium range wireless communication channels explicitly designed for automotive use and a corresponding set of protocols and standards. Other candidate wireless technologies are Cellular, Satellite, and WiMAX. VANETs can be envisioned as the extremely important entity of the Smart Transportation Systems (ITS) [1, 3, and 6].

3. PRESERVATION NEED IN VANETS

As the operations of VANETs are diverse, their communications and/or system level preservation entail could be diverse too. Potential preservation measures should include a way of assuring that the packet/data was generated

by a trusted source, as well as a way of assuring that the packet/data was not tampered with or altered after it was generated.

VANETs pose some of the extremely challenging problems in MANETs and WSNs research. In addition, the issue of preservation in VANETs is particularly challenging due to the unique features of the network, such as high-speed mobility of network nodes or vehicles and the extremely large amount of network entities. It is obvious that any malicious user behavior, such as an alteration and replay attack of the disseminated messages, could be disastrous to other users. So in any situation, it is necessary to make sure that "life-critical preservation" information cannot be altered by attackers. A preservation system needs to be capable of establishing the liability of drivers, while preserving their secrecy as much as possible. Considering the aforementioned attacks and suggestion made in other works, VANET preservation should satisfy the following entails [7, 8]:

- Authentication: This is the extremely important entail in preventing extremely of the aforementioned attacks in VANETs. Vehicle responses to events should be based on legitimate messages (i.e., generated by legitimate users). Therefore we need to authenticate the OBUs, RSUs and senders of these messages.
- Verification of Data Consistency: The legality of messages also comprises their consistency with similar ones (those generated in close space and time), as the sender can be legal but the message contains false data. This entail is also known as "plausibility".
- Message Integrity: Message alteration is extremely common and crucial attacks in VANETs. We need to maintain the integrity of the message to prevent the alteration attacks.
- Availability: Attacks like (e.g., DoS by jamming) bring the VANETs down even the considered communication channel is robust. So, availability should be served by some other means.
- Non-repudiation: Drivers causing accidents should be reliably identified to prove his/her liability. Based on this principle, a sender will not be able to refuse the transmission of a message (it may be fundamental for investigation in determining the correct sequence and content of messages exchanged before the accident).
- Secrecy: People are increasingly cautious of being monitored or tracked. Hence, the secrecy of drivers or vehicle holders against unauthorized observers should be protected.
- Traceability and Revocation: Trace and disable abusing OBUs or RSUs by the authority.
- Real-Time Constraints: At the extremely high speeds typical in VANETs, meticulously time constraints should be respected. This ultimately imposes computation and communication wise efficient schemes.

4 VULNERABILITIES IN VANET

Of a lot of information transmitted through vehicular network, some information is able to use vulnerabilities of the vehicular environment so as to cause a fatal accident. Preservation vulnerabilities of vehicle include vulnerability of internal communication of vehicle, vulnerability of communication between vehicles, and vulnerability of traffic infrastructure, which are described as follows [9, 10].

4.1 Bogus Information

By spreading incorrect information to network, this attack influences a different driver's behavior. If an attack vehicle transmits bogus information on traffic situation to a neighboring victim vehicle, the victim travels to the intended path of the attacker on the basis of the bogus information.

4.2 Fake Position Information

This attack is used to induce the changes in a vehicle's known position, speed, and direction in order to avoid responsibilities from an accident.

4.3 ID Exposure

For position-tracking, a different vehicle's ID is exposed. In the logic of Big Brother, it is possible to monitor the travelling path of a vehicle targeted by an observer and use the information for other purposes. A passive attacker is able to reveal an identification of a target through VANET system, rather than a physical tool. Aside from an ID, a time, a position, travel information, and other kinds of personal information can be exposed.

4.4 Denial of Service

This attack is aimed at paralyzing communication or causing confusion in VANET, or triggering an accident. Jamming is a sort of DoS attack, which generates signals of a different vehicle's communication in a particular network area of VANET in order to paralyze communication.

4.5 Impersonation
An attacker uses an ID of an authorized vehicle in order to confuse neighboring vehicles.

4.6 Forgery
An attacker generates fake information in order to confuse other vehicles in a certain network area. A case in point is spreading false warnings like icy road warning in order to slow overall traffic.

