ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

Region-Based Secure Emergency Message Broadcasting In VANET

Dr.S.Soundararajan.Ph.D, P.K.Logapriya, A.Ramaleela, A.H.Suvesha

Professor, Department of Computer Science and Engineering, Velammal Institute of Technology, Chennai, Tamilnadu, India

UG Student, Department of Computer Science and Engineering, Velammal Institute of Technology, Chennai, Tamilnadu, India

ABSTRACT: The Vehicular Ad-Hoc Network (VANET), is a technology that uses moving cars as nodes in a network to create a mobile network. VANET turns every participating car into a wireless router or node and allowing cars at an approximate distance of 100 to 300 meters of each other to connect and in turn, produce a network with a large range. Since the network is open and accessible from everywhere in the VANET, it is expected to be an easy target for malicious users An attacker can pass false traffic information to discourage other vehicles using the road. A malicious node can generate a false packet in the network and create virtual jamming. An attacker will use VANET‘s shared data to trace somebody. Therefore, a symmetric cryptographic scheme known as DES algorithm has been introduced, whereas in this scheme a secret key has been used to encrypt and decrypt messages which provide the security in broadcasting the messages in VANET. Also considering the latency issue in message broadcasting, the proposed system will broadcast the secure message only to the region of interest or the region with high risk. Hence the proposed scheme will avoid both the latency and security issues occurred during the broadcast of emergency messages in VANET.

KEYWORDS: VANET, DES, SECURE.

I. INTRODUCTION

VANET is a term used to describe the spontaneous ad hoc network formed over vehicles moving on the roadway.VANETs are characterized by high mobility, rapidly changing topology etc. VANETS are considered as one of the most prominent technologies for improving the efficiency and safety of modern transportation systems. For example, vehicles will communicate detour, traffic accident, and congestion info with near vehicles early to reduce traffic congestion near the affected areas. It’s essentially a network of cars that are in constant communication.

Each automobile is aware of where it is, where it’s going and basically any other quantity that it can measure. Not only has every car been made “self-aware”, but it can also communicate with any other car on the road. If all the cars know where all other cars are, the cars headed for an imminent crash can warn their respective drivers and even apply autonomous control to avoid accidents. The dynamic nature of the vehicular ad-hoc network (VANET) imposes a lot of challenges in privacy preservation of credential or a data where there exist a set of intermediate vehicular nodes, which could not have the interest to work for providing services to different nodes within the network. The attacker may try to reveal the data. A major challenge in protocol design is how to develop reliable routing protocols for comfort applications to ensure that broadcasted messages are securely and successfully disseminated to all the other vehicles in a VANET.There are Some of the security requirements to be satisfied by the VANET. a)Authentication: It provides us a guarantee that data is engendered by an authentic client. b)Integrity: It ensures that the data at the sender and recipient side are the same. Alteration of the message is completed by approved users only. Recipient utilizes a similar procedure as used at sender facet to form a second digest from the message for comparing it with the initial message. This procedure ensures the integrity in data. So, we must always get to shield all messages against alteration attacks. c)Non-Repudiation: This avoids frauds from refusing their offenses because in this even if the attack occurs, it

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

will expedite the capability to recognize attackers. d)Availability: Vehicular networks will need real-time for many purposes so they must be accessible all the time. e)Confidentiality: All driver's privacy ought to be confined. This security demand is to ensure that information can barely be read by approved users.

