International Journal of Security and Its Applications
Vol. 10, No. 5 (2016) pp.261-274
http://dx.doi.org/10.14257/ijsia.2016.10.5.25

Security Analysis of Vehicular Ad Hoc Networks (VANETs): A Comprehensive Study

Dr. Nirbhay Kumar Chaubey

Assistant Professor, Department of Computer Science
Institute of Science and Technology for Advanced Studies and Research (ISTAR),
Vallabh Vidyanagar, Gujarat, India. Pin- 388120
nirbhay@ieee.org

Abstract

Vehicular Ad-hoc Networks (VANETs) is a technology that has been recently emerged, and brings a lot of research interests. Security is one of the important issues in VANET, it is considered a critical point in the development of robust VANET applications. In this paper, various dimensions of VANETs including its emerging applications, security issues, challenges, security threats and the existing solutions proposed by the different researchers are studied. Also author reviewed various type of VANET simulator available and presented possible key research area of VANETs.

Keywords: *Vehicular Ad hoc Networks (VANETs), Mobile Ad-hoc Networks (MANETs), V2V, I2V, V2I, DSRC, WAVE, OBU, RSU, security, attacks*

1. Introduction

Vehicular Ad-hoc Network (VANET) is a rising & most challenging research area to provide Intelligent Transportation System (ITS) services to the end users. With the rapid development of wireless technologies, people have started to enjoy wireless access everywhere, even in vehicles on the move. Today, car manufacturers and telecommunications industries have teamed up together to equip vehicles with wireless technologies which not only bring various information technology services to vehicles but also improve the safety on the road and traffic efficiency. VANETs have gained a lot of research attention for last few years.

Vehicular Ad-hoc Network (VANET) is a collection of vehicles in a wireless network that are dynamic in nature and communicate with each other and/or with nearby Road Side Units (RSUs). A VANET is a network that does not rely on any central administration for providing communication among the so-called On Board Units (OBUs) in nearby vehicles, and between OBUs and nearby fixed infrastructure usually RSU using a technique called, Dedicated Short Range Communication (DSRC). VANETs provide many new exciting applications and opportunities albeit transportation safety and facilitation applications. Security of vehicular networks remains the most significant concern in VANETs deployment – because it is mandatory to assure public and transportation safety. IEEE 1609.x, 802.11p and Wireless Access in Vehicular Environment (WAVE). WAVE is a layered architecture for devices complying IEEE 802.11 to operate on DSRC band. The IEEE 1609 family defines the architecture and the corresponding protocol set, services and interfaces that allow all WAVE stations to interoperate within the VANET environment. The WAVE architecture also defines the security of message exchange [1, 2].

ISSN: 2005-4262 IJGDC

The different standards of the 1609 WAVE architecture and their integration into the OSI reference model are summarized in Figure 1.

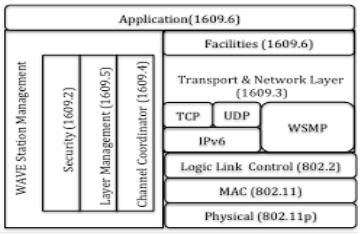

Figure 1. WAVE Architecture and Protocol Stack. [IEEE 1609.02013]

VANETs are responsible for the communication between moving vehicles in a certain environment. A vehicle can communicate with another vehicle directly that is called Vehicle to Vehicle (V2V) communication also known as Inter-Vehicle Communication (IVC) with Vehicle TO Infrastructure (V2I) and Infrastructure TO Vehicle (I2V) communications. Figure 2 shows a typical VANET scenario [3].

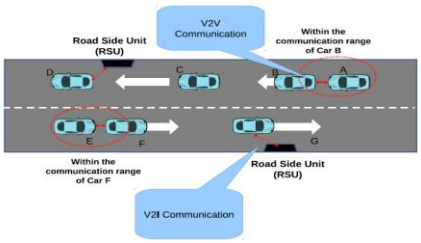

Figure 2. Creating an Ad-hoc Network using Vehicles (VANETs)[3]

The organisation of the paper is presented as follows: Section 2 discuss VANETs applications and characteristics. Section 3 presents challenging issues in VANETs. Next, security issues for VANETs are described in Section 4. Section 5 discusses related key research works. Section 6 describes popular simulations tools used for VANETs. Key research area discussed in Section 7 and the last section 8 presents the concluding remarks.

2. VANET Applications and Characteristics

There are many important applications of VANET. These applications can be categorized into two broad categories (i) safety related applications and (ii) user based applications [4]. Next, VANET characteristics are described.

i. Safety Related Application

These applications are used to increase the safety on the roads.

Road Traffic Safety: This applications work on reducing the number of fatalities/injuries on the roads by alerting the driver about dangers in advance.

