International Journal of Scientific and Technical Advancements
IJSTA
ISSN: 2454-1532

Vanets – A Novel Approach towards Creating Hi-Tech Network on Roads

Gagandeep Jagdev[1], Neha[2]
[1]Dept. of Computer Science, Punjabi University Guru Kashi College, Damdama Sahib (PB)
[2]Research Scholar (M.Phil. Comp. Appl.), Guru Kashi University, Talwandi Sabo (PB)
Email address: [1]drgagan137@pbi.ac.in

***Abstract*—** The credit of some of the most important innovations in the field of automotive industry goes to information and communication technology. The mobile communications have changed our lifestyle and it is possible to exchange information anywhere at any time. Today it has been made possible to use such mobile communication systems in vehicles too. A VANET is a special case of Mobile Ad hoc Networks (MANETs) in which vehicles moving on roads with wireless processing capabilities can create a spontaneous network. This new approach of sharing information among vehicles will enable several applications for safety, driver assistance, infotainment and urban sensing. These applications will be available in the forms of intra-vehicle, vehicle-to-vehicle and vehicle to infrastructure communication. The concept of these networked vehicles has gained popularity all over the world. The objectives behind this is to ensure greater security and make passengers time more enjoyable on road. VANETs are capable of providing information regarding traffic jams, weather conditions, accidents, hazardous road conditions and locations of facilities like gas stations and restaurants. VANETs helps in controlling the road network, maintain low vehicle operating costs and creating shorter and more predictable journey times. Today a large number of car manufacturers are launching vehicles loaded with onboard computing and wireless communication devices, sensors and navigation systems, all in preparation of deploying large-scale vehicular networks. By using different sensors, cameras and communication capabilities, vehicles can collect and interpret information with the purpose of assisting the driver to make a decision. The primary aim of this research paper is to elaborate the technology working behind VANETs and discussing its prospective aspects in coming future.

***Keywords*—** Road Networks, vehicle-to-vehicle communication, vehicle-to-infrastructure communication, VANETs.

I. INTRODUCTION

VANETs are a particular type of MANETs in which vehicle itself acts as a node and this node is equipped with transmission capabilities which are interconnected in some arbitrary manner to construct a network.

Often different topologies are created by the vehicles on road and are very dynamic and distributed non-uniformly. Standard MANET routing algorithms are not appropriate to transfer information about these kinds of networks. The presence of efficient navigation systems on every vehicle makes it aware of its geographical location and its neighbors. A routing approach comes into existence in which packets are forwarded to a destination simply by making choice of the nearest neighbor closer to the destination and such an approach is termed as Geographic routing. Increase in number of vehicles on road and of roadside traffic monitors has led to advancements of navigation systems and inexpensive wireless network devices. Keeping this in consideration, the Intelligent Transport System (ITS) have come up with an architecture termed as Wireless Access in Vehicular Environments (WAVE). WAVE enables both vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) wireless communications.

As per architectures of network, VANETs can be categorized into three different categories which are mentioned as under [1, 2].

Wireless Wide Area Network (WWAN) – In this kind of network the Aps (access points) of cellular gateways are fixed in order to allow direct communication between the vehicles and the access points. But the problem with this kind of network is of high cost involved in its installation which is not feasible.

Hybrid Wireless Network – In this category WWAN access points are used at certain points while an ad hoc communication provides access and communication in between those access points.

Ad Hoc V2V Network - The third and final category is the Ad Hoc V2V Communication which does not require any fixed access points in order for the vehicles to communicate. Vehicles are equipped with wireless network cards, and a spontaneous setting up of an ad hoc network can be done for each vehicle. It is this communication network which is often known as VANETs.