Here comes the problem arising during data dissemination and data sharing , such as 1)False Information generated by the attacker: An attacker can pass false traffic information like a jam is ahead but no jam in the road to discourage other vehicles using the road, 2)Generate Intelligent Collision: An attacker can inject intelligent collision 3)Jamming: A malicious node can generate false packets in the network and create virtual jamming 4) Tracking: An attacker can use VANET's shared information to track someone. Some of the possible security attacks are. A) DOS attack: This attack forbids the arrival of critical information by taking authority of resources of vehicles or by jamming the channel utilized by the Vehicular Network. B) Sybil attack: In this attack, attacker convinces the vehicles to take an alternate path by creating a large number of pseudonymous, and tell other vehicles about jam by claiming more than a hundred vehicles ahead. C) Replay Attack: This attack confounds the authorities and prevents vehicles identification in a hit and run accident by replaying transmission of previous data to seize benefit of the circumstances of the message at sending time. D) Routing attack: This attack either disturbs routing process of network or plunges the packets by exploiting the susceptibility of network
layer routing protocols. Black hole attack, warm hole attack, and grey hole attacks are the most common routing attacks in VANETs. E) Timing attack: Broadcasting of security message to the vehicle at the right time is one of the imperative requirements of VANET. Timing attack includes several timeslots to the message which leads to receiving of the message via a vehicle in accidental location rather than a safe location. F) Eavesdropping: This attack violates the confidentiality property and belongs to the attack network layer. A major target of this attack is to acquire access to private data. G)Location Trailing: This attack violates private property. In this, the attacker traces the vehicle and gets the confidential information about the driver by illegal trailing of the position or route followed by the car. H) Fake Information: In this, the Attacker transmits fake data in the network for its own profit. For paradigm, a nasty node can transmit fake data of intense traffic due to a mishap over road along with clearing his way. This is obviously a serious security hazard Thus there is the need for fast advancement and pervasive deployment in VANET that have faced various security threats and privacy concerns.

In this paper, we survey security aspects of Vehicular Adhoc Network (VANET) by implementing using DES algorithm. The Data encryption standard could be a block cipher, meaning a cryptographic key and algorithm are applied to a block of data simultaneously rather than one bit at a time. To encrypt an understandable text message, DES groups it into 64-bit blocks. Each block is enciphered using the secret key into a 64-bit ciphertext by means of permutation and substitution. The process involves sixteen rounds and might run in four completely different modes, encrypting blocks singly or creating every cipher block dependent on all the previous blocks. In our proposed framework we will be developed in java net beans environment.

II. LITERATURE REVIEW

In 2006, Sangho Oh Winlab et.al [23] provides the scalability of message flooding protocols in networks with various node densities, which can be expected in vehicular scenarios. Vehicle safety application requires reliable delivery of warning messages to nearby and approaching vehicles. Due to potentially large distances and shadowing the delivery protocol must forward messages over multiple hops, thereby increasing network congestion and packet collisions

In 2007, Feilong Tang et.al [22] proposes the topology of a vehicular ad hoc network (VANET) changes rapidly due to high-speed movement of vehicles, so traditional mobile ad hoc network (MANET) broadcast protocol may not work efficiently in VANET. This paper proposes a distance-based broadcast protocol called Efficient Directional Broadcast (EDB) for VANET using directional antennas. In EDB, only the furthest receiver is responsible to forward the packet in the opposite direction where the packet arrives.

In 2010, Celimuge Wu et.al [17] proposes much safety in Vehicular Ad hoc Networks (VANETs) are based on

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

the broadcast. Designing a broadcast protocol that satisfies VANET applications requirements is very crucial. In this paper, we propose a reliable and efficient multi-hop broadcast routing protocol for VANETs. The proposed protocol provides strict reliability in various traffic conditions. This protocol also performs low overhead by means of reducing rebroadcast redundancy in a high-density network environment.

In 2012, Yong Li et.al [11] presents the transmission opportunities between mobile nodes, the routing in delay-tolerant networks (DTNs) exploits the mechanism of opportunistic forwarding. Energy-efficient algorithms and policies for DTN are crucial to maximizing the message delivery probability while reducing the delivery cost. In this contribution, we investigate the problem of energy- efficient optimal beaconing control in a DTN. We model the message dissemination under variable beaconing rate with a continuous-time Markov model. Based on this model, we then formulate the optimization problem of the optimal beaconing control for epidemic routing and obtain the optimal threshold policy from the solution of this optimization problem.

