Enhancement of Inter-Vehicular Communication through a New Bandwidth Optimization Technique to Optimize the Performance of VANETs

Md. Torikur Rahman

[1]Uttara University, Department of Computer Science & Engineering, Dhaka, Bangladesh

Abstract: *Now is the age of information technology. World is advancing day by day. At present in this progressing world communication from one place to another has become so easy, less costly, and faster. This modern life is almost impossible with the help of these communication technologies. Vehicular Ad Hoc Networks (VANETs) is a special case of Mobile Ad Hoc Networks (MANETs) and on a whole a part of Intelligent Transport System (ITS). Recently the fields of VANET have yielded more and more popularity and thus VANETs have become a subject of great interest for the researchers to enforce research activities. But there are some communication system for inter-vehicular communication which uses high capacity of bandwidth and a big amount of internet speed. Thinking of this, I propose a new bandwidth optimization technique for the improvement of inter-vehicular communication to optimize the performance which will more efficient in terms of time delay and number of packets drop in VANATs. The effectiveness of the proposed algorithm can redirect a new way towards optimization development in network communication and device junction technology.*

Keywords: VANETs, MANETs, RSU, V2V, V2I, Leaky Bucket, FIFO, Bandwidth Optimization

1. Introduction

VANETs [1] are a subclass of Mobile Ad Hoc Networks (MANETs). They are considered as an application to MANETs as they are widely based on MANETs fundamentals. VANETs are special kind of networks that are formed between moving vehicles on an as-needed basis [2] [3]. Among the characteristics of VANETS one worth mentioning characteristic is that VANETs can easily operate in an infrastructure-less structure and can also cope up with the rapid changes of the network topology [1]. Along with the safety applications, VANETs disseminate important and real-time information to the nodes such as weather information, transit systems, internet access, mobile e-commerce, and other multimedia applications. VANETs afford a large collection of routing protocols to confirm autonomous communication between the moving vehicles on the road [3]. In a VANET network the vehicles care equipped with various communication systems which uses high capacity of bandwidth and a big amount of internet speed so that they can communicate among themselves along with the road-side infrastructures. In this paper I have put my concern on the working principle, major components, various network architectures, security and existing bandwidth optimization technique of VANETs besides the basic terminologies. Finally, I proposed a new bandwidth optimization technique for the improvement of inter-vehicular communication to optimize the performance which will more stable in terms of time delay and number of packets drop in VANATs.

2. Vehicular Ad Hoc Network

Vehicular ad hoc network (VANET) is a special case of mobile networks, where vehicles equipped with computing/communicating devices (called "smart vehicles") are the mobile wireless nodes. However, the movement pattern of these mobile wireless nodes is no more random, as in case of mobile networks, rather it is restricted to roads and streets. Vehicular networks have hybrid architecture; it is a combination of both infrastructure and infrastructure-less architectures.
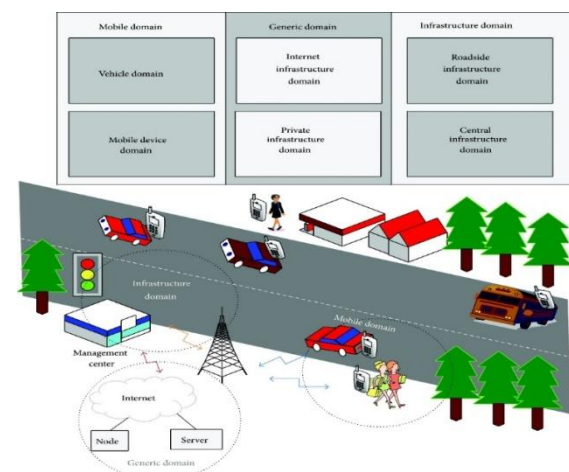

Figure 1:VANETs system domains [4]

2.1 How Does VANET Work?

Vehicular Networks System consists of large number of nodes, approximately number of vehicles exceeding 750 million in the world today, these vehicles will require an authority to govern it, each vehicle can communicate with other vehicles using short radio signals DSRC (5.9 GHz), for range can reach 1 KM. This communication is an Ad Hoc communication that means each connected node can move freely, no wires required. The routers used called Road Side Unit (RSU), the RSU works as a router between the vehicles on the road and connected to other network devices. Each vehicle has OBU (on board unit) and TPD (Tamper Proof Device). VANET has mostly gained the attention of today's research efforts, while current solutions to achieve secure VANET, to protect the network from adversary and attacks,

to reduce packet delay still not enough, trying to reach a satisfactory level, for the driver and manufacturer to achieve safety of life and infotainment [5]. The need for a robust VANET networks is strongly dependent on their security & privacy features, packet routing and delay reducing.