The purpose of VANET is to allow wireless communication between vehicles on the road including the roadside wireless sensors, enabling the transfer of information to ensure driving safety and planning for dynamic routing, allowing mobile sensing as well as providing in-car entertainment. As VANETs have unique characteristics which include dynamic topology, frequent disconnection of the networks, and varying environments for communication, the routing protocols for traditional MANET such as Ad hoc On-demand Distance Vector (AODV) are not directly usable for VANETs. Researchers have developed a variety of efficient routing protocols for VANETs including Greedy Perimeter Stateless Routing (GPSR) (Karp and Kung, 2000); Greedy Perimeter Coordinator Routing (GPCR) (Lochert et al., 2005); and GpsrJ+ (Lee et al., 2007). The current issue, however, is that the range of the wireless sensors on vehicles is limited to a few hundred meters at most and the traffic conditions in a vehicular urban environment often change dynamically. Other

Gagandeep Jagdev and Neha, "Vanets – A novel approach towards creating hi-tech network on roads," *International Journal of Scientific and Technical Advancements*, Volume 2, Issue 4, pp. 215-220, 2016.

than that, VANET routing protocols also face other problems including the issue of unstructured roads, the difference in the sizes of the intersections in a certain area, the sharp curves of the roads, uneven slopes, and other obstacles such as large buildings, traffic lights, trees, and sign boards. As it is impractical to spend excessively on rebuilding or restructuring the existing roads in urban environments, a routing protocol for the purpose of a larger distance of data communication in one-to-one and one-to-many transfers specifically for VANETs need to be developed [3].

II. ARCHITECTURE OF VANETS

The advances in mobile communications and the current trends in ad hoc networks allow different deployment architectures for vehicular networks in highways, urban and rural environments to support many applications with different QoS requirements. The goal of a VANET architecture is to allow the communication among nearby vehicles and between vehicles and fixed roadside equipment's leading to the following three possibilities (Fig. 1).

- Vehicle-to-Vehicle (V2V) ad hoc network- This network allows the direct vehicular communication without relying on a fixed infrastructure support and can be mainly employed for safety, security, and dissemination applications.
- Vehicle-to-Infrastructure (V2I) network: allows a vehicle to communicate with the roadside infrastructure mainly for information and data gathering applications.
- Hybrid architecture: combines both Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I). In this scenario, a vehicle can communicate with the roadside infrastructure either in a single hop or multi-hop fashion, depending on the distance, i.e., if it can or not access directly the roadside unit. It enables long distance connection to the Internet or to vehicles that are far away.

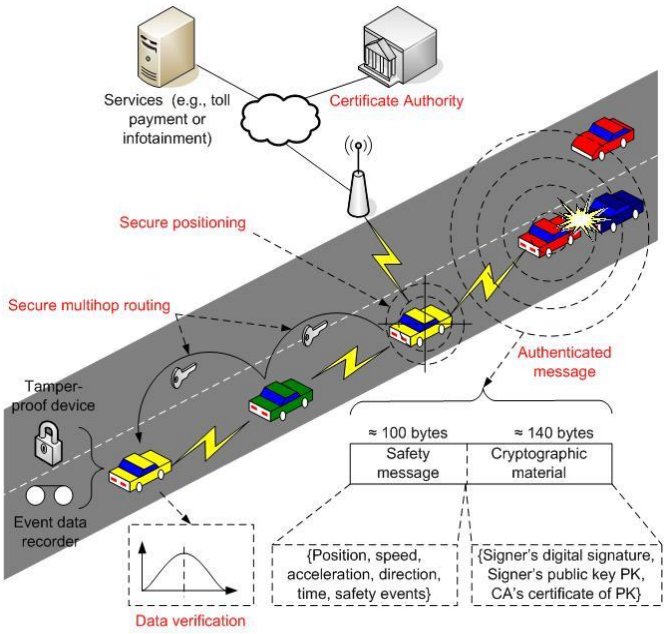

Fig. 1 Figure shows real time working of VANETs on road

Architecture of VANET is comprised of many entities. Along with vehicles, there are certain other entities involved in VANET that perform basic operations of this network. All these entities communicate with each other in several ways.