4.7 In-transit Traffic Tampering
This attack is aimed at impeding normal communication through the deletion or change of a message to transmit in vehicle travelling.

4.8 Vehicle Information Tampering
This attack is aimed at tampering with internal information of vehicle (e.g., speed, position, sensing information). In the attack, a speed, a position, and other kinds of information are served incorrectly. Like forgery, this attack also forges information. What is difference is that this attack uses sensors or internal devices, rather than transmitted information, in order to change internal information and trigger malfunction of a vehicle.

4.9 Information Block
This attack uses the features of the protocol used in VANET. If the protocol transmits the information of a vehicle in transmission to its neighboring vehicle favorably positioned for transmission, the information stops being transmitted. At this time, an attacker cheats the vehicle in transmission as if it is the vehicle favorably positioned for transmission, and consequently the victim vehicle stops transmitting information. As a result, by stop transmitting information which should be sent to other vehicles, it is possible to cause confusion.

4.10 Tunnel
By sending fake information to a vehicle that enters and exits in and from places with temporary no service of GPS service, such as a tunnel, this attack makes it possible for the vehicle to update incorrect information.

4.11 Wormhole
This is a sort of disturbance attack. By sending meaningless information, though authorized, it is possible to disturb network.

4.12 Jungle Communication
This is the expansion of Bogus Information attack. By sending information to each vehicle and continuing to change it, it is possible to change the initial information to different information.

5 RELATED WORKS
Ram [11] proposed preservation mechanisms for symmetric and asymmetric algorithms to secure the preservation of routing protocol and protecting personal information from malicious insertion and modification of data in the open access environment of VANET. Nirbhay [12] analyzed the preservation entail and proposed solutions to preservation problems in VANET environment. To ensure preservation in VANET, he proposed to consider certain attributes which includes Authentication, Availability, Non-Repudiation, Access control, Secrecy, Confidentiality, Data Verification, Integrity, Real time assurances. Chen [13] observed that there is a preservation problem in the routing protocol information due to the characteristics of large-scale networks, fast mobile nodes, and frequently changing topology structures in VANET. He proposed a preservation mechanism for data encryption, preservation authentication, and intrusion detection to protect the integrity and consistency of network information. Tomar [14] considered the problem of optimizing traffic flow in a vehicular network where some vehicle interferes with each others. Then, he allocated the time slots by the RSU using the SINR model to maximize the time slot utilization in the vehicular network. In this paper, he presented the model for the interference range messages to prevent the potentially interfering nodes from initiating new transmissions.

Tomar proposed Spatial Division Multiple Access (SDMA) to optimize channel allocation and throughput for secure transmission of messages. Vijayakarthika [15] presented CAN (Controller Area Network) DELIVER, which is part of a complete system for providing car drivers and passenger's pervasive access to needed data while on the road. The proposed method reduced a delay time of data communication and increase communication efficiency by using the preservation mechanism of designating RSU as a proxy server and providing reliable data communication between vehicles. Vijayalakshmi [12] pointed out that in order to serve preservation services to all users in the VANET environment, the problem of preservation and scalability should be solved. Nam [16] proposed a VANET performance analysis method that uses the AODV (Ad-hoc On Demand Distance Vector) and DSDV (Destination Sequenced Distance Vector) throughput, packet loss rate, and

average delay time as parameters. Pham [21] designed the secured linkability protocol using pseudonym-based encryption and Bloom filter Private Set intersection technique and a context-aware trust management scheme working compatibly with the linkability protocol.

Donato [17] proposed Desync mechanism to improve transmission performance through the recalculation of transmission delay. The proposed mechanism uses ABSM and AID protocols to reduce a collision and maximize a transmission speed. Kaur [18] proposed Decision Packet. All nodes that create a path from a departure node to a destination node make a check with the hash value of Decision Packet so that an attacker is less likely to change a hop count. One attacker is able to use multiple IDs to attack VANET. To solve the Sybil attack detection problem, Rahvari [19] proposed the mechanism to detect an attack and secure authentication, non-repudiation, secrecy protection and data integrity through encryption.

