CHAPTER 1

INTRODUCTION

1.1 PREAMBLE

A Vehicular Adhoc Network (VANET) is a decentralized type of wireless network which does not rely on a pre-existing infrastructure. These networks are suitable for a wide range of applications that relate to vehicular communication to avoid roadside accidents and traffic congestion. In Vehicular Ad Hoc Networks, moving vehicles acts as the nodes of the network. This research based on VANET, which propose a new method to address the security issues by implementing the advanced registration of Mobile Nodes (MN) before the handover process that consequently reduces the traffic congestion and overcome the signal interruption due to mobility, by providing a temporary or guard node to replace the lost node and to provide the seamless connectivity.

This research focuses on reducing the packet loss ratio, delay that occurs during handover on providing seamless connectivity between homogeneous and heterogeneous network. The new method uses the predictive policy with Access Prediction Network (APN) to reduce the Packet loss ratio and handover delay by predicting the future handover. In addition to that, safety transmissions of Binded Update (BU) data are estimated using asymmetric cryptography to efficiently manage the handover mechanism in multihoming network environment. The results of the proposed method are optimized to maintain a balanced value of the threshold by the network to avoid delay and data loss.
1.2 VEHICULAR NETWORKS

Researchers of National Institute of Standards and Technology (NIST) demonstrated an ad hoc network prototype for reporting the disaster of building fires and mines collapse in August 2008. Unmanned vehicles with autonomic operation can be sent to dangerous regions that cannot be faced directly by human community to report the observations as command to the control centers. This thesis focuses on Vehicular Ad Hoc Networks (VANETs) in which the mobile nodes are being replaced by vehicles (Raya & Hubaux, 2005; Harsch et al. 2007; Zeadally et al. 2010).

In recent years, the technical advancement of the car manufacturers such as Ford, GM, and BMW had made them introduce their new vehicles equipped with GPS receivers and navigation systems to include significant computing power inside their cars. This technology allows the vehicle to communicate with other vehicles in addition to the road side stations. Road side stations are sited in vital section of the road like traffic signals. The communication device is also known as On Board Units (OBU). VANET allows communication with other vehicles of the network, base stations. The base stations are connected to backbone network so that the other application and services can be provided to the vehicles.

The Federal Communication Commission (FCC) allocated a bandwidth of 75MHz around the 5.9GHz band for vehicle to vehicles and vehicles to roadside infrastructure communications through the Dedicated Short Range Communications (DSRC) services (Olario & Weigle, 2009; Moustafa & Zhang, 2009).

Kashif Naseer Qureshi & Abdul Hanan Abdullah (2013), discussed the emergence of vehicular networks that enabled several useful Intelligent
Transport Service (ITS) applications, both safety and non-safety applications such as automatic road traffic alerts dissemination, dynamic route planning, service queries (e.g., parking availability), audio/video filesharing during mobility and context-aware advertisement.

1.2.1 Communications in Vehicular Networks

The communication between vehicles and the infrastructure is classified based on three types of domains namely In-vehicle domain, Ad hoc domain, Infrastructural domain (Saif-Al-Sultan et al. 2013). Faezipour et al. (2012), categorized the types of communication in VANET into intravehicle communication, Vehicle to Vehicle communication (V2V), Vehicle to roadside Infrastructure communication (V2I), vehicle to broadband cloud communication as shown in Figure 1.1.

![Figure 1.1 Communications in Vehicular Environment](Source: Faezipour et al. 2012)

**Vehicle to Roadside Infrastructure Communications**

This method of communication is based on the roadside infrastructure. Vehicles connect to other vehicles or to the Internet via roadside access points positioned along the roads. The access points can be
either installed specifically for providing Internet access to vehicles or may be a open 802.11 (WiFi) access points along city streets. This method helps the vehicles to connect to the Internet using high data rates of 11Mbps than through the cellular network. Access points installation cost along the roads to obtain reasonable coverage is found to be the major drawbacks (Olario & Weigle, 2009; Faezipour et al. 2012; Saif-Al-Sultan et al. 2013).

**Vehicle-to-Vehicle Communications**

Internet-based communications to and from vehicles will be based on the method of choice used for communications. However, the Wi-Fi-ready vehicles open the way for adhoc networks of moving vehicles. The advantage is the availability of distinct, high bandwidth network to the existing infrastructure network and the drawback is the need for new set of protocols that are able to satisfy the throughput and delay requirements of applications (Olario & Weigle, 2009; Faezipour et al. 2012; Saif-Al-Sultan et al. 2013).

1.3 **VEHICULAR ISSUE AND CHALLENGES**

Vehicular challenges are broadly classified into broad categories namely Technical challenges, Security Challenges, Routing Challenges, Socio-Economic challenges (Chen et al. 2011; Hartenstein & Laberteaux, 2008; Lin et al. 2010; Saif-Al-Sultan et al. 2013).

1.3.1 **Technical Issues**

The characteristics of VANETs also provide a vital role in forwarding the packets. The forwarding challenges that were identified during the packet transmission are next hop selection, queuing disciplines, and paths durations. DSR/GPSR protocols maintain lists of neighbours, to determine the next hop. Maintaining updated lists requires frequent “hello” packet
broadcasting between the nodes of the network. But too much of broadcasting also leads to overhead. Thus, to use accurate node positions in the selection of the next hop without incurring too much overhead acts as a main challenge in vehicular networks.

The occurrence of high mobility in a network changes the network topology and channel condition quickly thus, does not support tree structure. The traffic load is found to be low in rural areas and high in urban resulting in unbounded network size, these are the challenges related to communication. During the rush hour, the traffic load is high, which leads to frequent network partitions.

1.3.2 Routing Issues

Due to the high mobility of active nodes and topology changes, designing an efficient routing protocol which would deliver the data within the specific time period with few drop in packets are the primary challenge in any VANET environment. According to Chen et al. (2011), designing a routing protocol suits the environment with a high density of vehicles with close distances between them and has an impact on improving many factors like packet delivery ratio, scalability and reliability.

1.3.3 Security Issues

Among all the challenges of the VANET, security has got less attention so far. VANET packets may contain life critical information hence it is necessary to make sure that these packets are not attacked by the intruder; likewise the liability of drivers is established by informing them the traffic environment correctly at specified time (Hartenstein & Laberteaux, 2008; Mostofa Kamal Nasir et al. 2013). The size of network, mobility, geographic relevancy, makes the implementation difficult and distinct from other security
problems encountered in a general communication network. In Vehicular Networks, the time factor is a critical one, as, the message should be delivered with the maximum of 100ms (Ram Shringar Raw et al. 2013). So in order to achieve this constraint in real scenario, the fast cryptographic algorithm should be used and at the same time, the message and entity authentication also should be carried out in time (Khairi et al. 2015).