In 2014, Tim Leinmüller et.al [10] provides inter-vehicle to roadside communication (V2X communication) allow both passenger safety and driving comfort to be improved significantly. For example, a vehicle detecting an icy road could inform the following vehicles and thereby prevent accidents. Vehicle to roadside communication could be used near construction sites to warn the vehicle driver about a reduced number of lanes or to give him advice for an alternative route. For improved traffic efficiency, vehicles could exchange the latest traffic flow information. The advantages of V2X communication have been recognized in many regions of the world.

In 2018, Hany F.Atlam et.al [2] considered the rapid the growth of the Internet of Things (IoT) applications, the classic centralized cloud computing paradigm faces several challenges such as high latency, low capacity, and network failure. To address these challenges, fog computing brings the cloud closer to IoT devices. The fog provides IoT data processing and storage locally at IoT devices instead of sending them to the cloud. In contrast to the cloud, the fog provides services with faster response and greater quality. Therefore, fog computing may be considered the best choice to enable the IoT to provide efficient and secure services for many IoT users. This paper presents the state-of-the-art of fog computing and its integration with the IoT by highlighting the benefits and implementation challenges.

In 2018, Hina Tabassum et.al [3] Providing network connectivity to mobile users is a key requirement for cellular wireless networks. User mobility impacts network performance as well as user perceived service quality. For efficient network dimensioning and optimization, it is therefore required to characterize the mobility-aware network performance metrics such as the handoff rate, handoff probability, sojourn time, direction switch rate, and users' throughput or coverage. This characterization is particularly challenging for heterogeneous, dense/ultra-dense, and random cellular networks such as the emerging 5G and beyond 5G (B5G) networks.

III. PROPOSED SYSTEM

In the proposed system, a new position based protocol is used to broadcast secure emergency message in VANET environment. By this system, messages are broadcasted only in their region of interest so that delivery latency will be decreased. If a vehicle in the environment detects a dangerous event, it immediately generates and broadcasts an emergency message to vehicles in the region of interest, so that the vehicles can take preventive measures to avoid an accident. Once the messages are generated to the corresponding event, the messages are encrypted by using the DES algorithm, such that the attacker would not intrude to modify the message and cause an attack. Thus, these encrypted messages will be broadcasted to vehicles which are needed to take action to avoid an accident. In VANET environment it is a great challenge to deliver messages to right vehicles without delivery latency. Although various protocols proposed to broadcast emergency message in VANET environment they suffer problems, like some protocols required collecting nearby secure information to broadcast message which again increases delivery latency. Here the proposed methodology will be suitable for scenarios like vehicles applying emergency brake, lane change triggering during ambulance arrival and vehicle overtaking.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

IV. ARCHITECTURE

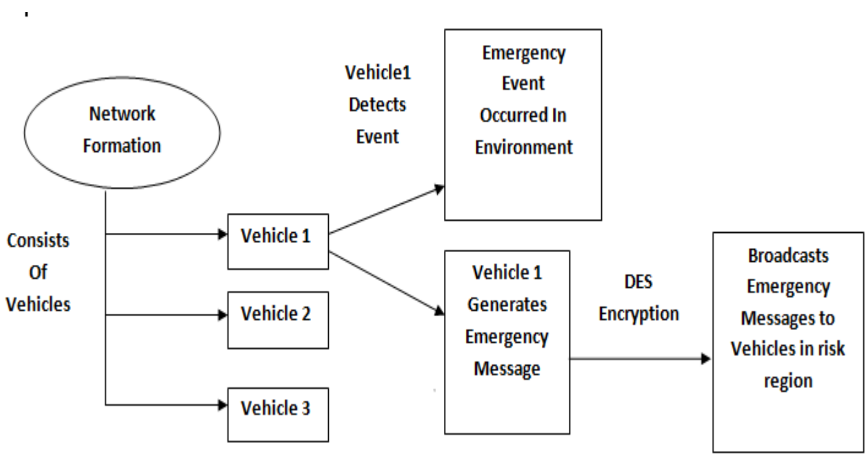

Fig 1.1 Illustration of the system model

After the formation of the VANET network, consider in the environment there are three vehicles then any emergency event has been occurred to a vehicle 1 then the vehicle 1 will broadcast the encrypted emergency message to their neighbouring vechicles to reduce the accidents. This incident was illustrated in Fig 1.1.