Cooperative Driving: The drivers play very important role in this application. Like violation warning, turn conflict warning, curve warning, lane merging warning etc. and significantly decrease the life-endangering accidents. In fact, many of the accidents come from the lack of cooperation between drivers.

Traffic optimisation: Traffic can be optimized by the use of sending signals like jam, accidents etc. to the vehicles, accordingly, they can choose their alternate path and also save time.

ii. User Based Application

Following are the services for the user.

Peer to peer application: These applications are very much useful to provide services like sharing multimedia files, movies, songs etc. among the vehicles in the network.

Internet Connectivity: People can connect with the Internet all the time. Thereby, VANET provides the constant connectivity of the Internet to the users.

Comfort and Quality of Road Travel :These applications provide comfort for travelers like 'advanced traveller information systems', 'electronic payment systems', 'electronic toll collection', locate the fuel station etc.

Characteristics of VANET

VANET has its own distinct characteristics, which are summarised as follows [5]:

High Mobility: Nodes in VANETs generally are moving at high speed. This makes difficult to predict a node's position and making protection of node privacy.

Dynamic Topology: Due to high node mobility and vehicles random speed, the node position changes frequently. Thus, network topology in VANETs regularly changes. The link connection between the vehicles in VANET has frequent disconnections because of the high movement of the nodes and frequent change in the environment.

Unbounded network size: Network size of VANET is geographically unbounded. It means, VANET can be implemented for one city, several cities or for countries.

Frequent exchange of information: Ad hoc nature in VANETs motivates the nodes to collect information from the other vehicles and RSU. Therefore, the information exchange among node becomes frequent.

Wireless Communication: VANET is designed for the wireless environment; nodes are connected and exchange their information via wireless. Consequently, security measure must be considered during communication.

Time Critical: The delivery of information to the nodes in VANET must be done within time limit so that it can perform the action accordingly, e.g. critical medical emergency messages must be delivered on time in order to save human lives.

Use of Other Technology: Most of the vehicles in VANET are capable of integrating their own system with other available technologies such as Global Positioning System (GPS).

No Power Constraint: VANET nodes do not have issue of energy and computation resources unlike other MANET devices. This can be utilised for efficient processing of complex and computational hungry routing/security mechanisms.

Better Physical Protection: The VANET nodes are physically better protected, hence, nodes are more difficult to compromise physically and reduce the effect of infrastructure attack.

Mobility Modeling: *A*n accurate mobility model is required for highly dynamic environment of VANET. The mobility of VANETs cannot be captured by general mobility models of MANETs and special mobility models by making use of traffic flow theory, should be proposed. ***Predictable Mobility Patterns*****:** Most of the vehicles move on pre-defined roads and highways in VANET environment. This allows the use of predictable mobility patterns in network design.

Geographic position available: Accurate positioning systems like GPS with integrated electronic maps are quite popular in cars, as vehicles equipped with these tools, provide location information for routing purposes.

3. Challenging Issue In VANET

There are some challenges to deploy the VANETs, can be categorized into following (i) technical challenges and (ii) social and economical challenges [6]:

3.1. Technical Challenges

Following are some technical challenges discussed:

The lack of a centralized infrastructure: In VANET, there are no centralized infrastructure in charge of synchronization and coordination of transmissions makes that one of the hardest tasks in the resulting decentralized and self-organizing VANETs is the management of the wireless channel to reach an efficient use of its bandwidth.

Network Management: Due to high mobility, the network topology and channel condition change rapidly. Due to this, we can't use structures like tree because these structures can't be set up and maintained as quickly as the topology changed.

Congestion and collision Control: The unbounded network size also creates a challenge. The traffic load is low in rural areas and night in even urban areas. Due to this, the network partitions frequently occurs while in rush hours the traffic load is very high and hence network is congested and collision occurs in the network.

Environmental Impact: VANETs use the electromagnetic waves for communication. These waves are affected by the environment. Hence to deploy the VANET the environmental impacts have to be considered.

MAC Design: VANET generally use the shared medium to communicate hence the MAC design is the key issue.

Security: As VANET provides the road safety applications which are life critical therefore security of these messages must be satisfied. Security and privacy requirements in VANETs have to be balanced.

The radio channel: The radio channel in VANET scenarios present critical features for developing wireless communications that degrade strength and quality of signals.

VANET Standardization: The need for standardization of VANET communications should allow flexibility as these networks have to operate with many different vendors equipment.

Real-time communication: This is very much necessary because no delay can exist in the transmission of safety-related information. This implies that VANET communication requires fast processing and exchange of information.

3.2. Social and Economic Challenges

Apart from the technical challenges, social and economical challenges should also be considered to deploy the VANET. It is difficult to convince manufacturers to build a system that conveys the traffic signal violation because a consumer may reject such type of monitoring. On the other hand, consumer appreciates the warning message of police trap. So to encourage the manufacturer to deploy VANET will get little incentive.

