Volume 3, Issue 10, October 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Efficient and Secure Handover Scheme for VANETS

Mithil A. Wasnik*, Rahul Sathawane

Assistant Professor
RGCER, Nagpur
RTM Nagpur University, India

Abstract— ***A Vehicular Ad-Hoc Network or VANET is a technology were the moving cars act as terminals so that it can create a mobile network. In VANET every car which is participating in a network turns into a wireless router or node. The range between the communicating vehicles is about approximately 100 to 300 meters. In WAVE (Wireless Access in vehicular Environments) the terminal devices are moving with the much higher speeds, due to this many of the charectertics will be hampered (eg: QOS, Streaming etc).The Hampering of this charectertics may result in the increase in the latency. The traffic in VANETS goes on varying. Therefore there is an every chance that these mobile hosts may become failure. The security is an important criterion to keep VANETS threat free. So therefore this paper presents an efficient Quality Enhancement scheme to improve handoff performance in Vehicular Adhoc Networks. A Recovery scheme and security features is also proposed in this paper. Our Proposed scheme periodically collects the states of the base stations by Access Point Co ordinator (APC) and predicts the intensity of the traffic at the next moment. Moreover the recovery scheme recovers the lost information if at all the the handoff scheme fails.***

Keywords— ***Vehicular Adhoc Networks, EDCA, ITS, BSC, AES***

I. Introduction

For providing various infotainment services number of service providers and network operators are attracted by Vehicular Adhoc Networks (VANETs).VANETS are the part of ITS. Intelligent Transport Systems (ITS) have advanced applications which, without embodying intelligence as such, aim to provide innovative services such as transport and traffic management which enable various users to be better informed and make safer, more coordinated, and 'smarter' use of transport networks. ITS has become the hot topic in the research field because of the traffic congestion and a synergy of new information technology for simulation, real-time control, and communications networks. The world has been witnessing the traffic congestion due to the increase in the globalization, increase in the motorization, growth in population, urbanization. The density of population has also result in traffic congestion.

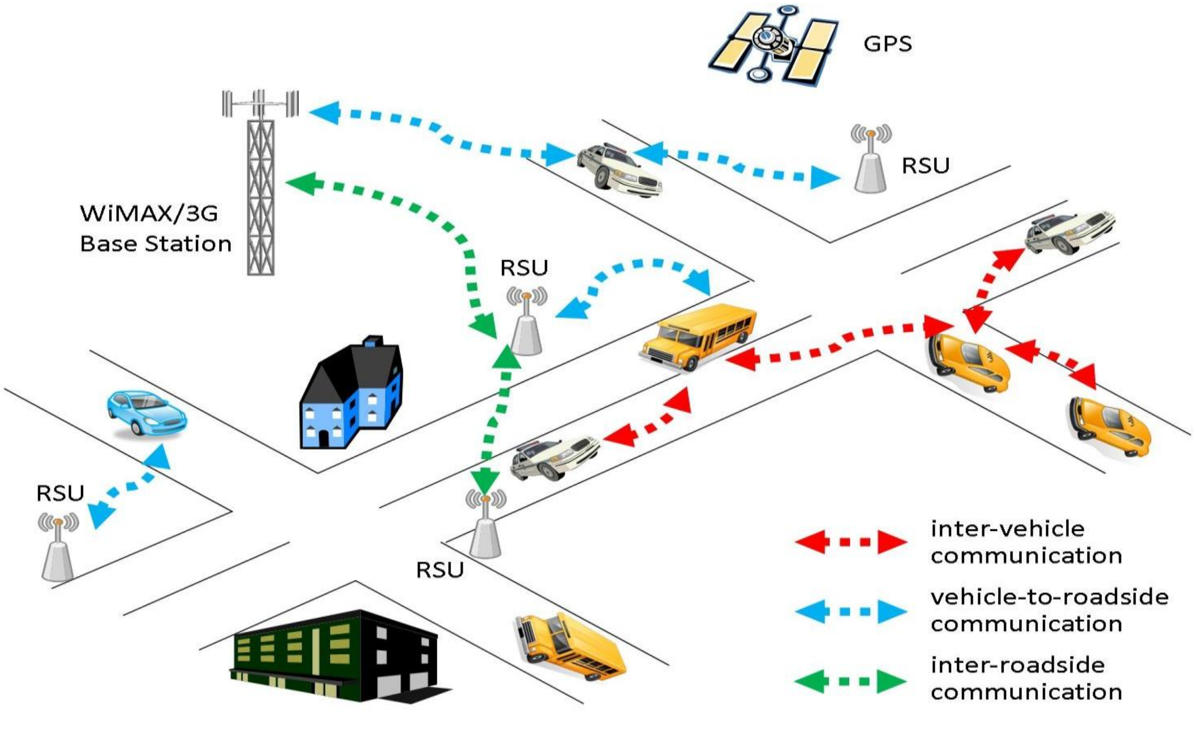
GPS
WiMAX/3G
Base Station
RSU
RSU
RSU
RSU
RSU
inter-vehicle communication
vehicle-to-roadside communication
inter-roadside communication

Fig 1: Example of Intelligent Transport System

Efficiency in the transportation is reduced by the congestion which results in the increase in the consumption of fuel, travel time, air pollution and 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. It has been used in every aspect of Life.