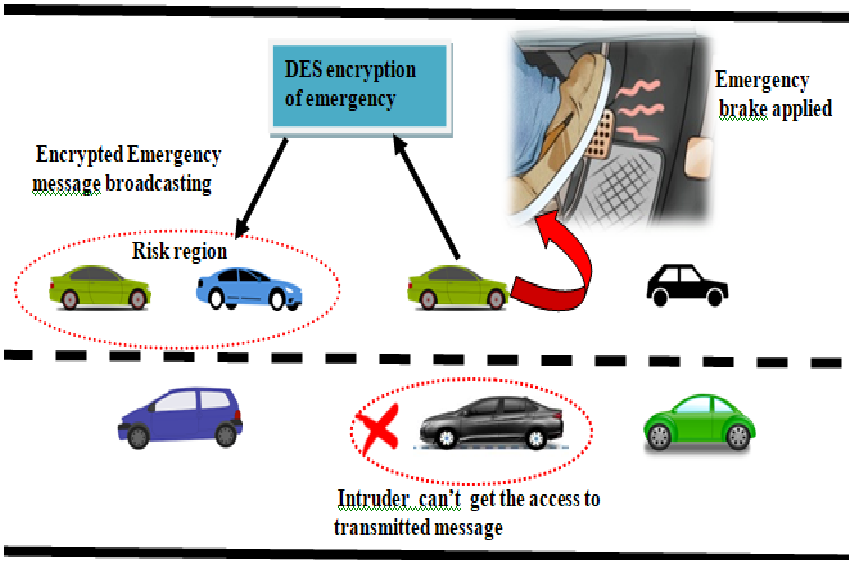

Fig 2.1 Illustration of the system working model

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

In this Fig 2.1, to reduce accidents whenever any vechicle applies the emergency brake then that the applied vechicle will broadcast the event to the neighbouring vehicle specifically located at the risk region.On receiving the message the neighbour vehicle will take the actions correspondingly. Also the emergency messages are being encrypted through DES algorithm so the intruders are not able to change or steal the life saving messages.

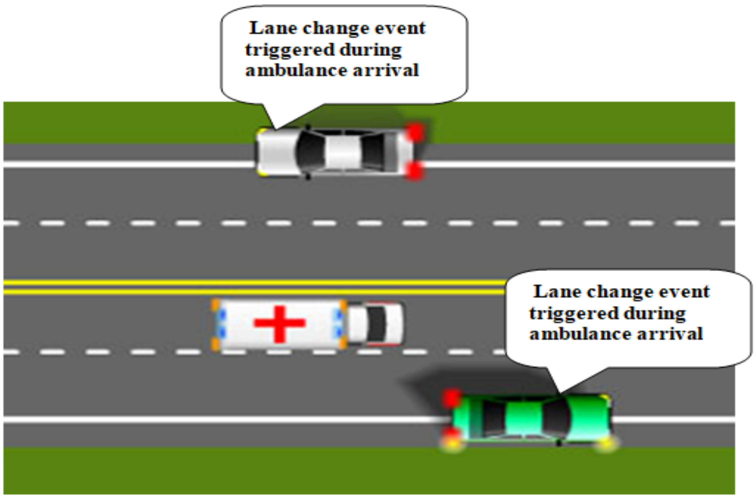

Fig 2.2 Illustration of the system working model

In VANET environment on any arrival of the ambulance, the vehicles on the road will be receiving the message regarding that the arrival of the ambulance. The vehicles which received the message will changes their lane on the road. This is the incident has been illustrated in the above Fig 2.2.