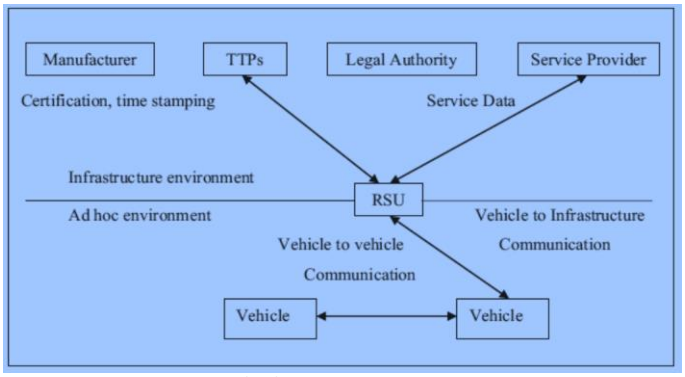

Fig. 2. Working of Infrastructure and Ad hoc environment.

Infrastructure environment in which, entities can be permanently interconnected. It is mainly composed by those entities that manage the traffic or offer an external service. On one hand, *manufacturers* are sometimes considered within the VANET model. As part of the manufacturing process, they identify uniquely each vehicle. On the other hand, the *legal authority* is commonly present in VANET models. Despite the different regulations on each country, it is habitually related to two main tasks - *vehicle registration* and *offence reporting*. Every vehicle in an administrative region should get registered once manufactured. As a result of this process, the authority issues a license plate. On the other hand, it also processes traffic reports and fines. Trusted Third Parties (TTP) are also present in this environment. They offer different services like credential management or time stamping. Both manufacturers and the authority are related to TTPs because they eventually need their services (for example, for issuing electronic credentials like passwords). *Service providers* (SPs) are also considered in VANETs. They offer services that can be accessed through the VANET. Location-Based Services (LBS) and Digital Video Broadcasting (DVB) are two examples of such services (Fig. 2) [4].

Ad-hoc environment in which, sporadic (ad-hoc) communications are established from vehicles. From the VANET point of view, they are equipped with three different devices. Firstly, they are equipped with a communication unit

(OBU, On-Board Unit) that enables Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I, I2V) communications. On the other hand, they have a set of **sensors** to measure their own status (e.g. fuel consumption) and its environment (e.g. slippery road, safety distance). These sensorial data can be shared with other vehicles to increase their awareness and improve road safety. Finally, a Trusted Platform Module (TPM) is often mounted on vehicles. These devices are especially interesting for security purposes, as they offer reliable storage and computation. They usually have a reliable internal clock and are supposed to be tamper-resistant or at least tamper-evident (Raya et al, 2005, 2006). In this

Gagandeep Jagdev and Neha, "Vanets – A novel approach towards creating hi-tech network on roads," *International Journal of Scientific and Technical Advancements*, Volume 2, Issue 4, pp. 215-220, 2016.

way, sensitive information (e.g. user credentials or pre-crash information) can be reliably stored (Fig. 2) [4, 5].

III. Communication Patterns in VANETs

A. V2V Warning Propagation

There are situations in which it is necessary to send a message to a specific vehicle or a group of them. For example, when an accident is detected, a warning message should be sent to arriving vehicles to increase traffic safety. On the other hand, if an emergency public vehicle is coming, a message should be sent for preceding vehicles. In this way, it would be easier for the emergency vehicle to have a freeway. In both cases, a routing protocol is then needed to forward that message to the destination (Fig. 3) [1, 2].

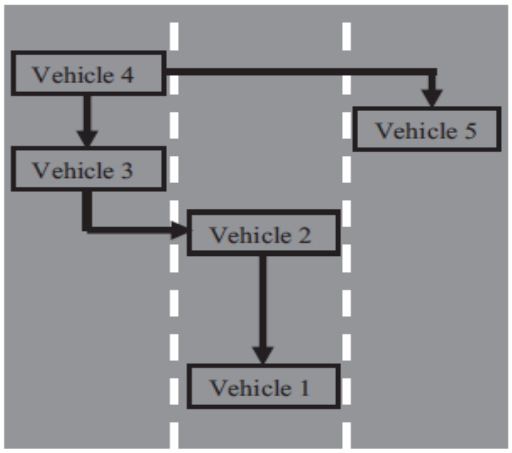

Fig. 3. Vehicle-to-Vehicle warning propagation

B. V2V Group Communication

Under this pattern, only vehicles having some features can participate in the communication (Fig. 4). These features can be static (e.g. vehicles of the same enterprise) or dynamic (e.g. vehicles on the same area in a time interval).

