CHAPTER I

INTRODUCTION TO VANETS

1.1 PERVASIVE NETWORK

Pervasive Networking is perceived as the ability to communicate and access the same types of services-anytime, anywhere. This is regardless of the location, type of network or type of device used to access the network. There is a convergence of technology, business needs and end-user interest that is driving the development of networks to support pervasive communications, whether wireless or wire line, whether for home, business, hotel, and coffee shop or on the move. Electrical contractors are most likely benefiting from the fact that Pervasive Networking takes place over a LAN (wired or wireless).

The Pervasive Network consists of mobile nodes which are arranged independently in the environment and also they change their position dynamically. The best examples of Pervasive Network are Mobile ad-Hoc Network (MANET), Wireless Mesh Network WMN and Vehicular Ad hoc Network (VANET). A MANET consists of mobile nodes that are arranged autonomously in the network environment. The nodes in MANET dynamically change its position because the topology of the network changes frequently. It is very difficult to provide the reliable routing in MANET. The applications of Pervasive Network include Military Applications, Road Safety Systems and also for some critical applications.

Pervasive Network (PN) is a network which can grant different services from a Single Access point. One of the applications of these networks is appeared as VANET. Vehicular ad-hoc Network is a network which contains vehicles as their participants. The Vehicle to Vehicle Communication and the vehicle to road side base station can be possible in VANET.

1.1.1 Challenges and Issues

The security challenges are faced in Pervasive Network is because of the weak link between the nodes. Some of such challenges faced are listed:

- As the nodes are distributed in the wireless medium, it can communicate by making use of signal propagation through air medium. So, it is easy to faucet.
- The nodes present in the pervasive environment are resource limited. So, it requires proficient schemes with less overhead.
- Due to its dynamic nature, the self-organizing, self-healing algorithm is required to tolerate the security attacks.
- The Pervasive Network is vulnerable to denial of service attack.

The attacks occurred in Pervasive Network are broadly classified into two: Passive and Active attacks. Eavesdropping falls into the category of passive attack. In this, the intruder captures the data while it is transmitted. On the other hand in the active attack, the malicious node misleads other nodes to affect the communication.

All types of ad-Hoc networks come under Pervasive Networks. In this research work, the Vehicular Ad hoc Network is taken to provide the security from location based attack.

1.2 VANET

Vehicular Ad Hoc Networks (VANETs) The networks that interconnect vehicles on road are called Vehicular Ad hoc Networks (VANETs). “A mobile ad hoc network (MANET) consists of mobile nodes that connect themselves in as decentralized, self-organizing manner and may also establish multi-hop routes. If mobile nodes are cars, this is called vehicular ad hoc network”. “The main target of research in VANETs is the improvements of vehicle safety by means of inter vehicular communication (IVC)”. Several different applications are emerging in VANETs. These applications include safety applications to make driving much safer, mobile commerce and other information services that will inform drivers about any type of congestion, driving hazards, accidents, traffic jams. VANETs have several different aspects compared to MANETs, in that the nodes move with high velocity because of which the topology changes rapidly. VANETs are also prone to several different attacks. Therefore, the security of VANETs is indispensable. VANETs pose many challenges on technology, protocols, and security, which increase the need for research in this field.

A Vehicular Ad Hoc Network or VANET is a technology that uses moving cars as nodes in a network to create a mobile network. VANET turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 meters from each other to connect and, in turn, create a network with a wide range. As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile network is created. It is estimated that the first systems that will integrate this technology are police and fire vehicles to communicate with each other for safety purposes. VANETs come under the category of wireless ad-hoc network. In vehicular ad-hoc network, the node may be a vehicle or the road side units. They can communicate with each other by allowing the wireless connection up to a particular range.

Inter-Vehicular Communications (IVC) also known as vehicular ad hoc networks (VANETs) have become very popular in recent years. A Vehicular Ad hoc Network is a special type of Mobile Ad hoc Networks (MANETs is a kind of wireless ad hoc networks and is self-configuring network of mobile routers connected by wireless links) which use vehicles as nodes. The main difference is that mobile routers which build the network are vehicles like cars or trucks. Several different applications are emerging with regard to vehicular communications. For example, safety applications for safer driving, information services to inform drivers about the driving hazards and other business services in the vicinity of the vehicle. Government, corporations, and the academic communities are working on enabling new applications for VANETs. A main goal of VANETs is to increase road safety by the use of wireless communications. To achieve these goals, vehicles act as sensors and inform each other about abnormal and potentially hazardous conditions like accident, traffic jams and glazes. Vehicular networks closely resemble ad hoc networks because of their rapidly changing topology. Therefore; VANETs require secure routing protocols. Numerous Applications are unique to the vehicular setting. These applications include safety applications that will make driver safe, mobile commerce, roadside services that can intelligently inform drivers about congestion, businesses, and services in the vicinity of the Vehicle. VANETs, especially compared to MANETs are characterized by several unique aspects. Nodes move with high velocity, resulting in high rates of topology changes. Because of rapidly changing topology due to vehicle motion, the vehicular network closely resembles an ad hoc network. The constraints and optimizations are remarkably different. From the network perspective, security and scalability are two significant challenges. A formidable set of abuses and attacks become possible. Hence, the security of vehicular networks is indispensable. The growing importance of inter-vehicular communications (IVC) has been recognized by the government, corporations, and the academic community. Government and industry cooperation has funded large IVC partnerships or projects such as Advanced Driver Assistance Systems and CarTALK 2000 in Europe, and FleetNet in Germany. VANETs pose many challenges on technology, protocols, and security which increase the need for research in this field.

Vehicular ad hoc networks (VANETs) are expected to support a large spectrum of mobile distributed applications that range from traffic alert dissemination and dynamic route planning to context-aware advertisement and file sharing. Considering the large number of nodes that participate in these networks and their high mobility, debates still exist about the feasibility of applications that use end to end multi hop communication. The main concern is whether the performance of VANET routing protocols can satisfy the throughput and delay requirements of such applications. Analyses of traditional routing protocols for mobile ad hoc networks (MANETs) demonstrated that their performance is poor in VANETs. The main problem with these protocols, e.g., ad hoc on-demand distance vector (AODV) and dynamic source routing (DSR), in VANET environments is their route instability. The traditional node-centric view of the routes (i.e., an established route is a fixed succession of nodes between the source and the destination) leads to frequent broken routes in the presence of VANETs' high mobility, as illustrated in Fig. 1.1. Consequently, many packets are dropped, and the overhead due to route repairs or failure notifications significantly increases, leading to low delivery ratios and high transmission delays.

One alternative approach is offered by geographical routing protocols, e.g., greedy–face–greedy (GFG), greedy other adaptive face routing (GOAFR), greedy perimeter stateless routing (GPSR), which decouple forwarding from the nodes identity. These protocols do not establish routes but use the position of the destination and the position of the neighbor nodes to forward data. Unlike node-centric routing, geographical routing has the advantage that any node that ensures progress toward the destination can be used for forwarding. For instance, in Figure 1.1, geographical forwarding could use node N2 instead of N1 to forward data to D. Despite better path stability, geographical forwarding does not also perform well in city-based VANETs.

Its problem is that, oftentimes, it cannot find a next hop (i.e., a node that is closer to the destination than the current node). The recovery strategies in the literature are often based on planar graph traversals, which were shown to be ineffective in VANETs due to radio obstacles, high node mobility, and the fact that vehicle positions are constrained on roads rather than being uniformly distributed across a region.

