http://www.jctjournals.com

ISSN(ONLINE):2278 - 3814

Volume-12, Issue-11, November 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

[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— A few years ago, the automotive field of IoT was considered a theoretical concept; Today we already see the possibility of not only driving without a car, but also the use of IoT in smart cars, including parking, Safety Protection. It protects the environment, life and traffic flow. We found that there is an urgent need to implement simple and effective security techniques in vehicular ad hoc networks (VANETs) to ensure fast mobility of network nodes and leverage the base station gateway along the path of taking the process to different VANETs. This will reduce the communication overhead initialization time and security key initialization each time the node moves to a new station area. In this work, we use security techniques used in sensor networks to implement VANET security, and simulation analyzes show that the communication is secure and successful and can be inherited from other sub-VANETs. The contribution of this paper is to improve the scheduling process with as little cryptographic computational overhead as possible and to make it suitable for high mobility using security procedures in VANETs; It guarantees security by allowing rapid authentication from one VANET to another depending on its direction in the traffic network.

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

I. INTRODUCTION

Infrastructure. Aside from wellbeing measures, VANET likewise offers some benefit included administrations like email, sound/video sharing and so forth. Dedicated Short Range Communication (DSRC) is the recurrence band that is utilized as a DSRC conveys security and non wellbeing messages in whole system by utilizing its security and non security channels. Non wellbeing applications are identified with solace of the travelers and to enhance the movement framework. Stopping accessibility and toll accumulation administrations are cases of these applications. Security is a critical issue particularly in this sort of system where one changed message can makes issue for the clients from numerous points of view. Aggressors make issue specifically and in a roundabout way by propelling diverse sort of assaults. DSRC likewise bolsters utilization of understood Internet conventions for the Network and Transport layers, i.e., Internet Protocol rendition 6 (IPv6), User Datagram Protocol (UDP) and Transmission Control Protocol (TCP). These conventions, characterized by the Internet Engineering Task Force (IETF), are steady and very much reported in different spots.

Modulation Technique	Coded Bit Rate (Mbps)	Coding Rate	Data Rate (Mbps)	Data Bits per OFDM Symbol
BPSK	6	1/2	3	24
BPSK	6	3/4	4.5	36
QPSK	12	1/2	6	48
QPSK	12	3/4	9	72
16-QAM	24	1/2	12	96
16-QAM	24	3/4	18	144
64-QAM	36	2/3	24	192
64-QAM	36	3/4	27	216

Figure 1.1. Data Rate Options in a DSRC 10 MHz OFDM Channel

The blockage and related vehicle convenience issue is joined by a steady danger of mischances also. Wireless access in vehicular condition (WAVE) is a multi-channel approach, held for one control channel from 5.855 to 5865 GHz, for high accessibility, low inertness vehicle wellbeing correspondences . An improvement was required on IEEE 802.11standard to help applications from the

ISSN(ONLINE):2278 - 3814

Intelligent Transportation Systems (ITS) . The 802.11p standard is implied for VANET correspondence and utilizations Dedicated Short Range Communication (DSRC) range.

Figure 1.2. Traffic conditions of different cities or country

VANET security applications rely upon the trading of wellbeing data among vehicles (C2C correspondence) or between vehicle to foundation (C2I Communication) utilizing the control channel. RSA is one of the essential practicable open key cryptosystems and is for the most part used for secure data transmission [5]. In such a cryptosystem, the encryption key is open and complexities from the unscrambling key which is kept puzzle.

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

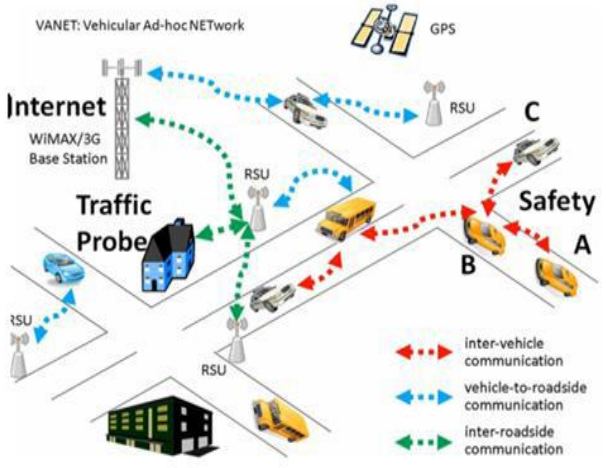

Figure 1.3 Communication pattern of vehicles

II. LITERATURE REVIEW

[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.

