International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 6 Issue: 12 17 - 21

An Efficient Approach for Secure Message Dissemination with HDL based Wireless Control Protocol over VANET

Pawandeep Singh Chhabra
M.Tech Scholar
Department of Electronics and Communication
TIT Engineering College, Bhopal(M.P.)

Prof. Divya Jain
Assistant Professor
Department of Electronics and Communication
TIT Engineering College, Bhopal(M.P.)

***Abstract*—**Several vehicular ad hoc network (VANET) have focused on specific techniques in perspective of IEEE 802.11p, which outlines the standard for remote access for vehicular conditions. A wide combination of employments for road security and movement profitability are relied upon to answer the desperate call for all the more sharp, greener, and increasingly secure adaptability. Regardless of the way that IEEE 802.11p is considered as the genuine standard for all over the place correspondences in vehicular condition, accomplices have starting late inquired about the usability of Long haul Development (LTE) to encourage vehicular applications. Secure correspondence among vehicle and Framework/Street side unit (V to I/R) over VANET and distinguishing exact assailant vehicle is a noteworthy test over VANET in current age. In this paper, executing productive encryption systems i.e. AES and RSA calculation and plan Equipment portrayal dialect based remote control convention in Xilinx condition. In remote control likewise incorporate ODMRP convention arrangement model for VANET simulation. Throughput, time, packet delivery ratio etc, are main parameter of this work.

***Keywords*- -** *AES, VANET, MANET, IEEE, LTE, V to I/R, ODMRP.*

*****

I. INTRODUCTION

In Currently, the increasing number of vehicles has caused some problems. One of them is a traffic jam and often accidents occurred, so these problems lead to a need of a technological system that can help us reducing those negative effects. Intelligent Transportation System (ITS), one of promising answers, is a combination of intelligent transportation system with information technology to improve accessibility, efficiency and security of transportation. ITS technology could provide real-time information to road users related to the road situation such as when there are traffic accidents or congestions occurred on a particular road area. The presence of this technology could give solutions or alternatives for road users can avoid the traffic jam. ITS also can support information about the condition of existing vehicles for the vicinity, so it can help users to avoid the accident. One of ITS technologies that is still in development is Vehicular Ad-Hoc Network (VANET) [1].

VANET right now still has a few deterrents to its improvement that requires much expense for advancement and testing. So far there is still no nation that has truly connected the VANET framework industrially. On the other hand, the advancement and research about VANET is as yet ongoing in spite of the fact that VANET arrange displaying has been done as simulation [1]. The incessant trade of routing vectors or connection state tables, activated by continuous topology changes, yields unnecessary channel and preparing overhead. Restricted data transmission, constrained power, and versatility of system has make the multicast protocol configuration especially difficult. To beat these limitations, we have built up the on-Demand Multicast Routing Protocol (ODMRP). ODMRP applies on-demand routing methods to dodge channel over head and enhance versatility. It utilizes the concept of sending bunch [5], a lot of hubs responsible for sending multicast information on most limited ways between any part matches, to manufacture a sending network for each multicast gathering.

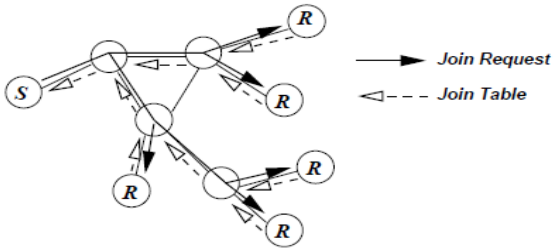

Figure1: On-Demand Procedure for Membership Setup and Maintenance.

II. REVIEW

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.

The RSA count incorporates three phases: key age, encryption and unscrambling. RSA incorporates an open key and a

private key. The overall public key can be known by everyone and is used for scrambling messages. Messages mixed with individuals as a rule enter must be decoded in a sensible measure of time using the private key [7].The advancement and wide use of remote correspondence advances have changed human lives by giving the most accommodation and adaptability ever in getting to Internet administrations and different applications. Of late, analysts conceptualized conveying vehicles, offering ascend to vehicular specially appointed systems (VANETs), which are the fundamental concentration of designers who long to transform autos into clever machines that impart for wellbeing and solace purposes.