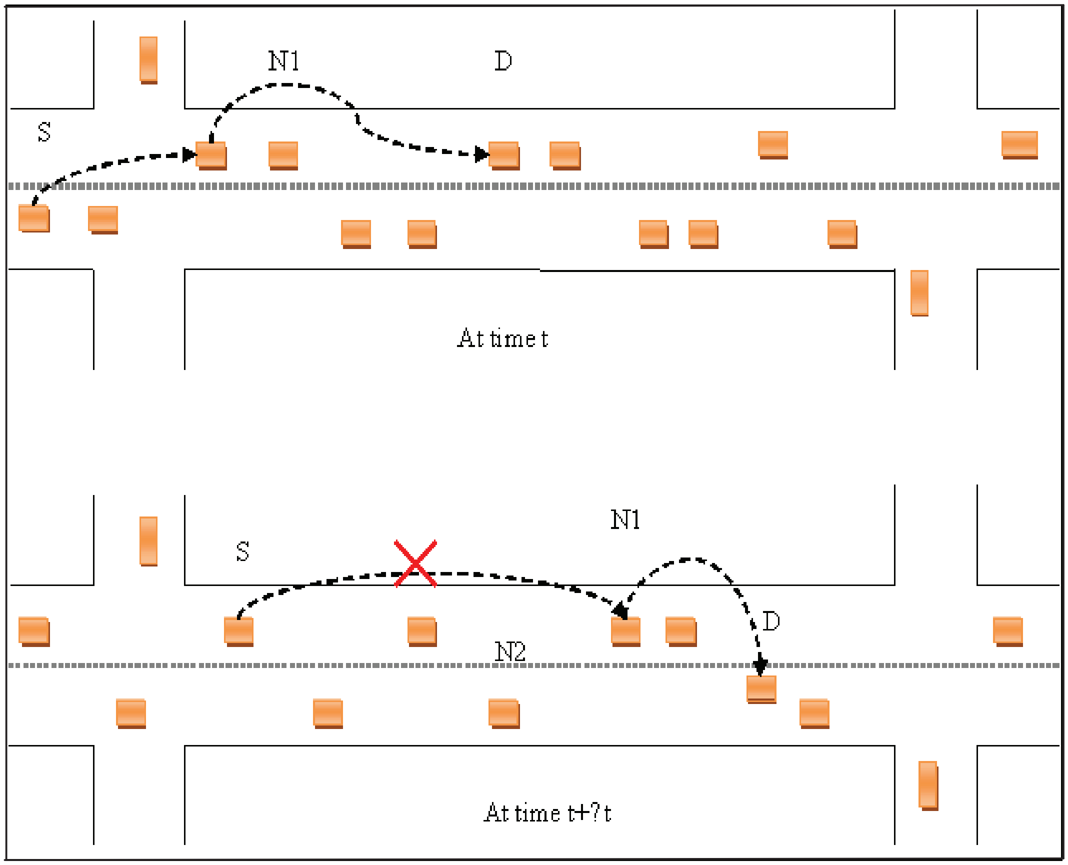

Figure 1.1 Pre-established routes frequently break in highly mobile VANETS

Vehicular ad hoc network (VANET) can offer various services and benefits to VANET users and thus deserves deployment effort. VANETs with interconnected vehicles and numerous services promise superb integration of digital infrastructure into many aspects of our lives, from vehicle to-vehicle, roadside devices, base stations, traffic lights, and so forth. A network of a huge number of mobile and high-speed vehicles through wireless communication connections has become electronically and technically feasible and been developed for extending traditional traffic controls to brand new traffic services that offer large traffic-related applications. Safety information exchange enables life-critical applications, such as the alerting functionality during intersection traversing and lane merging, and thus plays a key role in VANET applications. The attractive features of VANETs inevitably incur higher risks if such networks do not take security into account prior to deployment. For instance, if the safety messages are modified, discarded, or delayed either intentionally or due to hardware malfunctioning, serious consequences such as injuries and even deaths may occur.

Unlike traditionally wired networks are protected by several lines of defense such as firewalls and gateways, security attacks on such wireless networks may come from any direction and target all nodes. Therefore, VANETs are susceptible to intruders ranging from passive eavesdropping to active spamming, tampering, and interfering due to the absence of basic infrastructure and centralized administration. Moreover, the main challenge facing vehicular ad hoc networks is user privacy. Whenever vehicular nodes attempt to access some services from roadside infrastructure nodes, they want to maintain the necessary privacy without being tracked down for whoever they are, wherever they are and whatever they are doing. It is considered as one of the important security requirements that should be paid more attention for secure VANET schemes, especially in privacy-vital environment. A number of security threats to vehicular ad hoc networks have been addressed.

1.2.1 VANET Model Overview

There are many entities involved in a VANET settlement and deployment. Although the vast majority of VANET nodes are vehicles, there are other entities that perform basic operations in these networks. Moreover, they can communicate with each other in many different ways. In this Section, firstly a description about the most common entities those appear in VANETs, is provided. In the second part, a analysis of the different VANET settings that can be found among vehicles and the remaining entities, is made.

Common VANET entities: Several different entities are usually assumed to exist in VANETs. To understand the internals and related security issues of these networks, it is necessary to analyze such entities and their relationships. Figure 1.2 shows the typical VANET scheme.

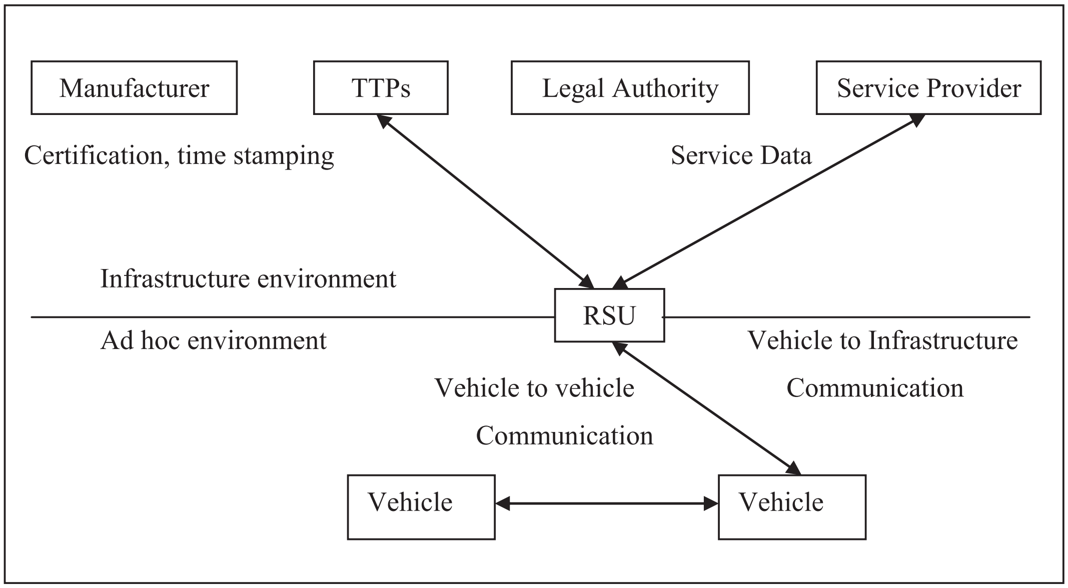
Manufacturer
TTPs
Legal Authority
Service Provider
Certification, time stamping
Service Data
Infrastructure environment
RSU
Ad hoc environment
Vehicle to Infrastructure Communication
Vehicle to vehicle Communication
Vehicle
Vehicle

Figure 1.2 VANET model

As shown in Figure 1.2, two different environments are generally considered in VANETs:

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.

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 way, sensitive information (e.g. user credentials or pre-crash information) can be reliably stored.

As mentioned before, VANETs as communications network impose several unique requirements. Vehicles move at a relatively high speed and, on the other hand, the high amount of vehicles present in a road could lead to an enormous network. Thus, a specific communication standard, called Dedicated Short Range Communications (**DSRC**) has been developed to deal with such requirements (Armstrong Consulting Inc.). This standard specifies that there will be some communications devices located aside the roads, called Road-Side Units (**RSU**). In this way, RSUs become gateways between the infrastructure and vehicles and vice versa.

1.2.2. VANET Settings

Several applications are enabled by VANETs, mainly affecting road safety. Within this type of application, messages interchanged over VANETs have different nature and purpose. Taking this into account, four different communication patterns can be observed:

V2V Warning Propagation (Fig. 1.3): 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.

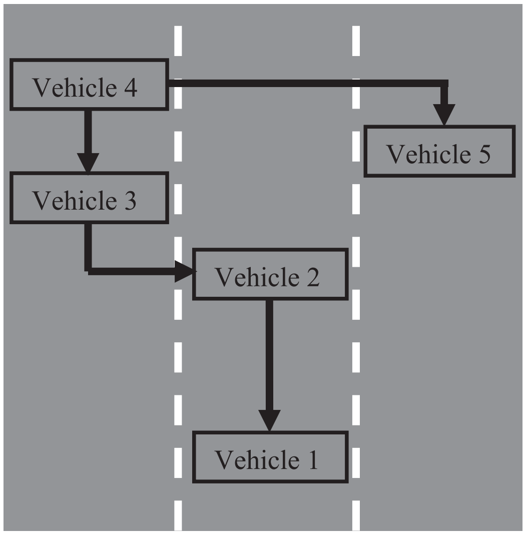

Figure 1.3 Warning Propagation

V2V Group Communication (Fig. 1.4): Under this pattern, only vehicles having some features can participate in the communication. 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).

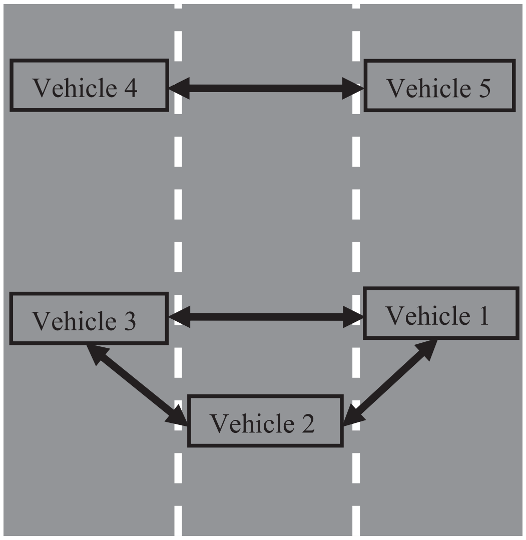

Figure 1.4 V2V group Communication

V2V Beaconing (Fig. 1.5): 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.

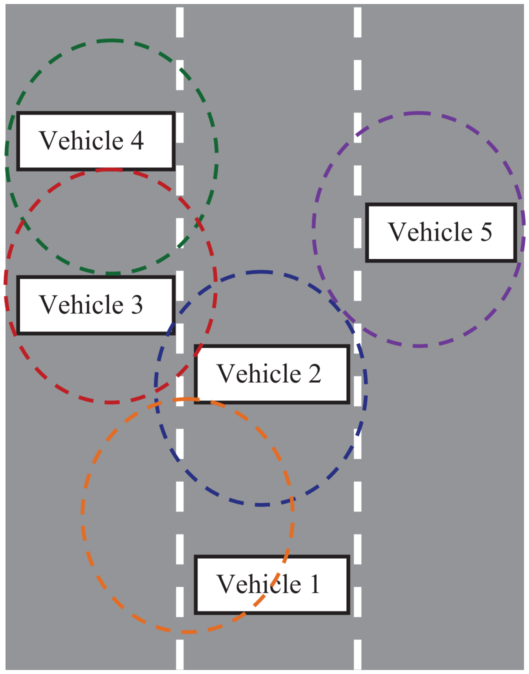

Figure 1.5 V2V Beaconing

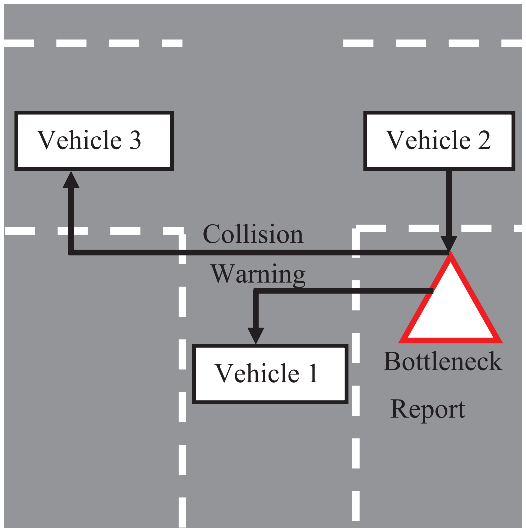

Figure 1.6 V2I warning

I2V/V2I Warning (Fig. 1.6): 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.