V. MODULE DESCRIPTION

a)Network Formation:
In this module, we create a network consisting of nodes. Each node acts as a vehicle and has its own distance and range. We create nodes by giving latitude and longitude as input which in turn describes the vehicle location. Each node will be dynamic in a position that is changing its position dynamically. We create 'n' the number of nodes based on our requirement to form network environment or network formation.

b)Neighbor Calculation:
After network formation based on each node latitude and longitude neighbor calculation will be calculated. We calculate neighbor to send messages among nodes and communicate among them. Data will be sent to the destination from source via neighbors if both source and destination are not within their communication range.

c)Emergency Event Occurred:
In VANET environment many emergency events can occur like for example Partial Brake, Emergency Brake, and Overtaking etc. When an emergency event occurs it creates chaos in the environment. Based on the emergency event occurred an emergency message will be created.

d)Broadcasting Emergency Message:
After an emergency event occurred an emergency message will be created by the vehicle. Emergency message will be created based on the type of event occurred. Many emergency events may occur in the environment. For example events like a sudden break, Partial Brake, Overtaking, ambulance takeover etc are some of the examples of the emergency event. If a vehicle detects a dangerous event, it immediately generates and broadcasts an emergency

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

message to the vehicles in the region of interest (or target region with safety risks), such that the nearby vehicles can take effective actions to avoid a traffic accident. In essence, the emergency message, which contains life-critical and time-sensitive information, should be disseminated to all targeted vehicles in a very efficient and effective.

VI. RESULTS

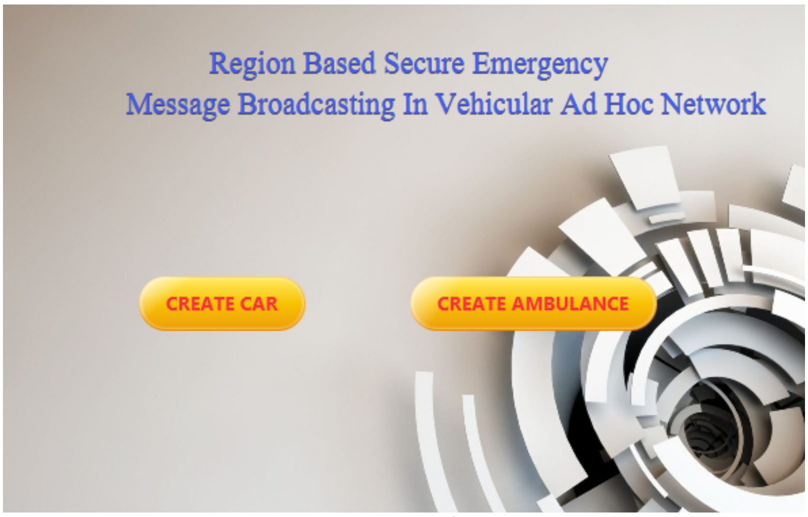

Fig 3.1 Illustration of home page

In the above Fig 3.1 illustrates that the home page for creating the cars and the ambulance in the VANET environment

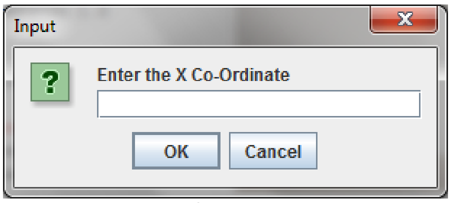

Fig 3.2.1 Illustration of entering the X coordinates

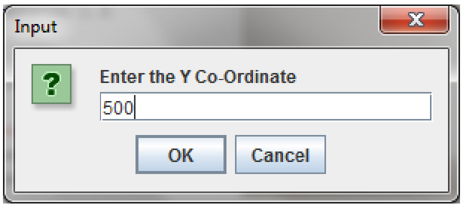

Fig 3.2.2 Illustration of entering the Y coordinates

Fig 3.2.1,Fig 3.2.2 Illustrates for placing the created vehicles in the VANET environment by entering the coordinates of X and Y values which will be the lattitude and longitude position of the vehicles.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