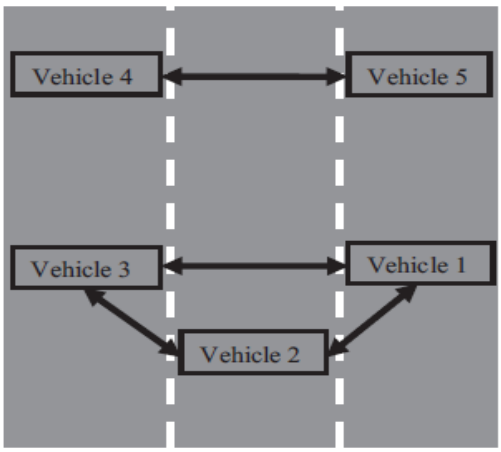

Fig. 4. Vehicle-to-Vehicle group communication.

C. V2V Beaconing

Beacon messages are sent periodically to nearby vehicles. They contain the current speed, heading, braking use, etc. of the sender vehicle. These messages are useful to increase neighbor awareness. Beacons are only sent to 1-hop communicating vehicles, i.e. they are not forwarded. In fact, they are helpful for routing protocols, as they allow vehicles to discover the best neighbor to route a message (Fig. 5).

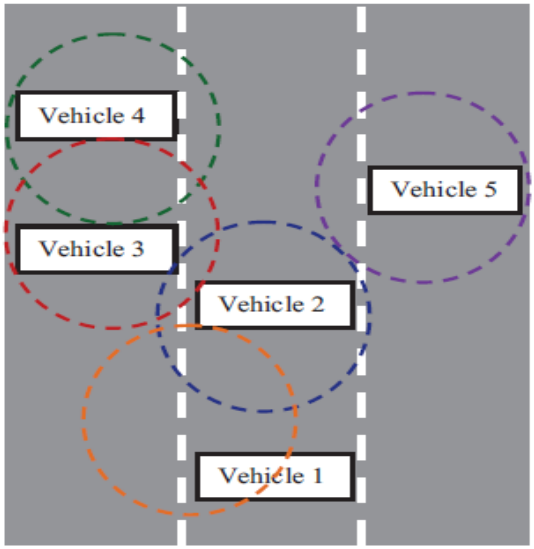

Fig. 5. Vehicle-to-Vehicle Beaconing.

D. I2V/V2I Warning

These messages are sent either by the infrastructure (through RSUs) or a vehicle when a potential danger is detected. They are useful for enhancing road safety. As an example, a warning could be sent by the infrastructure to vehicles approaching to an intersection when a potential collision could happen (Fig. 6) [2].

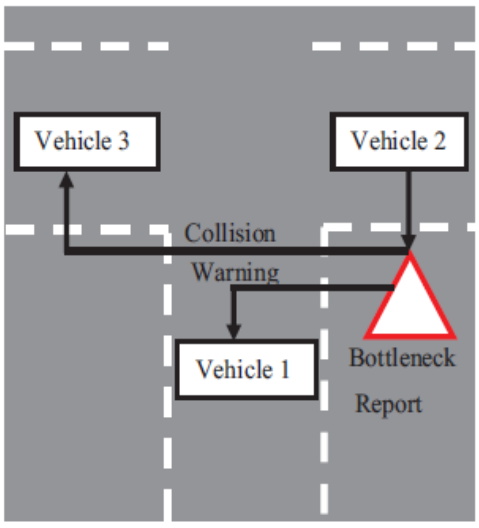

Fig. 6 Vehicle-to-Infrastructure warning

IV. Attacks In VANETs

The attackers in VANETs can be classified broadly into four categories which are mentioned as under [6, 10].

