http://www.jctjournals.com

ISSN(ONLINE):2278 - 3814

Volume-12, Issue-10, October 2023

JOURNAL OF COMPUTING TECHNOLOGIES (JCT)

International Journal

Page Number: 01-06

An Efficient Approach for Secure Message Dissemination with HDL based Wireless Control Protocol over VANET:- A Review

[1]*Sarita Marskole*, [2]*Prof. Nishi Pandey*, [3]*Prof. Abhishek Agwekar*

[1] *M.Tech Scholar*, [2]*Assistant Professor* ,[3]*Head of department*

[1, 2, 3] *TIEIT Bhopal, M.P., India*

Abstract— Several vehicular ad hoc network (VANET) thinks about have concentrated on specialized strategies in view of IEEE 802.11p, which frames the standard for remote access for vehicular conditions. A wide assortment of uses for street security and activity productivity are expected to answer the dire call for more quick witted, greener, and more secure versatility. In spite of the fact that IEEE 802.11p is considered as the true standard for out and about correspondences in vehicular environment, partners have as of late researched the ease of use of Long Term Evolution (LTE) to help vehicular applications. Secure communication between vehicle and Infrastructure/Road side unit (V to I/R) over VANET and identifying accurate attacker vehicle is a major challenge over VANET in modern age.In this thesis, implementing efficient encryption techniques i.e. AES and RSA algorithm and design Hardware description language based wireless control protocol in Xilinx environment. In wireless control also include ODMRP protocol configuration model for VANET simulation. Throughput, time, packet delivery ratio etc, are main parameter of this work.

Keywords : Long Term Evolution (LTE), vehicular ad hoc network (VANET), AES and RSA

I. INTRODUCTION

Vehicular ad hoc networks (VANETs) are used for communication between vehicles and roadside equipment. Intelligent vehicular ad hoc networks (InVANETs) are a kind of artificial intelligence that helps vehicles to behave in intelligent manners during vehicle-to-vehicle collisions, accidents. Vehicular ad hoc networks (VANETs) are utilized for correspondence among vehicles and roadside gear. Astute vehicular ad hoc networks (InVANETs) are a sort of man-made reasoning that encourages vehicles to act in insightful conduct amid vehicle-to-vehicle impacts, mishaps. Smart telephone ad hoc networks (Ranges) use the current equipment (fundamentally Bluetooth and Wi-Fi) in financially accessible advanced mobile phones to make distributed networks without depending on cell transporter networks, wireless passages, or traditional system framework. Ranges vary from traditional center point and talked networks, for example, Wi-Fi Coordinate, in that they bolster multi-jump transfers and there is no thought of a gathering leader so companions can join and leave voluntarily without obliterating the system. Internet-based versatile ad-hoc networks (iMANETs) is a sort of wireless ad hoc arrange that bolsters Web conventions, for example, TCP/UDP and IP. The system utilizes a system layer directing convention to connect portable hubs and build up courses distributed and consequently. Hub-Spoke MANET – Numerous sub-MANETs might be associated in an exemplary Center Spoke VPN to make a topographically dispersed MANET. In such kind of networks typical ad hoc steering calculations does not have any significant bearing specifically? One execution of this is Diligent Framework's Cloud Relay.

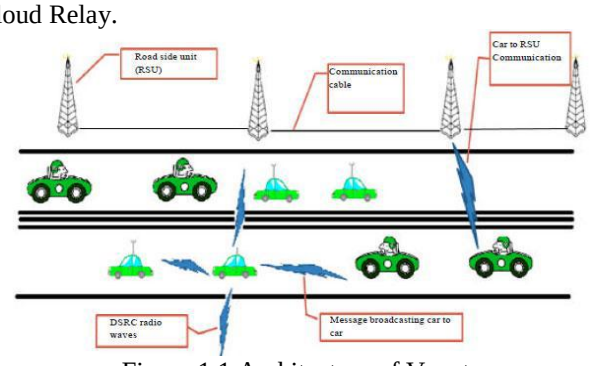

Figure 1.1 Architecture of Vanet

A. Vanet Architecture

A vehicular correspondence framework involves various interfacing substances that it is arrange extensively as: Users, Network hubs, and Authorities.