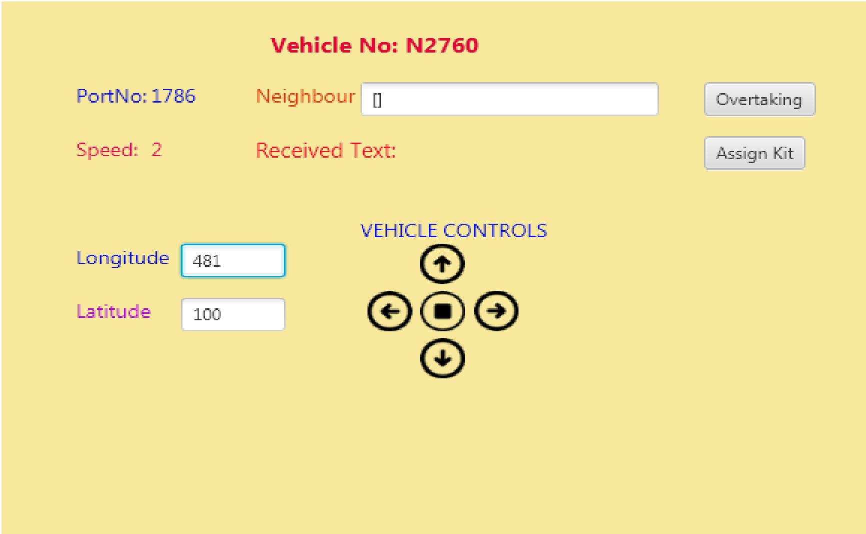

Fig 3.3 Illustration of the car node without neighbour

After creating and placing the car node in the VANET environment. The created car can have their vehicle number and information about their neighbouring car node and then the information about any emergency event will be displayed on this page. This page is illustrated in the above Fig 3.3

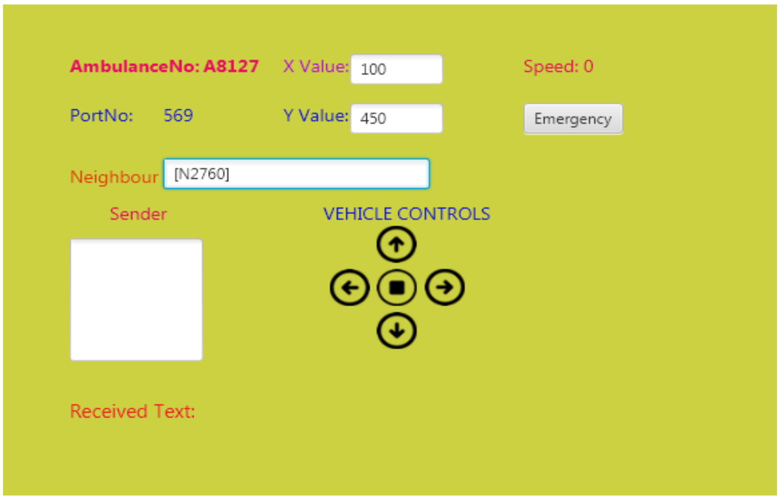

Fig 3.3 Illustration of the Ambulance Node With Neihgbour

The above figure illustrates the controller box of the ambulance node . The created ambulance can have their vehicle number,latitude longitude position,port number which is for communication between vehicles,speed of the vehicle ,arrows for directing the vehicle, information about their neighbouring car node and then the information about any emergency event will be displayed on this page.Whenever the emergency button is clicked it will generates emergency messages and broadcast to the neighbour vehicles ,which in turn changes their lane and give way to ambulance.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