In the plan of Macintosh conventions for remote sensor systems (WSN) it is important to satisfy a few prerequisites, for example, low vitality utilization, adaptability, effortlessness, and so on. These prerequisites are difficult to satisfy from the perspective of execution on FPGA or ASIC innovations. Along these lines, in this work it is distinguish a few difficulties experienced amid the structure of Macintosh convention for WSN. For a portion of these difficulties, potential arrangements are talked about. To outline the proposed arrangements SMAC convention is picked. VHDL plan of the S-Macintosh conventions is tentatively confirmed on the Altera EP2C5 FPGA advancement framework.

III. PROPOSED WORK

The fundamental commitments of this thesis can be outlined as takes after.

1) It is propose a novel approach for clients to begin their associations in the VANET security.

3) it is clarify hybrid cryptographic approach that gives significantly higher safety efforts contrasted with existing ones and break down the execution of our approach utilizing scientific and recreation implies.

3) Simulate vehicle ad hoc network model using HDL and Simulink.

4) Design VHDL wireless control protocol architecture for FPGA Xilinx system.

IV. FLOW CHART

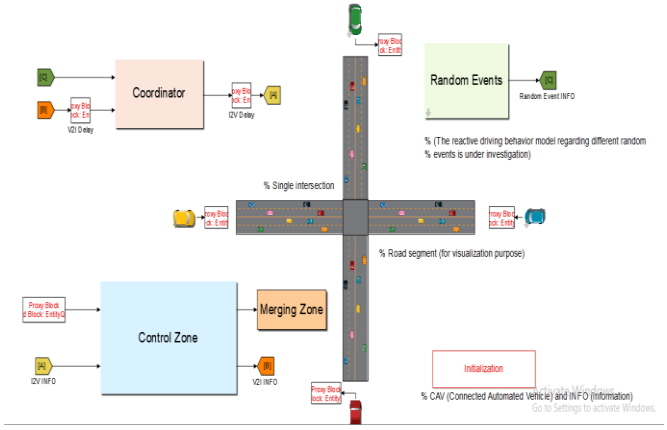

Fig 2: Flow chart of proposed method

VANETs are liable to visit arrange disconnections particularly in low rush hour gridlock regions. Because of this a few occasions in the street may go undetected while the identified occasions may not be transmitted on time. The second issue it with keeping up a synchronized clock inside the system. Only then the messages imparted between the hubs will be important. To conquer the above issues and make the framework progressively dependable it is propose to incorporate roadside remote sensor hubs along with the vehicular hubs in the system. The roadside remote sensor hubs can be conveyed at settled separations and discuss remotely with the vehicular hubs. They assume an essential job in keeping the system connected and ensure message transmission.

The time delay propagation rates in a Vehicular Impromptu System, where vehicular connectivity is upheld by both Vehicle-to-Vehicle (V2V) and Vehicle-to-Framework (V2I) protocols. In our vision, consistent connectivity issues in a VANET with close-by system foundation, can be settled by a pioneering decision of a vehicular protocol somewhere in the range of V2V and V2I. Such a decision is taken by every vehicle at whatever point it needs to transmit messages. Our system - called as Vehicle-to-X - speaks to a handoff strategy somewhere in the range of V2V and V2I, and the other way around, so as to keep vehicles connected autonomous of portability issues and movement situations. it is examine the time delay as an execution metric for protocol exchanging, and present the time propagation rates which happen when vehicles are transmitting cautioning messages, by means of V2V or V2I.

V. SIMULATION RESULTS

it is showing if person is unauthorized and he has no decryption key.

