Analysis of Hand Over Scheme for VANETS

Mithil A.Wasnik[1], S. S. Dorle[2]

[1]M. E. Student (Mobile Technology),
Department of Computer Science and Engineering
G. H. Raisoni College of Engineering, Nagpur, India
mithilwasnik@rediffmail.com

[2]Professor in Electronics Engineering,
Department of Electronics Engineering
G. H. Raisoni College of Engineering, Nagpur, India
ssdorle@gmail.com,

Abstract- ***Vehicular Adhoc Network is one of the fastest exploring technologies. In VANETs lot of work has been done. There are many issues in Vanets which have been addressed by the researchers like Congestion, Intelligent System, and Security. One of the main problems in VANETs is complete automation. The geographical area selection is one of the main problems which can arise while working with VANETs. In WAVE (Wireless Access for Vehicular Environment) the nodes are usually mobile vehicles or nodes. Since the terminal nodes are mobile they perform handover more frequently than in other wireless communication networks. But the multimedia streaming and VOIP will be seriously hampered by too frequent Handover and high latency. In today's scenario many Handover scheme are based on the signal strength which is received from the Base station which does not suit for vehicular environment. In VANETs the regional traffic and scenario keeps on changing with time.***

Keywords: Vehicular Adhoc Networks, ITS, Handover

1. Introduction

With the increase in emergence of new communication technologies specially in the field of microelectronic, communication and signal processing, allowed a development of tiny devices with low consumption of energy and capable of performing high computation wirelessly. Vanet is a new emergence in technology which recently got great attention from academician and researchers. Vanets has enhanced the transportation system with security and efficiency. For eg: Acknowledgements of the ambient condition (snow, fire) traffic in road condition (emergency, construction and congestion). In contrast to other sensory system, in Vanets the energy consumption is the secondary factor since the vehicles supply sufficiently high electric power. In inter vehicular system security and privacy are critical and challenging factors. For this reason, in this work it was given to more emphasis the aspects related to the inter vehicular communication and security.

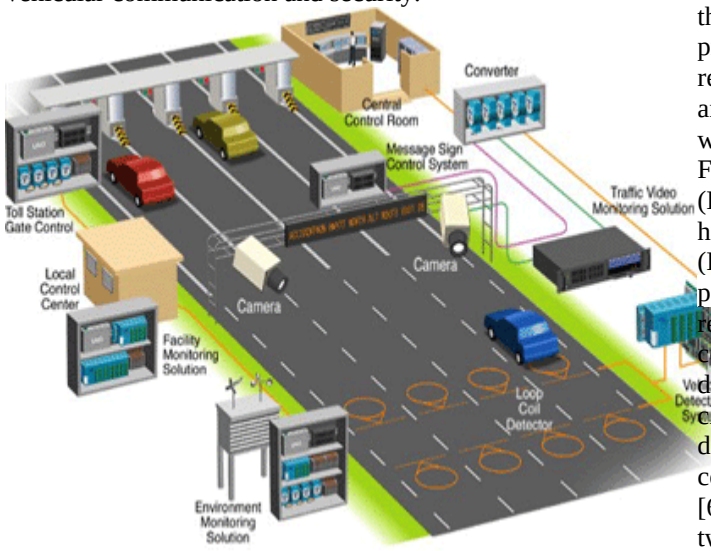

Fig 1: Example of Intelligent Transport System

Congestion reduces the efficiency in the intelligent transport system, which in turn increases the congestion of fuel and pollute the environment, increase travel time, sound pollution too. ITS has very wide range of application. From the basic management of traffic (Car navigation, signal control, management of container system, automatic number plate, speed organization). ITS has also involved in the advanced application that becomes the part and parcel of every human life such as the parking information, weather information, tracking of vehicles etc. Its has been used in every aspect of Life.

2. Related Work

Recently communication measure for emergency management have gained much research attention .This section present related work on propsed methord of communication. A lot of work has been in progress to solve the traffic congestion problem in VANETs. The work in [1] presents a checkpointing and recovery algorithm a study of recent checkpoint and recovery algorithm is done and analysis is done on their advantages and disadvantages. The work in [2] proposed two adaptive algorithms, named the Fast Rate Adaptation (FRA) and Early Rate Reduction (ERR), that are launched when the Handover is from low to high capacity (LOW-to-HIGH) or from high to low capacity (HIGH-to-LOW), respectively.The scheme proposed in [3] predicts the model parameters that affect application state recovery are analyzed. The proposed scheme is also compared with the existing scheme and the advantages and disadvantages are also configured. In [4] two main properties checkpointing and recovery are proposed. In [5] authors derived two techniques which prevents the wireless communication from any kind of threats. The work done in [6] deals with tradeoff analysis between the cost invested by t two mobility Handover strategies for maintaining the logging and checkpoint information before failure scheme is proposed. In [7] proposes Optimal QoS for highly dynamic

Vehicular Ad hoc Network (QVANO). The work in [8] deals with the comprehensive study of possible attacks and their possible solutions.