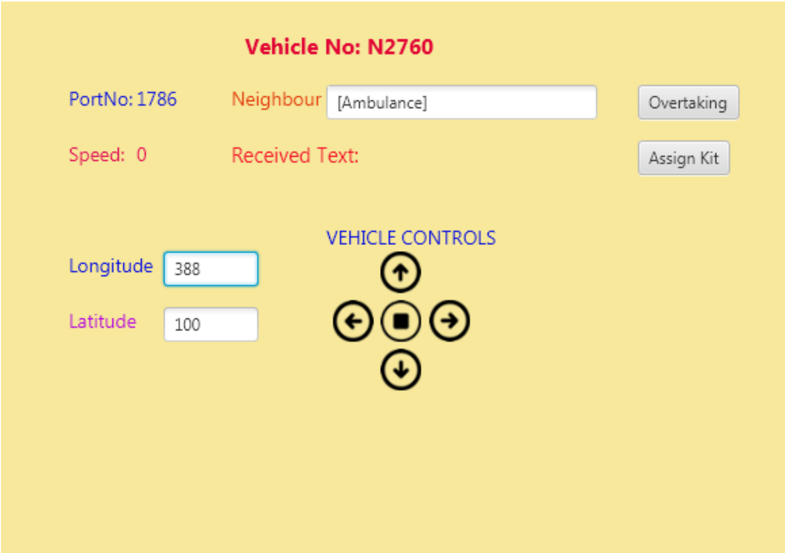

Fig 3.4 Illustration of the Car Node with neighbor

After creating and placing the vehicle node in the VANET environment. The created vehicle can have their vehicle number and information about their neighbouring vehicle node and then the information about any emergency event will be displayed on this page.

Fig 3.4 Illustration of the VANET Environment

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

Above figure represents the virtual VANET Environment where we can find the created nodes performing its functionalities assigned to it.

VII. CONCLUSION

Thus we have proposed a position-based broadcast protocol for secure emergency messages propagation in VANETs environment. By this scheme, the vehicles just depend on the information including in a received message to judge whether to rebroadcast the message, which can reduce the delivery latency and driver will have more time to take actions to avoid accident happening. Since messages are just broadcasted along their regions of interest, the proposed protocol can efficiently reduce unnecessary rebroadcasts and collisions. It is concluded that whenever any vehicle does an emergency action which in turn securely broadcast the emergency message in advance to the neighbor vehicle which is at risk. So that the accidents will be reduced.

VIII. ACKNOWLEDGMENT

We are grateful to the almighty for the successful completion of this paper. Special appreciation goes to professor Dr.S.Soundararajan, of Velammal Institute of Technology and everyone who provided their contribution and assistance throughout the project.