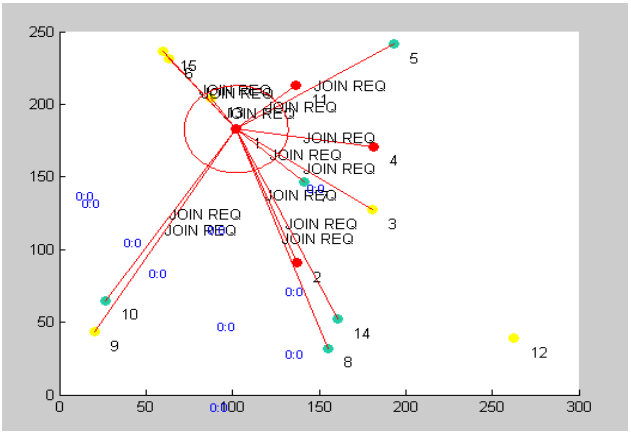

Figure 3: Joining request of VANET simulation

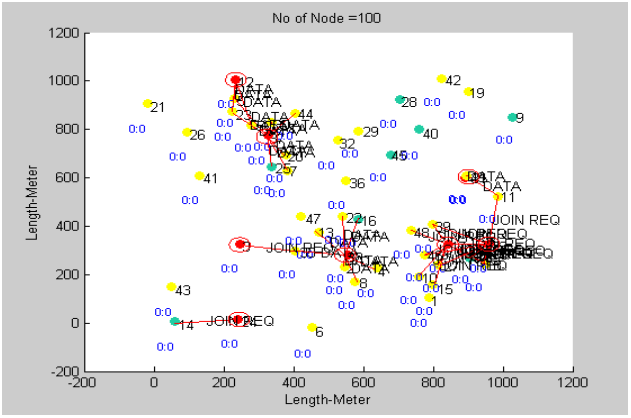

Figure 4: 100 Node Simulation of VANET using ODMRP

Xilinx Smarter Solutions for backhaul are optimized for low footprint to minimize BoM cost and power consumption, and embed hardware level intelligence which reduces the software dependency. The solutions are designed keeping in mind the requirements posed by legacy voice-centric networks as well as data-driven packet-switched IP networks, supporting TDM and Ethernet payload interfaces.

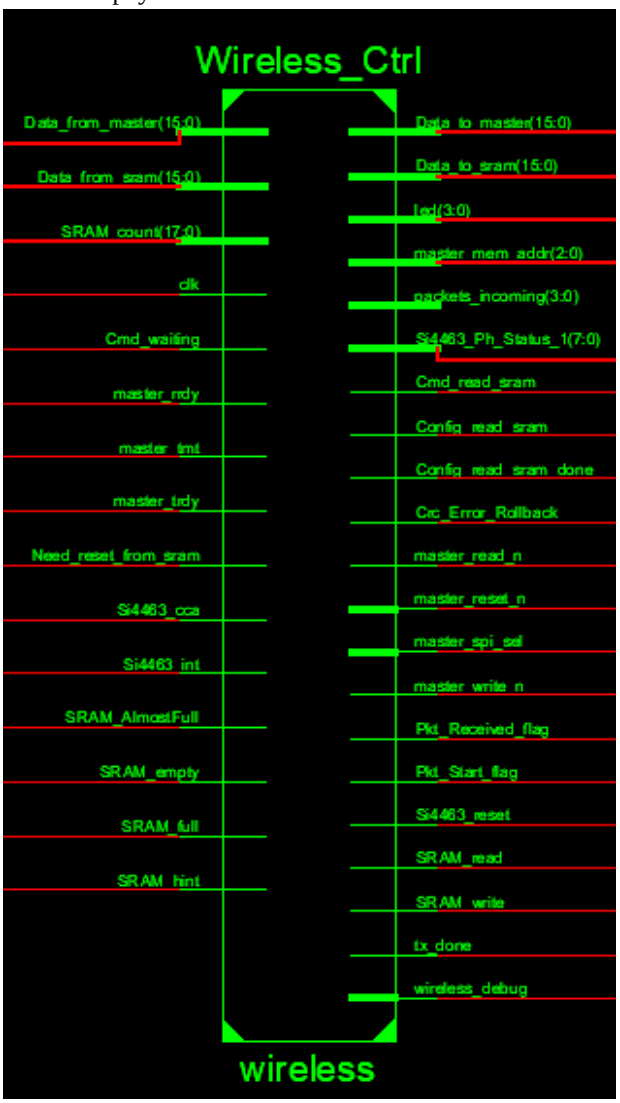

Figure 5: VHDL Design of Wireless control protocol

In the structure of remote protocols for remote sensor systems (WSN) it is important to satisfy a few prerequisites, for example, low vitality consumption, versatility, effortlessness, and so forth. These prerequisites are difficult to satisfy from the perspective of implementation on FPGA or ASIC advances. Continuous systems, for example, mechanical system, field transport, etc, have been getting to be one fundamental component to grow huge scale and helpful inserted frameworks. As one vital branch, the remote method of realtime organizes likewise raises an ever increasing number of attentions.

A. RESULT COMPARISON

In our research work following parameters are generating, in which some parameters are improved .The major work of our research is simulation of vehicular network in MATLAB environment.