3. Handover Process

In wireless communication the term handover or Handover refers to the process in which transferring an ongoing call or data session from one channel connected to the core network to another. In satellite communications it is the process of transferring satellite control responsibility from one earth station to another without loss or interruption of service. The term *handover* is more common, and is used within international and European organisations such as ITU-T, IETF, ETSI and 3GPP and standardised within European originated standards such as GSM and UMTS The term handover is more common than Handover in academic research publications and literature, while Handover is slightly more common within the IEEE and ANSI organisations

3.1 Purpose of Handover

There are many reasons in telecommunications why handover is carried out. Some of the reasons are explained below.

- When the terminal device is moving from the range of one base station to the range of another base station. While moving the call is transferred to the another cell to avoid call termination.
- When the capacity of the cell is used up to connect the call and a new call which is present in the over lapping area of the two cells is transferred to that second cell to free some channels of the first cell.
- In non-CDMA networks when the channel used by the phone becomes interfered by another phone using the same channel in a different cell, the call is transferred to a different channel in the same cell or to a different channel in another cell in order to avoid the interference.
- When user behaviour changes e.g. Fast travelling user, cell of umbrella type etc.
- a handover (see further down) may be induced in order to reduce the interference to a smaller neighbouring cell due to the "near-far" effect even when the phone still has an excellent connection to its current cell;

One of the basic types of handover in wireless communication is when the call from its current cell (source) is transferred to another cell (target). Such type of handover in which the source and target cells are different is known as intercell handover. The main aim of intercell handover is to maintain the connection when the subscriber is moving from source cell to the target cell. There is a special type of handover in which the source and target cells remains the same and only the channels are changed. This special type of handover is known as the intracellular handover. The purpose of intra-cell handover is to change one channel, which may be interfered, or fading with a new clearer or less fading channel.

3.2 Types of Handover

Handover is classified broadly in two – soft handover and hard handover. The soft Handover can be divided into two types- multiway soft handover and softer handover. Hard handover can be further classified into intra and intercell handover.

A hard handover is also known as “Break before Make” connection. In the handover the Base Station handover the change of MS call to another cell and then the call is drop under the supervision of MSC. In hard handover the user is transferred to the cell of new base station Secondly, first the link to prior BS is terminated. FDMA (Frequency Division Multiple Access) and TDMA (Time Division Multiple Access) is primarily used by hard Handover. In this multiple access techniques (FDMA, TDMA) to minimize channel interference different frequency ranges are used. So it is almost difficult to communicate with both Base Station when the Mobile Station moves from one BS to another.

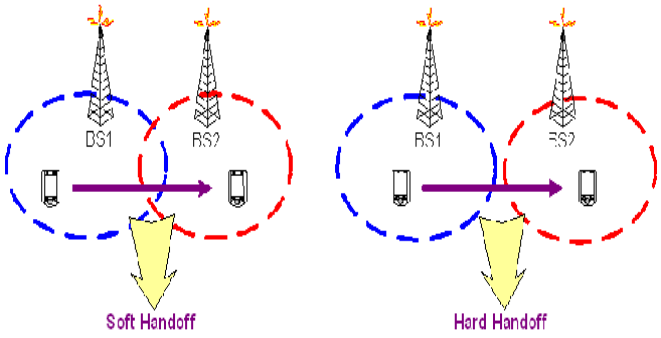

Fig 2: Types of Handover

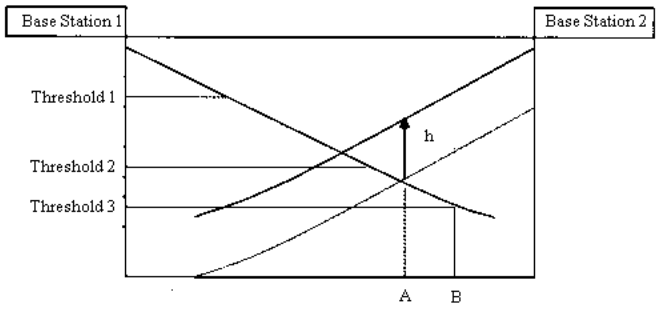

Fig 3: Handover Initialization

3.3 Comparison of Handover

The advantage of handover is that at the time of handover the Call uses only single channel. Time duration of hard handover is very small is not perceptible by the user. In the old days when analog signals where used it could be heard as a dot. Another added advantage of the hard handover is that the phones hardware needs not to be capable of receiving two or more channels at same time. This makes the hard handover simple and cheaper. But the disadvantage is that if the handover fails, the call may be disrupted or even may get dropped. Technologies that use the hard handover have the capability to connect to the source cell if the connection cannot be made to the target cell.