In the communication of VANET, DoS attacks such as Sybil Attack, and selfish driver attack can occur. Gandhi [20] proposed RRDA (Request Response Detection Algorithm) to detect DoS attacks. The proposed model uses a hash table to reduce DoS attacks of a forgery vehicle, transmits packets to all vehicles in between a departure and a destination, and updates a hop count. The model was found to reduce packet delay and request retransmission in the way of evaluating packets with a hop count and updating through the limitation of a counter capacity. RoselinMary [21] proposed APDA (Attacked Packet Detection Algorithm) to transmit a message safely against preservation threats like DoS (Denial of Service) in the VANET environment. The proposed APDA minimizes a delay overhead at the beginning in order to improve preservation of a VANET system. Nitish [22] proposed Multi Operating Channels Model to protect vehicle network against the attacks that can trigger malfunction of network and data confidentiality loss in the VANET environment. To examine the proposed model, the researcher analyzed Message Suppression Attack, Denial of Service Attack, SYN flooding Attack, Alteration Attack, Link spoofing Attack and Link withholding Attack, and Fabrication Attack. As a result, the model improved preservation.

Mohammed [23] proposed IDS (Intrusion Detection System) operation technology in the VANET environment by classifying detection technology into Signature based system, Anomaly detection system, and Specifications based system. Amarpreet [24] proposed EAPDA (Enhanced Attacked Packet Detection Algorithm) to prevent network performance deterioration of vehicles and RUS from Denial of Service attacks such as Sybil attack, Alteration attack, and Selfish Driver attack in the VANET environment. DoS attacks are detected with time slot. Compared to conventional algorithms, the EAPDA had higher response, less delay and more throughputs.

Grzybek [25] served stable community detection in the dynamic mobile network in consideration of vehicles' high mobility in the VANET. Therefore, the researcher expanded LPA (Label Propagation Algorithms) for community detection [26] and SandSHARC (Stability and Network Dynamics over a Sharper Heuristic for Assignment of Robust Communities) in the dynamic mobile network, and proposed the evaluation framework for examining the stability of a detected community. Hussain proposed a technique that was found to protect secrecy through multiple anonymities, track a path by saving a Beacon message in Cloud, assurance safe and conditional anonymity through the operation of anonymity withdrawal, and have fewer operations than conventional techniques. Hussain [27] proposed CaaS (Cooperation as a Service) architecture which has three sub objects- TIaaS (Traffic Information as a Service), WaaS (Warning as a Service), and IfaaS (Infotainment as a Service)-for for VANET Clouds. In the proposed architecture, communication between cloud infrastructure and vehicles is accomplished by GT (Gateway Terminals), and positioning based encryption is applied to keep secrecy for a vehicle's position and identification. Park [28] designed the framework based on vehicular preservation entail, including RSU (Road Side Unit) authentication, message integrity, confidentiality, secrecy protection, non-repudiation, and availability in order for safe communication in the vehicular cloud environment.

As an encryption standard of a communication message between vehicles, BSM (Basic Preservation Message) defined in 'SAE J2735' was used in order to design an authentication and message protocol. In this way, the designed model was found to secure stability and efficiency from the preservation threats such as forgery attack, data tampering and MITM, repudiation, and information leak in the vehicular cloud environment with the combination of the VANET and internet based cloud environment. Park [29] pointed out that in 802.11 MAC protocol as an 802.11p based technology, if a node with low transmission rate holds a channel long, a node with high transmission rate is standardized downward to the low transmission rate; and a rise in nodes leads to a high probability of collision. Therefore, the researcher proposed the algorithm that makes a CWmin value low to reduce the back off time of a node of holding a channel and sets CWmin value large to lower a collision probability in order for a node with good channel status to have a high probability of holding a channel. Fengzhong [30] proposed the solution to the problem of preservation and secrecy protection in the VANET open access environment. The proposed method was efficient for reducing much time and calculation cost in the process of examination and withdrawal. It improved the process of certificate revocation.

In order to improve a conventional warning message transmission type in the urban areas with poor radio environment, Lee [31] designed the method in which all nodes use neighboring nodes' information to calculate

Forwarding Priority of themselves and neighboring nodes; and a node with the highest forwarding priority becomes a transmission node to send a warning message. Also, for the blind spots, the researcher proposed the algorithm to select the next transmission node and send a warning message to a blind spot.