The security issues also make a big impact for the researcher to take it for consideration. Therefore, security issue is considered in this work among other issues for enhancement. The Figure 1.2 presents the security challenges and security requirements faced by the VANET environment.

![Security issues in VANET](image)

**Figure 1.2 Security issues in VANET**

- Data Consistency Liability - In VANET, even authenticate node can perform malicious activities in certain situations which may lead to accidents or may disturb the network. This inconsistency
has to be avoided by initiating the correlation among the received data from different node on particular information.

- Low tolerance for error - Some protocols are designed on the basis of probability. The message transfer has to be done in short duration and so a small error in probabilistic algorithm may cause malfunction in the network.

- Key Distribution - All the security mechanisms implemented in VANET are dependent on the keys generated. Each message is encrypted and needed to be decrypted at receiver end, either with the same key or different key. Also in a public key infrastructure trust on CoA become a major issue.

- High Mobility – Though the computational capability and energy supply in VANET is same as the wired network, the high mobility of VANET requires the less execution time of security protocols to achieve the same throughput of the wired network. Hence the design of security protocols must use certain approaches that reduce the execution time.

- Low complexity security algorithms - Current security protocols such as SSL/TLS, DTLS, WTLS, generally uses RSA based public key cryptography. RSA algorithm uses the integer factorization on large prime number which is NP-Hard. So the decryption of the message that uses RSA algorithm becomes very complex and time consuming. Hence there is a need to implement alternate cryptographic algorithm like Elliptic Curve Cryptosystems and for bulk data encryption, AES can be used.
• Transport protocol choice - To secure transaction over IP, DTLS should be preferred over TLS as it operates over connectionless transport layer. The IPSec which secures IP traffic should be avoided as it requires too many messages to set up. However IPSec and TLS are used when vehicles are not in motion.

1.3.4 Security Requirements

The following security requirements have to be satisfied before they are deployed.

• No confidentiality - The issue of data secrecy or confidentiality is a concern in this network environment

• No key distribution - Most mobile network security architecture includes provisions for key distribution. This is not the only case when an encrypted channel is set up; it also requires sharing of key for authentication and data integrity reasons. Key distribution is unnecessary for two reasons namely no bulk data is transmitted (on a continuous basis) either among cars or between cars and roadside infrastructure and vehicles traveling at high speeds (as most do on highways) will likely spend little time within a cell of a given base station. Also, vehicles communicating in an ad hoc network broadcast their data, hence, pair-wise (or group-wise) key distribution is not needed.

• No handover - The notable security features of mobile networks are the secure hand-over protocol e.g., as a node moves from one cell to another, its state (including any on-going connection data) is handed over from one base station to the next. However,
explicit handover is not needed (Ram Shringar Raw et al. 2013; Wasnik et al. 2013)

- No battery power concern - This is actually the most important distinguishing factor of the network environment. Practically in all mobile networks, CPU power consumption is a paramount concern. This includes not only power utilized for reception and transmission but also the power necessary to perform cryptographic operations on weak and battery challenged computing devices such as packet radios or cell phones. In our case, power consumption is not relevant since a running vehicle provides an ample source of battery power.

- No CPU speed issues-In many mobile networks, the related concern are the processors with low speed of the mobile node. Hence, there is usually a goal to minimize the use of cryptography because of the relatively long delay.

- Extreme time sensitivity-All data transmitted over network is time sensitive. Time synchronization is also extremely important. Moreover, the system must be in tolerant of replays (hostile and otherwise).

Among the various security requirement and challenges, high mobility and handover is taken for consideration in this work because it is the root causes of others issues in any networks.

1.4 HANDOVER

The problem of seamless connectivity becomes even more challenging as vehicles move across overlapping heterogeneous wireless environment (Muhammad et al. 2012). In such cases, frequent switching from
serving network to a target network may occur, which degrade the network performance. When Mobility Management (MM) is classified by layer concept, mobility can be divided into two parts:

- **Horizontal mobility**: Mobility on the same layer. Generally referred as the mobility within the same access technologies.

- **Vertical mobility**: Mobility between different layers. Generally referred as the mobility between different accesses technologies.

Handover is a process in which a mobile node maintains its node’s connection to be in active sessions, even if the access point of the mobile node changes. This access point is called as Point of Attachment (PoA). One of the major requirements for MM in the Next Generation Networks is to support the mobility across the heterogeneous access networks. The next generation a network is composed with the characteristics of heterogeneous access networks which makes a big distinction between horizontal handover and vertical handover;

- **Horizontal handover**: Handover within same access networks which is generally referred to as the Intra-AN handover.

- **Vertical handover**: Handover across heterogeneous access networks which is generally referred to as the Inter-AN handover.

### 1.4.1 Horizontal Handover

The main concern of horizontal handover is to maintain the on-going services, although there may be a change of IP address due to the movement of a mobile node. Maintaining on-going service is done by
thrashing the change of IP address (e.g., Mobile IP) or updating the changed IP address dynamically (e.g., mSCTP).

To hide the change of IP address during the movement of a mobile node, Mobile IP maintains two types of IP address; one permanent IP address (Home address) might be used above transport layer and one changeable IP address (Care-of address) might be used under transport layer. The majority of handover mechanism includes horizontal handover because they focus on maintaining the on-going services without any interruption even though the IP address is changed.

1.4.2 Vertical Handover

Wireless networks adopt a heterogeneous broadband technology model to guarantee seamless connectivity in mobile communications. A Vertical Handover is a process which preserves users’ connectivity on-the-move and following changes of network. Vertical Handover schemes can be classified on the basis of the criteria and parameters adopted for initiating a handover from the serving network to the target network.

Xiaohuan Yan et al. (2010), has surveyed the various vertical handover decision algorithms that can be used in the heterogeneous environment. Vertical handover happens when a mobile node moves across heterogeneous access networks. It differs from the horizontal handover both in the access technology as well as the IP address usage, because the mobile nodes moves across different access network using different access technology. The main concern of vertical handover is to maintain on-going services by concerning the change of IP addresses, the change of network interfaces, QoS characteristics etc (Zhu et al. 2011).
Vertical Handover Parameters

The decision for vertical handoff is estimated based on the parameters like Bandwidth, Received Signal Strength (RSS), Signal to Inference Ratio (SIR), cost, latency, security, velocity, battery power, user preferences, service capacities and Quality of Service (QoS). During each handover, these parameters have to be monitored to decide the handoff.

Received Signal Strength (RSS)

RSS is the most widely used criterion because it is easy to measure and is directly related to the service quality. Majority of existing horizontal handover algorithms use RSS as the main decision criterion, but it is not enough for a complete decision. RSS represents the strength of the signal received; the Vertical Handoff is feasible i.e. the handover occurs if and only if the RSS of the BS or Access Point (AP) falls above the threshold level.