Correspondence examples of vehicles are following-

(i) Inter-vehicle correspondence

(ii)Vehicle-to-street side correspondence

(iii)Inter-street side correspondence

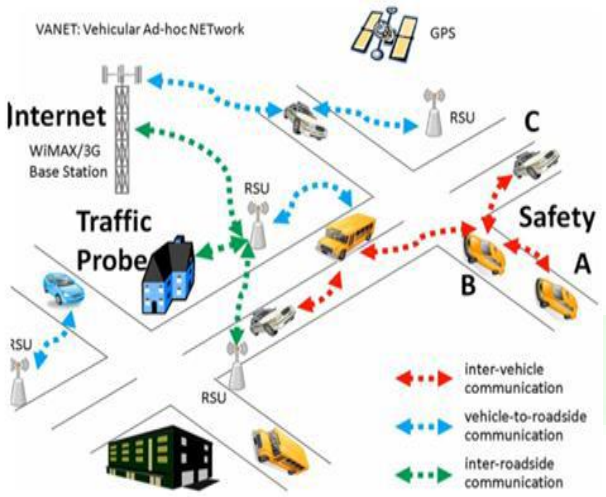

Figure 1.2 Communication pattern of vehicles

II. LITERATURE REVIEW

A. Review Of Secure Message Dissemination

[1] SeyhanUcar, Sinem ColeriErgen, and Oznur Ozkasap, Individual " Multihop Cluster-Based IEEE 802.11p and LTE Hybrid Architecture for VANET Safety Message Dissemination".IEEE transactions on vehicular technology, VOL. 65, no. 4, April 2016, Several vehicular ad hoc network (VANET) studies have focused on communication methods based on IEEE 802.11p, which forms the standard for wireless access for vehicular environments. In networks employing IEEE 802.11p only, the broadcast storm and disconnected network problems at high and low vehicle densities, respectively, degrade the delay and delivery ratio of safety message dissemination. Recently, as an alternative to the IEEE 802.11p-based VANET, the usage of cellular technologies has been investigated due to their low latency and wide-range communication. However, a pure cellular-based VANE communication is not feasible due to the high cost of communication between the vehicles and the base stations and the high number of handoff occurrences at the base station, considering the high mobility of the vehicles. This work proposes a hybrid architecture, namely, VMaSC-LTE, combining IEEE 802.11p-based multichip clustering and the fourth generation(4G) cellular system, i.e., Long-Term Evolution (LTE), with the goal of achieving high data packet delivery ratio (DPDR) and low delay while keeping the usage of the cellular architecture at a minimum level.

[2] X. Yue, B. Chen, X. Wang, Y. Duan, M. Gao and Y. He, "An Efficient and Secure Anonymous Authentication Scheme for VANETs Based on the Framework of Group Signatures," in IEEE Access, vol. 6, pp. 62584-62600, 2018,Vehicular ad hoc networks (VANETs) have stimulated interests in both academic and industry settings. Once deployed, they would bring a new driving experience to drivers. However, in an open-access environment, privacy is one of the greatest challenges, as drivers want to keep their personal information protected. Therefore, many authentication protocols have been proposed as solutions to the privacy issue. In most of the existing protocols, to prevent the revoked entity from generating a valid authentication information, the verifiers must frequently download the revocation list from one or more remote authorities to keep thelist up-to-date, which greatly increases the workload of the remote authority. In this work tocope with such challenging concerns, based on the idea of group signatures, it is propose a novel authentication protocol scheme by using the complete sub-tree method to achieve membership revocation, which ensures forward security.