The steps to link VANET with vehicle:
- Each vehicle is provided with Wi-Fi/Wi-Max device
- Unique ID and IP Address for each vehicle
- Each node can communicate with each other node
- Any vehicle can register its identity to a roadway WAP

Collective information stored by the WAPs at a dynamic server database.

2.2 Components of VANET

Road Side Unit (RSU) is the device located on the roadside that computes and provides connectivity support to the passing vehicles. RSUs are one of the major components of vehicular communication system in which vehicles and these RSUs are the communicating nodes [5]. They provide each other with important information like safety alerts and traffic information.
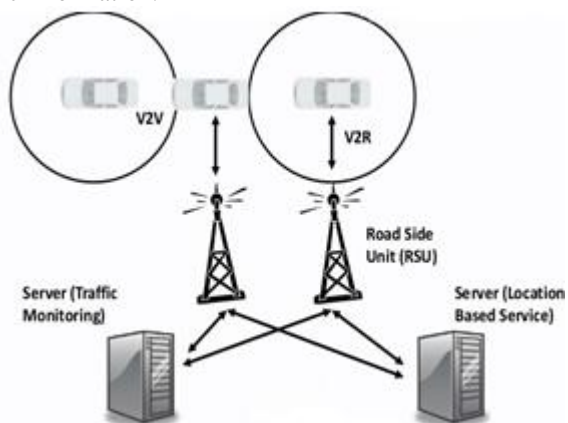

Figure 2: Road Side Unit (RSU)

Tamper-Proof Device (TPD) is another component of vehicles in VANET. This device holds the vehicle secrets, all the information about the vehicle like keys, driver's identity, trip details, speed, route etc. On-Board Unit (OBU) is a device which is inside the vehicle which processes the data collected from various sensors fitted inside the vehicles and outputs the conditions of the vehicles. Vehicles in a VANET network are equipped with embedded systems called "On-Board Units" (OBUs). OBUs are used for positioning, monitoring and billing. Moreover the OBUs have infrared interfaces for communicating with stationary control passages on the highways.
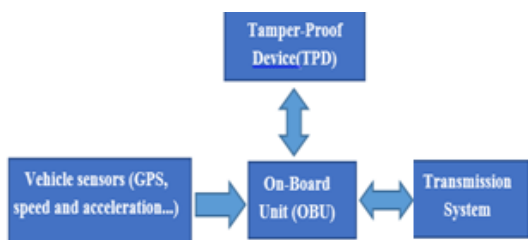

Figure 3: OBU and TPD

2.3 Structure of VANET

Vehicular ad hoc networks have mixed architecture; it is a grouping of both infrastructure and infrastructure-less architectures. The straight vehicle to vehicle communication is called V2V communication. It is infrastructure-less or ad hoc in nature. In this type of communication, the vehicles traveling within communication range of each other form an ad hoc network [6]. On the other hand, the vehicle to infrastructure communication is known as V2I communication which has infrastructure architecture where vehicles connect to contact points positioned along roads. These access or contact points are known as road side units (RSUs). Vehicles communicate with other vehicles/wired nodes through these RSUs. To deliver various services to vehicles, RSUs are generally connected to each other and to the Internet. The direct RSU to RSU communication is also referred as I2I communication. The vehicles of VANET networks are equipped with computing devices that enable these vehicles to communicate with each other. That's why these vehicles are called "smart vehicles".
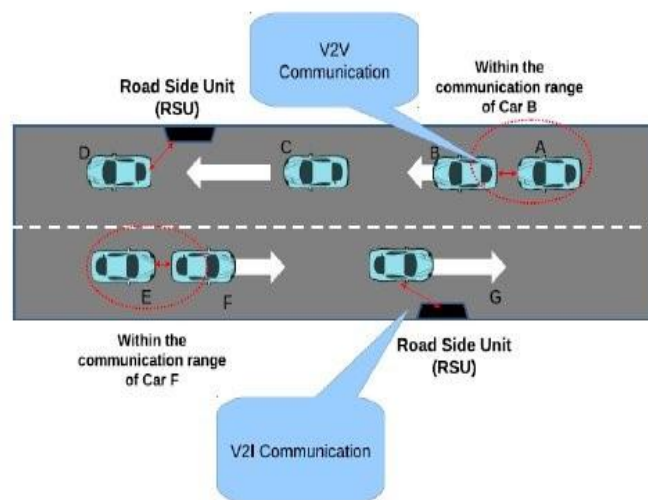