Available Bandwidth

Bandwidth is a measure of the width of a range of frequencies. It refers to the data rate supported by a network connection or interface. It measures the amount of data transferred over a specific connection in a given amount of time. In order to provide seamless handoff, there is a need to manage bandwidth of mobile node during movement. Higher offered bandwidth ensures lower call dropping and call blocking probabilities, thus providing higher throughput.

Network Throughput

Network throughput refers to the average data rate of successful data or message delivery over a specific communication links. As network throughput is considered in dynamic metrics for making decision of Vertical
Handover, which is one of the important requirement to be considered for the Vertical Handover.

**Network Load**

Network load is to be considered during effective handoff. It is important to balance the network load to avoid drop in quality of services. Variation in the traffic load among cells will reduce the traffic carrying capacity. To provide a high quality communication service for mobile nodes and to enhance the high traffic attention has to be paid to the network load when there is a variation in traffic.

**User Preferences**

The user preferences refer to the user preferred networks, application requirements (real time, non-real time), service types, QoS have to be considered as a major factor during handover in next generation wireless networks.

**Cost**

The cost has to be minimized during Vertical Handover in wireless networks. The call arrival rates and handoff call arrival rates are analyzed using the cost function.

**Speed**

In vertical handoff algorithms, the speed at which the mobile terminal moves plays a vital role in creating decisions binding effect than the traditional horizontal handoff decision algorithms. When a user travels at high speed within a network coverage area it is not advised to initiate the vertical handoff process because after a short period of time, the user will have to go
back to the initial network because it would get out from under cover network host.

**Power Consumption**

The wireless devices running on battery need to limit the power consumption. If the battery level decreases, switching from a network to another network with low power consumption can provide a longer usage time. The power requirement becomes a critical issue especially if the handheld battery is low. In such situations, it is preferable to transfer to an attachment point to extend the battery life. The attachment to the closest AP or BS is known to consume the least power at a given instant. So if battery level is low, the MT must handoff to the closest AP or BS provided RSS is above the threshold level. The number of users also increases the congestion and in turn even the nearest AP or BS consumes more power.

In this work, Vertical Handover mechanism is used as effective handover mechanism that supports homogenous and heterogeneous network because optimal handover decision is achieved by estimating the various parameters and thus guarantees the seamless connectivity.

### 1.5 PROTOCOL IN VANET

The protocols of VANET are being classified based on the type of communication provided by the network structure. Though there are two types of communications available in VANET namely V2V and V2I, the protocols differ for each type (Marwa et al. 2013).
1.5.1 Vehicle to Vehicle communication Protocols

Cooperation among inter-vehicular networks and sensor networks placed within the vehicles or along the road need to be further analyzed (Li & Wang, 2007; Lin et al. 2010; Kayhan & Marwan, 2013). Figure 1.3 shows the different types of routing protocols used in VANET Environment.

![Figure 1.3 VANET Protocols](image)

1.5.2 Vehicle to Infrastructure Communication Protocols

Vehicles gather information and application with the help of road side infrastructure. Mobility Management scheme aims to reduce the control overhead and improve bandwidth utilization during Internet-to-VANET
multicasting communication (Younas & Awan, 2013). This research work focuses on two types of mobility management schemes namely

- Host-based mobility management
- Network-based mobility management

**Host-based mobility management**

In such Mobility Management Scheme, the Mobile Host/Mobile Node (MH/MN) which moves from one network to another involving signaling process which requires protocol stack modification and IP address change on the MN for to maintain the session continuity during handover. This signaling process includes movement detection, Router Solicitation Request (RtSolReq), Duplicate Address Detection (DAD) and Binding Updates (BUs) etc. Host Based Mobility Schemes have been used for different applications including real time services and associated protocols are Mobile IPv6 and Fast Handovers for MIPv6 (FMIPv6)(Ahmadi, 2012).

**Mobile IPv6**

Mobile IPv6 is a global mobility management protocol. MIPv6 has been proposed to support the network layer mobility. In NEMO, the mobile router is defined to extend the MN of MIPv6 by adding ability routing between its PoA and subnet which moves with the MR. MIPv6 are designed to handle the terminal mobility and that is not suitable for handling the NEMO. This protocol allows MN to maintain the connectivity to the Internet while moving from one network to another network. Each MN is identified using its Home Address. When connecting through a foreign network, the MN receives RA message. To obtain the information, Router Solicitation (RS) and Router Advertisement (RS) messages are exchanged between MR
and AR. Then, the MR creates NCoA and Duplicate Address Detection (DAD). If the CoA is usable, then the MN sends its location information to it’s HA to perform Binding Update (BU), which intercepts packets for the MN and tunnels them to the MN’s current location (Perkins et al. 2011).

**FMIPv6**

MIPv6 is improved as Fast Mobile IPv6 (FMIPv6) to support the Handover. One of the problems of NEMO BS in the context of ITS is that the packet loss and handover latency during the handover session which is inherited from MIPv6. This problem is more decisive in NEMO as MNNs in a network move at the same time. FMIPv6 reduces the packet loss by employing buffering and tunneling. But the tunneling approach may sustain packet loss during the handover. FMIPv6 is designed for a single MN, a tunnel between the PAR and NAR is established during the handover which is used for single MN (Ryu et al. 2014).

**Network-based mobility management**

Network Mobility (NEMO) protocol was introduced in 2005, for network mobility problems. As base station is not directly accessed by all users, as mobile host can only be accessed by using Mobile Routers (MR). Mobile routers have their own home address. When the MR moves to a foreign access router it requires Care of Address (CoA) from the visited network. When it receives its CoA it sends the updated message to it’s HA (Home Address). HA of the MR forward this message to all data packets. The network mobility solutions like NEMO leads to reduced handoff, scalability, reduced complexity (Shukla & Tyagi, 2013; Younas & Awan, 2013).
1.6 NETWORK MOBILITY

To maintain a vehicle’s Internet connectivity for a group of nodes that are moving together, Network Mobility Basic Support (NEMO BS) was developed by the Internet Engineering Task Force. NEMO BS is considered in ITS standards because it is a protocol that is able to provide network mobility.

Mobile IPv6 manages mobility for only one host, whereas the NEMO Basic Support (RFC 3963) manages mobility for a entire network. Such a network can be a PAN (Personal Area Network, a small network made of IPv6 sensors and PDAs), or any other access network deployed in cars. Running Mobile IPv6 on each node can be posh, especially for little devices such as sensors. NEMO Basic Support does not need any special feature rather it needs only a little bit changes on the router. Internet topology movements are handled by the router, which is known transparently to the hosts (Devarapalli et al. 2005; Soto et al. 2009).