There exist other communication patterns over VANETs (e.g. related to multimedia access, location-based services, etc.). In particular, vehicles could use different communication media like cellular networks (e.g. GSM/GPRS) to get such services. However, we will focus on V2V and V2I road safety communication patterns over VANETs, as they will be more challenging from the security point of view. In fact, each communication pattern has a different set of security requirements.

1.2.3. System Architecture and Working of VANETs

Vehicular Networks System consists of large number of nodes, approximately number of vehicles exceeding 750 million in the world today, these vehicles will require an authority to govern it, each vehicle can communicate with other vehicles using short radio signals DSRC (5.9 GHz), for range can reach 1 KM, this communication is an Ad Hoc communication that means each connected node can move freely, no wires required, the routers used called Road Side Unit (RSU), the RSU works as a router between the vehicles on the road and connected to other network devices. Each vehicle has OBU (on board unit), this unit connects the vehicle with RSU via DSRC radios, and another device is TPD (Tamper Proof Device), this device holding the vehicle secrets, all the information about the vehicle like keys, driver's identity, trip details, speed, route …etc.,.

The **architecture** of VANET implies that the communicating nodes in a VANET are either vehicles or base stations. Vehicles can be private (belonging to individuals or private companies) or public (i.e., public transportation means, e.g., buses, and public services such as police cars). Base stations can belong to the government or to private service providers. As shown in figure 1.7 the vehicles can communicate with each other and communicate with Road Side Units (RSU) interchangeably.

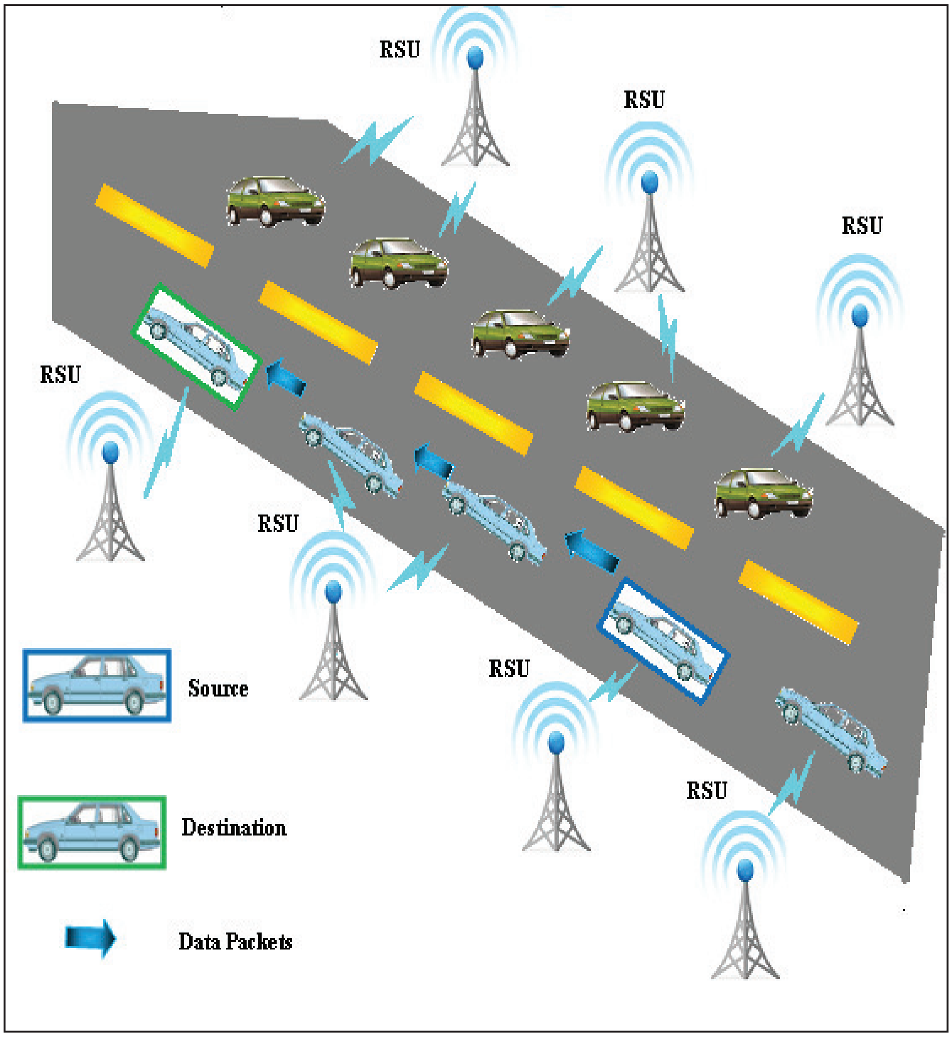

Figure 1.7 Architecture of VANET

The scale of VANETs is another feature that sets them apart. With hundreds of millions of nodes distributed everywhere, VANETs are likely to be the largest real world mobile ad hoc network.

Vehicular ad hoc networks are important technology for future developments of vehicular communication systems. Such networks composed of moving vehicles, are capable of providing communication among nearby vehicles and the roadside infrastructure. Modern vehicles are equipped with computing devices, event data recorders, antennas, and Global Positioning System (GPS) receivers making VANETs realizable. VANETs can be used to support various functionalities such as vehicular safety, traffic congestion reduction, office-on wheels, and on-road advertisement. Most nodes in a VANET are mobile, but because vehicles are generally constrained to roadways, they have a distinct controlled mobility pattern. Vehicles exchange information with their neighbors and routing protocols are used to propagate information to other vehicles.

1.2.4 Possibility of Attacks in VANET

Besides having advantages of the proxy re-encryption method for authentication, there are still some attacks that can be possible that are explained as follows:

- **Denial of Service (DoS) attack:** Attackers may seek to initiate excessive authentication requests in order to exhaust the resources of the Access Point (AP). A general solution would be to limit the number of authentication requests which can be processed in a unit of time period. This method can guarantee that the server is not overwhelmed by DoS. But this could also delay a request. The implementation of the schemes must take such tradeoffs into consideration.

- **Eavesdropping**: Since the session key is calculated based on the nonces contributed by the car and the AP respectively. Both of the car's nonce and the AP's nonce are encrypted by the public key of the SP during transmission. The attacker can reveal the session key, if he/she got the SP's private key, or an appropriate re- encryption key/private key pair.
- **Masquerade Attack:** An unauthorized car which did not subscribe service from the SP may overhear the authentication messages on the air and try to have it authenticated to the AP by replaying them. The attacker can get the car's public key and certificate and replay the car's authentication request. If the nonce n1 (randomly chosen) by the AP, matches with the one chosen earlier, then the attacker can decrypt the response message from the AP which is encrypted by the car's public key.
- **Key Bootstrapping and Rekeying:** Anonymous keys are preloaded by the transportation authority or the manufacturer, but with different consequences. Moreover, while ELPs (Electronic License Plate) are fixed and should accompany the vehicle for a long duration (potentially its life cycle), anonymous key sets have to be periodically renewed after all the keys have been used or their lifetimes have expired. This renewal can be done during the periodic vehicle checkup (typically yearly) or by similar procedures. In addition to the ELP and anonymous keys, each vehicle should be preloaded with the Certificate Authority's (CA) public key.
- **Tamper-Proof Device**: The use of secret information such as private keys incurs the need for a tamper-proof device in each vehicle. In addition to storing the secret information, this device will be also responsible for signing outgoing messages. To reduce the risk of its compromise by attackers, the device should have its own battery, which can be recharged from the vehicle, and clock, which can be securely resynchronized, when passing by a trusted roadside base station.

The access to this device should be restricted to authorized people. For example, cryptographic keys can be renewed at the periodic technical checkup of the vehicle.

1.2.5 Vehicular Networks Challenges

- **Mobility:** The basic idea from Ad Hoc Networks is that each node in a MANET is mobile, and can move from one place to another within the coverage area, but the mobility speed is limited. But, in Vehicular Ad Hoc Network nodes moving with high speed, vehicles make connection with other vehicles which are available inside its communication range, and this connection exists for only a few seconds as each vehicle goes in its direction, and these two vehicles may never meet again. So securing mobility challenge is a hard problem.
- **Volatility:** The connectivity among nodes can be highly ephemeral, and maybe will not happen again, vehicles travelling through coverage area and making connection with other vehicles, these connections will be lost as each car has a high mobility, and may travel in opposite direction. Vehicular networks lacks the relatively long life context, so personal contact of user's device to a hot spot will require long life password and this will be impractical for securing Vehicular Communication (VC).
- **Privacy VS Authentication:** The importance of authentication in Vehicular Ad Hoc Networks is to prevent Sybil Attack. To avoid this problem, they can give a specific identity for every vehicle, but this solution will not be appropriate for the most of the drivers who wish to keep their information protected and private.
- **Privacy VS Liability:** Liability will give a good opportunity for legal investigation and this data cannot be denied (in case of accidents), on the other

hand the privacy must not be violated and each driver must have the ability to keep his personal information from others (Identity, Driving Path, and Account Number for toll Collector etc.).