A. Insider vs. Outsider

Gagandeep Jagdev and Neha, "Vanets – A novel approach towards creating hi-tech network on roads," *International Journal of Scientific and Technical Advancements*, Volume 2, Issue 4, pp. 215-220, 2016.

If the attacker is a member node who can communicate with other members of the network, it will be known as an *Insider* and able to attack in various ways. Whereas, an o*utsider*, who is not authenticated to directly communicate with other members of the network, have a limited capacity to perform an attack (i.e., have less variety of attacks).

B. Malicious vs. Rational

A *malicious* attacker uses various methods to damage the member nodes and the network without looking for its personal benefit. On the contrary, a *rational* attacker expects its own benefit from the attacks. Thus, these attacks are more predictable and follow some patterns.

C. Active vs. Passive

An *active* attacker can generate new packets to damage the network whereas a *passive* attacker only eavesdrops the wireless channel but cannot generate new packets (i.e., less harmful).

D. Local vs. Extended

An attacker is considered as local if it is limited in scope, even if it possesses several entities (e.g., vehicles or base stations). Otherwise, an extended attacker broadens its scope by controlling several entities that are scattered across the network. This distinction is especially important in wormhole attacks.

E. Network Attacks

In Network Attacks, attackers can directly affect other vehicles and infrastructure. These attacks are on the high level of danger because these affect the whole network.

F. Application Attacks

In Application Attacks class, the objectives of attackers are applications that provide added service in VANETs. The attacker is mainly interested in changing contents used in applications and abusing it for their own benefits.

G. Timing Attacks

It is a type of attacks in which attackers' main objective is to add some time slot in original message, for example, to create delays in order to block this message come to the receiver before the expiration of its lifetime.

H. Social Attacks

All unmoral messages, which trigger bad emotions of other drivers, are classified into the class Social
Attacks.

I. Monitoring Attacks

Finally, attacks in which monitoring and tracking activities are performed are laying in the class Monitoring Attacks.

V. Basic Security Prerequisites In VANETs

Security is prime concern when we talk about any technology and so is the case in VANETs. The three aspects to be covered regarding security are confidentiality, integrity and availability and are mentioned as under [8].

A. Confidentiality

In a group, none except group members are able to decrypt the messages that are broadcasted to every member of group; and none (even other members) except a dedicated receiver member is capable to decrypt the message devoted to it.

B. Integrity

It ensures that data or messages delivered among nodes are not altered by attackers. A node should be able to verify that a message is indeed sent and signed by another node without being modified by anyone. In order to gain this property, data Verification is also required. Once the sender vehicle is authenticated, the receiving vehicle performs data verifications to check whether the message contains the correct or corrupted data.

C. Availability

The network should be available even if it is under an attack without affecting its performance. This concept of VANETs is not different from itself in other kinds of networks but not easy to ensure because of the mobility in high speed of vehicles.

Besides three main security requirements above, the following security aspects should be also satisfied in VANETs [7, 9]:

- *Privacy* - The profile or a driver's personal information must be maintained against unauthorized access. Two different cases need to be handled here.
  (a) Communications between vehicles and RSUs: Privacy means that an eavesdropper is impossible to decide whether two different messages come from the same vehicle.
  (b) Communications between vehicles: Privacy means that determining whether two different valid messages coming from the same vehicle is intensely burdensome for everyone except a legitimate component.
- *Traceability and revocability* - Although a vehicles real identity should be hidden from other vehicles, there should be still a component (e.g., Trace Manager) that has the ability to obtain vehicles' real identities and to revoke them from future usage.
- *Non-repudiation*
  Drivers must be reliably identified in case of accidents. A sender should have mandatory responsibility in transmitting the messages for the investigation that will determine the correct sequence and content of messages exchanged before the accident.
- *Real-time constraints*
  Since vehicles are able to randomly move in and quickly move out to a group of a VANET for a short duration, real-time constraints should be maintained.
- *Low Overhead*
  All messages in VANETs are time critical. Thus, "low overhead" is essential to retain the usefulness and validity of messages.