The NEMO Basic Support Protocol has been standardized for IPv6 [RFC3963] but drafted for IPv4. Under NEMO, a Mobile Router (MR) acts as the MN in carrying out the mobility functions. Nodes that are attached to a MR are referred to as Mobile Network Nodes (MNNs), which are not aware of the network’s mobility and do not involve in implementing any mobility functions and it does not send and receive signaling messages during the handover session. MRs sends BU to their HAs. However, BU from MRs contains the Mobile Network Prefix (MNP). HAs bind entire network prefixes to the MR’s CoA and forward all packets for that network (prefix) to the MR. Figure 1.3 shows architecture of NEMO. This NEMO BS protocol helps used to maintain session continuity between the MNNs and the CNs, whereas the MR changes its point of attachment.
1.7 LITERATURE REVIEW

This section presents the background and related work literature in the handover domain in VANET, NEMO based handover, NEMO+ based handover, IPV6 protocol based handover and various handover techniques in VANET. This section concludes with the findings of the literature surveyed.

1.7.1 Various Handover Processes in VANET

Valery Naumov & Thomas Gross (2007), applied the position based routing method called Connectivity Aware Routing (CAR) and it was designed particularly for inter-vehicle communication in a city or highway environment. A discriminating property of CAR is the ability to not only establish positions of destinations but also find out paths connected between source and destination pairs. These paths are auto changed on the fly, not including a new discovery process. The Guards support to track the current position of a destination, although it is moving a substantial distance from its
initially known location and this protocol contains four parts such as the destination location, path discovery, data packet forwarding along the found path maintenance with the help of guards and error recovery. The connectivity aware protocol depends on PGB and AGF which give a scalable low overhead routing algorithm for inter-vehicle communication both in the city and on the highway and the CAR protocol is capable to locate destinations without using an idealized location service rather than relying completely on information of the road layout. The comparative evaluation of CAR with other routing methods demonstrates that the CAR protocol data delivery rate is improved. The path discovery phase is the main issues that have to be handled by constructing a smallest amount of infrastructure in the form of guards along a path from a source to a destination, allowing efficient communication between two moving nodes.

Meenakshi Saini & Sandeep Mann (2010) identified that while the vehicle is moving fast there may be the occurrence of frequent handoffs which may lead to packet loss and packet delay problem. The handoff procedure refers to the sequence of messages exchanged by access points and a mobile unit producing in a convey physical layer connectivity and state information from one access point to another access point with respect to the mobile unit in consideration. Based on the type of network technologies involved, the handover technique can be divided into two types horizontal or vertical. Mobile-assisted, network-controlled and mobile-controlled handover are all based on the entity and MS or access network that create the handover decisions.

Mohamed Alnas et al. (2010), application of improvement of fast mobile IPv6 handover depends on link layer information and also it present the performance calculations in terms of the packet loss and handover latency
applying evolution models. The link layer information and link layer trigger are used for improving the overall performance towards fast handover in Mobile IPv6. The Internet Engineering Task Force (IETF) which gives seamless handover operation in Mobile IPv6 networks that trigger the information from the MN is used to get a valid new care of address (nCoA) as it is still connected to the prior link, and then a bidirectional tunnel is created between the old Access Router and the new Access Router with the purpose of reducing packet loss during the handover process. The proposed analysis in this research was an improved fast handover method in Mobile IPv6 by using the link-layer information. In this method the performance was analyzed by simulating the proposed method in IST-CIMS NS-2 to acquire the fast Mobile IPv6 handover performance resulting in the name of handover latency and packet loss. FMIPv6 method also performs better on the handover latency and the packet loss, while the fast handover protocol is designed to reduce the packet loss and the latency during a handover process. Mobile IP and S-Mobile IPv6 protocol are observed the poor performance when the channel availability occurs. This method can reduce the handover latency and packet loss.

Chandavarkar & Ram Mohan Reddy (2011), used the Mobile IPv6 (MIPv6) for mobility management for packet switching using standardized wireless networks. This mobility management of heterogeneous networks not only anticipates network related parameters but also the location information, terminal-velocity, battery power, user-user profile & preferences and service capabilities of QoS etc. MIPv6 provides a lot of improvements, but it still has some disadvantages in organizing flawless and capable handover of mobile nodes at the network layer, that affects the overall performance, packet delay, signaling overhead and causing packet loss. Handoff classification based on the features like network type, number of connections, administrative
domains, frequencies engaged, necessity of handoff and user control are allowed in the handover process. Further, Handover management performance is determined through the parameters such as handover delay (latency), handover failure probability, number of handovers, and throughput.

Kaveh Shafiee et al. (2011) investigated the VHO strategies in a random inter-distance scenario with both Vehicle to infrastructure and Vehicle to Vehicle communication abilities. The combination of WLAN plus cellular plus ad hoc networking strategies are considered in this work in the name of transmission times and transmission costs. Performance based transfer to access technology, economical reasons and availability which manages the active connections is known as inter technology or Vertical Handoff (VHO). The distributed Vertical handoff decision-making algorithm is used to eliminate the need for organizing a data processing, decision making centre in the core network and the packet traffic among the centre and nodes. This optimal VHO decision is commonly based on some factors such as the available capacity of all access technology, the cost of transmitting traffic in that network and vehicle speed, among others. The vehicular heterogeneous network involves of WLAN and cellular systems and reduces the cost of communications or alternatively reduces the communication time. The use of vertical handoff is a suitable choice in lower speeds, as it would be better to avoid vertical handoff and wait for the cellular network at higher speeds. It provides understanding guidelines for optimal vertical handoff decision making based on the characteristics of the network in addition to the user mobility profile.

Ganan et al. (2013) maintained the ubiquitous connectivity that remains a challenge because of high vehicle speed and non-homogeneous nature of the network. Getting access to the network infrastructure should be
controlled and authorized. The authentication process acquires a non-negligible delay that results in packet loss and other issues during handoffs processing stage. So there is a need to define a secure and fast handoff method to handle this situation. Even if some solutions have been given in IEEE 802.11r and 802.11i standards, the handoff latency is more than 50 ms. The IEEE 802.11f standard describes the basic architecture of communications between RSUs to support vehicle roaming from one RSU to another during the handoff stage. IEEE 802.11i describes the different security services by providing data integrity, access control and data confidentiality, data authenticity. IEEE 802.11r rectifies major issues of the 802.11i by offering a three level key hierarchy (started moreover from a Master Session Key (MSK) produced during an EAP authentication or a PSK) and a supporting architecture that permits the OBU to evaluate fast transition between the RSUs within the same so called mobility domains without the required to run EAP authentication during individual movement. Control and Provision for Wireless Access Points was designed to give interoperability between different vendors, allowing vehicles to roam freely. Fast handoff protocols like that HOKEY, CAPWAP and 802.11r perform better than the 802.11i protocol. Among the fast handoff protocols, CAPWAP and 802.11r perform better than HOKEY in a vehicular state.