- **Network Scalability:** The scale of this network in the world approximately exceeding the 750 million nodes, and this number is growing, another problem arises when there is no global authority to govern the standards of this network, for example: the standards for DSRC in North America is deferent from the DSRC standards in Europe, the standards for the GM Vehicles are deferent from the BMW one.
- **Bootstrap:** At this moment only few number of cars have the equipment required for the DSRC radios, so if they make a communication they have to assume that there is a limited number of cars that will receive the communication, in the future they must concentrate on getting the number higher, to get a financial benefit that will encourage the commercial firms to invest in this technology.

1.2.6 Need for VANET Security

Taking into account the different entities and data at stake, in this Section a catalog of security requirements is built. First of all, **entity identification** imposes that each participating entity should have a different and unique identifier. However, identification itself does not imply that the entity proves that it is its actual identity and this requirement is called **entity authentication**. Each of the application groups (enabled by the communication patterns previously introduced) has different needs regarding to these requirements. V2V warning propagation needs identification to perform message routing and forwarding – identifiers are essential to build routing tables. Sender authentication is also needed for liability purposes. Imagine that a regular vehicle sends a notification as if it were a police patrol. It should be then needed to prove the identity of the emitting node. In group communications, it is not required to identify or authenticate the communicating peers. The only need is to show that both participating entities have the required attributes to become group members – this is the **attribute authentication** requirement. In fact, this is the only communication pattern that needs this requirement. In beaconing, identification and authentication of the sender is needed. Nearby vehicles can then build a reliable neighbor table. Both requirements are also present in I2V warnings, where only messages sent by the infrastructure are credible. Infrastructure warnings are sent to all passing vehicles within an area, so identification or authentication of the receiver is not needed. On the contrary, V2I warnings also require the emitting vehicle to be identified and authenticated. In this way, only vehicles with a trustworthy identity will be able to send such messages. Accomplishing the cited requirements should not imply less privacy.

In fact, **privacy preservation** is critical for vehicles. In the vehicular context, privacy is achieved when two related goals are satisfied – ***untraceability*** and ***unlinkability***. First property states that vehicle´s actions should not be traced (i.e. different actions of the same vehicle should not be related). On the other hand, second property establishes that it should be impossible for an unauthorized entity to link a vehicle´s identity with that of its driver/owner. However, this privacy protection should be removed when required by traffic authorities (i.e. for liability attribution). This requirement is present in all V2V communications. In fact, privacy should not get compromised even if different messages (no matter if under different communication patterns) are sent by the same vehicle. It does not apply to I2V warnings, as the sender (i.e. the infrastructure) does not have privacy needs.

Non-repudiation requirement assures that it will be impossible for an entity to deny having sent or received some message. It is needed for the sender in V2V warnings and beacons. In this way, if a vehicle sends some malicious data, there will be a proof that could be employed for liability purposes. In group communications it is not generally required, as the emitting node could be any of the group members. With respect to I2V and V2I warnings, non-repudiation of origin is needed, so wrong warning messages can be undoubtedly linked to the sending node. Non-repudiation of receipt is not currently needed, but it will be in the future. Currently, accident responsibility relies only on the human driver. However, in the future there are some envisioned applications that would automate partially the driving task. In such situation, not receiving a warning message could be critical for liability attribution.

Another important security requirement in vehicular communications is **confidentiality**, that is, to assure that messages will only be read by authorized parties. This requirement is only present in group communications, in which only group members are allowed to read such information. The remaining VANET settings transmit public information. In fact, this requirement is not considered in some previous works. Nevertheless, for the sake of completeness, it will be taken into account in this overview.

The **availability** requirement implies that every node should be capable of sending any information at any time. As most interchanged messages affect road traffic safety, this requirement is critical in this environment. Designed communication protocols and mechanisms should save as much bandwidth and computational power as possible, while fulfilling these security requirements. It is present on all communication patterns, that is, it affects not only V2V communications, but also I2V ones.

Finally, related to the information itself, data integrity and accuracy must be assured. Both needs are globally referred as **data trust**. Data at stake should not be altered and, more importantly, it should be truthful. It also implies that received information is fresh (i.e. refers to the current state of the network). False or modified data should lead to potential crashes, bottlenecks and other traffic safety problems. For this reason, data trust must be provided on all VANET communications.

The security design of VANET should guarantee the following:

1. Message Authentication, i.e. the message must be protected from any alteration.
2. Data integrity does not necessarily imply identification of the sender.
3. Entity Authentication, so that the receiver is not only ensured that sender generated a message, in addition has evidence of the liveliness of the sender.
4. Conditional Privacy must be achieved in the sense that the user related information, including the driver's name, the license plate, speed, position and traveling routes.
5. In some specific application scenarios, Confidentiality, to protect the network against unauthorized message injection, message alteration, and eavesdropping, respectively.

An important feature of VANET security is the Digital Signature as a building block. Whether in inter-vehicle communications or communications through infrastructure, authentication (using signatures) is a fundamental security requirement since only messages from legitimate senders will be considered. Signatures can also be used to guarantee data integrity (i.e., the message being sent is not modified). Message confidentiality remains an option in VANETs depending on the specific application because it is quite fundamental to secure such communications in many other networks. For instance, safety related messages do not contain sensitive information and thus encryption is not needed.

1.3 ATTACKS IN VANET

Once the security requirements have been established for VANETs, many attacks can be identified to compromise them. In this section an elaborate discussion is made on these attacks, explaining how they can be performed and their potential consequences. For the sake of clarity, attacks have been classified depending on the main affected requirement.

1.3.1 Attacks on Identification and Authentication

- **Impersonation** is the case where an attacker pretends to be another entity. It can be performed by stealing other entity´s credential. As a consequence, some warnings sent to (or received by) a specific entity would be sent to (or received by) an undesired one.
- **False attribute possession** is a subtype of impersonation, in which the attacker tries to show the possession of an attribute (e.g. to be a member of an enterprise) to get some benefit. It could be performed if false credentials could be built, or if revoked credentials could be used normally. As a consequence, a regular vehicle could send messages claiming to be a police patrol, letting it to have a freeway.
- **Sybil** attacker uses different identities at the same time. In this way, a single vehicle could report the existence of a false bottleneck. Sybil attacks have been regarded as serious security threat to ad hoc and sensor networks. They impair the potential applications of VANETs by creating an illusion of traffic congestion. In the opinion of researchers, VANETs are facing a number of security threats, which impairs the efficiency of many VANETs potential applications and poses threat to even life safety. In Sybil 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.

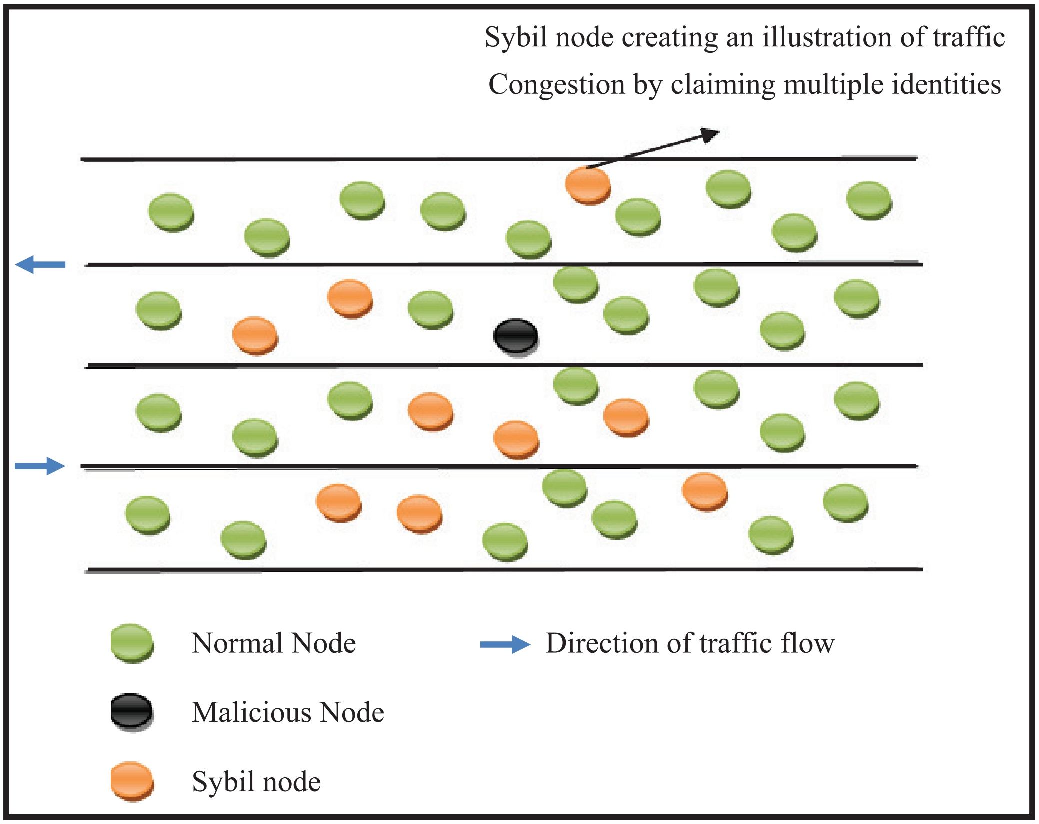
Sybil node creating an illustration of traffic
Congestion by claiming multiple identities
Normal Node
Direction of traffic flow
Malicious Node
Sybil node

Figure 1.8 Sybil Attacks in VANET

Generally, in Sybil attack, a malicious node illegitimately takes on multiple identities. In mobile networking, each node gets the information of the neighboring node by receiving periodic beacons from neighbors in which they claim their identity. A malicious vehicle can manage to get identities of other vehicle by non-technical means such as stealing or it can also borrow from its friends. In the above Fig. 1.8 the malicious node M creates an illusion of traffic congestion by claiming multiple identities thereby convincing other vehicles that there is a traffic jam and makes them to choose alternate route so that he makes his path clear.