[3] A. Tolba, "Trust-Based Distributed Authentication Method for Collision Attack Avoidance in VANETs," in *IEEE Access*, vol. 6, pp. 62747-62755, 2018.A vehicular ad hoc network (VANET) is a collection of mobile vehicles that aids roadside communication through vehicle-to-vehicle and vehicle-to-infrastructure operation modes. The network is autonomous and, hence, requires a wide range of security measures to protect its communications from attack. Recent studies on VANET security have focused on resolving the issues due to computation and distribution density of the vehicles. Probability distribution measures have been administered for detecting collision attacks, which increases the computational complexity. In this work a trust-based distributed authentication (TDA)method that relies on a global trust server and vehicle behavior for avoiding collision attacksis proposed. This method ensures both inter-vehicular and intra-vehicular communication security in the network. In addition, a channel state routing protocol (CSRP) is proposed toimprove the communication reliability among the vehicles. Reliable vehicles are identified according to the on-board unit (OBU) energy and the channel state of the vehicle to deliver seamless communication. The biased methods are assimilated to improve the communication reliability by avoiding collision attacks and improving secured packets flow in VANETs. In particular, the CSRP minimizes the energy exploitation of OBUs and time delay. TDA improves the security of the network by improving the collision recognition rate and the broadcast rate.

[4] C. Zhang, K. Chen, X. Zeng and X. Xue, "Misbehavior Detection Based on Support Vector Machine and Dempster-Shafer Theory of Evidence in VANETs," in *IEEE Access*,vol. 6, pp. 59860-59870, 2018.Vehicular ad hoc networks (VANETs) support safety and comfortable driving through frequent information exchange among intelligent vehicles. As an open access environment,VANETs are vulnerable to security threats, such as electronic attack and privacy disclosure. In this work it is propose a misbehavior detection mechanism based on a support vector machine (SVM) and Dempster–

Shafer theory (DST) of evidence to resist false message attack and message suppression attack. The proposed mechanism includes data trust mode land vehicle trust model. The data trust model uses an SVM-based classifier to detect false messages based on message content and vehicle attributes. The vehicle trust model consists of a local vehicle trust module and a trust authority (TA) vehicle trust module. The local vehicle trust module uses another SVM-based classifier to evaluate whether the vehicle is credible based on the behavior of the vehicle in terms of message propagation. Then, the TAvehicle trust module uses DST to aggregate multiple trust assessment reports about the same vehicle and derives a comprehensive trust value. Simulation results show that Gaussian kernel best fits our models compared with other functions. In addition, the true positive rateof our data trust model is higher than the model based on back propagation neural network. Moreover, our two models are more robust than basic majority voting, weighted voting, andBayesian inference in terms of true positive rate under various scenarios.

[5] S. Kanchan and N. S. Chaudhari, "SRCPR: Sign Re Crypting Proxy Re-Signature insecure VANET Groups," in IEEE Access, vol. 6, pp. 59282-59295, 2018.Vehicular Ad hoc Network is an emerging area as a key component of the intelligent transport system. Despite the immense researches going on in this area, it is yet to be deployed at its full scale due to lack of trust, safety, and confidentiality in the network. Moreover, the security algorithms proposed till now are complex, and calculations involved are difficult to be completed within the strict real-time constraints. This work introduces the SignRe Crypting Proxy Re-signature scheme, which reduces the time taken for encryption at sender side as well as for decryption at receiver side. Signcryption reduces the computation cost by converting two steps of signature and encryption into one, whereas re-encryption and re-signature enable Alice to decrypt and sign a message on behalf of Bob. These three terminologies altogether with group signature make the proposed algorithm robust, secure, and efficient. The compromised vehicle is revoked from group using dynamic accumulators, and security is verified using automated validation of Internet security protocols and applications.

[6] F. Qu, Z. Wu, F. Wang and W. Cho, "A Security and Privacy Review of VANETs,"in IEEE Transactions on Intelligent Transportation Systems, vol. 16, no. 6, pp. 2985-2996,Dec. 2015.

Vehicular ad hoc networks (VANETs) have stimulated interest in both academic and industry settings because, once deployed, they would bring a new driving experience to drivers. However, communicating in an open-access environment makes security and privacy issues a real challenge, which may affect the large-scale deployment of VANETs. Researchers have proposed many solutions to these issues. it is start this work by providing background information of VANETs and classifying security threats that challenge VANETs. After clarifying the requirements that the proposed solutions to security and privacy problems in VANETs should meet, on the one hand, it is present the general secure process and point out authentication methods involved in these processes. A detailed survey ofthese authentication algorithm followed by discussions comes afterward. On the other hand, privacy preserving methods are reviewed, and the tradeoff between security and privacy is discussed. Finally, it is provide an outlook on how to detect and revoke malicious nodes more efficiently and challenges that have yet been solved.