Park [32] proposed ICRC algorithm, an efficient placement algorithm of RSU (Roadside Unit) which is an imperative factor for transmitting, collecting, and analyzing traffic information in the VANET environment. The ICRC algorithm determines initial RUS candidate positions on the basis of IP (Intersection Priority) and ED (Even Distribution) methods, and then removes a RUS with strong connection of RSU candidate positions in order to minimize the number of RSUs. According to the performance comparison, in the roads with good connection of intersections, both IP and ED based ICRA had excellent performance; in the complex roads with bad connection of intersections, ED based ICRA had better performance than IP.

In order to serve vehicle authentication and conditional secrecy protection for safe communication of V2 V, Kim [33] proposed the batch verification technique to prevent unnecessary group subscription in previous studies using group signature technique. The proposed method met various preservation entail on the basis of group signature. And, the Bloom Filter based batch verification method was found to improve node-by-node calculation efficiency more than conventional methods. According to the research, when vehicles communicate through a wireless channel, it is imperative to assurance preservation vehicle communication against various attacks, such as injection of wrong information and change and reproduction of a distributed message. Using PKI (Public Fundamental Infrastructure) is able to meet such entail as entity authentication, message integrity, non-repudiation, and personal information protection. If a vehicle cancels communication by going out of a region, efficient certificate revocation is entail d. Also, if a vehicle enters in a new region, it is entail d to update a certificate of the region efficiently. Therefore, the researcher proposed the preservation mechanism to reduce a message loss rate caused by message check delay in the way of shortening the time of message authentication.

6. OBJECTIONS

VANETs pose some of the extremely challenging problems in MANETs and sensor network research. Some of the fundamental objections [7, 8] which directly or indirectly associated to preservation of VANETs are summarized below.

- Mobility: In general sensor networks often assume a relatively static network, and even MANETs usually assume limited mobility. For vehicular networks, mobility is the norm, and it will be measured in miles, not meters, per hour. This high mobility causes frequent disconnect; hence make the communications highly unreliable which makes preservation more challenging. The mobility patterns of vehicles on the same road will show strong correlations. Each vehicle will have a frequently shifting set of neighbors, many of whom it has never communicated with before and is unlikely to communicate with again. The short-lived nature of interactions or communications in a VANET will limit the efficacy of reputation-based schemes. For instance, rating other vehicles based on the authenticity of their incident reports is unlikely to prove useful; a specific driver is unlikely to receive multiple reports from the same vehicle. Additionally, as two vehicles may only be within communication range for an extremely short period (e.g. few seconds), we cannot rely on protocols that entail significant communication between the sender and receiver.
- Secrecy vs. Preservation: Like other IP-based networks (e.g. Internet, MANETs, etc.), it highly desirable to bind each driver or vehicle to a single identity to prevent Sybil or other spoofing attacks. For instance, in the congestion control scheme, it is necessary to prevent one vehicle from claiming to be hundreds in order to create the illusion of a congested road. Authentication is a fundamental preservation entail for VANETs that serves valuable forensic evidence and allows us to use external mechanisms, such as traditional law enforcement, to deter or prevent attacks on VANETs. However, drivers or other vehicle users value their secrecy and are unlikely to adopt systems that entail them to abandon their anonymity. For instance, if we try to prevent spoofing in a way that reveals each vehicle's permanent identity, then we may violate drivers' or users' secrecy entail. So secrecy compliant preservation guideline are needed that will entail codifying legal, societal and practical considerations. Extremely countries have widely divergent laws interesting their citizens' right to secrecy. As extremely vehicle makers operate in multinational markets, they will need preservation solutions that satisfy the extremely stringent secrecy laws, or that can be customized to meet their legal obligations in each market. Authentication schemes must also consider societal expectations of secrecy against practical considerations. Vehicles today are not fully anonymous as each vehicle has a publicly displayed license plate that uniquely identifies it and identifies the holder of the car, given access to the appropriate records. Hence, drivers have already sacrificed a portion of their secrecy while driving. So, preservation guideline in VANETs should build on these existing compromises instead of encroaching any additional upon a driver's right to secrecy.
- Availability: Number of VANETs operations especially preservation -associated entail real time, or

near real-time, responses and hard real- time assurances. Other operations may tolerate some margin in their response times; still this entail is faster than those expected in traditional WSNs or MANETs. However, attempts to meet real-time demands could make operations vulnerable to Denial of Service (DoS) attacks. For instance, in the deceleration operation, a delay of even less than a second can render the message meaningless. The problem is additional aggravated by the unreliable communications. The current DSRC standard serves an acceptable latency and high data rate; the authenticity is still missing [14]. Since vehicles moving in opposite directions will remain within communications range for only a few seconds, opportunities to retry a broadcast will be limited.