II. LITERATURE REVIEW

Recently communication measure for emergency management has gained much research attention .This section present related work on proposed method of communication. A lot of work has been in progress to solve the traffic congestion problem in VANETs. The work in [1] is based on increase in the network range of RSU (Road Side Unit) by a dissimation method. The work is also based on the information of the OBU (Onboard Unit). The work in [2] provided a scheme for performing collision free traffic formation. The Quality Scanning scheme proposed in [3] predicts the future traffic scenario base d on the information given by the AP (Access Points).In [4] a protocol is analysed has some other weaknesses also further improvements were proposed to avoid those security problems. Besides user privacy, the key features of scheme are including no verification table, freely chosen password, mutual authentication, low computation and communication cost, single registration, session key agreement, access control, and being secure against the related attacks. In [5] Lingyun et al. worked on an encryption scheme to ensure the consistency of the message. The work done in [6] relates the information recovery from the mobile nodes. They also proposed the scheme to reduce the recovery time and cost. The repudiation management scheme proposed in [7] is used to check the spreading of false message, also proposed a protocol to collect and aggregate reputation information further also proposed a fuzzy computational model to represent reputation traffic formation. A context free protocol has been proposed in [8] by Song et.al. that does not rely on observation and selfish behaviour detection. In [9] Chang et. al. a hash function of collision resistant has been discussed and provided an authenticated Diffie Hellman key exchange. In [10] author presented a new and efficient wireless authentication protocol to provide user anonymity. The scheme is based on the hash function and smart cards, and mobile users only do symmetric encryption and decryption. In proposed protocol, it takes only one round of message exchange between the mobile user and the visited network, and one round of message exchange between the visited network and the corresponding home network. Choi et.al in [11] proposed a revocation mechanism and this mechanism were applied to cellular networks and WLAN. KEM (Key Encapsulation Mechanism) proposed in [12] is use of data protection approach which is based on secret sharing scheme in order to achieve an efficient data reading process.

III. HANDOVER PROCESS

When we talk about wireless communication the most important feature is mobility. Continuous services are usually achieved with the help of Handover (or handoff) from one cell to another. Handover is often referred to a process of changing the frequency, spreading codes, time slot while the connection is in progress, with respect to the current connection. Handover is often referred as a crossing of boundary of cell or by detoriation in the quality of signals are in current channel. Handover is often categorized into Soft and Hard handoff. They are characterized by "make before break" and "break before make". In soft handover both the new and being used resources are held during handoff process. In hard handoff the resources which are being used are released first and then new resources are used. The handoff schemes which are cheaply designed tend to generate very high signalling traffic and therefore there is a tremendous decrease in the QoS. In cellular communication the handover holds an critical place because the neighbouring cell are always using disjoint subset of frequency bands , so there must be a collaboration between the mobile station and the currently serving base station. Some of the Condition that might affect the performance of the handover is decision making, priorities strategies during overloading.

A) Types of Handover

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

B) Handover Initiation

Handover process is initiated when the old connection is broken and the connection with the new base Station is established. Various initiation criteria determine the performance evaluation of handover. Multipath nature of radio waves can be eliminated by the rapid fluctuations. The mean strength of signal of BS1 reduces as the MS goes away from it. Similarly the mean strength of signal of BS2 increases as the MS approaches it.

i)Relative signal strength

This method is based on the strongest received BS all time. This decision depends upon received signal of mean measurement. This method endeavour many handoffs which are not necessary, when the signal of current BS is still at agreeable level.

ii) Threshold enabled relative strength of signal

This process allows the MS to prefer handoff if the signal which it is using is comparatively low (less than the threshold) and the other signal is neighbouring cell is stronger. The relative value compared to strength of signal of two base stations at point which they are equal determine the effect of threshold.

iii)Relative Strength of signal with hysteresis

The current signal which the MS is using drops below a threshold and the BS which is next target is stronger than the current are given hysteresis margin this scheme is enabled.

v)Prediction Techniques

This technique is based on the future value of the reduced signal strength. This technique was proposed so that we can get better result with result with respect to reduction in number of handoff, the relative strength of signal without threshold and hysteresis.