B. Review Of Fpga Based Wireless Control Protocol

[7] Slamet Indriyanto, Muhammad Najib Dwi Satria, Andira Rizky Sulaeman, Rifqy Hakimi, Eueung Mulyana "Performance Analysis of VANET Simulation on Software Defined Network" IEEE conference 2017

The rapid technology development in the transportation system is urgently needed today along with increasing number of vehicles. Vehicular Ad-Hoc Network (VANET) has-been viewed as one of the enabling technologies that provide a wide variety of services suchas vehicle road safety, enhancing traffic efficiency, reducing the level of accident and road congestion. In this work the authors demonstrate how VANET could be simulated on Software Defined Networking (SDN) emulator which is Mininet Wi-Fi and then measure the simulation performance namely delay, throughput, and packet drop between vehicles. Fullreachability between vehicles has been performed between the connected vehicles for the same Road Site Unit (RSU) and between two different RSUs.

[8] E. Kaljić and A. Akšamović, "Challenges in the design of the MAC protocols for wireless sensor networks using VHDL," 2014 X International Symposium on Telecommunications (BIHTEL), Sarajevo, 2014, pp. 1-6.In the design of MAC protocols for wireless sensor networks (WSN) it is necessary to fulfill some requirements such as low energy consumption, scalability, simplicity, etc. These requirements are not easy to fulfill from the viewpoint of implementation on FPGA or ASIC technologies. Therefore, in this work it is identify some challenges encountered during the design of MAC protocol for WSN. For some of these challenges, potential solutions are discussed. To illustrate the proposed solutions SMAC protocol is chosen. VHDL design ofthe S-MAC protocols are experimentally verified on the Altera EP2C5 FPGA development system.

[9] A. M. Bhavikatti and S. Kulkarni, "VHDL Modeling of Wi-Fi MAC Layer for Transmitter," 2009 IEEE International Advance Computing Conference, Patiala, 2009,pp. 1-5.For the wireless communication in radio frequency range, IEEE 802.11 is one of the many standards available. IEEE 802.11b defines the medium access control layer [MAC] for wireless local area networks. The wireless local area network, WLAN is dominated by IEEE802.11 standard. It becomes one of the main focuses of the WLAN research. Now most of the ongoing research projects are simulation based as their actual hardware implementation is not cost effective. The main core of the IEEE 802.11b standard is the CSMA\CA, Physical and MAC layers. But only MAC layer for transmitter is modeled in this work using theVHDL. The VHDL (Very High Speed Hardware Description Language) is defined in IEEE as a tool of

creation of electronics system because it supports the development, verification, synthesis and testing of hardware design, the communication of hardware design data and the maintenance, modification and procurement of hardware. It is a common language for electronics design and development prototyping. The main purpose of the IEEE 802.11standard is to provide wireless connectivity to devices that require a faster installation, such as Laptops, PDA's or generally mobile devices inside a WLAN. MAC procedures are defined here for accessing the physical medium, which can be infrared or radio frequency. Here WiFi MAC transmitter module is divided in to 5 blocks i.e. data unit interface block, controller block, pay load data storage block, MAC header register block, data processing block. In this work, it is are considering only two blocks i.e pay load data storage block & data processing block. So other blocks i.e. data unit interface block, controller block, MAC header register block are not discussed further in this work.