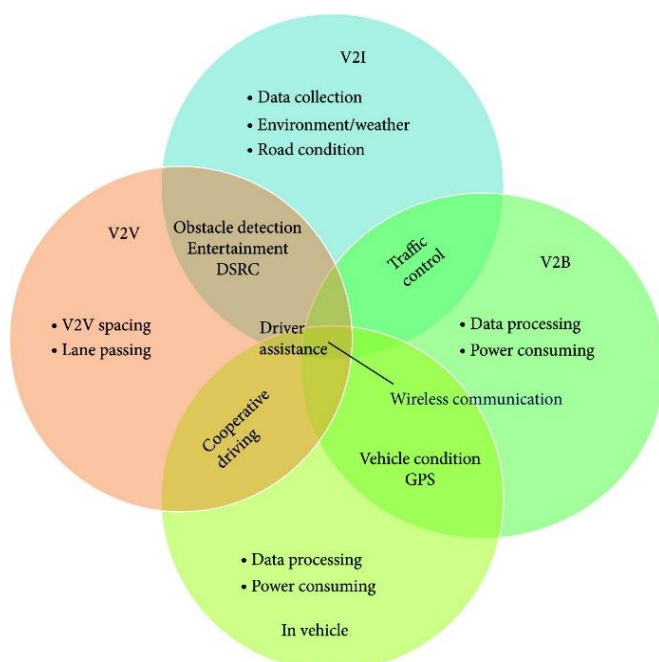**Figure 4:** V2I and V2I Communication

Figure 5: Key functions of each communication type.

3. Analysis for Bandwidth Optimization

Bandwidth management is the procedure of managing and controlling the communications (traffic, packets) through measurement on a network link, to ensure the avoidance of flooding the link to its maximum range of capacity or over flooding the link, which would result in a network congestion and poor performance within the network. It is measured in bits per second (bit/s) or bytes per second (B/s) [7].

Bandwidth optimization is a technique that can measure and utilize the capacitive bandwidth within the whole system. Now a day's bandwidth management is a problem as the number of internet users are increased day by day. Even using local LAN, a limit of bandwidth must be controlled among all the users those are provided through the PBX system, or the bandwidth will be wasted among the caller and called party, vehicle to vehicle or vehicle to infrastructure communication in VANETs network and also may be wasted between the link and the end point [8].

3.1 Existing Technique for Bandwidth Optimization

There are many BW managing and optimizing options, they are listed below:

- Traffic Shaping (Rate limiting): Leaky bucket, Token bucket, TCP rate control- it adjusts the TCP window size as well as controlling the rate of ACK's being returned to the sender [9]. The traffic conditioning phase has this main component: traffic meter, packet marker, traffic shaper, and traffic policer. Through these
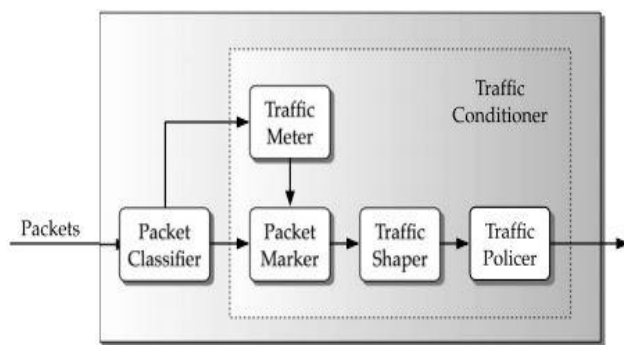

Figure 6: An operational framework for differentiated services.

Since shaping takes place at an egress interface in the router, it may be necessary to classify a packet to a flow earlier, possibly at the ingress interface. There are two predominant methods for traffic shaping:

Traffic smoothing: This method eliminates bursts and presents a steady stream of traffic to the network, which can be implemented using a leaky bucket algorithm [15].

Traffic burst shaping: This method shapes burst of predetermined size by averaging over a time window, which can be implemented using a token bucket algorithm.