Mithil Wasnik & Dorle (2013) found complete automation and geographical area selections are the main problems in VANET. The Various handover schemes depend on the signal strength that is received from the base station which does not match the vehicular network environment. This analysis depends on the quality of service required for vehicles with dynamic mobility. The highly concerned factors in vehicular network are reliability and timely delivery of information.
Kumaran & Shaji (2014), identified that in the Vehicular Ad-hoc Networks, continuous connectivity is a main problem, because of high vehicle speed and always it changes topology of the network. In future, vehicles are fully equipped and networked with multiple network interface cards with On-board computers and promising wireless technologies. In this process, the vehicle to vehicle and vehicle to infrastructure method is used to contact the internet service. Further this research identified that the heterogeneous wireless access mode of vertical handover provides continuous connectivity between vehicles and infrastructure. Some necessary procedures are used in a vehicular network handoff process and this is one of the most important factors which affects the handover process. Further in this research, the various type of parameters used for VHO process and advanced methods of vertical handover decisions are reviewed and the vertical handover method is used to assure vehicular network connectivity in which, the different types of metrics invoked to trigger handover decisions with the introduction of RSS requirements, mobile terminal location information and quality of service parameters. The integration of different handover parameters develop multi criteria based handover decision making algorithm for efficient handover process.

Wararkar & Dorle (2015), applied the concept of Ant Colony Optimization (ACO) methodologies in vehicular networks based on the vehicle speed and position, the Ant-based algorithm executes well in the dynamics of similar networks and suits to the conditions properly. ACO meta-heuristic algorithm is used to improve the speed, resolution of hard optimization problems by taking benefit of the available processing power to find out the shortest data transfer path to increasing the throughput. The optimizing techniques highlight the security, Quality of Service, routing and broadcasting techniques for inter vehicular network data during handovers.
1.7.2 NEMO Based Handover Process

The NEMO MR operation is supported by NEMO+ with Nested NEMO networks and NEMO will provide clear benefit by augmentation of available message transfer and intelligent usage of available information and is also able to provide available benefit with little overhead.

Pascal et al. (2008), proposed a NEMO basic support (NEMO BS) protocol which gives a technique for enabling whole networks of IPv6 hosts to benefit internet access and continue reachable through constant, unmatched addresses although their underlying location in the internet changes. This NEMO model also supports entire mobile networks get connected to other mobile networks, resulting in Nested NEMO networks. NEMO+ suite of protocols are designed to optimize performance in nested NEMO networks. The NEMO+ is an efficient method in vehicular networks, the lightweight method to support nested NEMO networks. NEMO+ protocols establish a single additional hop to the end to end path. Hai Lin & Houda Labiod (2010), studied and analyzed the handover mechanism with interdomain and intradomain without changing the available IPv6 configuration, besides solving problems of void zone. However requirement of resources is more than using NEMO as here the encapsulated pockets are being used. When nested level is increased more than three stage produced handover, latency and bandwidth results inefficiently. The probability of session handoff supported by NEMO was analyzed, besides developing the analytical models for it. Apart from that it also analyzed the aspects of road intersections, the velocity and the delay happened in the delay (Zhu et al. 2011).

Rana et al. (2011), proposed the micro NEMO++ protocol, not only to provide flawless connectivity of Internet but also to eliminate the single point problem failures besides it also provide good performance than
NBSP and Micro NEMO. Taha et al. (2013), observed that, establishing fake point by using the concept of concealment, with many number of MNNs choosing the established fake point to create confusion among the hackers. This technique is called as obfuscation techniques that establish a exact location of user that the Wide area with present schemes of privacy.

Salman et al. (2013) applied Router Discovery and Duplicate Address Detection (DAD) that has direct impact on the handover procedure. The collaboration of multiple mobile routers in transporting the traffic of one another during handover process, outputs in minimum level of packet loss. The context (n, 1, 1) configuration of multihomed network mobility is applied in the processing stage. The Multiple Mobile Router Handoff Management (MMHM) methods provide continuous connectivity for the MNN and minimize the handoff delay and packet loss during handover process. In this method, only one tunnel enables to carry the traffic to/from the mobile network. It is clearly noticeable that the MMHM method suits more when compared to NEMO BSP for real time applications.

Shukla & Tyagi (2013), applied the NEMO approach illustrating the movement of vehicles from one network to another network. The purpose of proposed architecture is to support mobility among mobile network across heterogeneous network. The multiple Mobile Router (MR) based handover method in which MRs considerably receive packet destined for all other, provides no service disruption and appreciably minimize packet loss during handover process besides the handover latency leads to the packet loss. This architecture gives a mobile network and also the seamless mobility across heterogeneous networks. The overlapped reception of packet from dissimilar Access Router’s (AR’s) appreciably minimizes the packet loss during handover process without minimizing the handover latency. An efficient
physical-layer location privacy scheme was proposed in which two nodes cannot select the same fake point so as to increase the network performance with less routing delay (Taha et al. 2013).

Vaishnavi et al. (2014), applied Network Mobility Approach in vehicular ad hoc network. In which, She explained the communication between Infrastructure to Vehicle and Vehicle to Vehicle, ie. NEMO Based VANET and Nested NEMO Based VANET. Further she stated that communications is handled between the vehicles and road side units. These self-configuring networks composed a set of vehicles and elements of roadside infrastructure connected with one another without any underlying infrastructure, to send and receive information, also to provide the security alerts during heavy traffic. In a Nested NEMO, the messages are forwarded between vehicles and also between road side units to vehicle. This work focuses on the issue of minimizing the message delay, overhead and energy consumption during the communication of message.

Yuh et al. (2014), analyzed the method of reducing the complexity of handover process while keeping the devices connected to the internet as to execute the handoff process at the time of users leaving the old subnet and entered in to new subnet. However, the loss in handoff may be occurred because of signal weakness as vehicles are moving in rapid way. In order to overcome this problem, this study used a model that acquire an IP address from the another vehicle and execute the pre hand off procedure to reduce the delay occurred in handoff and maintenance of internet connectivity. Bokor et al. (2014) studied the performance of prediction-based handovers using NEMO in multihomed scenarios. Isabel et al. (2014), analyzed the aspect of using VARON, a NEMO based protocol and outcome of implementing this protocol in real time scenario.
Optimized MIH-assisted P-NEMO design for vertical handover mechanisms used the concepts of IEEE 802.21 to gather information for optimized handover decision making and also it was identified that while using the NEMO application, the dependence of standardization is occurred in the area of infrastructure network and suggested the ways to overcome it by reducing the complexity thus leads to better performance of vertical handover (Nouri et al. 2014).

Balasubramanian & Vijayalakshmi (2014), proposed a hybrid privacy preserving scheme that deals with power variability and concealment techniques using Nested nemo based Vanet hotspots to prevent the attackers from localizing the MNN and making the MNN to select the same fake point by creating the estimation error thus confusing the attacker.