Table-I: Simulation Parameters of proposed work

Simulation time	50(s)-100(s)
MAC layer protocol	802.11p
Number of mobile nodes	100
Topology	1200m X 1200m
Traffic loading speed	1 CBD packet/s
Routing protocol	ODMRP
Maximum bandwidth	100mbps
Traffic	Constant bit rate
Maximum speed	2-10m/s
Packet size	512 bytes

RSA based encryption key-administration plans for a VANET have been performed. From the outcomes it has been demonstrated that there is an expansion in the effectiveness of the framework when there is a plan set up. There is a considerable enhancement in the information communication n between the hubs after key administration systems have been utilized. This method can be utilized in security-delicate applications like police and government offices where VANETs are progressively being utilized.

Table-II Comparison of previous work with proposed work

S.NO.	PARAMETRERS	PREVIOUS WORK	PROPOSED WORK
1	Simulation time	300 s	100 s
2	Route protocol	AODV	ODMRP
3	Number of vehicle or node	100	100
4	Packet Delivery Ratio	1%	2.9 %
5	Average End To End Delay	0.005 ms	0-0.001 ms
6	Throughput Performance	5000Kbps	6800kbps

Table-III Summary of device utilization of xilinx

Logic Utilization	Used	Available	Utilization
Number of Slice Registers	1435	54576	2%
Number of Slice LUTs	2985	27288	10%
Number of fully used LUT-FF pairs	1089	3331	32%
Number of bonded IOBs	66	296	22%
Number of BUFG/BUFGCTRLs	1	16	6%
Number of DSP48A1s	3	58	5%

Table 5.6 is showing descryption of using register and other component to make VHDL wireless control protocol.

VI. CONCLUSION

It is investigated a vigorous and versatile geographic multicast protocol and security calculation in VANET. In this, the two information bundles and control messages are transmitted along proficient tree-like ways without the need of unequivocally making and keeping up a tree structure. In this work displayed, execution of ODMRP routing protocol are thought about as far as the execution parameters, for example, bundle conveyance proportion, Normal end to end delay and routing overhead by utilizing MATLAB and VHDL, Xilinx for various number of hubs (25, 50, 75,100) for respite times 2 Secs. From the outcomes plainly at low portability rate ODMRP performs better if there should arise an occurrence of parcel conveyance proportion however it performs inadequately as far as normal end to end delay and routing overhead. At high system load and versatility ODMRP performs well as for parcel conveyance proportion and normal end to end delay. Anyway obviously when versatility is low, ODMRP performs well among the three and when portability is high MAODV performs well. In simulation results, accomplish a lot higher bundle conveyance proportion and lower control overhead, normal way length and normal joining defer when contrasted and other protocol by shifting moving paces, hub densities, gather sizes and system ranges.

ODMRP depends on work (rather than tree) sending. It applies ondemand (instead of occasional) multicast course construction and enrollment upkeep. Simulation results demonstrate that ODMRP is powerful and productive in unique environments and scales well to countless individuals. The benefits of ODMRP are:

- Low channel and capacity overhead
- Use of exceptional and most brief courses
- Heartiness to have versatility
- Upkeep and exploitation of different repetitive ways
- Adaptability to countless

It has introduced the implementation of remote control protocol on FPGAs utilizing VHDL. The proposed networkarchitecture has diverse layer modules, and it is conceivable to effectively increment or diminish the quantity of signs and layers. FPGAs can be utilized for convenient, secluded, and reconfigurable equipment solutions for remote systems.

Simulation results (utilizing ISIM) of the FPGA implementation of the remote controller have demonstrated an attractive exactness.

REFERENCES

[1]. Seyhan Ucar, Sinem Coleri Ergen, 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

[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.

[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 Support Vector 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 in Secure VANET Groups," in IEEE Access, vol. 6, pp. 59282-59295, 2018.

[6]. Khaleel Mershad and Hassan Artail "A System for Secure and Proficient Information Obtaining in Vehicular Specially appointed Systems." IEEE Exchanges On Vehicular Innovation, Vol. 62, No. 2, February 2013

[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

[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 for Transmitter," 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," 2008 4th Southern Conference on Programmable Logic, San Carlos de Bariloche, 2008, pp. 179-182.

[11]. Z. Stamenkovic, "A novel MAC protocol for industrial WLAN: Hardware aspects," 2018 13th International Conference on Design & Technology of Integrated Systems In Nanoscale Era (DTIS), Taormina, 2018, pp. 1-1.

[12]. S. K. Shah and D. D. Vishwakarma, "FPGA implementation of ANN for reactive routing protocols in MANET," 2012 IEEE International Conference on Communication, Networks and Satellite (ComNetSat), Bali, 2012, pp. 11-14.