Leaky Bucket Algorithm: The Leaky Bucket Algorithm used to control data rate in a network. It is implemented as a single-server queue with constant service time. If the bucket (buffer) overflows, then packets are discarded [10].
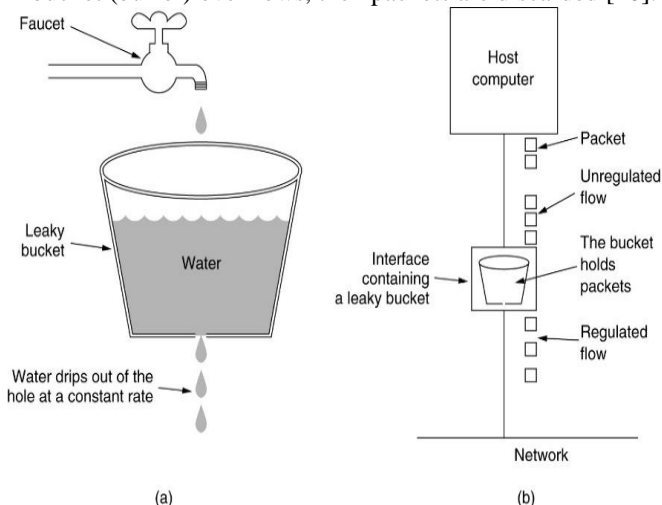

Figure 7: (a) A leaky bucket with water.
(b) A leaky bucket with packets.

- Scheduling Algorithms: Weighted fair queuing (WFQ), queuing, Weighted (WRR), Deficit weighted round robin (DWRR), Hierarchical Fair Service Curve (HFSC) [11].
- Congestion Avoidance: RED, WRED works as port queuing buffer network scheduler and lowers the usual property of TCP global synchronization, Policing.
- Bandwidth Reservation Protocols / Algorithms: Resource reservation protocol (RSVP), Constraint-based Routing Label Distribution Protocol (CR-LDP), Top-nodes algorithm.
- Traffic Classification: Categorizing traffic according to some policy in order that the above techniques can be applied to each class of traffic differently [12].

3.2 Proposed Algorithm

Proposed algorithm is based on the "leaky bucket" algorithm. But it is very different than normal leaky bucket. As all know the leaky algorithm uses bucket which can contain both incoming and outgoing packets, shape them send them at a constant or optimal rate. But leaky algorithm uses fixed size of buckets and that cannot contain the overflow data as a result there are fall of packets, and there resides the drop probability. Here, the data packet drops and for this the bandwidth (bw) is wasted or it can say bandwidth doesn't utilize properly. Being modified and changed the algorithm using FIFO queue as the number of queue equal to the no of buckets for traffic shaping (burst, noise) and processing the incoming packets then resend the overflow data through the next bucket fixing a time limit to transfer all the packets within a session and so on. The algorithm is effective for shaping the traffic, since all the packets are sent ensures 0% of data packet's loss in a fixed delay time provides effectiveness on channel capacity, also provides optimality with capacitive controlled bandwidth to a link and endpoint channel. Same work follows in case of caller and called party through data packet transferring.
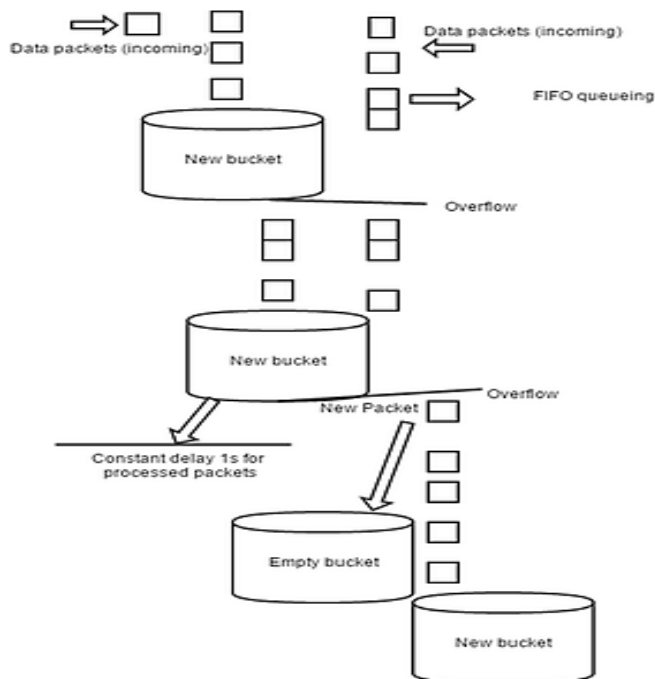
Figure 8: Proposed Algorithm with 0% Packet Loss