- Low Tolerance for Errors: Many operations can afford preservation protocols that rely on probabilistic schemes. However, in VANETs' preservation (mission-critical) associated operations, even a small probability of error will be unacceptable. Number of vehicles in the world is in billions, even if an operation that functions correctly 99.99999999% of the time, the operation is still more likely to fail on at least one vehicle than function correctly on all vehicles. So margin of error of any preservation protocol in VANETs based on deterministic or probabilistic scheme is infinitesimally small. Additionally, for many operations, preservation must focus on prevention of attacks, rather than detection and recovery. In MANETs it may suffice to detect an attack and alert the user, leaving recovery and clean-up to the humans. However, in much preservation -associated VANETs operations, detection will be inadequate, as by the time the driver can react, the warning may be too late. So preservation must focus on preventing attacks in the first place, which entail s extensive foresight into the types of attacks likely to occur.
- Fundamental Distribution: Fundamental distribution is often a fundamental building block for preservation protocols. In VANETs, fundamental distribution faces several significant objections. First, vehicles are manufactured by many different companies, so installing fundamentals at the factory would entail coordination and interoperability between manufacturers. If manufacturers are unable or unwilling to agree on standards for fundamental distribution, then we could turn to government-based distribution. Within a country it can hierarchically go to states and then dimeticulously s that make the coordination complicating. The government can impose standards, but doing so would entail significant changes to the current infrastructure for vehicle registration, and thus is unlikely to occur in the near future. However, without a system for fundamental distribution, operations like traffic congestion detection may be vulnerable to spoofing, Sybil attacks. A potential method for secure fundamental distribution would be to empower the Motor Vehicles licensing authority to take the role of a Certificate Authority (CA) and to certify each vehicle's public fundamental. Unfortunately, this method has number of weaknesses. Moreover, certificate-based fundamental establishment has the danger of violating driver secrecy, as the vehicle's identity is revealed during each fundamental establishment. So finding a realistic and secrecy friendly fundamental distribution technique is a challenging issue in VANETs.
- Cooperation: Successful deployment of VANETs will entail cooperation amongst vehicle manufacturers, consumers, and the government, and reconciling their frequently conflicting interests will be challenging. For instance, law-enforcement agencies might quickly adopt a system in which speed-limit signs broadcast the mandated speed and vehicles automatically reported any violations. Understandably, consumers might reject such invasive monitoring, giving vehicle manufacturers little incentive to include such a feature. Equally, consumers might appreciate an operation that serves an early warning of a police speed trap. Manufacturers might be keen to meet this demand, but law-enforcement is unlikely to do so.

7 RESEARCH TRENDS OF VANET PRESERVATION

According to the analysis on previous studies on Vehicle Preservation, there were studies to overcome the attacks on vulnerabilities in the VANET environment. The studies have actively been conducted since the mid 2000 s including the development of wireless communication technology. Up to now, many studies are being performed on routing protocols for safe communication and secrecy protection against various attacks.

The suggested preservation entail in the VANET environment are authentication, availability, non-repudiation, access control, secrecy protection, confidentiality, data verification, and data integrity in consideration of high mobility, dynamic topology, and other VANET features.

They focused on reliable communication for routing protocols and minimized communication delay time in order for safe communication. Regarding algorithm design in the VANET environment, there are studies on the algorithms for attack detection and prevention, preservation in the cloud environment, and efficient communication improvement. In particular, since 2014, VuC (VANET using Clouds) has continued to be studied in order to increase the structural efficiency of data processing in the VANET environment, predict a situation far away to go out of spatial caused by a vehicle's position, and solve the problems of preservation and secrecy.

