I J C T A, 9(20), 2016, pp. 203-211

Intensification of Packet Delivery and Meliorating Security in VANET using ONE Simulator

Sonam Singh*, **Rajeev Kumar Singh**** **and Dr. Uday Pratap Singh*****

ABSTRACT

VANETs are peculiar classification of MANETs.It includes roadside base and automobiles.The interaction between these two makes the vehicular network smart and increases the safety for both humans and automobiles. Vanets is basically used to make the transportation framework intelligent, interactive, intermutual so that it reduces the mischances that happens on the streets.its is used for infotainment purpose, it allows users to exchange different media like audio, video, etc also with this they can share important messages for example like road jam on the next street, landslide on the xyz road. so we can say its a combination for both information and entertainment.Therefore it makes the human and automobile smarter than before.In our proposed work we have implemented Advance encryption standard(AES)in spray and wait router and improved the packet delivery and securityAlso we have compared this work with the elliptic curve cryptography (ECC) security algorithm and the novelty of our work is proved by our result. We have implemented this whole scenario in opportunistic network environment (ONE) simulator.

Keywords: VANET, AES, ECC, Routing ONE Simulator

1. INTRODUCTION

VANETs are MANETs subspace in which discussion hubs are frequently automobiles. VANET has two elements: roadside base and automobiles.The roadside base step as circulation point for automobiles and is static at its place and and automobile step as portable nodes as they move frequently without being stationary at one place. This kind of system ought to look at elemental and abundance of specific automobiles scattered in various streets. Also vehicles can stay in contact with distinguishing vehicles to vehicles(V2V) and to obtain some conveyer, they can even interface with a system vehicles to infrastructure(V2I). This underpinning is thought to be put along the streets. VANETs join substances together with automobiles and roadside base. Interaction between automobiles and automobile to infrastructure are the two vitals relating ways, which permits moveable hubs to interact with each other and with the roadside base. VANETs have pulled in extensive deliberation as a promising innovation for rearranging the conveyance approach and providing broadband offerings to automobiles.

In VANETs, security and secrecy are analysed as major challenge. The impish hub can produce various confusions that can create fake data like deceiving messages of traffic tie-up and adversity.Automobiles drift at various velocities; consequently creating a changing topology; and that causes automobiles to depart the network and new automobiles to get in the network. The principal aimof VANET is to basically make a smart Transport framework. In a VANET all hubs collaborate by interchanging information of blockade and accidental cautionary while driving. It sets further to advance the status of avenue.

* Department of Computer Science Engineering and Information Technology Madhav Institute of Technology & Science, Gwalior, Madhya Pradesh, India, *Email: starr.sonu@gmail.com*

** Department of Computer Science Engineering and Information Technology Madhav Institute of Technology & Science, Gwalior, Madhya Pradesh, India, Email: rajeev.mits1@gmail.com

*** MITS Gwalior.

Delay tolerant networking is used to tackle technical problems in the hetergeneous network wanting endless connectivity. Delay Tolerant Networks (DTNs) authorizes data transfer when portable hubs are just discontinuously associated. Since the availability is not anticipated that would be reliable in DTN, it utilizes what is known as a store-convey and-forward steering system. In this, the halfway versatile hubs convey information parcels when they get it and forward it to the following hub as and when contact is built up. As DTN relies on upon portable hubs to convey information, the execution of steering the information exclusively relies on upon whether the hubs interact with each other or not.

Delay tolerant systems (DTNs) speak to a class of remote frameworks that for all intents and purposes need least to none foundation and would bolster the usefulness of systems encountering visit and enduring parcels. DTNs are proposed to manage situations including heterogeneity of guidelines, irregular network between nearby hubs, absence of contemporaneous end-to-end joins and outstandingly high postpones and mistake rates. Likewise the portable hubs accessible in tested situations can be to a great degree constrained in their assets [1].

2. ADVANCE ENCRYPTION STANDARD

AES has a settled square estimation of 128 bits and a key estimation of 128, 192, or 256 bits, while Rijndael [2] can moreover be extraordinary with block and key sizes in any more than one of 32 bits, with