[10] J. E. O. Reges and E. J. P. Santos, "A VHDL CAN Module for SmartSensors," 2008 4th Southern Conference on Programmable Logic, San Carlos deBariloche, 2008, pp. 179-182.Communication modules are required for smart sensors interface with the sensor network. In this work, a VHDL (VHSIC hardware description language) implementation of a CAN (controller area network) interface for smart sensors is presented. The scope of this work is the medium access control (MAC) sub layer. Therefore, it deals with the transfer protocol, control of frames, arbitration, error checking and error signaling. In accordance with the CAN protocol (versions 2.0 A and 2.0 B), the interface can be divided into blocks to perform various communication tasks. In the implementation presented in this work, each block is a VHDL project entity described in the behavioral style. The performance of each entity is analyzed separately. Next, all entities are interconnected in the structural style. The final description has been synthesized into a Xilinxreg Spartan-Il XC2S50 FPGA. Finally, a comparison between this implementation and the HurriCANe, a freely available core, is performed

III. PROBLEM IDENTIFICATION

Message Authentication and Integrity: Message ought to be ensured against any modification and in this manner the beneficiary of a message ought to verify the sender of the message. However respectability doesn't basically suggest recognizable proof of the sender of the message. Message Non-Repudiation: The sender can't preclude from securing sent a data message. Substance Authentication: The recipient isn't exclusively guaranteed that the sender produced a message, however furthermore has confirmation of the likeness of the sender. Access Control: Access to particular administrations gave by the foundation hubs, or distinctive hubs, is chosen locally by police. As a piece of access administration, approval sets up what each hub is permitted to attempt and do in VANET. Accessibility: The system and applications should remain operational even inside the nearness of deficiencies or malevolent conditions. Obligation Identification: Users of vehicles are at risk for their consider or coincidental activities that disturb the operation of different hubs, or the transportation framework. Versatility: The fundamental thought from Ad Hoc Networks is that every hub in the system is portable, and can move starting with one place then onto the next inside the scope territory, yet at the same time the portability is restricted, in Vehicular Ad Hoc Networks hubs moving in high versatility.

VANETs are required to help a wide assortment of utilizations, running from wellbeing identified with notice and other esteem included administrations. Be that as it may, beforeputting such applications into training, distinctive security issues, for example, validness and trustworthiness must be explained in light of the fact that any pernicious conduct of clients. Its predictable that VANETs will consolidate an assortment of remote techniques for transmission utilized by Quiet and in view of various sorts of correspondence media, for example, WAVE, Security Issues in Vehicular Specially appointed Systems infrared, cell phone, 5.9 GHz Committed Short-Range Correspondence (DSRC), WiMAX, Satellite, Bluetooth, RFID, and so forth. The present condition of every one of these guidelines is trialuse along these lines, the field of vehicular applications and advancements will be founded on an entomb disciplinary exertion from the divisions of correspondence and systems administration, car gadgets, street operation and administration, and data and administration provisioning.

IV. PROPOSED METHODOLOGY

A. Flow Chart

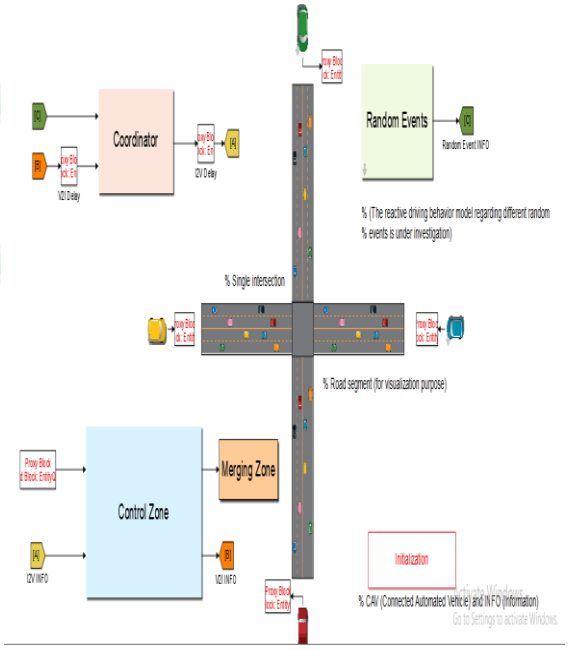

Fig 4.1 Flow chart of proposed method

So the following steps are involving for security.