4. Security Issues In VANET

Security in VANET is a challenging problem for researchers in the era of cyber threats. The message passing from one vehicle to another vehicle may be hacked by an intruder who creates vulnerability in the systems performance [7], [8]. In this section, security challenges, security requirements, attackers on VANETs and various attacks in the VANET are studied.

4.1. Security Challenges in VANET

The challenges of security must be considered during the design of VANET architecture, security protocols, cryptographic algorithm etc. The following list presents some security challenges:

Real time Constraint: Most of the applications in VANET require time critical messages, like collision avoidance, hazard warning and accident warning information etc. Hence strict deadlines for the delivery of messages must be met.

Data Consistency Liability: In VANET even authenticate node can perform malicious activities that can cause accidents or disturb the network. Hence a mechanism should be designed to avoid this inconsistency.

Location Awareness: The increased reliance of VANET on GPS or other specific location based instruments may affect its applications in case of occurrence of any error.

Low tolerance for error: Some protocols are designed on the basis of probability. VANET uses life critical information on which action is performed in very short time. A small error in probabilistic algorithm may cause danger.

Key Distribution: In VANETs, security mechanisms implemented reliant on keys. Each message is encrypted and need to decrypt at receiver end either with same key or different key. Keys distribution among vehicles is a major challenge in designing a security protocols.

Incentives: Manufactures are interested to build applications that consumer likes most. Very few consumers will agree with a vehicle which automatically reports any traffic rule violation. Hence successful deployment of VANET will require incentives for vehicle manufacturers, consumers and the government is a challenge to implement security in VANET.

High Mobility and Volatility: Computational capability and energy supply in VANET is nearly same as the wired network node but the high mobility of VANET nodes requires the less execution time of security protocols for same throughput that wired network produces.

Tradeoff between authentication and privacy: For the authentication of the messages that are to be transmitted, it is required to track the vehicles for their identification. This is not feasible as most consumers will not like others to know about their personal identification. Therefore this has to come in balance and a tradeoff must be maintained between the authentication and privacy of the nodes.

Network Scalability: The scale of the vehicular network in the world is exceeding continuously and as this number is growing, another problem is arising. Further, we know that there is no global authority to govern the standards for this network in the world.

4.2. Security Requirements in VANET

VANET must satisfy some security requirements before they are deployed. To ensure security in VANET, we need to consider certain attributes which includes followings [9]:

Authentication: Authentication ensures that the message is generated by the legitimate user. In VANET a vehicle reacts upon the information came from the other vehicle hence authentication must be satisfied. The identity of the nodes in the network must be ensured.

Availability: Availability requires that the information must be available to the legitimate users when it is needed, and sometimes it must have fast response time for specific applications, any delaying even if it takes milliseconds will make the message meaningless.

Non-Repudiation: A sender cannot deny the fact of having sent the message and receiver cannot deny that not received the message. Only specific authorities with complete authorization are allowed to identify a vehicle.

Access control*:* It ensures that all the nodes in the network perform their functions according to the roles and privileges authorized to them.

Privacy: The privacy of a node against the unauthorised node should be guaranteed. This is required to eliminate the massage delay attacks. The personal and private information of drivers and vehicles must not be available to unauthorized access.

Confidentiality: Secrecy must be provided to sensitive material being sent over the VANET, like in certain commercial applications.

Data Verification: A regular verification of data is required to eliminate the false messaging.

Integrity: Messages sent over the network should not be corrupted. Possible attacks that would compromise their integrity are malicious attacks or signal failures producing errors in the transmission.

Real time guarantees*:* Many safety related applications in VANET depend on strict time guarantees. It ensures that the time constraint is met in case of safety related applications like collision avoidance.

4.3. Attackers on VANETs

To secure the VANET, it is very important to discover who the attackers are, what are their nature, and capacity to damage the system. Based on the capacity, these attackers are of the following three types.

i. **Insider and Outsider**: Insiders are the authenticated members of network whereas outsiders are the intruders and hence limited capacity to attack.

ii. **Malicious and Rational**: Malicious attackers have not any personal benefit to attack; they just harm the functionality of the network. Rational attackers have the personal profit hence they are predictable.

iii. **Active and Passive**: Active attackers generate signals or packet whereas passive attackers only sense the network.