Yuh et al. (2014) used Network Mobility management and it is used to effectively reduce the difficulty of handoff procedure and maintain the mobile devices connected to the Internet. When the vehicle move fast, the handoff and packet loss problem occur in the network when throughput is low. To overcome this type of issues, a novel NEMO protocol for vehicular ad hoc is proposed. While every car is moving in an unchanged direction with high moving speed, the vehicle adopts this protocol to obtain IP address from the vehicular network through vehicle to vehicle communications. The vehicle can rely on the support of the vehicle to execute the pre-handoff procedure or it can get its new IP address through multi-hop relays from the car on the paths of the same or opposed direction and thus minimize the handover delay and manage the connectivity to the internet. Further the incorporation of the cooperative vehicles mobile router helps to execute pre handoff procedure and helps the when vehicles enter a new subnet and to find out the mobile router of the cooperative vehicle to minimize handoff latency.
This scheme is also able to minimize both handoff delay and packet loss rate in addition with the overall delay and packet loss.

Khairi & Amine Berqia (2015) applied the Network Mobility (NEMO) approach with MIPv6 which helps to maintain the connectivity for vehicles moving from one access point to another access point. The main problem addressed in VANET is the issues related to security and Quality of service. The NEMO BS is used to handle mobility of terminal in the highly mobile VANET and the main requirements of vehicular networks applications are the quality of service, security and privacy features. The QoS and security are actually controlled by the wireless environment such as dynamic topology changes because of the high speed of vehicles. Further, this work stated that NEMO provides a promising solution to handle the disconnections of the network nodes when the high speed of vehicles entering into other network. The quality of service and security are main issues in VANET applications because they are directly connected to the safety of the people.

Lee (2015) used seamless communication mobility management and IP based mobility management protocols. The efficient mobility management method depends on route prediction in VANET and the reliable communication within vehicle that travels in fast moving area provided network mobility management. The complex issue of the design of scalable routing algorithms has been the avoidance of frequent path interruption roots by vehicles mobility. The Mobility management method is used to minimize the handover latency because handover within the highway are handled locally through the technology handover within a single domain and these roots advantages are increasing handover speed and reducing packet loss when performing transition thus leads to minimizes the signaling overhead by BU that all MH/MR initiates.
Pratibha et al. (2015), had proposed a new methodology of combining NEMO feature with MPTCP during multihoming, thus improving throughput, handover performance and avoid excess and unnecessary tunneling. Dang et al. (2015), examined the adaptive handover scheme which is used to be considered as a network of fixed nodes located arbitrarily in a pre-determined area to sense environment factors. Mobile nodes called as robot nodes are also used during the handover process.

Sheikh et al. (2016), observed that while using NEMO BS protocol, providing connectivity through Geo-Stationary Satellite would ensure the minimum data packet losses that enhance the performance of protocol in a significant way. Shayla et al. (2016), compared the advancement of qualitative factors with NEMO protocol’s benefits and drawbacks to explore the schemes based on current multihoming of NEMO.

1.7.3 IPV6 Protocol Based Handover

Bechler & Lars Wolf (2005), has proposed MMIPv6, is a communication protocol that combines multihop IPv6 based vehicular network into an internet. This protocol is efficient and highly optimized for scalability and it handles the mobility of vehicles. In addition to that, this protocol was designed to maintain IPv6 based mobile nodes arranged in ad hoc networks, also it is able to combine vehicle managed in IPv6 based multihop vehicular network into the internet and this was optimized for scalability and efficiency provided for the MMIPv6 protocol. The key conception was proactive service discovery protocols for Internet gateways which gives connectivity to the Internet. This protocol combined with an optimized mobility management protocol helps to organize the mobility of the vehicles. The proactive nature of the foreign agent discovery, MMIP6 scales fit with the size of the ad hoc network. MMIP6 is a suitable method to large-
scale multihop vehicular network into the Internet that comes along with an insignificant impact on the communication performance.

Chiang et al. (2008) used to select a Common Ahead Point (CAP) as the tunnel source to forward packets. The CAP can transfer the packets to PAR and NAR through the small transmission path. Packets sent from the data centre to vehicles could be transferred through CAR to NAR directly and it did not travel to PAR during handover processing stage. The Packet Forwarding Control (PFC) method is to choose a proper forwarding point for delivering packets over the tunnel. During handover process the packet delivery will base triangle packet transmission and the lengthy packet delivery path reduces the handover performance, particularly in the delay sensitive applications for example voice and multimedia. The main purpose of PFC method is fast tunneled packet delivery and very short bICASTing path. Tunneled packets would be transferred to vehicles from the forwarding point as a substitute of the original access router to minimize packet delivery time during handover process.

Uma Nagaraj & Deesha (2011) used the basic model of IPV6 for geographic addressing and various modes of communication for efficiency, road safety. Based on the application, the sender may send the message to the receivers in different area based on the application required. The IPV6 protocol provides expanded address space, enhanced mobility support, embedded security and configuration. It is the most suitable technologies which can support communication in vehicular network. The main advantage of IPV6 multicast is efficiently used for network to broadcast the messages on the network. The communication is ensured between the end points which are well established in vehicle, roadside, or anywhere in the internet. Geonetwork uses communication between the end points. The IPv6 protocol support the
different way of commutation between the end points as one among the following such as unicast, geounicast, geobroadcast, multicast and geoanycast.

Jose Santa et al. (2012), used the novel communication stack to handle the condition of continuous and secure IPv6 vehicular communications and uses the ISO/ETSI principles for the development of cooperative Intelligent Transportation System and it depends on standardized technologies based on Network Mobility (NEMO) protocol to provide an integral organization of IPv6 mobility. The proposed stack reaches these aspects by integrating standardized technologies for the base of NEMO, mobility traffic securization (IP sec and IKEv2), multihoming (MCoA) and handover management (IEEE 802.21). The real testbed is used to analyze where handoffs occur between 3G and 802.11p technologies. This method is used by the communication stack to support the handover optimization and covers the seamless transition between attachment points of vehicular networks. While the support to the handover optimization offered by the ITS communication stack is displayed through the mobility use case, a real testbed support with communications features is used to validate and evaluate the real performance of the stack design.

Lee et al. (2012), presented a new mobility support protocol in which the host-based distributed mobility management support protocol was designed. The performance of the proposed protocol is compared with the MIPv6 across the throughput and handover latency. Victor et al. (2013), studied the design and performance evaluation of PMIPv6 solution in a VANET based geo networking domain and the improvement in overall performance is analyzed under real traffic traces of orbital highway.
Wang et al. (2014), proposes a mobility handover scheme (MHVA) which uses a espouse an advanced mobility handover process with less packet loss rate, reduced handover cost, short handover delay and found that MHVA cost is lower when compared to MIPv6. Lee et al. (2013), compared the various host based mobility management protocols and the network based mobility management protocols and analyzed the performance of IPV6 mobility management protocols and summarized a positive feedback on their handover performance. Shukla et al. (2013), focuses the network mobility approach in VANET and the model also describe the movement of vehicles from one network to other network for heterogeneous network.