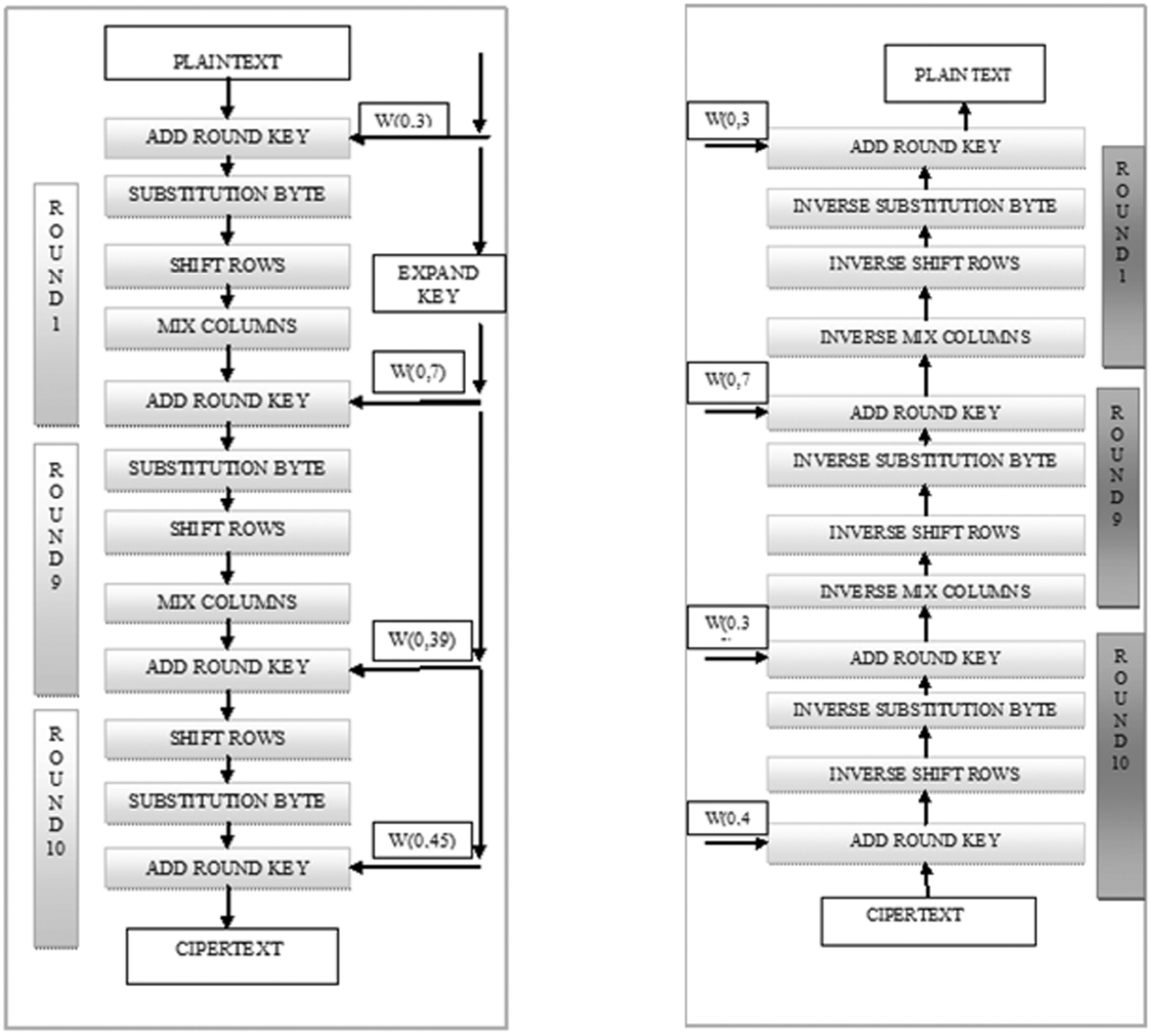

Figure 1: (a) AES Encryption (b) AES Decryption

no under 128 bits and a most noteworthy of 256 bits. Expecting one byte makes back the initial investment with eight bits, the settled square size of 128 bits is 128/8 = 16 bytes. AES takes a shot at a 4×four bunch of bytes, termed the state (models of Rijndael with a predominant square size have additional fragments inside the state). The AES cipher is assigned as an amount of reiteration of coversion adjusts that transforms input (original text)to output(cipher text). Each round includes a couple making consideration of strides, including one who relies on upon the encryption key. A collection of inverse rounds are utilized to change cipher message again into the primary plain-message content utilizing the proportional encryption key. Over the top level delineation of the computation Key Expansion utilizing Rijndael's key timetable.The following is the encryption decryption procedure [2]:

1. Initial Round

2. Add Round Key

3. Rounds

Sub Bytes—A non-straight substitution step the spot every byte is supplanted with yet another in venture with a lookup desk.

Shift Rows—A transposition step where each and every row of the state is moved consistently a specific amount of steps.

Mix Columns—A blending operation which manages the sections of the state, joining the four bytes in each fragment

Add Round Key—each byte of the state is mixed with the round key; all circular key is become from cipher key using a key schedule.

Final Round (no Mix Columns)

1. Sub Bytes

2. Shift Rows

3. Add Round Key

3. LITERATURE SURVEY

Horng SJ, Tzeng SF, Pan Y, Fan P, Wang X, Li T, Khan MK. b [9] proposed a strategy that subjugate the flaws of SPECS. Also this strategy can achieve exquisite operational productivity between vehicles and road side units (RSUs) in terms of signature verification delay and transmission overhead as compared to BLS, ECDSA and SPECS. This strategy allows the trust authority to restore and nullify the real identity of an arbitrary vehicle through any message signature.

Vipin Bondre, Sanjay Dorle, Shashant Jaykar, Sagar Kawle [10] proposed an alternate way for emergency rescue applications in a network. They have taken few specifications like packet delivery ratio, packet loss ratio, average delay and throughput in deliberation with AODV protocol and excelled them with the new AOMDV protocol in a defined route. This new protocol have shown better results and is quick and dutiful multipath protocol in case of any emergency.