4.4. Attacks in the VANET

In order to get better protection from attackers, it is essential to have the knowledge about the attacks in VANET against security requirements. These attacks are based on (i) Identification and Authentication (ii) Attack on privacy (iii) Attack on availability (iv) Routing attack and (v) Attack on non-repudiation discussed below:

(i) Attack on Identification and Authentication

Impersonate: In this attack, attacker assumes the identity and privileges of an authorized node, either to make use of network resources that may not be available to it under normal

circumstances, or to disrupt the normal functioning of the network, usually this attack is performed by active attackers and attacker could be insider or outsiders. This attack can be performed by following two ways:

False attribute possession: In this scheme an attacker steals some property of legitimate user and later with the use of attribute claims that it is who (legitimate user) that sent this message. By using this type attack a normal vehicle can claim that he/she is a police or fire protector to free the traffic.

Sybil: In this type of attack, a malicious vehicle claims to be at multiple locations with multiple identities thereby creating an illusion of traffic congestion. The malicious node can even spoil the proper functioning of the network by injecting false information.

(ii) Attack on privacy

Session hijacking: Most authentication process is done at the start of the session. Hence it is easy to hijack the session after connection establishment. In this attack attackers take control of session between nodes.

Identity revealing: Generally a driver is itself owner of the vehicles hence getting owner's identity can put the privacy at risk.

Location Tracking: The location of a given moment or the path followed along a period of time can be used to trace the vehicle and get information of driver.

(iii) Attack on availability

Network Denial of Service: Denial Of Service (DOS) attacks aim to make the network unavailable to its legitimate vehicles. DoS attacks can be carried out in following ways [10].

Jamming: In this technique the attacker senses the physical channel and gets the information about the frequency at which the receiver receives the signal. Then he transmits the signal on the channel so that channel is jam.

Distributed DoS attack: In this attack, multiple attackers attack the victim node and prevents legitimate user from accessing the service.

SYN Flooding: In this mechanism large no of SYN request is sent to the victim node, spoofing the sender address. The victim node send back the SYN-ACK to the spoofed address but victim node does not get any ACK packet in return. This result too half opens connection to handle by a victim node's buffer. As a consequence the legitimate request is discarded.

(iv) Routing attack

In this type of attack, the attacker either drops the packet or disturbs the routing process of the network. Following are the most common routing attacks in the VANET [11] - [12]:

Black Hole attack: In this attack, a malicious node pretends to have an optimum route for the destination node and indicates that packet should route through this node after transmitting the fake routing information. The impact of this attack is that the malicious node can either drop or misuse the intercepted packets without forwarding them.

Worm Hole attack: In this attack, an adversary receives packets at one point in the network, tunnels them to another point in the network, and then replays them into the network from that point. This tunnel between two adversaries are called wormhole.

It can be established through a single long-range wireless link or a wired link between the two adversaries. Hence it is simple for the adversary to make the tunnelled packet arrive sooner than other packets transmitted over a normal multi-hop route.

Gray Hole attack: This is the extension of black hole attack. In this type of attack the malicious node behaves like the black node attack but it drops the packet selectively. It can be performed by three ways (i) malicious node may drop incoming packets while allow some packets to pass (ii) malicious node may behave as normal for some time and malicious for a certain time and (iii) malicious node may drop incoming packets from some specified nodes for some time and later on it behaves as a normal node. These different types of behavior make attack difficult to detect. Grayhole attack finally disrupts the network's performance by interfering with the route discovery process.

Denial of Service (DoS) attack: can be done by the network insiders & outsiders. An insider attacker may jam the channel after transmitting dummy messages & thus, stops the network connection. An outsider attacker can launch a DoS attack by repeatedly disseminating forged messages with invalid signatures to consume the bandwidth or other resources of a targeted vehicle. The impact of this attack is that, VANET losses its ability to provide services to the legitimate vehicles.

In Illusion attack, attacker tries to purposely manipulate his/her sensor readings for giving falsifies information about his/her vehicle. As a result, the system reaction invokes and false traffic warning messages are broadcast to neighbors. The impact of this attack is that it can easily change the driver's behavior by spreading the wrong traffic information & can cause accidents, traffic jams and reduces the vehicular network efficiency by dropping the bandwidth consumption. Existing message authentication & message integrity approaches cannot secure networks against this attack as the malicious vehicle directly manipulates & misleads the sensors of its own vehicle to produce & broadcast the wrong traffic information

Security is an important issue for routing in VANETs, because many applications will effect life-or-death decisions and illicit tampering can have devastating consequences. Security is an important issue for routing in VANETs, because many applications will effect life-or-death decisions and illicit tampering can have devastating consequences. The characteristics of VANETs make the secure routing problem more challenging and novel than it is in other communication networks. Another challenge related to routing is efficient data dissemination and data sharing in VANETs. Additional areas for improvement include the integration of privacy and security mechanisms into routing protocols and the establishment of priority routes for emergency and safety messages.

(v) Attack on non-repudiation:

Eavesdropping: This is a most common attack on confidentiality. This attack is belongs to network layer attack and passive in nature. The main target of this attack is to get access of confidential data.