1) RSA Algorithm

2) AES(Advance encryption standard)

B. RSA Algorithm

RSA incorporates an open key and a private key. General society key can be known by everyone and is used for scrambling messages. Messages encoded with the all inclusive community enter must be unscrambled in a sensible measure of time using the private key. The keys for the RSA estimation are delivered the going with way:

1. Choose two particular prime numbers p and q. For security purposes, the number's p and qought to be picked aimlessly, and ought to be of comparable piece length.
2. Compute n = pq. n is utilized as the modulus for both the general population and private keys. Its length, normally communicated in bits, is the key length.
3. Compute φ(n) = φ(p)φ(q) = (p − 1)(q − 1) = n - (p + q 1), where φ is Euler's totient work.
4. Choose a whole number e with the end goal that 1 < e <φ(n) and gcd(e, φ(n)) = 1; i.e., eand φ(n) are co prime. e is discharged as people in general key example .e having a short piece length and little Hamming weight brings about more productive encryption – most ordinarily 216 + 1 = 65,537. Notwithstanding, considerably littler estimations of e, (for example, 3) have been appeared to be less secure in a few settings.
5. Determine d as d ≡ e−1 (mod φ(n)); i.e., d is the multiplicative backwards of e (modulo ϕ (n)). This is all the more plainly expressed as: explain for d given d·e≡ 1 (mod φ(n)). Thisis frequently processed utilizing the broadened Euclidean calculation. Utilizing thepseudocode in the Secluded whole numbers area, inputs an and n compare to e and φ(n),individually. d is kept as the private key example.

People in general key comprises of the modulus n and the general population (or encryption) example e. The private key comprises of the modulus n and the private (or decoding) type d,which must be kept mystery. p, q, and φ(n) should likewise be kept mystery since they can be utilized to ascertain d.

The Advanced Encryption Standard (AES) is the most noteworthy standard of the piece figures, so its security is of foremost significance. In any case, the key timetable of AES has an unmistakable shortcoming that specifically helps the execution of best assaults. To battlethese shortcomings, it is propose an alternate way to deal with the AES Key Calendar outline. it is show that it stays away from the shortcoming of the current key timetable. The examination of frail key calendars has prompted the rules for powerful key timetable plan that gets from surely understood and acknowledged outline standards for piececalculations in the more extensive sense. Our outline takes after these key timetable rules.

V. CONCLUSION

It is analyzed a robust and scalable geographic multicast protocol and security algorithm in VANET. In this, both data packets and control messages are transmitted along efficient treelike paths without the need of explicitly creating and maintaining a tree structure. In this work presented, performance of ODMRP routing protocol are compared in terms of the performance parameters such as packet delivery ratio, Average end to end delay and routing overhead by using MATLAB and VHDL, Xilinx for different number of nodes (25, 50,75,100) for pause times 2 Secs. From the results it is clear that at low mobility rate ODMR Performs better in case of packet delivery ratio but it performs poorly in terms of average end to end delay and routing overhead. At high network load and mobility ODMRP performs well with respect to packet delivery ratio and average end to end delay. However it is clearthat when mobility is low, ODMRP performs well among the three and when mobility is high MAODV performs well. In simulation results, achieve, much higher packet delivery ratio and lower control overhead, average path length and average joining delay when compared with other protocol by varying moving speeds, node densities, group sizes and network ranges. ODMRP is based on mesh (instead of tree) forwarding. It applies on demand (as opposed to periodic) multicast route construction and membership maintenance. Simulation results show that ODMRP is effective and efficient in dynamic environments and scales well to a large number of multicast members. The advantages of ODMRP are:

- Low channel and storage overhead
- Usage of up-to-date and shortest routes
- Robustness to host mobility

Maintenance and exploitation of multiple redundant paths Scalability to a large number of nodes It has presented the implementation of wireless control protocol on FPGAs using VHDL. The proposed network architecture has different layer modules, and it is possible to easily increase or decrease the number of signals as well as layers. FPGAs can be used for portable, modular, and reconfigurable hardware solutions for wireless networks. Simulation results (using ISIM) of the FPGA implementation of the wireless controller have shown a satisfactory accuracy.