Hero et al. (2014), converse a new effective handover solution that helps to eliminate the large amount of handover latency and high packet loss ratio. Bokor et al. (2014), discussed the performance evaluation of the handover management solution providing IPV6 and seamless internet access for NEMO based scenarios. Jose et al. (2014), addresses the new framework that provides a support for continuous and secure IPv6 vehicular communications using NEMO protocol. Lee et al. (2014), proposed a route prediction based vehicular mobility management scheme managed with MIPv6 that reduces the handoff latency, low signal costs and less packet loss.

Dahiya & Deswal (2014) used the heterogeneous wireless network (HWN) that is hybrid in nature which consists of access routers (AR) and Internet Service Providers (ISP) for providing communication and internet services to the VANET architecture. Internet Engineering Task force (IETF) used MIPv4/MIPv6 and Fast MIPv6 as mobility and handover management techniques as their standard protocols. An improvement of FMIPv6, tunneling concept using handover management method supports on simulating vehicular network state. During the handover processing stage, when a mobile
node is unable to send or receive packets at a particular period of time, switching delay and IP protocol operation occurs due to the handover latency. The packet loss and handover latency problems of MIPv6 leads to reduce the quality of service for multimedia service application and are solved through FMIPv6 protocol. This protocol provides low packet loss, signaling overhead, handover latency and minimizes the service interruption time. Tan et al. (2014), presented the NEMO based route optimization scheme based on mobile IPv6 and measured the performance and its overhead ratio.

Sadiq & Ali Safa (2014), proposed a smart handover prediction system for FMIPv6 protocol based on curve fitting model and proved its working to be positive in complex wireless environment. The NEMO BSP and seamless IP diversity based NEMO (SINEMO) was compared and found that the performance of NEMO BSP is found higher than that of SINEMO based on end-to-end packet loss probability, end-to-end packet delivery delay, handoff latency, and throughput degradation time during handoff (Kundu et al. 2014).

Gaddour et al. (2015), proposed an Objective Function based Fuzzy Logic (OF-FL) designed for RPL with link and node metrics to overcome the downside of the standard objective function. The authors also discussed the new design of Co-RPL to provide better QoS in dynamic environment. The performance of OF-FL in addition with Co-RPL is found to be improved compared to the available standard specification.

Salehian et al. (2015), analyzed the various mobility management protocols and identified the host-based, net-based and network mobility based wireless sensor network protocols. Islam et al. (2016), proposed and analyzed the performance of multihoming –based scheme MM – PNEMO, to support
mobility management and resulted that the performance of PNEMO has outraged the performance of NEMO BSP.

Wong et al. (2015), compared the various methodologies like Tree Information Option (ROTIO), Port Address Translation (PAT), Optimized Link State Routing Protocol (OLSR), and Routing Information Protocol next generation Protocol (RIPng) and found that ROTIO helps to root out the pinball routing problem and RIPng helps to overcome high overhead problem in IPv6 based routing.

Aarthi (2015), has analyzed the effect of applying EFNEMO protocol over the tunneling and handover latency, so as to analyze the packet loss and packet cost and found to be effective. Wang etal. (2016), proposes a new framework based on IPV6 mobility suitable for urban vehicular networks and its performance results that the framework found to reduce the handover cost and delay and lowers the packet loss.

Ruchita et al. (2016), discussed the various protocols like MIPV6, HMIPv6, FMIPv6, PMIPv6, their handover and also discussed the challenges of host based mobility management and parameter to evaluate the protocols. Krishnan et al. (2016), proposed a novel approach that can effectively reduce the delay during handover when compared to PMIPv6. This approach also focuses on the multiple interfaces in the multi-homing domain and also discusses about the security issues.

Hamidi et al. (2016), made a comparative study on the various IPv6 based protocols based on the temporal and energy factor for the targeted applications. Pedro et al. (2016), has analyzed the performance of the secured NEMO channel and concluded that the addition of IPv6 security to NEMO channel helps to increase the confidentiality, integrity and authenticity though
there is a light degrade in the overall performance. Hero et al. (2016), has elaborated a survey on proxy mobile IPv6 handover and the HO procedure of PMIPv6 protocols. The survey also states that the MN does not require the necessity to participate in the mobility-related signaling in PMIPv6.

1.7.4 Security Issues in VANET during Handover

Mansik et al. (2015), has put forward a protocol that deals with session keys by inducing the handover and mutual authentication based on PUF devoid of revealing vehicle ID thus protecting the driver's privacy.

Singh et al. (2015), spotlighted the various authentication schemes in wireless network that have evolved in last one a decade.

Chen et al. (2015), proposes, a secure public transport Multimedia on Demand (MoD) system for VANET that helps to protect the transmission of multimedia data during long travel by defending against known attacks, authenticity, confidentiality and integrity issues.

Daojing et al. (2015), proposes a novel protocol named Hashhand that eliminates the security vulnerabilities using session key update mechanism and found to be feasible for practical mobile networks. Dorrle et al. (2016), study reports the security issue by identifying and reporting the transceiver the real position of malicious nodes, thus improving the security during data transfer in a vanet environment.

Raja et al. (2016), has proposed a light weight security protocol for communication that reduces the overhead during the secured data transfer in VANET environment. Karn et al. (2016), conducted a survey on different detection schemes available to detect the Sybil attacks caused when any
malicious vehicle acquire multiple identities in any heterogeneous environment.

Vampire attacks lead to high energy consumption, thus created the problem of reduction of network life time. This study employed LEACH protocol to solve the vampire attack with the selection of alternative node with full energy as temporary header for current communication by increasing the network capacity and lifetime (Jagnade et al. 2016).

From the literature survey, it is found that the existing NEMO mechanism supported only homogenous network and its extended version (NEMO+) followed single hop communication mechanism. In Fast NEMO (fNEMO), a tunnel between a previous access router and a new access router may be occasionally overloaded with traffic destined for MNNs. This is because the tunnel established in fNEMO is for just one MN as in FMIPv6 that cannot be used for the whole network. There exists a chance of false binding during the handover process. Security is restricted among vehicle to vehicle communication.

The analysis of above said literature, leads to the identification of the pitfalls like Burrow burden need to be reduced, Signal loss should be avoided when node is out of range, Packet loss during handover, reducing the handover delay, Security threats. Therefore, it is necessary to propose a new mechanism that supports above requirement in VANET environment.

1.8 PROBLEM STATEMENT

In the VANET environment, a new optimized handover mechanism has been implemented to support secure and seamless connectivity between nodes of networks by establishing the connections
before and after handover thus minimizing the handover delay, overhead and packet loss.