As presented in the VANET model, TPMs mounted on vehicles can store sensitive information like identifiers. In this way, the Sybil threat is alleviated. However, security mechanisms must be designed to provide identification and authentication, thus protecting against impersonation attacks.

1.3.2 Attacks on Privacy

Attacks on privacy over VANETs are mainly related to illegally getting sensitive information about vehicles. As there is a relation between a vehicle and its driver, getting some data about a given vehicle´s circumstances could affect its driver privacy. These attacks can then be classified attending to the data at risk:

- **Identity revealing** is a condition of getting the owner´s identity of a given vehicle that could put its privacy at risk. Usually, it is assumed that, a vehicle´s owner is also its driver, so it would simplify getting personal data about that person.
- **Location tracking** is also a privacy attack. The location of a vehicle in a given moment, or the path followed along a period of time are considered as personal data. It allows building that vehicle´s profile and, therefore, that of its driver.

Mechanisms for facing both attacks are required in VANETs. They must satisfy the tradeoff between privacy and utility. In this way, security mechanisms should prevent unauthorized disclosures of information, but applications should have enough data to work properly.

1.3.3 Attacks on Non-Repudiation

The main threat related to non-repudiation is denying some action by some of the implicated entities. Non-repudiation can be circumvented if two or more entities share the **same credentials**. This attack is different from the *impersonation* attack described before – in this case, two or more entities collude to have a common credential. In this way, they get indistinguishable, so their actions can be repudiated.

Credential issuance and management should be secured in VANETs to alleviate this threat. Although reliable storage has been assumed in vehicles (by their TPMs), having identical credentials in different vehicles should be avoided. Moreover, mechanisms that provide a proof of participation have to be also implemented.

1.3.4 Attacks on Confidentiality

- **Eavesdropping** is the most prominent attack over VANETs against confidentiality. To perform it, attackers can be located in a vehicle (stopped or in movement) or in a false RSU. Their goal is to illegally get access to confidential data. As confidentiality is needed in group communications, mechanisms should be established to protect such scenarios.

1.3.5 Attacks on Availability

- As any other communication network, availability in VANETs should be assured both in the communication channel and in participating nodes. A classification of these attacks, according to their target, is as follows:
- **Network Denial of Service (DoS)**: It overloads the communication channel or makes its use difficult (e.g. interferences). It could be performed by compromising enough RSUs, or by making a vehicle to broadcast infinite messages in a period of time.
- **Routing Anomalies,** is a particular case of network attacks that could lead to DoS. In this case, attackers do not participate correctly in message routing over the network. They drop all received messages (**sinkhole attack**) or just a few ones according with their interests (**selfish behavior**).
- **Computation DoS** overloads the computation capabilities of a given vehicle. Forcing a vehicle to execute hard operations, or to store too much information, could lead to this attack.

1.3.6 Attacks on Data Trust

Data trust can be compromised in many different ways in VANETs. **Inaccurate data calculation and sending** affects message reliability, as they do not reflect the reality. This could be performed by manipulating in-vehicle sensors, or by altering the sent information. Imagine that a vehicle reports an accident in road NH-7, while it really took place in NH-9. Such information should compromise such messages´ trust. Even worse, sending **false warnings** (e.g. the accident didn´t take place) would also affect the whole system reliability. In this way, mechanisms to protect against such inappropriate data should be put in practice in vehicular contexts.

1.3.7 Authentication Scheme in VANET

The scenario for VANET communication includes communicating entities of the service providers (SP), the cars, and the access points (AP) operated on behalf of service providers. The SPs and the APs can communicate with each other by some application-layer proprietary protocols via Internet. The APs are deployed along the roadside with reasonable wireless coverage to facilitate communication. A car typically belongs to one wireless network service provider, and communicates with the APs for accessing the internet along the road it travels through. When it travels, it also roams into wireless coverage that provide by other authorities. To make the authentication process time-efficient, traditional solutions using centralized Authentication Server (AS) is not preferable because of the large amount of messages exchanged among the cars, the APs and the ASs. If the overlay network interconnecting the APs and the ASs is based on Internet, the delay for exchanging authentication messages could be prohibitive given the shortness of communication duration between the fast moving car and an individual AP. Thus the authentication protocols are devised such that after the car initiates communication requests until the communication session is established, the protocol should involve as less parties as possible besides the car and the AP, and as less on demand communication over Internet as possible besides the wireless link between the two communicating parties. In addition, the number of messages exchanged in order for authentication should be controlled. In the design, the user authentication will be performed at the APs, i.e., the user will prove to the AP that it is a legitimate one. A more strict security will require the AP to prove it as a legitimate one as well, so to have mutual authentication.

During the authentication, the two parties will negotiate a secret session key for the communication afterwards. The session keys could be established in a way that synchronizes the update at both the car and the AP so to allow location privacy countermeasures.

1.3.8 Security Aspects Restricted to VANET

Generally, attacks cause anomalies to the network functionality. A lot of previous studies have investigated security vulnerabilities of routing protocols for wireless networks. Also, there are attacks in which malicious nodes advertise fake locations to their neighbor nodes.

- Position verification techniques to thwart position spoofing attacks.
- Traceability by trusted network authorities (e.g., network administrator) for privilege revocation once misbehavior is detected.
- Identity and location privacy preserving mechanisms against unlawful tracing and user profiling.
- Non-frameability of an honest user, who cannot be falsely accused of having misbehaved.
- Detecting and correcting malicious data to ensure data consistency.

- The system must have light overheads in terms of computational costs and high efficiency.
- Preventing impersonation attacks, that is, no one can impersonate another authorized member to cause service abuse problems and to damage the security of VANETs.
- Preventing eavesdropping, in other words, an intruder cannot discover some valuable information from communications between members in VANETs.

Malicious attackers may damage the network by announcing fake node locations. Such attacks are even more difficult to mitigate.

1.3.9 Privacy Challenges

During a long-distance trip in high speed, a vehicular user could roam across multiple APs either belonging to their home wireless domain or to domains owned by different authorities including various service providers. This poses challenges on privacy and network performance to the current public wireless networks access protocols. The privacy challenge comes from traffic logging at AP's and at home domain in current public wireless LAN roaming protocols. As a result, home and visited networks can acquire much personal information, e.g., the home network knows the current location of a mobile user, and the visited network knows the mobile user's identity and its home domain. Privacy in vehicular networks has to deal with threats that try to correlate received identifiers, or to correlate them to real-world identity, or to have position-identifier pairs. The performance challenge originates from the exchange of authentication messages between a user and its home domain when roaming. Mobile wireless communication has introduced new ***Location Privacy*** issue. Location Privacy is defined as an identity not being associated with a location, or a series of locations.

1.4 VEHICULAR COMMUNICATION

Rapid advances in wireless technologies provide opportunities to utilize these technologies in support of advanced vehicle safety applications. In particular, the new Dedicated Short Range Communication (DSRC) offers the potential to effectively support vehicle-to vehicle and vehicle-to-roadside safety communications, which has become known as Vehicle Safety Communication (VSC) technologies. DSRC enables a new class of communication applications that will increase the overall safety and efficiency of the transportation system.

Intelligent Transportation Systems (ITS) are the future of transportation. As a result of emerging standards, such as 5.9 GHz dedicated short-range communication, vehicles will soon be able to talk to one another as well as their environment. A number of applications will be made available for vehicular networks that improve the overall safety of the transportation infrastructure. For instance, the system will be able to monitor traffic to coordinate traffic lights so that traffic flows smoothly. Sensors will use feedback from vehicles to detect traffic jams. Public safety vehicles will broadcast, via the wireless channel, to change traffic signals in order to respond quickly to an emergency. Cars will communicate with one another to drive cooperatively, therefore avoiding collisions and improving efficiency. These are some of the possible applications, in the future, that will be possible with the advent of the DSRC standard. Considering the tremendous benefits expected from vehicular communications and the huge number of vehicles, it is clear that vehicular ad hoc networks (VANET) are likely to become the most relevant realization of mobile ad hoc networks.

The appropriate integration of on-board computers, roadmaps, and GPS positioning devices along with communication capabilities, opens tremendous opportunities, but also raises formidable research challenges. DSRC is a candidate for use in a VANET, is a short to medium range communication service that supports both public safety and private communication. The communication environment of DSRC is both vehicle-to-vehicle and vehicle-to/from-roadside.

The VANET aims to provide a high data rate and at the same time minimize latency within a relatively small communication zone. A number of novel problems are associated with a VANET because of the unique characteristics of the network. To begin, the main differences between a VANET and a MANET are a MANET typically has no infrastructure available. In the case of a VANET, it is possible to strategically place access points along the side of the road, and in turn allow vehicles' access to the services available from the infrastructure. Also, one of the greatest challenges is the vehicles in the network move at greater speeds than most other MANETs, leading to a network that can frequently become fragmented. Scalability is one challenge to which there are some solutions available in the literature [43]. Furthermore, security and privacy are a crucial concern for a VANET.