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

So the following steps are involving for security.

1) RSA Algorithm

2) AES(Advance encryption standard)

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 q ought 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., e and 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)). This is frequently processed utilizing the broadened Euclidean calculation. Utilizing the pseudocode 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 battle these 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 piece calculations in the more extensive sense. Our outline takes after these key timetable rules.

ADVANCED ENCRYPTION STANDARD

AES is a symmetric square figure with a piece size of 128 bits. Key lengths can be 128 bits,192 bits, or 256 bits; 8 called AES-128, AES-192, and AES-256, individually. AES-128utilizations 10 rounds, AES-192 utilizations 12 rounds, and AES-256 utilizations 14 rounds. The primary circle of AES9 plays out the accompanying capacities:
Sub Bytes () Shift Rows () Mix Columns () Add Round Key ()
The initial three elements of an AES round are intended to cryptanalysis through the strategies for "disarray" and "dissemination." The fourth capacity really scrambles the information. Dissemination implies designs in the plaintext are scattered in the ciphertext .Perplexity implies the relationship between the plaintext and the cipher text is clouded.
An easier approach to see the AES work request is:
1. Scramble every byte (SubBytes).
2. Scramble every line (ShiftRows).
3. Scramble every section (MixColumns).
4. Scramble (AddRoundKey).
A term connected with AES is "the State," a 'middle cipher,'11 or the ciphertext before the
last round has been connected. AES designs plaintext into 16 byte (128-piece) squares, and
regards every piece as a 4x4 State cluster. It then performs four operations in each round. The
exhibits contains line and section data utilized as a part of the operations, particularly
Mix Columns() and Shift rows().

PROCESS OF PROPOSED WORK

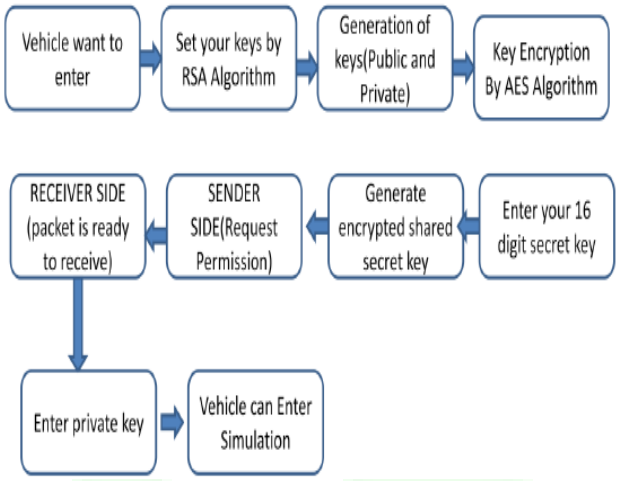

Figure 4.6 Steps of proposed work

Step 1: Set keys by RSA Algorithm (Enter prime number for p and q)
Step 2:Generation of keys and key generationn time
Step 3: Vehicle side- Key Encryption By AES Algorithm
Enter your 16 digit secret key
16 digit final key
ASCII Code of the entered Message
Encrypted shared secret key, cipherdata
Define an arbitrary series of 16 plaintext bytes
% in hexadecimal (string) representation
% in the AES-Specification
Step 4: SENDER SIDE
Enter the message to encrypt with symmetric key
Convert plaintext into hexadecimal ,
This is your final message
Convert the plaintext to ciphertext,
% using the expanded key, the S-box, and the polynomial transformation matrix
disp (' ')
Display cipherdata
Step 5: Receiver Side
Packet is ready to receive
use private key to decrypt received message
Convert the ciphertext back to plaintext
% using the expanded key, the inverse S-box,
% and the inverse polynomial transformation matrix
Message decryption time

ISSN(ONLINE):2278 - 3814

In case of wrong private key-you may be attacker or use decryption key and Last chance to
press your private key to decrypt message
key decryption time
Convert the ciphertext back to plaintext
% using the expanded key, the inverse S-box,
% and the inverse polynomial transformation matrix
message decryption time
Step 6 : vehicle running environment

V. SIMULATION AND RESULT

In this section, the performance of all the approaches will be analyzed and compared. Toexamine the performance in various environmental scenarios, it is necessary to implement alarge geographical deployment, which requires numerous vehicles and is generally toocostly. Design of VANET in HDL simulation, VHDL wireless control protocol in Xilinx and secure communication in CAN toolbox.