Repudiation: The main threat in repudiation is denial or attempt to denial by a node involved in communication. This is different from the impersonate attack. In this attack two or more entity has common identity hence it is easy to get indistinguishable and hence they can be repudiated.

5. Related Work

To provide secure VANET, many researchers present a set of solutions to solve different security problems which are discussed in this section.

Isaac, J.T.; Zeadally, S.; Camara, J.S. in [7] surveys the major security attacks and presents the corresponding countermeasures and cryptographic solutions.

Researchers in [13] – [16] dealt with routing protocols and gave effective solutions so that the communication between the nodes is computational effective and leading to less congestion of network traffic.

Yong Hao, Yu Cheng, and Kui Ren in [17] proposed a solution of group formation combined with RSU is illustrated, which resulted in easy revocation of malicious vehicle, location privacy protection is improved and the system maintenance becomes flexible.

Wang, J., Yan, W in [18] suggested a new protocol for message checking, this protocol involves checking the Certificate Validity (CV) of the sender, the receiver of the message checks the CV of the message sender, the result of checking has three cases: in the first case, the receiver will consider the message if the sender has a valid certificate, second case occurs when the sender has invalid certificate, in this case the receiver will not regard the message, in the third case, the sender has not CV at all, the receiver will inform the RSU with the sender and check the received message, if it is correct the RSU will issue CV for the sender, otherwise it will issue invalid certificate and record vehicle's identity into the Certificate Revocation List (CRL).

To protect vehicular network against Sybil attacks, researchers B. Liu, B. Khorashadi, H. Du, D. Ghosal, C-N. Chuah and M. Zhang in [19] proposed a solution involves using on road radar, where each vehicle can see surrounding vehicles and receive reports of their GPS coordinates. By comparing what is seen to what has been heard, a vehicle can corroborate the real position of neighbors and isolate malicious vehicles.

Jinyuan Sun; Chi Zhang; Yanchao Zhang; Yuguang Fang in [20] proposes an identity based security system for VANET to solve the conflicts between privacy and tractability very effectively. The system uses a pseudonym based scheme to preserve user privacy. It uses a threshold signature based scheme to enable tractability for law enforcements. This is particularly attractive to service providers since they can achieve better efficiency of their services.

Chowdhury, P.; Tornatore, M.; Sarkar, S.; Mukherjee, B., Wagan, A.A.; Mughal, B.M.; Hasbullah, H. in [21] proposed a hybrid technique that takes advantage of both asymmetric and symmetric cryptographic schemes. The technique employs hardware that integrates both asymmetric and symmetric cryptography modules for safety messaging.

Azogu, I.K.; Ferreira, M.T.; Hong Liu in [22] proposes an Asymmetric Profit Loss Markov (APLM) model to measures integrity level of the security schemes for VANET content delivery. The model uses Markov chains to record the system’s ability to adjust itself given profit and loss. Given the measurement by the model as heuristics, integrity schemes for VANET can be optimized to provide better content delivery.

Researchers G. Samara, and W. Al-Salihy in [23] proposed using of Vehicular Public Key Infrastructure (VPKI), every node sends a safety message, it signs that message with its private key, and attaches it with Certificate Authority (CA). The receiver party of the message, will get the public key of the sending party by using the certificate, and check the signature of that sender, using its certified public key, but this solution requires that the CA public key be known by the receiver party.

Azogu, I.K.; Ferreira, M.T.; Larcom, J.A.; Hong Liu in [24] explores security metrics for VANET that can in turn guide the design of defense mechanisms against jamming style Deny of Service attacks. The researchers propose a new class of anti jamming Defensive mechanisms: hideaway strategy, the effectiveness of this new class is investigated through the simulations. The researchers implement a simulation package integrating VANET modules (OBU and RSU) and attack/defense modules along with traffic simulation. Result shows that the hideaway strategy achieves steady efficiency advantage over traditional anti jamming schemes.

Prabhakar, M.; Singh, J.N.; Mahadevan, G. in [25] proposed an essential complements to the passive mechanisms of encryption. For inputs as given security measures of the VANET, the defensive mechanism adopts game theoretic approaches and is comprised of three stages(i) uses heuristics based on ant colony optimization to identify known and

unknown opponents (ii) Nash Equilibrium is employed for selecting the model for a given security problem and (iii) enables the defensive mechanism to evolve over traffic traces through the game theoretic model from the first stage.