Dedicated Short-Range Communication

Dedicated Short-Range Communication (DSRC) is a standard that aims to bring vehicular networks to North America. Traffic fatalities have been a long standing problem in the United States, as in the rest of the world. As an indication of the severity of the problem, in 1999 there were 6,279,000 motor vehicle accidents that accounted for 41,611 deaths in the United States. In 1991, the US Congress passed the Intermodal Surface Transportation Efficiency Act of 1991 that resulted in the creation of the first generation of Intelligent Transportation System (ITS). The goal of the ITS program is to incorporate technology into the transportation infrastructure to improve safety.

The first generation of the Dedicated Short-Range Communication (DSRC) system operates at 915 MHz and has a transmission rate of 0.5 Mbps. This project had limited success and was used primarily by commercial vehicles and for toll collection. One example of a first generation DSRC application is exposes that is used for electronic toll collection. The second generation of DSRC started in 1997 when ITS America requested that the Federal Communication Commission (FCC) allocate an additional 75 MHz of bandwidth. In October 1999, the FCC allocated the 75 MHz of bandwidth in the 5.9 GHz band for the second generation of DSRC.

Since the allocation of the bandwidth, standardization bodies have been working on the implementation details of 5.9 GHz DSRC. The North American DSRC standards program aims at creating an interoperable standard for use in the United States, Canada, and Mexico. The primary goal of the project is to enable drivers to receive up-to-date information regarding their surrounding environment, thereby reducing traffic accidents.

Furthermore, 5.9 GHz DSRC must have a low cost and be very scalable. In addition, the 5.9 GHz DSRC should require no usage fee from the users to access the network. In this section, the characteristic of 5.9 GHz DSRC are given along with a comparison to 915 MHz DSRC. Next, a comparison of the possible wireless solutions for DSRC is given. Following this, some of the additional technologies that are used in DSRC are explained. Finally, the architecture of the VANET is described.

1.4.1 Characteristics of 5.9 GHz DSRC

DSRC is meant to be a complement to cellular communications by providing very high data transfer rates in circumstances where minimizing latency in the communication link and isolating relatively small communication zones are important. DSRC is also known as WAVE (Wireless Access in Vehicular Environments). Furthermore, an IEEE task group is currently working on the IEEE 802.11p standard for both the PHY layer and the MAC layer of DSRC. The primary reason why the

MAC and PHY layers are being developed under 802.11 is to ensure that the standard remains stable over time. One of the cited problems of the original 915 MHz DSRC is that few implementations completely followed the standard.

Instead, most of the original DSRC implementations were based on proprietary solutions. Realizing that proprietary implementations were one of the main causes of 915 MHz DSRC's lack of success, the new 5.9 GHz DSRC is an open standard. The 5.9 GHz DSRC overcomes many of the weaknesses associated with 915 MHz DSRC. To begin with, an increased amount of bandwidth is available for 5.9 GHz DSRC. Also, the 5.9 GHz DSRC spectrum is composed of seven channels of 10 MHz each. One channel is reserved for the control channel and six additional channels are service channels, whereas 925 MHz DSRC standard only supports the use of one or two channels. Next, 5.9 GHz DSRC supports high speed data transfers ranging from 6 Mbps to 27 Mbps. Under certain circumstances, the data rate can reach 54 Mbps when two service channels are combined to form one 20 MHz channel. On the contrary, 915 MHz DSRC supports a data rate of only 0.5 Mbps. Also, the transceivers used in vehicles required a reduced transmit power compared to 915 MHz DSRC. In addition, the communication range is increased for 5.9 GHz DSRC.

Transmission ranges of up to 1000 m are supported by 5.9 GHz DSRC, but typically the transmission range is shorter to promote greater frequency reuse. The transmission range that is used is based on the type of application and the channel in use. Next, the interference potential for 5.9 GHz DSRC is much lower than for 915 MHz DSRC. The only interference in the 5.9 GHz band comes from sparsely located military radars and sparsely located satellite uplinks, whereas 925 MHz DSRC suffers from considerable interference. The 902-928 MHz band is full of traffic. Other devices that occupy the band are 900 MHz phones, rail car AEI readers, and wind profile radars. Table 1 contains a comparison between 925 MHz DSRC and 5.9 GHz DSRC.

Table 1.1 Comparison of DSRC Technologies

	902 – 928 MHz band	5850 – 5925 MHz
Spectrum	12MHz	75MHz
Data Rate	0.5Mbps	6Mbps -27Mbps
Interference potential	High	Low
Coverage	One communication zone	Overlapping Communication Zone
Maximum Range	300ft	1000 m
Minimum Separation	1500ft	50ft
Channel Capacity	1 to 2 channels	7 channels
Downlink Power	Nominally less than 40dBm	Nominally less than 33dBm
Uplink Power	Nominally less than 6dBm	Nominally less than 33dBm

Large arrays of applications are being developed for DSRC. The applications of DSRC are categorized into the following four classes.

- Vehicle-to-Vehicle applications transmit messages from one vehicle to another.
- Vehicle-to/from-Infrastructure applications in which messages are sent either to or from vehicle to a Road Side Unit (RSU).
- Vehicle-to-Home is a class of application that is used when a vehicle is parked at the driver’s residence, for purposes such as transferring data to the vehicle.
- Routing Based applications are used when the intended recipient is greater than one-hop away.

Based on these four application classes, the DSRC applications can be further categorized as safety and non-safety applications. Furthermore, the application messages of DSRC applications may be either event driven or periodic. The event driven messages are sent when a certain event occurs. For instance, when a vehicle is involved in a collision it will generate a message to warn other vehicles that an accident has occurred. On the other hand, periodic messages are repeatedly transmitted at a specific interval, such as a vehicle announcing its state or a RSU broadcasting the status of a traffic light. This forms the basis of the type of applications that are possible in a VANET.

DSRC supports a number of different network protocols for interoperability in the hope of gaining widespread adoption. To begin, DSRC supports the long-established TCP/IP protocol, which allows IP based routing in DSRC. As a result of supporting TCP/IP, most of the traditional Internet applications are available in the VANET. Next, WAVE Short Message Application is used for the majority of vehicle-to-vehicle safety communications. The reason that IPv6 is not used for many of the safety applications is because of the size associated with IPv6 headers. The IPv6 headers are a minimum of 40 bytes which is close to the size of a typical safety message. The average size of a safety message is approximately 100 bytes. To increase the overall performance of the network and allow more vehicles access to the network, the requirement of using the IPv6 protocol was removed in favor of the WAVE Short Message Application protocol. There is also the C2CCC - Car 2 Car Communication Consortium protocol that is being developed for VANETs in Europe.

The DSRC standard is still a work in progress. Many of the final details of DSRC are unknown at the present time. As the standardization process continues, new features are sure to be added and some of the original features of the proposal may be removed.

1.4.2 Evaluated Wireless Technologies for DSRC

A number of wireless solutions were evaluated for use as the primary communication medium for DSRC. A requirement of the wireless technology is, its latency must be 100 ms or less, offer high throughput, and have communication range of 100 m to 1000 m. In addition, the wireless technology must support a number of diverse communication schemes. First, the wireless technology should support both one-way communication allowing a vehicle to send a broadcast message and two-way communication allowing two vehicles to establish a dialog with each other. Second, the technology must also support both point-to-point communications where a message is intended for a specific location and point to multipoint communication where a message is intended for multiple receivers. Third, one-way or two-way communication may be either point-to-point or point-to-multipoint.

The wireless technologies were evaluated based upon how well they meet the requirements of DSRC. In the end, a modified version of 802.11a was chosen as the primary means of communication for DSRC. A number of the other evaluated technologies were found unacceptable for one reason or another. For instance, both cellular systems and satellite systems offer a significant amount of bandwidth but have too high of latency to be considered useful for some applications of DSRC. A further drawback of cellular technology is its lack of broadcast support. Furthermore, the cost of the wireless technology must be low. At the present time both cellular and satellite technologies are expensive. In comparison, the cost of wireless access for DSRC is free because the technology is based on ad hoc networks. Also, infrastructure costs of DSRC are much cheaper than both cellular and satellite.

1.4.3 Complementary Technologies

A number of additional technologies will be used in DSRC, as a complement to 802.11a. To begin, a digital map is required by each vehicle in the VANET. A digital map enables the application of an enhanced vehicle navigational system. Another use of a digital map is for location-based routing. A major challenge of DSRC is the dissemination of new maps, such as when traveling to a city never visited before or dissemination of an updated map when a road is altered. A further requirement of DSRC is that all vehicles must be able to determine their location. Global Positioning Systems (GPS) provides a great solution to the problem of determining a vehicle's location. The main drawback of GPS is the location can only be determined when there is a clear path to the satellite, which means that GPS will not work in all situations (such as when vehicle pass through a tunnel). Next, sensors are used to provide additional input to the system. Both vehicles and RSUs (i.e., RSU are stationary devices that are mounted road side that function similar to access point) are equipped with sensors that monitor the local conditions. To illustrate, sensors placed along the roadway can detect conditions such as ice on the road so that drivers are able to alter their driving. A RSU receives input from the sensor that ice is on the road and then transmits this information to the vehicles in the location. Finally, another technology that is sure to be initially included in DSRC is radar because not all vehicles in the future are likely to be DSRC enabled. A radar device is added to a RSU so that it is able to detect vehicles lacking a DSRC transceiver. The RSU can then relay location information about a non-DSRC equipped vehicle to the other vehicles in the VANET. Although the 802.11a protocol is the core component of the system, a number of complementary technologies will also find their way into DSRC.