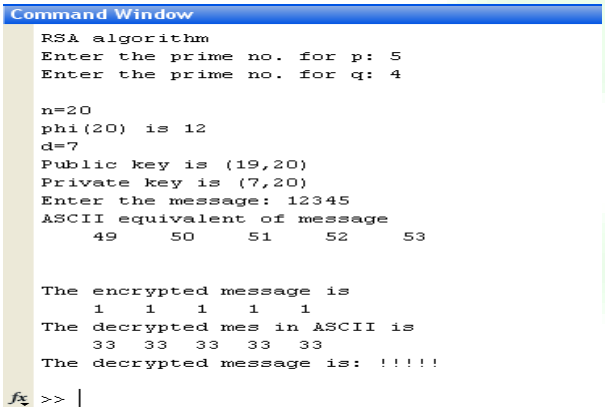

Fig 5.1 Proposed Algorithm for Security

In above figure it is showing name of the author and just for press enter key our code will bestarted.

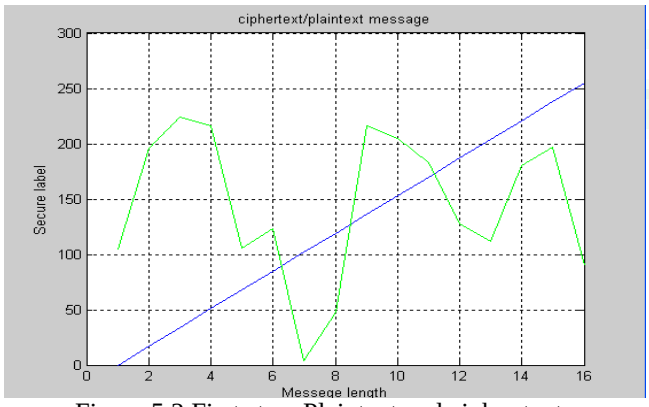

Figure 5.2 First step_Plaintext and cipher text

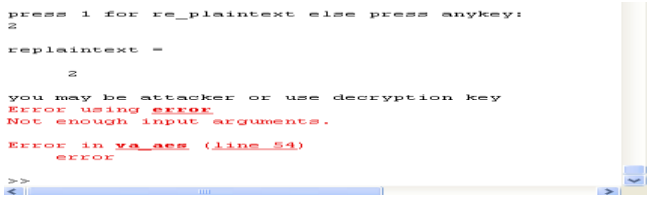

Figure 5.3 When Unauthorized communication
In above figure it is showing if person is unauthorized and he has no decryption key.