1.9 RESEARCH OBJECTIVES

The main objectives of the proposed work are

i. To eliminate the burrow burden by implementing advanced registration of the mobile nodes with New Concern of Address (NCoA) before the handover process thus reducing the traffic congestion.

ii. Due to mobility in nature, signal interruption can be overcome by a temporary or guard node that replaces the lost node thereby providing the seamless connectivity between the heterogeneous networks.

iii. To reduce the packet loss ratio during handover between the heterogeneous networks.

iv. To reduce the handover delay using Predictive Policy for advance registration of NCoA with mobile router to Home agent.

v. To establish the secure transmission of Binded Update (BU) data from MIM attacks and DoS attack, proprietorship of the HoA, and reachability of the CoA are estimated using Elliptic Curve Cryptography (ECC) in multi homing environments.

vi. To optimize the handover process using fuzzy concept in multi homing environments
1.10 PROPOSED METHODOLOGY

The efficient and secured handover mechanism has been developed that supports lossless connectivity among the nodes of multi-homing networks in this work. The proposed methodology is developed as four stage process which is mentioned in Figure 1.4. Each stage of process is provided as a contribution.

Contribution 1 : Secured Token Based Handover Algorithm in VANET
Contribution 2 : Efficient Fast Handover NEMO+ in homogenous scenario
Contribution 3 : Secured Efficient Fast Handover Multihoming Based NEMO+
Contribution 4 : Optimization of SEFMNEMO+ using Fuzzy in Multihoming scenario

Contribution 1: Secured Token Based Handover Algorithm in VANET

In VANET, if a nodal vehicle drop out of the signal or out of the network, then it is necessary to replace the lost node with guard node for repairing the disconnection of the network. The fastest route is identified to transmit the data efficiently. During handover, the Secured Token Based Handover (STBH) algorithm is used to secure the data transmission in homogenous network that formulates a token based allocation process using First Come First Serve (FCFS) technique. The token based allocation process is utilized for allocating the token to handover node based on requisition of token. Based on token priority, guard node is allocated to the handover node that facilities the seamless data transmission. Whenever a node drops out of
signal, the delay in switching to the other nearby network has to be handled by allocating a temporary guard vehicle.

![Methods and Techniques Diagram]

**Figure 1.5 Proposed methodologies**

**Contribution 2: Efficient Fast Handover NEMO+ in homogenous scenario**

In homogenous network, Efficient Fast NEMO+ (EFNEMO+) method is proposed that allows the registration of Mobile Router (MR) to Home Agent (HA) in advance to fasten the handover. Simultaneously, tentative registration to HA is completed before real handover occurs. During the handover, Mobile Network Nodes (MNN) transmits the packets among
MR and New Access Router (NAR) in different path, but not over the burrow between Previous Access Router (PAR) and NAR with the aim to minimize the burrow burden and redundancy. To improve the packet transmission to the destination network, the triad protocol namely Tree Discovery (TD), Network in Node Advertisement (NINA), Reverse Route Header (RRH) is used.

**Contribution 3: Secured Efficient Fast Handover Multihoming Based NEMO+**

In Secure and Fast Handover Multihoming based NEMO+(SEFMNEMO+), EFNEMO+ scheme is redefined by applying the Private Key-based Binding Update (PKBU) protocol to provide the safety transmission of BU data from the challenger attack like hacking, MIM attacks and DoS attack in Multihoming scenario. The PKBU protocol helps to justify the address ownership of the MN by creating a 128-bit private key. The interchanging of messages within the nodes in the PKBU protocol is done in three stages. The first stage is to establish the partnership of the MR’s IP address. The second stage is to justify the reachability of MR. The last stage is to ensure partnership of MR and reachability of HoA and CoA using improved Elliptic Curve Cryptography (ECC).

**Contribution 4: Optimization of SEFMNEMO+ using Fuzzy approach in Multihoming scenario**

Based on the serving PoA, fuzzy rule sets are framed and applied to calculate the Vertical Handoff factor thereby determining the necessity of handoffs. The final VHO factor obtained is compared with a predetermined threshold value that determine the necessity of handoff from the serving PoA. A balanced value of the threshold has to be maintained by the network to avoid the delay and data loss. Also the security is being optimized by
transferring the data packets to the right node by checking the transmitting power and original location of the node.

1.11 ORGANIZATION OF THESIS

Based on the research work done, the thesis is organized into 7 chapters.

- **Chapter 1** systematically explores the VANET paradigm by providing insight to the different services, the various challenges in providing services; security issues related to VANET communications. This chapter summarizes the background to research in this thesis. These include the reviews of relevant protocols, handover domain in VANET, NEMO based handover, NEMO+ based handover, IPV6 protocol based handover and related research on handover process in VANET. The chapter concludes with the findings of the literature survey, the problem statement and also objectives of the research work.

- **Chapter 2** describes the initial work “Secured Token Based Handover (STBH) Algorithm” which uses the token system in FCFS basis to ensure the lossless data transfer in a network. The traffic alert scenario is created for the implementation of the STBH algorithm and its results are being discussed in this chapter. It deals with the detailed study of Secured Token Based Handover techniques used to handover the packet within network.

- **Chapter 3** discuss about the implementation of vertical handover mechanism on NEMO+ basic protocol thus creating the EFNEMO+ that handles the handover efficiently by
minimizing the data loss in homogeneous network scenario. The results are being discussed under specific parameters in this chapter.

- **Chapter 4** introduces the Multihoming scenario where the data transfer between the heterogeneous network environments is applied to the EFNEMO+ that results in SEFMNEMO+ methodology. The results are found to ensure the secured and efficient data transfer between the heterogeneous environments.

- **Chapter 5** discusses about the necessity of optimization of the network created and also provides an overview on the fuzzy logic applied to optimize the results of SEFMNEMO+.

- **Chapter 6** discusses about the simulation tool, experimental simulation setup and result of the proposed works.

- **Chapter 7** discusses about the concluding remarks with a recommendation of enhancements for future applications.

### 1.12 SUMMARY

This chapter discussed about the various challenges faced in the vehicular network during communication. This chapter also briefed the reviews of NEMO, NEMO+, IPV6 protocol and Handover process methods. From the review it is found that the existing NEMO methods are not effective in packet loss rate, distribution pattern, channel quality, handover latency, quality of service, signaling overhead and message overhead. The NEMO+ protocol is found to perform better than the other protocol during the handover in a homogeneous network and also IPV6 protocol provides the communication between the end points in the network thus providing the seamless connectivity between the communicated networks. From the review,
the limitations are identified in existing NEMO+ and found that there is a need to propose a method that would provide an efficient and fast secured handover mechanism between the heterogeneous networks. Thus, the objective to enhance the NEMO+ protocol with IPV6 to support homogeneous and heterogeneous network is focused in this research.