The advantage of soft handover is that the connection with the source cell is broken only when the reliable connection with the target cell is established. So there are lesser chances that the soft handover may fail. Bigger advantage comes

from the mere fact that simultaneously channels in multiple cells are maintained and the call could only fail if all of the channels are interfered or fade at the same time. The reliability of soft handover is high as compared to soft handover. The handover occurs when there is poor coverage. The reliability comes at the cost of more complex hardware

3.4 Implementation of Handover

Each cell has a list of potential target cell in cellular network for Handover in practical sense. The potential cell in which the subscriber moves as a target is called as neighbouring cell and the list which every cell possesses is called as the neighbouring list. Different algorithm can be used for implementing algorithm. During handover different parameters are monitored such as QoS, RSSI, NI, Bandwidth of the channel are accessed and decide when the handover is necessary. The downlink and uplink channels can be monitored for performing handover. The handover can be demanded by phone or the base station to another base station of the target cell. The phones and base station in the target base station monitors the parameters and best target is selected. In analog systems the parameters used as criteria for requesting a hard handover are usually the received signal power and the received signal-to-noise ratio (the latter may be estimated in an analog system by inserting additional tones, with frequencies just outside the captured voice-frequency band at the transmitter and assessing the form.

3.5 Reasons for Failure

There can be reasons for the failure in the handover. One of the reasons for the failure is Frequency Reuse i.e. frequency of the cell cannot be used reused. Whenever the user moves from source cell to target cell different frequency are used. But when the user moves to a target cell where all frequency is used, the call is terminated. Also, there is the problem of signal interference where adjacent cells overpower each other resulting in receiver desensitization.

3.6 Handover Prioritization

For handling and managing Handover different techniques and strategies are used. In order to avoid termination of call of call ongoing call Handover request should be given priority to new call this is called as Handover prioritization.
There are two techniques:

- Guard Channel Concept: Some channels are exclusively reserved for Handover only.
- Queueing: Queuing of Handovers is possible because there is a limited time interval. Between the limit times the received signal level goes below Handover threshold and the time the call is terminated due to insufficient signal level.

4. Security in Wireless Communication

There are various security threats which posses to the adhoc networks. Adhoc network are infrastructure less. They are defined as the peer to peer network with nodes connecting to each other wirelessly without any access point. Adhoc networks have very little security between them. Security can be provided to the adhoc networks with the help of some encryption techniques.

4.1 Security Goals

1. Availiability: Ensures protection against Denial of Service attacks. Attacker can use jamming technique
   In the Mac layer. The attacker can disrupt the routing protocol in the network layer.

2. Confediencelity: Ensures no information is leaked.

3. Integrity: Message is never transmitted during transmission.

4. Authentication: Node should ensure its identity.

5. Non-repudiation Ensures that the origin of a message cannot deny having sent the message

5. Conclusion

This paper presents an analysis done in Vanets to secure data and transfer it without any problem. This analysis based on the quality of service on demand for vehicles on dynamic mobility. Reliability and timely information delivery are highly concerned factors in VANETs. At last while considering the infrastructure less network, and new network which are smart enough like VANET a better Handover mechanism plays an important role in the handover process between the vehicular nodes during the vehicles are running on the road then mobile agent plays an important role in retrieving the information during the Handover process.

References

[1] Sourav Basu, Sayantan Palchaudhuri, Sheuly Podder, Meghla Chakrabarty “A Checkpointing and Recovery Algorithm Based on Location Distance, Handover and Stationary Checkpoints for Mobile Computing Systems” IEEE
[2] 2009 International Conference on Advances in RecentTechnologies in Communication and Computing
[3] Ling-Jyh Chen, Guang Yang, Tony Sun, M. Y. Sanadidi, and Mario Gerla ”Enhancing QoS Support for Vertical Handovers Using Implicit/Explicit Handover Notifications” IEEE 2009.
[4] J.C. Miraclin Joyce Pamila, K. Thanushkodi “Log Management Support for Recovery in Mobile Computing Environment “(IJCSIS) International Journal of Computer Science and Information Security, Vol. 3, No. 1, 2009
[5] Yogita Khatri “DISTANCE BASED ASYNCHRONOUS RECOVERY APPROACH IN MOBILE COMPUTING ENVIRONMENT” International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.3, May 2012
[6] Philippe Golle, Dan Greene, Jessica Staddon “Detecting and Correcting Malicious Data in VANETs” IEEE 2009
[7] Ing-Ray Chen, Baoshan Gu, Sapna E. George, and Sheng-Tzong Cheng “On Failure Recoverability of Client-Server Applications in Mobile Wireless Environments” IEEE TRANSACTIONS ON RELIABILITY, VOL. 54, NO. 1, MARCH 2005
[8] Prabhakar Rontala Subramaniam, Prof. Arunkumar Thangavelu, Chitra Venugopal “ QoS for highly dynamic Vehicular Ad hoc Network Optimality” 2011

11th International Conference on ITS Telecommunications

[9] AJAY RAWAT, SANTOSH SHARMA, RAMA SUSHIL "VANET: SECURITY ATTACKS AND ITS POSSIBLE SOLUTIONS" Journal of Information and Operations Management ISSN: 0976–7754 & E-ISSN: 0976–7762, Volume 3, Issue 1, 2012, pp-301-304