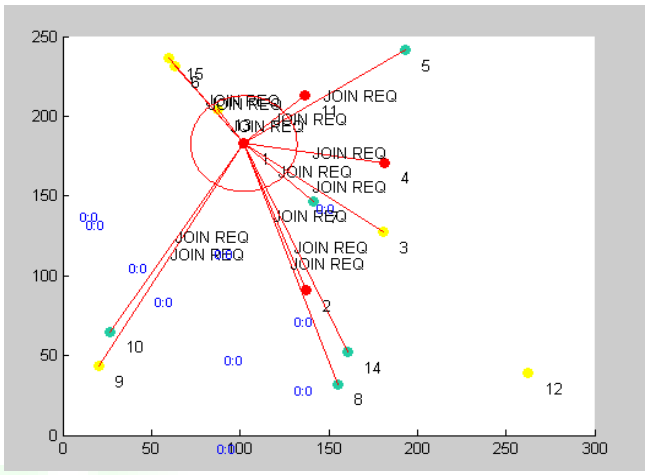

Figure 5.4: Joining request of VANET simulation

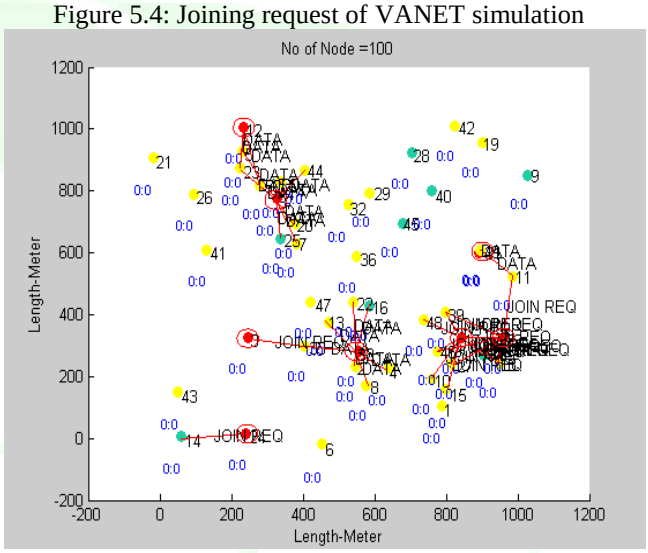

Figure 5.5: 100 Node Simulation of VANET using ODMRP

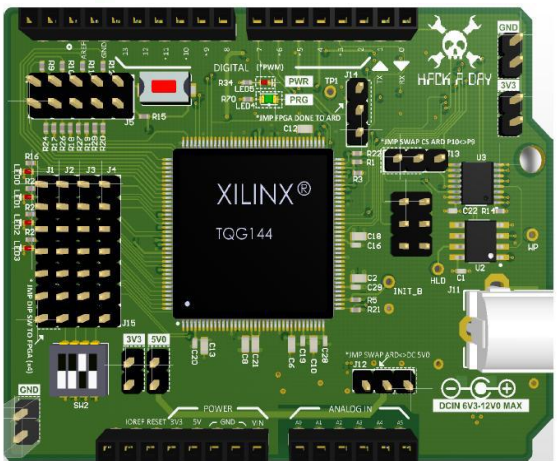

Figure 5.6 Xilinx FPGA Chip design

The Xilinx Alliance Program is an ecosystem of qualified IP providers, system integrators,and hardware suppliers that can accelerate your design productivity and get you to

ISSN(ONLINE):2278 - 3814

market faster. Alliance Program members are equipped to maximize the advantages of Xilinx Devices in developing market- and domain-specific solutions. A field-programmable gate array (FPGA) is an integrated circuit (IC) that can be programmed in the field after manufacture. FPGAs are similar in principle to, but have vastly wider potential application than, programmable read-only memory (PROM) chips. FPGAs are used by engineers in the design of specialized ICs that can later be produced hard-wired in large quantities for distribution to computer manufacturers and end users. Ultimately, FPGAs might allow computer users to tailor microprocessors to meet their own individual needs. Xilinx Smarter Solutions for backhaul applications enable operators to benefit from smooth capacity upgrades encompassed by increased network intelligence.

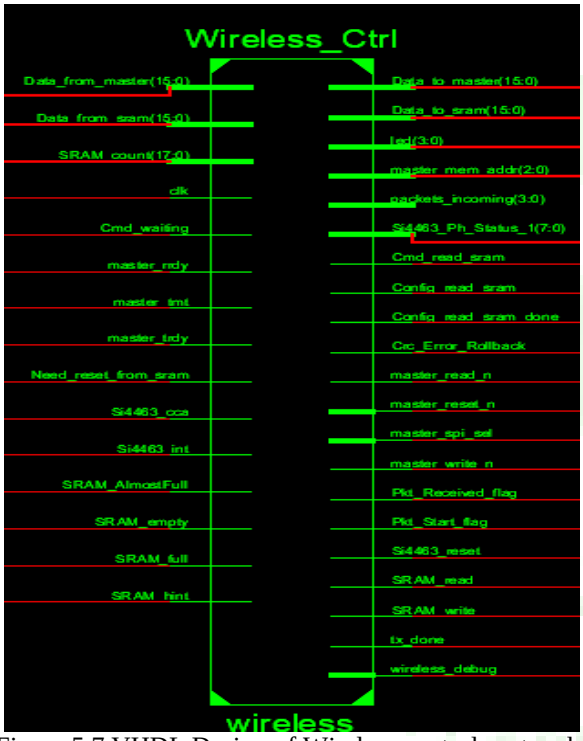

Figure 5.7 VHDL Design of Wireless control protocol

RESULT ANALYSIS

Table I shows different parameters which included in simulation duration.

Table-5.1: Simulation parameters

System Environment	Windows 10
Time	100 ms to 1000 ms
Node	100
Protocol	ODMRP
Length	1200-1200

Table II shows different protocol comparison by using different author.