There is an average delay time for packet data intervals between links to end point packet transfer. It makes the average delay time fixed for this algorithm. So, it gives every time an optimal rate of packet transfer per second [13].
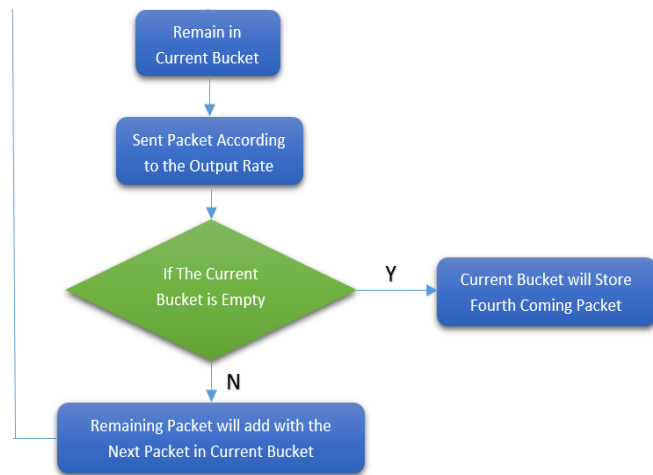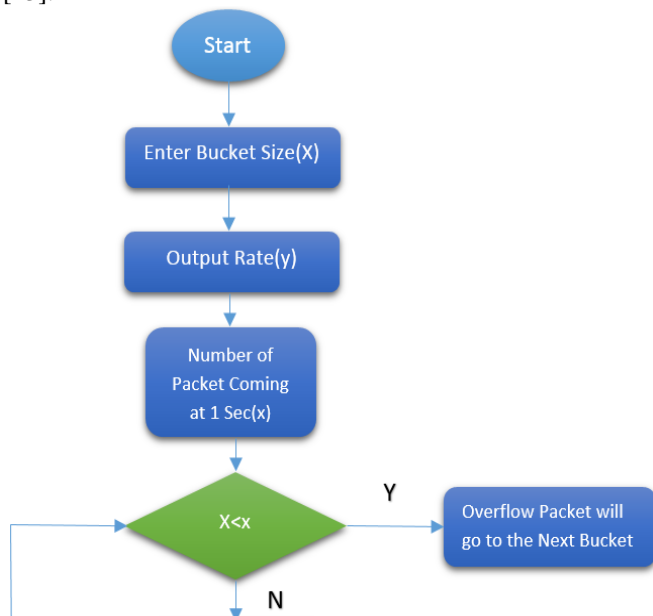

Figure 9: Proposed Algorithm Flowchart

4. Security in Vehicular Ad Hoc Network

Security Goals: To secure a Vehicular Ad Hoc Network, a security protocol must satisfy the following attributes: confidentiality, integrity, availability, authenticity [14].

- Confidentiality ensures that classified information in the network is never disclosed to unauthorized entities. Sensitive information, such as strategic military decisions or location information requires confidentiality [15].
- Integrity guarantees that a message being transferred between nodes is never altered or corrupted. Data can be altered either intentionally by malicious nodes in the network or accidentally because of benign failures, such as radio propagation impairment or through hardware glitches in the network [16].
- Availability implies that the requested services (e.g. bandwidth and connectivity) are available in a timely manner even though there is a potential problem in the system. Availability of a network can be tempered for example by dropping off packets and by resource depletion attacks [17].
- Authenticity is a network service to determine a user's identity. Without authentication, an attacker can impersonate any node, and in this way, one by one node, it can gain control over the entire network.