1.4.4 Vehicle-to-Vehicle versus Vehicle-to/from-Infrastructure

Two types of DSRC devices are used for communication in the VANET: an On-Board Unit (OBU) and a Road-Side Unit (RSU). First, each vehicle is equipped with an OBU which is a transceiver mounted within a vehicle along with a computational device. Each vehicle also has an Omni-directional antenna that the OBU uses to access the wireless channel. Furthermore, each vehicle has sensors to provide input to the OBU. The sensors record the local conditions of the vehicle. Second, RSU are stationary devices that are mounted road side. The RSU is similar to an OBU in that it has a transceiver, antenna, processor, and sensors. The RSU are strategically placed along the road in order to provide services to vehicles. For instance, a RSU may be placed near an intersection to improve the flow of traffic through that intersection and reduce accidents. Also, a commercial entity can deploy a RSU to provide value-added services to their customers. As an illustration, a gas station can use a RSU to collect electronic payments from their customers. The RSU may use either a directional antenna or an Omni-directional antenna depending on the type of application provided by the RSU.

A directional antenna is beneficial when the signal only needs to propagate in a specific direction. For example, a distribution company could use a RSU for access control at the gate of a warehouse. In doing so, only pre-approved vehicles would be allowed through the gate. Since the transmission is to a specific location, in this case the gate, a directional antenna is used. To conclude, a VANET is composed of OBUs and RSUs. Vehicular ad hoc networks are not pure ad hoc networks. An infrastructure of RSU will exist, which allows the VANET access an external network such as the Internet. Also, a RSU can communicate with another RSU through a wired infrastructure, making the communication between RSUs more reliable. To conclude, each RSU will require a license to operate the unit at a specific location and a specific frequency. The FCC requires a license for each RSU to maintain the integrity of the network and so that the services provided by commercial entities does not detract from the primary purpose of the network, thus ensuring safety. If the FCC did not regulate the spectrum, applications (such as multimedia services) would hinder the safety applications.

1.4.5 Intelligent Vehicle Applications Enabled by DSRC

A number of unique applications are being standardized for DSRC and similar projects worldwide. The goal of the standardization is to create a common set of application protocols. While there will be a common set of application protocol, the automobile manufacturers will be able to differentiate their products based on the user interface they provide to the driver. For instance, a simple user interface may only give the driver audio feedback. On the contrary, a more advanced user interface may provide the driver with a touch screen mounted within the dashboard, allowing the driver a visual display of the road. To conclude, each vehicle has an OBU that follows the DSRC specification, but each automobile manufacturer is able to interface the OBU with a proprietary user interface.

DSRC is composed of public safety and non-public safety applications. First, the objective of the public safety applications is the improvement of the overall safety of the transportation infrastructure. Second, the non-public safety applications increase the comfort of the driver by adding value-added services. Public safety applications are always given priority over the non-public safety applications.

1.4.6 Applications of DSRC

There are largely two classifications of applications: Public Safety Applications and Non-Public Safety applications.

Public Safety Applications

The public safety applications protect the safety of life, health, or property. The public safety services of DSRC are provided by either a governmental agency or a non-governmental organization under the authorization of a governmental agency. The Vehicle Safety Communication (VSC) project determined 34 possible safety applications for DSRC. These applications were analyzed to determine the potential safety benefit provided by the application.

The application analysis was based on the saving in terms of years saved from life lost, for both fatal and non-fatal accidents. Next, the applications were rated in terms of the estimated time before the application is commercially deployable. Near-term applications are deployable between 2007 and 2011. Mid-term applications are deployable between 2012 and 2016. Long-term applications are deployable beyond 2016. Furthermore, the applications were rated on their effectiveness in preventing accidents. Last, the applications were rated on their capability to operate based on the market penetration of DSRC enabled vehicles.

The VSC project team used this criterion to determine the safety benefit of the applications. **Traffic signal violation warning application** provides the greatest benefit in estimated functional life years saved by the applications that could be implemented in the short-term. Passing through an intersection is one of the most dangerous activities that one encounters while driving. The goal of this application is to reduce collisions at intersections. In this scenario, a RSU is placed near an intersection that has a traffic light. Infrastructure-to-vehicle communication is used to warn approaching vehicles of the status of the traffic light and to alert drivers of a potential light violation. The data sent to approaching vehicles includes the status of the light, the time of light changes, the traffic light location, and the direction of the light signals. When a vehicle receives a traffic signal violation warning message, computation is performed on the received data to determine if the driver is at risk of inappropriately entering the intersection and if so a warning is issued to the driver. The traffic signal violation warning is a simple one-way application that provides the greatest safety benefits of the VANET applications. More complex variations of this scenario are used for applications such as left-turn assistance and stop sign movement assistance.

Emergency electronic brake lights application is another short-term solution that provides a warning to a trailing vehicle when a vehicle in front of it applies its brakes. The emergency electronic brake light application is beneficial in situations where visibility is limited, such as poor weather conditions. The data contained in vehicle A's broadcast message is the deceleration rate and braking vehicle's location. When vehicle B receives the warning, an algorithm is invoked to determine the relevance of the message and whether or not the vehicle is endangered. If so, a warning is sent to the driver. The emergency electronic brake light application significantly reduces accidents by giving the driver a warning before they are able to visually sense the danger.

Curve speed warning application aids a driver as he approaches a winding stretch of road. Typically, a sign is posted on the side of the road to warn drivers to reduce their speed. The success that a driver has going through the curve is based solely upon his/her judgment. A curve warning system can tremendously improve the accuracy by guiding a driver through a curve using information such as the characteristics of the vehicle, the weather conditions, and the curves geometry. A RSU is placed at a potentially dangerous curve. Furthermore, the RSU can improve safety by using sensors to estimate the condition of the road. The RSU unit then periodically broadcasts warnings of the condition of the road through the curve.

When a vehicle receives the broadcast from the RSU, the information is then processed by the OBU. If the vehicle's velocity exceeds a safe speed of travel, a warning is issued to the driver. **Lane change warning is an application** that is expected to be implemented in the mid-term and assist a driver while changing lanes.

The lane change warning application is a vehicle-to vehicle application. Each vehicle receives periodic broadcast from the surrounding vehicles. Also, each vehicle maintains a table containing the vehicles in the immediate proximity. For this application to be successful, the vehicle locations maintained in the table must be very precise. When the driver signals his or her intent to change a lane, the OBU uses the received data to determine if the road conditions are safe to perform a lane change. One means triggering the application is when the turn signal is applied by the driver, which then invokes the lane change algorithm. If the attempted lane change puts the driver in danger, a warning is generated. The main drawback of the lane change warning application is that it requires that a high percentage of vehicles are DSRC equipped.

These are just a few examples of the safety applications that are possible in a VANET. The actual implementations of these applications may change over time. For example, more complex and accurate implementations of the traffic signal violation warning are possible. Also, the sizes of the application packets are typically small (between 100 and 500 bytes). The size of the application packets presents little problem in the realization of these applications. On the contrary, one of the initial barriers in implementing many of the DSRC applications is the low initial penetration rate of vehicles that are DSRC enabled. To conclude, as time passes and more vehicles become DSRC equipped, more DSRC applications will be implemented.

Non-Public Safety Application

The primary focus of DSRC is for the creation of safety applications, but a number of additional non- public safety applications have been proposed. The non-public safety services require licenses to provide the DSRC-based services. The FCC requires a license for service providers in an effort to eliminate services that would be detrimental to the VANET. Non-public safety applications increase the overall comfort of the driver. Electronic toll collection is one possible non-safety application. Instead of a driver having to stop at a toll booth to make a payment, the payment is made electronically through the network. Also, a number of entertainment features have been proposed for vehicular networks, such as the transferring of music and video files for in-car entertainment. Applications such as these will probably not be implemented in DSRC in the foreseeable future because of the limited bandwidth and the fundamental focus on safety applications.

The in-car entertainment application would consume a large amount of network resources. Although the organizations are approved to begin work on multi-media applications as long as they do not constrain the safety application or require any modifications to the safety protocol. Another possible application is instant messaging which enables the driver to send a message to another vehicle. The sent message could be either predefined or custom. In addition, enhanced route guidance and navigation enables a driver to make decisions on the path of travel, based upon the received information. In this application, a RSU transmits up to-date navigational information to the vehicles. Some of the possible information that is transmitted is construction advisories, road closings, detours, and parking restrictions. Finally, point-of-interest notifications are transmitted from the RSU containing information regarding places of interest in the area. Some of the possible data exchanged is the location of gas stations, restaurants, and lodging. For example, a RSU might broadcast the location of the gas stations in the area along with the prices of gas. These are some of the non-safety applications that are possible in a VANET. It is expected that commercial organizations will find numerous other uses for DSRC and the greatest innovation of DSRC will come from the non-safety applications.

1.5 PHYSICAL LAYER

The physical layer is the basic layer for communication and it is responsible for transmitting the raw bits on to wireless channel. First, the channel assignment of DSRC is described. Next, the control channel access is discussed along with the problem of coordinating the access of multiple channels in a vehicular network.