IV. SECURITY IN WIRELESS COMMUNICATION

Security plays an important role in the wireless communication due to its broadcast nature of wireless channels. The security in wireless communication has captured the attention of many researchers. The main aim of the security in wireless communication is to exploit the physical character tics of wireless channel. Various types of vulnerabilities have to be sustained such as noise, fading etc. during the transmission of signal. In order to improve the quality of digital communication various security approaches can be used. Communication security is a process of discovering and implementing the desired plans, procedures and policies to provide security to wireless communication from malicious attacks and risks. The action to be taken or the threats have to be full proof. Communication system includes four components- Physical security, network security, and administrative security.

Physical Security: - Enables the protection of all facilities where the communication system is placed. This include communication centre, sites of towers, maintaince facilities as well as communication devices itself. The security has to be provided when:

- Devices are in use
- Transported for maintainence
- While monitoring

Network Security: - It includes the protection of system (hardware and software) from threats and attack. Common network requirements for security include maintenance of user account, controlling of password and access of system. The program such as antivirus, firewall, detection of intrusion also plays an important role in maintaining security.
Communication Security: - It relates to the measure taken to enable the integrity and confidentiality of information transmitted on air. This can include the technique of encryption, the management and reprogramming of encryption keys.
Administrative Security: - Enables the procedural control to ensure the confidentiality and integrity and availability of communication system. A security program may include plans to ensure security, documentation, procedures and ongoing security measurements.

V. CONCLUSION

This Paper presents an Efficient Quality Enhancement scanning scheme with recovery and security feature to enhance the performance of the handoff. Thus in our scheme the BSC collects all information from the BS and does the calculation and sends the result back to the BS. If at all the handoff fails, recovery system is also embedded in our scheme which will be used for recovery of information from the base station. The security scheme is also provided in the scheme for securing VANETs for threats and attacks.

REFERANCES

[1] Pierpaolo Salvo,Francesca Cuomo, Andrea Baiocchi “Road Side Unit coverage extension for data dissemination in VANETs” Annual Conferance on Wireless on Demand network system and service 2012.

[2] Alpana Dahiya ,Madhu ,Niyati Bansal “Path Discovery in Vehicular Adhoc networks” Second International Conference on Advanced Computing & Communication Technologies 2012 IEEE, pp. 551-555.

[3] Tin-Yu Wu, Wei-Tsong Lee, Fong-Hao Liu, Hung- Lin Chan, Tsung-Han Lin ”An Efficient Pre-scanning Scheme for Handoff in Cooperative Vehicular Networks” IEEE 22nd International synopsium on personal, indoor and Mobile radio communication , 2011.

[4] D. He, M. Ma, Y. Zhang, C. Chen, and J. Bu, “A strong user authentication scheme with smart cards for wireless communications,” *Computer Commun.*, vol. 34, no. 3, pp. 367–374, 2011

[5] Lingyun Zhu, Chen Chen, Xin Wang, Azman Osman Lim ,“ SMSS: Symmetric-Masquerade Security Scheme for VANETs“ Tenth International Symposium on Autonomous Decentralized Systems IEEE 2011, pp. 617-622.

[6] Mrs. Suparna Biswas, Dr. Sarmistha Neogy “A Handoff based Checkpointing and Failure Recovery Scheme in Mobile Computing System” IEEE 2011, pp. 441-446.

[7] Qing Ding, Xi Li, Ming Jiang, XueHai Zhou ” Reputation Management in Vehicular Ad Hoc Networks” IEEE 2010.

[8] Chengqi Song and Qian Zhang "Protocols for stimulating packet forwarding in wireless Adhoc Networks" IEEE 2010

[9] C.-C. Chang, C.-Y. Lee, and Y.-C. Chiu, "Enhanced authentication scheme with anonymity for roaming service in global mobility networks," Computer *Commun.* vol. 32, no. 4, pp. 611–618, 2010.

[10] H.-C. Hsiang and W.-K. Shih,"Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment,"*Computer Standards & Interfaces*, vol. 31, no. 6, pp. 1118–1123, 2009.

[11] J. Choi, S. Jung, Y. Kim, and M. Yoo, "A fast and efficient handover authentication achieving conditional privacy in V2I networks," LNCS 5764. Springer, pp. 291–300, 2009.

[12] Takashi Matsunaka, Takayuki Warabino and Yoji Kishi "Secure Data Sharing in Mobile Environments" The 9th International Conference on Mobile Data Management 2008 IEEE.