Table-5.2: Comparison of Different Protocol

AUTHOR	PROTOCOL	PERFORMANCE
Hafez Seliem	Mac & Vdnet	60 S
Jos´E Grimaldo	AODV, OLSR, DSR,	1 S To 300 S
Forough Goudarzi	Routing Protocol	800 S
Bhuvaneswari Madasamy	MGOR	100s
Guiyang Luo	Sdnmac	300s

Packet Delivery Ratio (Throughput)= Data Rcvd / Data Sent

Control Overhead= Ctrl Bytes Sent / Data Bytes Rcvd

Forwarding Efficiency= Data + Ctrl Packets Sent / Data Packets Rcvd

Total Aggregated Traffic= Data + Ctrl PktsTx And Relayed / Ctrl + Data Pkts Rx

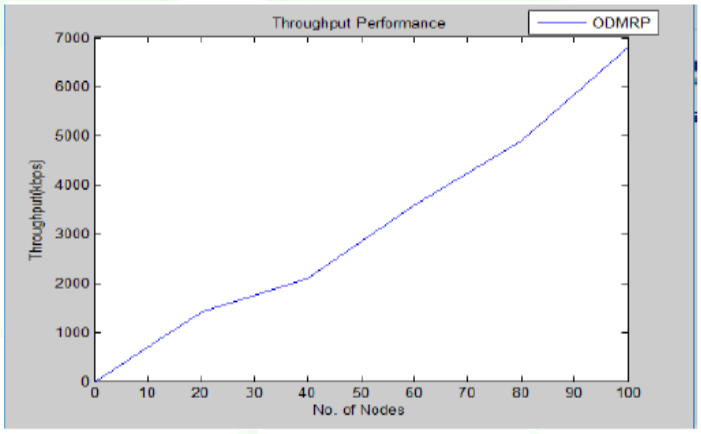

Figure 5.8: Throughput Performance

Figure 5.8 shows the performance of data rate or throughput. This is calculated by number of bits transmitted per second in ODMRP Protocol network.

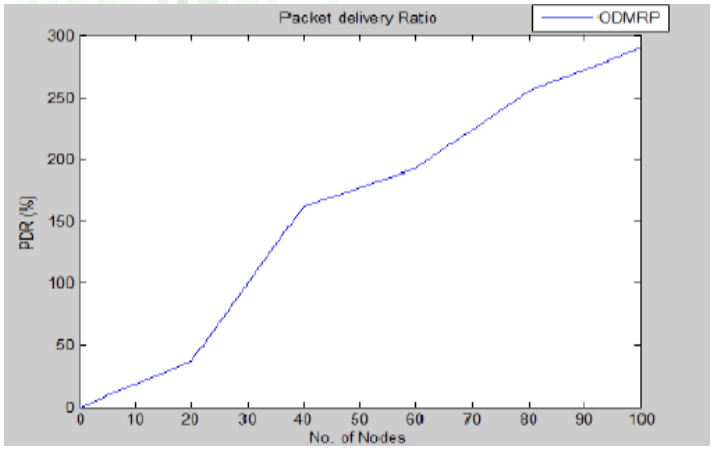

Figure 5.9 Packet Delivery Ratio

Figure 5.9 shows the performance of packet delivery ratio by using following formula Packet Delivery Ratio (Throughput)= Data Rcvd / Data Sent.

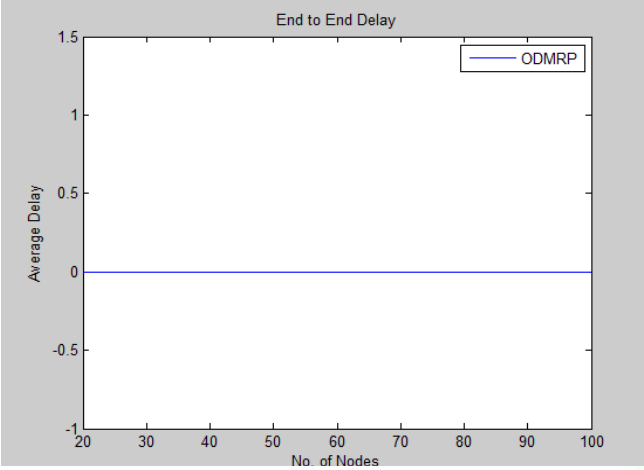

Figure 5.10 End to End Delay

Figure 5.10 shows the performance of average delay and end to end delay. Table 5.3 Comparative execution time (in seconds) and buffer size of encryption algorithms

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.