REFERENCES

[1] SeyhanUcar, SinemColeriErgen, and OznurOzkasap, Individual " MultihopCluster-Based IEEE 802.11p and LTE Hybrid Architecture for VANET SafetyMessage Dissemination".IEEE transactions on vehicular technology, VOL. 65, no. 4, April2016

[2] X. Yue, B. Chen, X. Wang, Y. Duan, M. Gao and Y. He, "An Efficient and SecureAnonymous Authentication Scheme for VANETs Based on the Framework of GroupSignatures," in IEEE Access, vol. 6, pp. 62584-62600, 2018.

[3] A. Tolba, "Trust-Based Distributed Authentication Method for Collision Attack Avoidance in VANETs," in IEEE Access, vol. 6, pp. 62747-62755, 2018.

[4] C. Zhang, K. Chen, X. Zeng and X. Xue, "Misbehavior Detection Based on SupportVector Machine and Dempster-Shafer Theory of Evidence in VANETs," in IEEE Access,vol. 6, pp. 59860-59870, 2018.

[5] S. Kanchan and N. S. Chaudhari, "SRCPR: SignReCrypting Proxy Re-Signature inSecure VANET

Groups," in IEEE Access, vol. 6, pp. 59282-59295, 2018.
[6] KhaleelMershad and Hassan Artail "A System for Secure and Proficient InformationObtaining in Vehicular Specially appointed Systems." IEEE Exchanges On VehicularInnovation, Vol. 62, No. 2, February 2013
[7] SlametIndriyanto, Muhammad Najib DwiSatria, Andira Rizky Sulaeman, Rifqy Hakimi, Eueung Mulyana "Performance Analysis of VANET Simulation on SoftwareDefined Network" IEEE conference 2017
[8] E. Kaljić and A. Akšamović, "Challenges in the design of the MAC protocols for wireless sensor networks using VHDL," 2014 X International Symposium on Telecommunications (BIHTEL), Sarajevo, 2014, pp. 1-6.
[9] A. M. Bhavikatti and S. Kulkarni, "VHDL Modeling of Wi-Fi MAC Layer forTransmitter," 2009 IEEE International Advance Computing Conference, Patiala, 2009, pp.1-5.
[10] J. E. O. Reges and E. J. P. Santos, "A VHDL CAN Module for Smart Sensors," 20084th Southern Conference on Programmable Logic, San Carlos de Bariloche, 2008, pp. 179-182.
[11] Z. Stamenkovic, "A novel MAC protocol for industrial WLAN: Hardwareaspects," 2018 13th International Conference on Design & Technology of IntegratedSystems In Nanoscale Era (DTIS), Taormina, 2018, pp. 1-1.
[12] S. K. Shah and D. D. Vishwakarma, "FPGA implementation of ANN for reactiverouting protocols in MANET," 2012 IEEE International Conference on Communication, Networks and Satellite (ComNetSat), Bali, 2012, pp. 11-14.
[13] S. K. Shah and D. D. Vishwakarma, "FPGA implementation of ANN for reactiverouting protocols in MANET," 2012 IEEE International Conference on Communication, Networks and Satellite (ComNetSat), Bali, 2012, pp. 11-14.
[14] A. Rathinam, V. Natarajan, S. Vanila, A. Viswanath and M. S. Guhan, "An FPGA Implementation of Improved AODV Routing Protocol for Route Repair Scheme," 2008First International Conference on Emerging Trends in Engineering and Technology, Nagpur, Maharashtra, 2008, pp. 971-974.
[15] Vishnu Mandava, Kiran Gururaj, L. Zakrevski and DurgaMisra, "VLSI design ofstability routing protocol for sensors in MANETs," International Conference on InformationTechnology: Research and Education, 2003. Proceedings. ITRE2003., Newark, New Jersey,USA, 2003, pp. 147-151.
[16] X. Lin, X. Sun, P.- H. Ho, and X. Shen, "GSIS: A protected and security safeguardingconvention for vehicular interchanges," IEEE Trans. Veh. Technol., vol. 56, no. 6, pp.3442– 3456, Nov. 2007.