6. VANET Simulations

Fundamentally, there are various techniques available to analyze the behavior of wireless networks, primarily these techniques are Analytical Modeling, Real Time Physical Measurements and Computer Simulations *etc*. Analytical models are mathematical models that have a closed form solution. Real Time Physical Measurements is the state of things as they actually exist, rather than as they may appear or may be thought to be and it may not be possible all the time. Computer Simulations is a practical approach to the quantitative analysis of a network. Simulation is usually a software package that runs on a computer for the purpose of simulating some sort of system, in order to get a better idea how the system functions. During the last decade simulation has become a very powerful and an important tool for planning, designing and controlling complex system. Nowadays an error in real life costs a lot of money. Further, Implementation of VANET in a real time system is a very challenging task. Many such implementations have been deployed in recent years and implementing such projects in a real time system requires complete simulation by measuring the performance of the system. In this section, different types of simulators (i) Traffic Simulators (ii) Network Simulators (iii) Embedded Vehicular Models, (iv) Advanced Vehicular mobility models and (v) Isolated Vehicular Models are presented.

6.1.1. Traffic simulators: Traffic simulators are mainly designed to simulate the urban intersections and highways. TRANSIM or VISSIM, CORSIM, PARAMICS, CARISMA and SHIFT are some of the traffic simulators. These simulators are validated and used for providing accurate mobility models, but these traffic simulators take more time in planning and transportation which increases the time complexity. To handle large traffic, quite a few open source traffic simulators are available like SUMO (Simulation of Urban Mobility). SUMO generates traces which are used by the network simulators. For traffic generation it takes the route assignments and for motion constraints it contains parsers for TIGER. MOVE (Mobility Model Generator for Vehicular Networks) tool is used to simplify the SUMO configuration and adds a GUI environment.

6.1.2. Network simulators: Network simulators are available to manage and control the network parts. These simulators are available as open source commercial and commercial tools in the market include Opnet and Qualnet with high network protocols and wireless suite. Omnet + + is a free tool for academic purposes but for commercial purposes it requires a license. Open source simulators are like ns-2, Glomosim, Swans and GTNets (Georgia Tech Network Simulator) are some of the network simulators.

6.1.3. Embedded models: Groovenet/Groovesim is the first tool to provide embedded vehicular mobility model. Groovesim is the model and Groovenet is the project for modelling. City Model tool is designed for embedding, implementing and testing routing protocols. Then, Bononi, L., Di Felice, M., Bertini, M., Croci, E. (Proc. ACM/IEEE Int. Symp. Modeling, Analysis and Simulation of Wireless and Mobile Systems, Torresmolinos, Spain, 2006) designed MoVes which provides driving patterns and a better mobility model. Gorgorin *et al.*, also found a simulator embedded with mobility and networking capabilities. Vuyyuru and Oguchi also designed a tool called Automesh which consists of a radio propagation block, network simulator and driving simulator(Proc. 4th IEEE/IFIP Wireless On demand Networks and Services, Austria, 2007, pp. 100–106). Then, Wang, S.Y., Chou, C.L., developed NCTUns simulation for

providing better mobility and networking capabilities (A Chapter of the Book Ad Hoc Networks: New Research, Nova Science Publishers, 2008, ISBN: 978-1-60456-895-0).

6.1.4. Advance mobility models: These models provide better networking features and motion features. Open source models are the TraNS tool with SUMO and NS-2. VGrid is used for study on traffic accidents after using the alert messages. MobiReal is developed mainly based on GTNets.

6.1.5. Isolated vehicular model: Isolated vehicular models are the mobility models with lack of interaction with the network simulators. It is divided into four parts: (i) Legacy Mobility Model : includes Random Waypoint model, Gauss-Markov model, Reference Point Group model, Random Walk model and Node Following model. These models are mainly meant for MANET study. For VANET, Freeway model and Manhattan model are designed. (ii) Improved Motion Constraints include Bonn Motion tool, Obstacle Mobility model, Voronoi model and so on. (iii) Improved Traffic Generator includes GEMM tool, CanuMobisim tool and so on. (iv) Improved Motion Constraints and Traffic Generator create interaction between the traffic generator and motion constraint. It includes tools like STRAW (Street Random Waypoint) tool, Stop Sign Model/Traffic Sign Model (SSM/ TSM) and Generic Mobility Simulation Framework(GMSF).

7. Key Research Areas in VANETs

Vehicular technology is gaining momentum as vehicles are increasing in a rapid manner. There are many research scopes which are to be mined to obtain new ideas and to provide services to the people.

(i) Quality of Service (QoS): Provision of certain quality of service levels in VANET is an important task. A network with minimum delay for data delivery, less retransmissions, and high connectivity time can provide certain QoS guaranteed to the users.

(ii) Network Security: As the nodes in VANET environment seek exchange of information among each other all the time. Designing a proper authentication mechanism and a trust based security protocol is an interesting and open research area in VANET.