8. CONCLUSION

Operations of Vehicular Ad-hoc Networks are extremely encouraging and varied. Bulk of the preservation allied VANETs operations are real time and job oriented, which entails meticulously assurance of protection and legitimacy. Lack of such preservation and secrecy in VANETs is one of the fundamental complications to the wide dissemination implementations of it. Shielding the VANETs including proper protection of the secrecy of drivers or vehicle holders is an extremely challenging assignment as they differ with each other in number of conditions. In view of this, the research work in this paper is summarized the attacks, equivalent protection entail and objections in VANETs. Some of the objections aren't yet attempted at their best level, which entail additional concentration. We have also presented the extremely accepted generic protection guideline which is based on avoidance as well detection schemes. Detection based mechanisms entail additional concentration as they appear probable in VANETs. Many operations in VANETs entail stack wide protection assistance moderately than individual layer from the VANETs' protocol heap. In this research paper we have also deliberated the ongoing works in the view of holistic method of protection. These methods are the prime interest of our future research.

REFERENCES

[1.] Ezell, S.: Explaining International IT Operation Leadership: Intelligent Transportation Systems. The Information Technology & Innovation Foundation (January 2010)
[2.] David Wang, C., Thompson, J.P.: Apparatus and method for motion detection and tracking of objects in a region for collision avoidance utilizing a real-time adaptive probabilistic neural network, US. Patent No. 5,613,039 (1997)
[3.] US Dept. Transportation, "Vehicle Preservation Communications Project Assignment 3 Final Report" (March 2005),
[4.] Raya, M., et al.: Securing vehicular communications. IEEE Wireless Communications 13(5), 8–15 (2008)
[5.] Zeadally, S., Hunt, R., Chen, Y.S., Irwin, A., Hassan, A.: Vehicular ad hoc networks (VANETs): status, results, and objections. Telecommunication Systems, 1–25 (2010)
[6.] Qian, Y., Moayeri, N.: Design of secure and operation-oriented VANETs. In: IEEE VTC 2008, pp. 2794–2799 (Spring 2008)
[7.] Raya, M., Hubaux, J.-P.: Securing Vehicular Ad Hoc Networks. J. Computer Preservation, Special Issue on Preservation, Ad Hoc and Sensor Networks 15(1), 39–68 (2007)
[8.] Parno, B., Perrig, A.: Objections in securing vehicular networks. In: Proceedings of the Workshop on Hot Topics in Networks, HotNets-IV (2005)
[9.] Raya, Maxim, and Jean-Pierre Hubaux. "Securing vehicular ad hoc networks." Journal of computer preservation 15, no. 1 (2007): 39-68.
[10.] Cho, Y., H. Lee, N. Park, D. Choi, D. Won, and S. Kim. "Preservation technology trend in VANET." Korea Inst Inf Secur Cryptol 19, no. 1 (2009).
[11.] Raw, Ram Shringar, Manish Kumar, and Nanhay Singh. "Preservation objections, issues and their solutions for VANET." International Journal of Network Preservation & Its Operations 5, no. 5 (2013): 95.
[12.] Vijayalakshmi, V., M. Sathya, S. Saranya, and C. Selvaroopini. "Survey on various mechanisms for secure and efficient VANET communication." In Information Communication and Embedded Systems (ICICES), 2014 International Conference on, pp. 1-5. IEEE, 2014.
[13.] Chen, Lu, Hongbo Tang, and Junfei Wang. "Analysis of VANET preservation based on routing protocol information." In Intelligent Control and Information Processing (ICICIP), 2013 Fourth International Conference on, pp. 134-138. IEEE, 2013.
[14.] Tomar, Ranjeet Singh, and Shekhar Verma. "Enhanced SDMA for VANET communication." In Advanced Information Networking and Operations Workshops (WAINA), 2012 26th International Conference on, pp. 688-693. IEEE, 2012.
[15.] Vijayakarthika, R., and V. Banumathi. "Efficient data dissemination for secured communication in VANET." In Current Trends in Engineering and Technology (ICCTET), 2014 2nd International Conference on, pp. 313-320. IEEE, 2014.
[16.] Nam, Jae-hyun. "Implementation of VANET simulator using Matlab." Journal of the Korea Institute of Information and Communication Engineering 20, no. 6 (2016): 1171-1176.
[17.] Donato, Erick Aguiar, Joao Guilherme Maia Menezes, Edmundo Roberto Mauro Madeira, and Leandro Aparecido Villas. "Impact of 802.11 p channel hopping on vanet communication protocols." IEEE Latin America Transactions 13, no. 1 (2015): 315-320.
[18.] Kaur, Harbir, Sanjay Batish, and Arvind Kakaria. "An method to detect the wormhole attack in vehicular adhoc networks." International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN) ISSN 2248-9738 (2012): 86-89.
[19.] Rahbari, Mina, and Mohammad Ali Jabreil Jamali. "Efficient detection of sybil attack based on cryptography in vanet." arXiv preprint arXiv:1112.2257 (2011).