Finally, non-repudiation ensures that the information originator cannot deny having sent the message. Non-repudiation is useful for detection and isolation of compromised nodes [18].
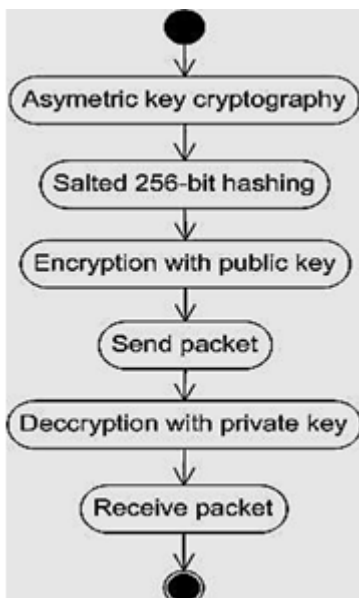
Figure 10: Flowchart of overall Security Mechanisms for VANETs

5. Simulation Results for Bandwidth Optimization in VANETs

5.1 Simulation Issues

- Time Delay
- Packet Drops: Packet loss in data networks is both common and expected. Many data protocols, in fact, use packet loss. The protocols identify the condition of the network and can reduce the number of packet loss in that network

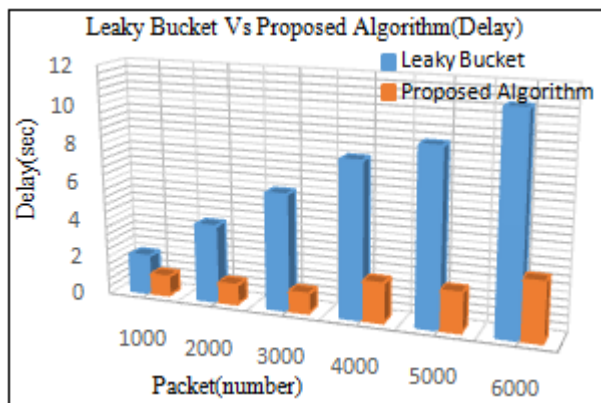### 5.2 Simulation Results (Graph)

Figure 11: Leaky Bucket vs. Proposed Algorithm (Delay)

Here leaky vs. proposed algorithm in terms of delay is showing. In the graph when 1000 packet send the delay is 2 second for Leaky bucket and 1 second for proposed algorithm. When 6000 packet send the delay is 11 second for Leaky bucket and 3 second for proposed algorithm. So, In Leaky bucket delay is increasing more than the proposed algorithm when the amount of packet is increased. That means less delay is happen in proposed algorithm.
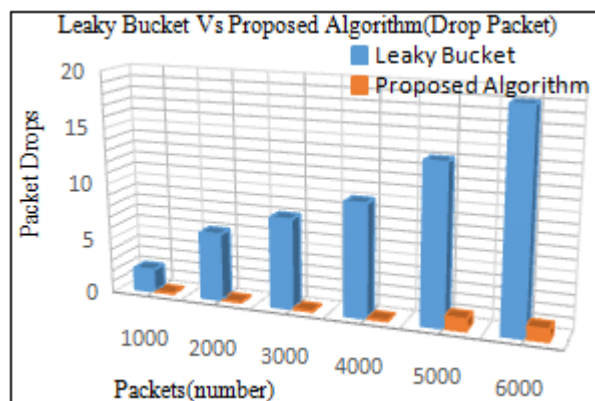

Figure 12: Leaky Bucket vs. Proposed Algorithm (packet drops)

Here leaky vs. proposed algorithm in terms of drop packets is showing. In the graph when 1000 packet send the drop packets is 2 for Leaky bucket and 0 for proposed algorithm. When 6000 packet send the drop packets is about 19 for Leaky bucket and 1 for proposed algorithm. So, In Leaky bucket the number of packets drop is increasing more than the proposed algorithm when the amount of packet is increased. That means less packet drop is happen in proposed algorithm.

5.3 Performance Comparison for 2000 Packets

Table 1: Performance comparison for 2000 Packets

Performance (%)	Leaky Bucket	Proposed Algorithm
Delay	2%	0.55%
Drop Packets	0.003%	0%

6. Conclusion

Vehicular Ad Hoc Networks (VANETs) provide one of the most emergent fields for research due to the high interest that Intelligent Transportation Systems (ITS) can offer in different sectors of our lives through the proper use of VANETs. It is such an emerging technology that enables a wide range of applications such as vehicle collision avoidance and road safety purpose by exchanging warning messages across vehicles and also that the VANET should increase the features by means of value-added services like navigation and location based services on road. To facilities' those services the proposed bandwidth optimization technique used to provide an improved and secure inter-vehicular communication to optimize the performance of VANETs. The effectiveness of the new bandwidth optimization technique in terms of time delay and number of packets drop can redirect a new way towards optimization development in network communication. Comparing others, it can be said that the working process of the algorithm is far better. With a view to different measurements, the new bandwidth optimization technique will be effective for pursuing optimizing platform.