(iii) MAC layer protocol: The main idea of designing the MAC protocol is to provide fast data exchanges. In the WAVE standard, the IEEE 802.11p protocol is used for wireless communication. The WAVE stack consists of IEEE 1609.1, IEEE 1609.2, IEEE 1609.3 and IEEE 1609.4 to provide services like security, resource allocation, safety applications, LLC management and network services etc.

(iv) Scalability and Robustness: Designing a scalable and robust network remains an unlock area of research in VANET. Many design approaches fall short when VANETs transform from sparse to high dense mode, or from high mobility to slow traffic scenarios.

(v) Image processing: By using advanced image processing algorithms, the vehicles can track a person by using cameras on the vehicles. This application is used for tracking terrorists on the roads. If a terrorist's image matches with the database image then the vehicle suddenly broadcasts the information to the nearby police station. The videos of the street can also be recorded for criminal investigation.

(vi) Co-operative Communication: A key challenge in VANET is establishing the communication among different nodes. Different concepts of co-operative communication from wireless network theory may not be directly applied to VANET. This co-operative communication, such as up to which extent nodes should exchange information among themselves, is one of the key research areas in the VANET design.

(vii) Mobility model: To enhance the performance of the network there should be a realistic mobility model which implements the traffic scenario. A mobility model can be designed by considering vehicles, buildings, roads, maps, driving patterns, vehicular density, driver's behavior and so on. This mainly supports in solving the routing problem where the vehicles are moving at a high speed

(viii) Efficient Routing Algorithms Design: In order to timely and properly sending data packets from one node to another node an efficient and secure routing algorithm is required. Design such an algorithm that can be implemented in multiple topologies of the network and satisfies VANETs requirements is an active area of research.

(ix) Fault tolerance: The VANET nodes can fail at any time because of hardware tampering or software fault and this leads to the generation of faulty nodes in the system. At the time of routing, if a vehicle sends data to a faulty vehicle then the data may be dropped and delay increases and for this reason, there should be a recovery mechanism which recovers or protects the network from these faults. These days, generation of new fault tolerance techniques is an emerging area of research.

8. Conclusion and Future Work

In this paper, we mainly analyzed the VANETs applications, challenges, requirements, attacks, security issues and its possible solutions proposed by the other researchers. Further, we have discussed VANETs simulators available and key research areas of VANETs. Security is the major issue to implement in VANET because many new types of attacks are being generated. In the future work, we intend to suggest new solutions and protocols which can detect and mitigate the malicious vehicles in VANETS with objective to reduce delay and the packet drops while maintaining the network throughput.

References

[1] S. Kumar Bhoi and P. Mohan Khilar, "Vehicular communication: a survey", The Institution of Engineering and Technology, vol. 3, no. 3, **(2013)** August, pp. 204-217.
[2] M. Raya, P. Papadimitratos and J.-P. Hubaux EPFI, "Securing Vehicular Communications", IEEE Wireless Communications, vol. 13, no. 5, **(2006)** October, pp. 8-13.
[3] S. ur Rehman, M. Arif Khan, T. A. Zia and L. Zheng, "Vehicular Ad-Hoc Networks (VANETs) – An Overview and Challenges", Journal of Wireless Networking and Communications, vol. 3, no. 3, **(2013)**, pp. 29-38.
[4] Y. Toor and P. Mühlethaler, "Vehicle Ad Hoc Networks: Applications and Related Technical issues", IEEE Communications surveys & Tutorials, 3rd quarter, vol. 10, no. 3, **(2008)**, pp. 74-88.
[5] H. Moustafa and Y. Zhang, "Vehicular networks: Techniques, Standards, and Applications", CRC Press, **(2009)**.
[6] P. Caballero-Gil, C. Hernández-Goya and A. Fúster-Sabater, "Securing Vehicular Ad-Hoc Networks", International Journal on Information Technologies & Security, vol. 1, **(2009)**, pp. 25-36.
[7] J. T. Isaac, S. Zeadally and J. S. Camara, "Security attacks and solutions for vehicular ad hoc networks", Communications, IET, vol. 4, no. 7, **(2010)** April 30, pp. 894, 903.
[8] J. Fuentes, A. González-Tablas and A. Ribagorda, "Overview of security issues in vehicular ad-hoc networks", Handbook of Research on Mobility and Computing: Evolving Technologies and Ubiquitous Impacts, **(2010)**, pp. 894-911.
[9] A. Yusri Dak, S. Yahya and M. Kassim, "A Literature Survey on Security Challenges in VANETs", International Journal of Computer Theory and Engineering, vol. 4, no. 6, **(2012)** December, pp. 1007-1010.
[10] C. S. R. Murthy and B. S. Manoj, "Ad Hoc Wireless Networks: Architectures and Protocols", PEARSON, ISBN 81-317-0688-5, **(2011)**.
[11] M. S. Al-kahtani, "Survey on security attacks in Vehicular Ad hoc Networks (VANETs)", 6th IEEE International Conference on Signal Processing and Communication Systems (ICSPCS), **(2012)**, pp. 1-9.
[12] I. Ahmed Sumra, I. Ahmad, H. Hasbullah and J. bin Ab Manan, "Classes of attacks in VANET", IEEE Saudi International in Electronics, Communications and Photonics Conference (SIECPC), **(2011)**.
[13] F. Hui, "A survey on the characterization of Vehicular Ad Hoc Networks routing solutions ECS 257", Winter, **(2005)**, pp. 1-15.