[20.] Gandhi, Usha Devi, and R. V. S. M. Keerthana. "Request response detection algorithm for detecting DoS attack in VANET." In Optimization, Reliabilty, and Information Technology (ICROIT), 2014 International Conference on, pp. 192-194. IEEE, 2014.
[21.] RoselinMary, S., M. Maheshwari, and M. Thamaraiselvan. "Early detection of DOS attacks in VANET using Attacked Packet Detection Algorithm (APDA)." In Information Communication and Embedded Systems (ICICES), 2013 International Conference on, pp. 237-240. IEEE, 2013.
[22.] Shukla, Nitish, Aarti Gautam Dinker, Nihal Srivastava, and Ankita Singh. "Preservation in vehicular ad hoc network by using multiple operating channels." In Computing for Sustainable Global Development (INDIACom), 2016 3rd International Conference on, pp. 3064-3068. IEEE, 2016.
[23.] Erritali, Mohammed, and Bouabid El Ouahidi. "A review and classification of various VANET Intrusion Detection Systems." In Preservation Days (JNS3), 2013 National, pp. 1-6. IEEE, 2013.
[24.] Singh, Amarpreet, and Priya Sharma. "A novel mechanism for detecting DOS attack in VANET using Enhanced Attacked Packet Detection Algorithm (EAPDA)." In Recent Advances in Engineering & Computational Sciences (RAECS), 2015 2nd International Conference on, pp. 1-5. IEEE, 2015.
[25.] Grzybek, Agata, Marcin Seredynski, Gregoire Danoy, and Pascal Bouvry. "Detection of stable mobile communities in vehicular Ad Hoc Networks." In Intelligent Transportation Systems (ITSC), 2014 IEEE 17th International Conference on, pp. 1172-1178. IEEE, 2014.
[26.] Leung, Ian XY, Pan Hui, Pietro Lio, and Jon Crowcroft. "Towards real-time community detection in large networks." Physical Review E 79, no. 6 (2009): 066107.
[27.] Hussain, Rasheed, and Heekuck Oh. "Cooperation-Aware VANET Clouds: Providing Secure Cloud Services to Vehicular Ad Hoc Networks." JIPS 10, no. 1 (2014): 103-118.
[28.] Park, Jung-oh, and Do-hyeon Choi. "A design of framework for secure communication in vehicular cloud environment." Journal of the Korea Institute of Information and Communication Engineering19, no. 9 (2015): 2114-2120.
[29.] Park, Sanghyun, and Nam-Il Kim. "Design of MAC algorithm assistanceing adaptive transmission rate on VANET." Journal of the Institute of Electronics and Information Engineers 49, no. 11 (2012): 132-138.
[30.] Qu, Fengzhong, Zhihui Wu, Fei-Yue Wang, and Woong Cho. "A preservation and secrecy review of VANETs." IEEE Transactions on Intelligent Transportation Systems 16, no. 6 (2015): 2985-2996.
[31.] Lee, Won Yeoul. "A performance enhancement of VANET warning message propagation on electric wave blind area problem in the urban environment." Journal of Korea Multimedia Society 17, no. 10 (2014): 1220-1228.
[32.] Park H, Hwang T, Jo Y, chi J (2014) An intersection connectivity-based RSU allocation algorithm in VANET. Korea Inf Sci Soc 10(1)
[33.] Kim, Su-Hyun, and Im-Yeong Lee. "A Research on Message authentication scheme based on efficient Group signature in VANET." Journal of the Korea Institute of Information Preservation and Cryptology 22, no. 2 (2012): 239-248.