References

[1] Hartenstein, Hannes, and L. P. Laberteaux. "A tutorial survey on vehicular ad hoc networks." IEEE Communications magazine 46, no. 6 (2008): 164-171.

[2] Bhoi, S. K., P. M. Khilar, M. Singh, R. R. Sahoo, and R. R. Swain. "A routing protocol for urban vehicular ad hoc networks to support non-safety applications." Digital Communications and Networks 4, no. 3 (2018): 189-199.

[3] Hussain, Syed Asad, Muddesar Iqbal, Atif Saeed, Imran Raza, Hassan Raza, Amjad Ali, Ali Kashif Bashir, and Adeel Baig. "An efficient   channel access scheme for vehicular ad hoc networks." Mobile Information Systems 2017 (2017).

[4] Liang, Wenshuang, et al. "Vehicular ad hoc networks: architectures, research issues, methodologies, challenges, and trends." International Journal of Distributed Sensor Networks 11.8 (2015): 745303.

[5] Anwer, M. Shahid, and Chris Guy. "A survey of VANET technologies." Journal of Emerging Trends in Computing and Information Sciences 5, no. 9 (2014): 661-671.

[6] DhilipKumar, V., D. Kandar, and C. K. Sarkar. "Enhancement of inter-vehicular communication to optimize the performance of 3G/4G-VANET." Optical Imaging Sensor and Security (ICOSS), 2013 International Conference on. IEEE, 2013.

[7] Guy, Pujolle,"Metamorphic Networks", Journal of Computing Science and Engineering 7.3 (2013): 198-203.

[8] Medhi, Deepankar,"Network routing: algorithms, protocols, and archi-tectures", Morgan Kaufmann, 2010.

[9] Farzanegan, Mahmoud Daneshvar, HosseinSaidi, and Mehdi Mahdavi,"A Scheduling Algorithm for Bursty Traffic: Controlling of Service Rate and Burst", Arabian Journal for Science and Engineering 39.6 (2014): 4753-4764

[10] Nakibly, Gabi,"Traffic Engineering Algorithms for IP and MPLS Networks: Novel and practical algorithms for routing optimization of large operational networks", Scholars Press, 2014.

[11] Ash, Gerald R.,"Traffic Engineering and QoS Optimization of Inte-grated Voice and Data Networks", Morgan Kaufmann, 2006.

[12] Dainotti, Alberto, Antonio Pescape, and Kimberly C. Claffy,"Issues and future directions in traffic classification", Network, IEEE 26.1 (2012): 35-40.

[13] Elhanany, Itamar,"High-performance packet switching architectures", Springer 2007.

[14] Androulidakis, Iosif I.,"PBX Security and Forensics: A Practical Ap-proach", Springer Science and Business Media, 2012.

[15] Md.Torikur Rahman, Md.JulkarNayeenMahi, and MilonBiswas " Performance Evaluation of a Portable PABX System Through Developing New Bandwidth Optimization Technique", International Conference on Electrical Engineering and Information and Communication Technology (ICEEICT), 2015.

[16] Raya, Maxim, and Jean-Pierre Hubaux. "Securing vehicular ad hoc networks." Journal of computer security 15, no. 1 (2007): 39-68.

[17] Samara, Ghassan, Wafaa AH Al-Salihy, and R. Sures. "Security analysis of vehicular ad hoc nerworks (VANET)." In Network Applications Protocols and Services (NETAPPS), 2010 Second International Conference on, pp. 55-60. IEEE, 2010.

[18] Md.Torikur Rahman, Md.JulkarNayeenMahi, "Proposal for SZRP Pro-tocol with the Establishment of the Salted SHA-256 Bit HMAC PBKDF2 Advance Security System in a MANET", International Conference on Electrical Engineering and Information and Communication Technology (ICEEICT), 2014.

Author Profile

Md. Torikur Rahman completed his B.Sc. and M.Sc. degree in Information Technology (IT) from Institute of Information Technology, Jahangirnagar University, Bangladesh. Presently, he serves as a Lecturer in the Department of Computer Science and Engineering, Uttara University, Bangladesh. He actively participated in number of national/ international conferences, seminars, workshops and journals. His current research interests are mainly in Telecommunication, Wireless Communications, Distributed Computer Networks, Network Security, Security Technique, Software Engineering, Software Architecture, Systems Designs and Algorithm Development, Embedded Systems, Big Data Management, and Bio -informatics.