1.5.1 Channel Assignment

The FCC allocated 75 MHz of the radio spectrum for DSRC. The 5.9 GHZ DSRC spectrum is composed of six service channels which are each 10 MHz Also, one control channel is provided by the DSRC standard, which is also 10 MHz As stated earlier, the FCC recommends no unlicensed use of DSRC band. The data rates possible for a 10 MHz channels are 6, 9, 12, 18, 24, and 27 Mbps with a preamble of 3 Mb/s. The modulation scheme used by DSRC is Orthogonal Frequency Division Multiplexing (OFDM). Also, the subcarrier frequency spacing of 802.11a is double that of DSRC. In addition, DSRC doubles the guard period in comparison to 802.11a. The following list contains the channels of DSRC and the type of applications that are supported by the channel.

- Channel 172 is reserved for medium power safety applications.
- Channel 174 is reserved for medium power applications that are shared by all.
- Channel 175 is a combination of channels 174 and 176.
- Channel 176 is reserved for medium power applications that are shared by all.
- Channel 178 is the control channel it support all power levels, safety application broadcasts, service announcements, and vehicle-to-vehicle broadcasts messages.
- Channel 180 is reserved for low power configurations and provides little interference when units are separated by 50 ft or more.
- Channel 181 is a combination of channels 180 and 182.

- Channel 182 is reserved for low power configurations and provides little interference when units are separated by 50 ft or more.
- Channel 184 is reserved for a high power service channel that is used to coordinate intersection applications.

The current wireless technology is only able to listen to one channel at a time. In the initial deployment of DSRC, each vehicle will have a single transceiver. The drawback of having a single transceiver is that only one channel at a time is able to be monitored. To overcome this problem, it is possible to equip either an OBU or RSU with multiple transceivers allowing them access to multiple channels simultaneously. To illustrate, if an OBU is equipped with two transceivers, one transceiver can monitor the control channel while communication is underway on a service channel. The drawback of having multiple radios is it increases the complexity and the cost. For the initial roll out of DSRC, it is envisioned that vehicles will have only a single transceiver. As a result of only being able to listen to single channel at time is channel coordination is needed.

1.5.2 Control Channel Access

Channel 178 is reserved for the control channel. The control channel is the most important channel of DSRC, and the efficient use of this channel is critical. Each OBU monitors the control channel for both broadcast safety messages and brief service channel announcements. The control is monitored by each vehicle and RSU. Since there is a limited amount of bandwidth available, communication on the control channel is brief. The FCC recommends that the control channel is used for messages that take less than 200μs to transmit. If the communication last longer than 200μs, another channel must be used.

Vehicles must periodically switch to the control channel to receive safety messages. A requirement of DSRC is that all vehicles must switch to the control channel every 100 ms and remain on the channel for a minimum amount of time. The purpose of vehicle switching to the control channel every 100 ms is to allow the reception of the safety broadcast from the surrounding vehicles. To guarantee that safety messages are not sent before the vehicles switch to the control channel, the time that the vehicles switch to the channel must be synchronized. One possible way to synchronize the control channel access is with the time received from a GPS unit. There are a number of proposals for the DSRC standard as to how to best implement synchronization with GPS for control channel access.

The control channel is also used for service announcements. When a service discovered is of interest to the OBU, it will switch from the control channel to the service channel to use the service. For instance, a RSU may provide the service of a map update. An updated map is then transferred to a vehicle. The OBU of a vehicle will discover the map update and switch to a service channel to begin the transfer of the new digital map. If the transfer takes too long to complete, the vehicle must switch to the control channel to receive safety messages and then switch back to the service channel to resume the file transfer. The control channel coordination allows a vehicle to correctly receive safety messages and also use the available services in the network.

1.5.3 Priority Issues in DSRC

The wireless transmission is made reliable with the introduction of an explicit acknowledgment mechanism. The intended receiver of a frame transmits an acknowledgment (ACK) which alerts the sender that the frame has been successfully received. If an ACK is not received by the sender of a frame, it is assumed that the frame was not successfully received, and another attempt is made to transmit the frame.

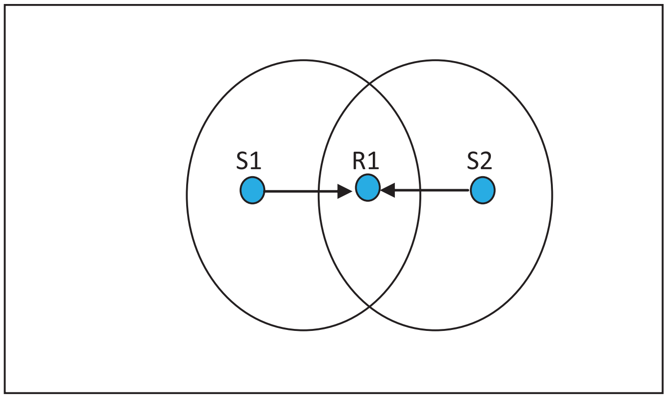

Figure 1.9 Hidden terminal problems

One of the main problems affecting the reliability of the Distributed Coordination Function (DCF) is known as the hidden terminal problem. The hidden terminal problem is the main cause of collisions in a wireless network. The hidden terminal problem occurs when there are two nodes that are outside the transmission range of each other but each transmits to a node that is shared between them. In Figure 1.9 above, nodes S1 and S2 cannot sense each other's transmissions. Therefore, the medium appears free to both S1 and S2. If both S1 and S2 were to transmit to R1 at the same time, a collision would occur at R1 and neither of the frames would be successfully received.

The hidden terminal problem is addressed by 802.11 with an optional Request-To-Send/ Clear-To-Send (RTS/CTS) exchange before any data is transferred. When node S1 has data to send, once it is able to gain access to the medium (e.g., after the nodes back-off timer expires), node S1 first transmits a RTS to the intended receiver R1. When R1 receives the RTS after a Short Inter-Frame Spacing (SIFS) has expired, node R1 will respond with CTS. When the CTS message is received at S1 it will signal to node R1 that S1 is ready to send a data frame. The hidden node problem is mostly eliminated, when S2 overhears the CTS transmitted from R1 it then sets the network allocation vector (NAV) for the amount of time it takes to complete the communication. Node S2 will then defer from accessing the wireless medium until the NAV expires and the transmission between S1 and R1 is complete. When S2 overhears the ACK sent from R1 it knows the transmission is complete. After the DCF Inter-Frame Spacing (DIFS) has elapsed nodes in the network can then begin to contend for access to the channel.

1.6 APPLICATIONS

VANET offers several benefits to organizations of any size. While such a network does pose certain safety concerns (for example, one cannot safely type an email while driving), this does not limit VANET's potential as a productivity tool. GPS and navigation systems can benefit, as they can be integrated with traffic reports to provide the fastest route to work. A computer can turn a traffic jam into a productive work time by having his email downloaded and read to him by the on-board computer, or if traffic slows to a halt, read it himself. It would also allow for free, VoIP services such as Google Talk or Skype between employees, lowering telecommunications costs [51] .

1.7 MOTIVATION FOR RESEARCH

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. Pervasive Network is one solution that is known for the capability of the nodes to arrange them autonomously in the network environment and exchange information on-the-move. All types of Ad hoc networks come under Pervasive Networks. In this dynamically changing environment, security while routing information is always a concern and it is quite challenging to provide security to the mobile nodes. Owing to the security demand present in the current world, this research work aims at providing suitable and efficient solutions to enhance both routing and security in the Pervasive Networks.

1.8 OBJECTIVES OF RESEARCH

- To analyze the VANET architecture, issues and challenges involved with routing in VANETs and to analyze the existing solutions to overcome such issues.
- To propose a Believer Based Protected and Efficient Routing (BBPER) protocol in Pervasive Networks to provide better security than existing multipath routing protocols.
- To design a Dynamic Endorsement Scheme (DES) that can be efficiently used to monitor and improve the authentication in VANETs
- To increase the reliability in the VANET with the reduction of number of retransmission of the data using a novel Recognition Based Data Dissemination Protocol (RBDP).

1.9 SCOPE OF RESEARCH

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. The security providing protocols find their scope in the current VANET applications to keep away from malicious activities from disrupting the performance of the network. Speed control, accident prevention, vehicle tracking and police patrolling, etc are some of the main application areas for the protocols proposed in this thesis. The scope of this research work not only pertains to the vehicular technologies but can be amended for applications in other network technologies like Mobile Ad hoc networks and Mobile Wireless Sensor Networks, etc, where mobility is present and security is a requirement.

1.10 ORGANIZATION OF THE THESIS

A brief outline of the various chapters of the thesis is summarized below.

Chapter 1: Provides a brief introduction to the Vehicular Ad hoc networks, their topology and architecture, challenges related to the design of VANETs, their advantages and applications. The main focus of this chapter is to discuss the security issues related to the communication operations in VANETs.

Chapter 2: Deals with review of literature survey about the communication protocols designed for and used in VANETs. The progresses of the protocol development that efficiently facilitate communication in VANETs are discussed in this chapter.

Chapter 3: Provides the methodology of design and analysis of the various protocols and schemes brought forth by this thesis along with an overall conceptual framework.

Chapter 4: Design of Believer Based Protected and Efficient Routing (BBPER) protocol in Pervasive Networks to provide better security than existing multipath routing protocols is presented in this chapter.

Chapter 5: Analysis and design of Dynamic Endorsement Scheme (DES) that can be efficiently used to monitor and improve the authentication in VANETs is presented in this chapter.

Chapter 6: Discussion about the design of Recognition Based Data Dissemination Protocol (RBDP) to perform efficient broadcasting is provided in this chapter.

Chapter 7: Results and discussion of each technique proposed by this research work are analyzed in a comparative manner in this chapter to figure out the best protocol of all for the operation of VANETs

Chapter 8: Concludes the overall work which has been done. It provides highlights on thesis work and suggestions for future work.