Gagandeep Jagdev and Neha, "Vanets – A novel approach towards creating hi-tech network on roads," *International Journal of Scientific and Technical Advancements*, Volume 2, Issue 4, pp. 215-220, 2016.

VI. CONCLUSION

Time has become the most essential resource as the future advances rapidly. To utilize the resource best, there is a need for communication on the move in a secure and efficient manner. Today VANET (Vehicular Ad-hoc Networks) has become a promising field of research as the world is advancing towards the vision of intelligent transportation systems. Dramatic increase in the number of vehicles equipped with computing technologies and wireless communication devices created new application scenarios that were not feasible before. These new scenarios include collision avoidance, emergency message dissemination, dynamic route scheduling, real-time traffic condition monitoring, high-speed tolling, information retrieval, and even distributed passengers teleconferencing. The opportunities that a VANET present are unlimited. The future introduction vehicular networks offer a tremendous opportunity to increase the safety of the transportation system and reduce traffic fatalities.

REFERENCES

[1] Saif Al-Sultan, Moath M. Al-Doori, Ali H. Al-Bayatti, and Hussien Zedan. A comprehensive survey on vehicular ad hoc network. Journal of Network and Computer Applications, 37(0):380 – 392, 2014.

[2] Mohammad S. Almalag, Michele C. Weigle, and Stephan Olariu. MAC Protocols for VANET, pages 599–618. John Wiley and Sons, Inc.,2013.

[3] National Science Fundation, 2012.

[4] S. GraÌLfling, P. Mahonen, and J. RiihijaÌLrvi. Performance evaluation of ieee 1609 wave and ieee 802.11p for vehicular communications. In Ubiquitous and Future Networks (ICUFN), 2010 Second International Conference on, pages 344–348, June 2010.

[5] European Telecommunications Standards Institute. Intelligent transport systems (its); radiocommunications equipment operating in the 5 855 mhz to 5 925 mhz frequency band. Technical Report ETSI EN 302 571 V1.2.0, ETSI, France, May 2013.

[6] Guilherme Maia, Cristiano Rezende, Leandro A. Villas, Azzedine Boukerche, Aline C. Viana, Andre L. Aquino, and Antonio A. Loureiro. Traffic aware video dissemination over vehicular ad hoc networks. In ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM '13), pages 419–426, 2013.

[7] P.S. Nithya Darisini and N.S. Kumari. A survey of routing protocols for vanet in urban scenarios. In Pattern Recognition, Informatics and Mobile Engineering (PRIME), 2013 International Conference on, pages 464–467, Feb 2013.

[8] M.A. Razzaque, AhmadSalehi S., and SeyedM. Cheraghi. Security and privacy in vehicular ad-hoc networks: Survey and the road ahead. In M.A. Razzaque, AhmadSalehi S., and SeyedM. Cheraghi, editors, Wireless Networks and Security, Signals and Communication Technology, pages 107–132. Springer Berlin Heidelberg, 2013.

[9] M. Slavik and I. Mahgoub. Spatial distribution and channel quality adaptive protocol for multihop wireless broadcast routing in vanet. Mobile Computing, IEEE Transactions on,12(4):722–734, April 2013.

[10] S. Zeadally, Y. Chen R. Hunt, A. Irwin, and A. Hassan. Vehicular ad hoc networks (vanets): Status, results, and challenges. to appear in Telecommunication Systems, 51(2-3), 2012.

Gagandeep Jagdev and Neha, "Vanets – A novel approach towards creating hi-tech network on roads," *International Journal of Scientific and Technical Advancements*, Volume 2, Issue 4, pp. 215-220, 2016.

ISSN: 2454-1532

Gagandeep Jagdev and Neha, "Vanets – A novel approach towards creating hi-tech network on roads," *International Journal of Scientific and Technical Advancements*, Volume 2, Issue 4, pp. 215-220, 2016.