REFERENCES

1. Daxin Tian, Chao Liu, Xuting Duan, Zhengguo Sheng, Qiang Ni, Min Chen, Victor C. M. Leung “A Distributed Position-Based Protocol for Emergency Messages Broadcasting in Vehicular Ad Hoc Networks” Published in IEEE Internet of Things Journal 2018.
2. Hany F.Atlam, Robert J. Walters 1 and Gary B. Wills(2018) “Fog Computing and the Internet of Things”.
3. Hina Tabassum, Mohammad Salehi, and Ekram Hossain(2018) “Mobility-Aware Analysis of 5G and B5G Cellular Networks”.
4. Hany F.Atlam, Robert J. Walters 1 and Gary B. Wills(2018) “Fog Computing and the Internet of Things”.
5. M. Chen, Y. Hao, L. Hu, K. Huang, and V. K. N. Lau, “Green and mobility-aware caching in 5G networks,” *IEEE Trans. Wireless Commun.*, vol. 16, no. 12, pp. 8347–8361, Dec. 2017.
6. X. Hou *et al.*, “Vehicular fog computing: A viewpoint of vehicles as the infrastructures,” *IEEE Trans. Veh. Technol.*, vol. 65, no. 6, pp. 3860–3873, Jun. 2016.
7. M. Chen *et al.*, “Mobility-aware caching and computation offloading in 5G ultra-dense cellular networks,” *Sensors*, vol. 16, no. 7, 2016, Art. no. E974.
8. D. Tian, J. Zhou, Y. Wang, G. Zhang, and H. Xia, “An adaptive vehicular epidemic routing method based on attractor selection model,” *Ad Hoc Netw.*, vol. 36, pp. 465–481, Jan. 2016.
9. H. Yoo and D. Kim, “ROFF: Robust and fast forwarding in vehicular ad-hoc networks,” *IEEE Trans. Mobile Comput.*, vol. 14, no. 7, pp. 1490–1502, Jul. 2015.
10. Tim Leinmüller, 1Robert K. Schmidt, 1Bert Böddeker, 2Roger W. Berg and 3Tadao Suzuki(2014)“A GLOBAL TREND FOR CAR 2 X COMMUNICATION
11. Y. Li et al., “Optimal beaconing control for epidemic routing in delay-tolerant networks,” IEEE Trans. Veh. Technol., vol. 61, no. 1, pp. 311–320, Jan. 2012.
12. J. Sahoo, E. H.-K. Wu, P. K. Sahu, and M. Gerla, “Binary-partitionassisted MAC-layer broadcast for emergency message dissemination in VANETs,” *IEEE Trans. Intell. Transp. Syst.*, vol. 12, no. 3, pp. 757–770, Sep. 2011.
13. M. B. Yassein, S. F. Nimer, and A. Y. Al-Dubai, “A new dynamic counter-based broadcasting scheme for mobile ad hoc networks,” *Simulat. Model. Pract. Theory*, vol. 19, no. 1, pp. 553–563, 2011.
14. D. C. Thomas and A. Agarwal, “An information propagation scheme for VANETs,” in *Proc. Intell. Transp. Syst.*, 2005, pp. 155–160. [24] M. Bakhouya, J. Gaber, and P. Lorenz, “An adaptive approach for information dissemination in vehicular ad hoc networks,” *J. Netw. Comput. Appl.*, vol. 34, no. 6, pp. 1971–1978, 2011.
15. M. Fukushima, “The latest trend of V2X driver assistance systems in Japan,” *Comput. Netw. Int. J. Comput. Telecommun. Netw.*, vol. 55,no. 14, pp. 3134–3141, 2011.
16. C. Weiß, “V2X communication in Europe—From research projects towards standardization and field testing of vehicle communication technology,” *Comput. Netw.*, vol. 55, no. 14, pp. 3103–3119, 2011.
17. Celimuge Wu, Kazuya Kumekawa And Toshihiko Kato(2010).” A Novel Multi-hop Broadcast Protocol for Vehicular Safety Applications”.
18. K. A. Hafeez, L. Zhao, Z. Liao, and B. N.-W. Ma, “A new broadcast protocol for vehicular ad hoc networks safety applications,” in *Proc. Glob. Commun. Conf. (GLOBECOM)*, Miami, FL, USA, Dec. 2010, pp. 1–5.
19. F. F. Hassanzadeh and S. Valaee, “Reliable broadcast of safety messages in vehicular ad hoc networks,” in *Proc. IEEE INFOCOM*, Rio de

Janeiro, Brazil, 2009, pp. 226–234.

20. Y.-T. Yang and L.-D. Chou, "Position-based adaptive broadcast for inter-vehicle communications," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, Beijing, China, 2008, pp. 410–414
21. [Online]. Available: http://www.who.int/mediacentre/factsheets/fs358/en/
22. D. Li, H. Huang, X. Li, M. Li, and F. Tang, "A distance-based directional broadcast protocol for urban vehicular ad hoc network," in *Proc. Int. Conf. Wireless Commun. Netw. Mobile Comput.*, Shanghai, China, 2007, pp. 1520–1523.
23. S. Oh, J. Kang, and M. Gruteser, "Location-based flooding techniques for vehicular emergency messaging," in *Proc. 3rd Int. Conf. Mobile Ubiquitous Syst. Netw. Services*, San Jose, CA, USA, 2006, pp. 1–9.

.