[14] J. Yin, T. El. Batt, G. Yeung and B. Ryu, "Performance Evaluation of Safety Applications over DSRC Vehicular Ad Hoc Networks", Proceeding of the 1st ACM International Workshop on Vehicular Ad Hoc Networks, **(2004)**, pp. 1-9.
[15] S. Y. Wang, "Predicting the Lifetime of Repairable Unicast Routing Paths in Vehicle-Formed Mobile Ad Hoc Networks on Highways", 15th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, (PIMRC), vol. 4, **(2004)**, pp. 2815-2829.
[16] L. Briesemeister, A. G. DaimlerChrysler, Berlin, Germany and G. Hommel, "Role-Based Multicast in Highly Mobile but Sparsely Connected Ad Hoc Networks", First Annual Workshop on Mobile and Ad Hoc Networking and Computing, (MobiHOC), **(2000)**, pp. 45-50.
[17] Y. Hao, Y. Cheng and K. Ren "Distributed Key Management with Protection Against RSU Compromise in Group Signature Based VANETs", IEEE GLOBECOM- 2008, pp. 4951-4955.
[18] J. Wang and W. Yan, "RBM: A role based mobility model for VANET", Proc. Int. Conf. Communications and Mobile Computing, vol. 2, **(2009)** January, pp. 437-443.
[19] B. Liu, B. Khorashadi, H. Du, D. Ghosal, C-N. Chuah and M. Zhang, "VGSim: An Integrated Networking and Microscopic Vehicular Mobility Simulation Platform", IEEE Communication Magazine Automotive Networking Series, vol. 47, no. 5, **(2009)** May, pp. 134-141.
[20] J. Sun, C. Zhang, Y. Zhang and Y. Fang, "An IdentityBased Security System for User Privacy in Vehicular Ad Hoc Networks", IEEE Transactions on, Parallel and Distributed Systems, vol. 21, no. 9, **(2010)** September, pp. 1227-1239.
[21] P. Chowdhury, M. Tornatore, S. Sarkar, B. Mukherjee, A. A. Wagan, B. M. Mughal and H. Hasbullah, "VANET Security Framework for Trusted Grouping Using TPM Hardware", Second International Conference on Communication Software and Networks, (ICCSN '10), **(2010)** February, pp. 309-312.
[22] I. K. Azogu, M. T. Ferreira and H. Liu, "A security metric for VANET content delivery", Global Communications Conference (GLOBECOM), no. 37, **(2012)** December, pp. 991, 996.
[23] G. Samara and W. Al-Salihy, "A new security mechanism for vehicular communication networks", Proceeding of the International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), **(2012)**, pp. 18-22.
[24] I. K. Azogu, M. T. Ferreira, J. A. Larcom and H. Liu, "A new antijamming strategy for VANET metrics directed security defense", IEEE Globecom Workshops (GC Wkshps), **(2013)** December, pp. 1344-1349.
[25] M. Prabhakar, J. N. Singh and G. Mahadevan, "Defensive mechanism for VANET security in game theoretic approach using heuristic based ant colony optimization", IEEE International Conference on Computer Communication and Informatics (ICCCI), **(2013)** January, pp. 1-7.

Author

Nirbhay Kumar Chaubey, Senior Member of IEEE, Member of ACM and LMCSI, currently working as an Assistant Professor and Head of Computer Science Department at Institute of Science & Technology for Advanced & Studies (ISTAR), Gujarat Technological University, Vallabh Vidyanagar, Gujarat, India. He obtained his PhD Degree in Computer Science from Gujarat University, Ahmedabad, India in year 2014. He has received IEEE Region 10 Outstanding Volunteer Award- Year 2015, IEEE Outstanding Branch Counselor Award- Year 2010, Gujarat Technological University (GTU) Pedagogical Innovation Awards (PIA) – Year 2015, Best Paper Award in 5th International Conference on Advanced Computing & Communication Technologies (ACCT-2015). His main research interests are in Wireless Ad Hoc and Sensor Networks, MANETs, VANETs and Underwater Sensor Networks, Personal and Mobile Communications, distributed and parallel computing etc.