Celimuge Wu, and Satoshi Ohzahata, Yusheng Ji, Toshihiko Kato [11] proposed a multi-hop broadcast protocol which is a combination of MAC and network layer, which when interact with the environment uses the best contention window size to send the packets of data and therefore provides high packet dissemination ratio and low end to end delay for varied schemes.

Lu Chen, Hongbo Tang, Junfei Wang in[12] discusses about the VANET and its characteristics like large scale network, high movable nodes, changing topological structures, divided networks with node

information and focuses on the security threats in different information type and provides possible research directions. They also evaluated that the network security issues are concerned with the compromise of all sorts of information.

Sandeep Mudigonda, Junichiro Fukuyama, Kaan Ozbay in [13], develops a customized algorithm for dynamic grouping which is able to hinder the broadcast storm and also capable of lessening broadcast time and usage of bandwidth. This algorithm provides an efficient common platform for varied applications of connected vehicles.

4. PROPOSED METHODOLOGY

In existing strategy in [14] author has used elliptic curve cryptography for the security purpose, but the issue which arises in it is the total processing time taken for encryption and decryption is too long and as a result of this it causes abstaining of packet delivery which is in other way worsening security. So, in our proposed work we have overcome this issue by using an existing cryptographic technique known as Advanced encryption standard(AES). We have implemented this technique in spray and wait router shown below in flowchart and found with our results that the processing time of this technique is much faster than the ECC technique; which therefore fastening packet delivery and bettering security perspective.In VANETs we need faster message delivery which can only be possible if encryption and decryption takes lesser time and with this implemented strategy we can achieve this goal very easily.

Algorithm:

Step1: initialize()

Step2: if(nodeis static)

{

Don’t pass the message

}

Else

Send data according to speed

Exchange summary vector

Step3: if(messageTTL!)

{

Just pass message with AESencryption // don’t send message

}

Step4: exit.

For cryptographic purpose, key size plays an efficient role in it.The larger the key size the more strong our encryption is.In this proposed strategy we have used AES-128 for encryption and decryption which is much secure than ECC.

We have implemented this whole scenario in one_1.5.1-RC2. Following is the flowchart for the proposed algorithm which represents the conditions for the message to pass or not.

5. SIMULATION ENVIRONMENT

For simulation we have used the opportunistic network environment (ONE) simulator. This simulator is specially used for delay tolerant networking(DTN) routing and application protocols evaluation and it is

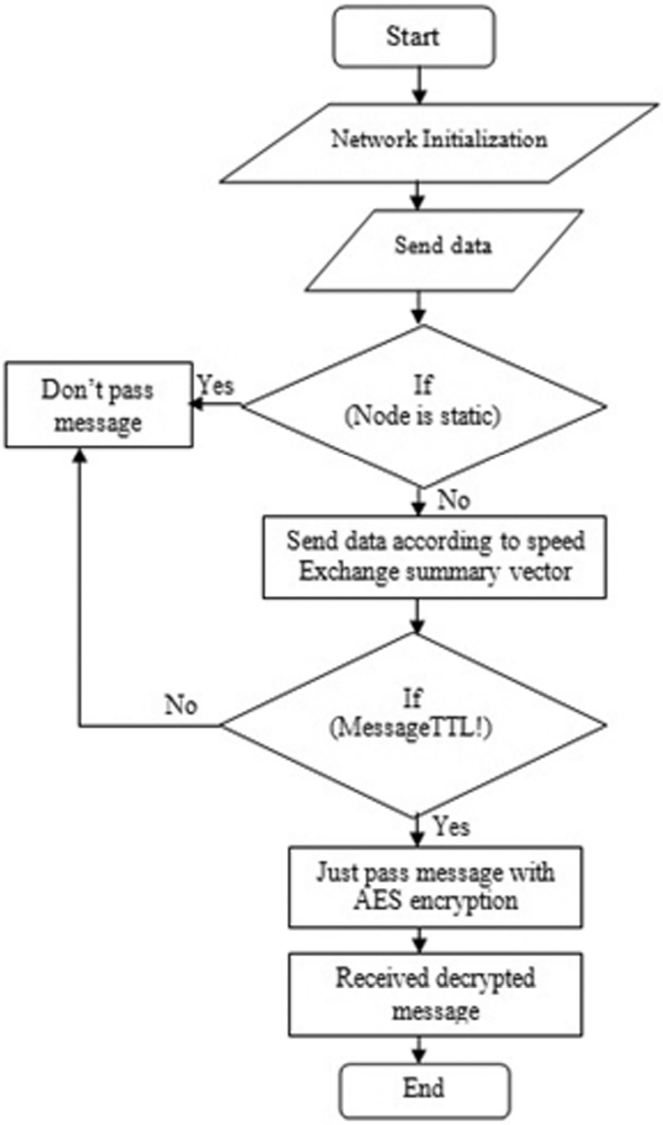

Figure 2: Flow Chart Diagram for Proposed Algorithm

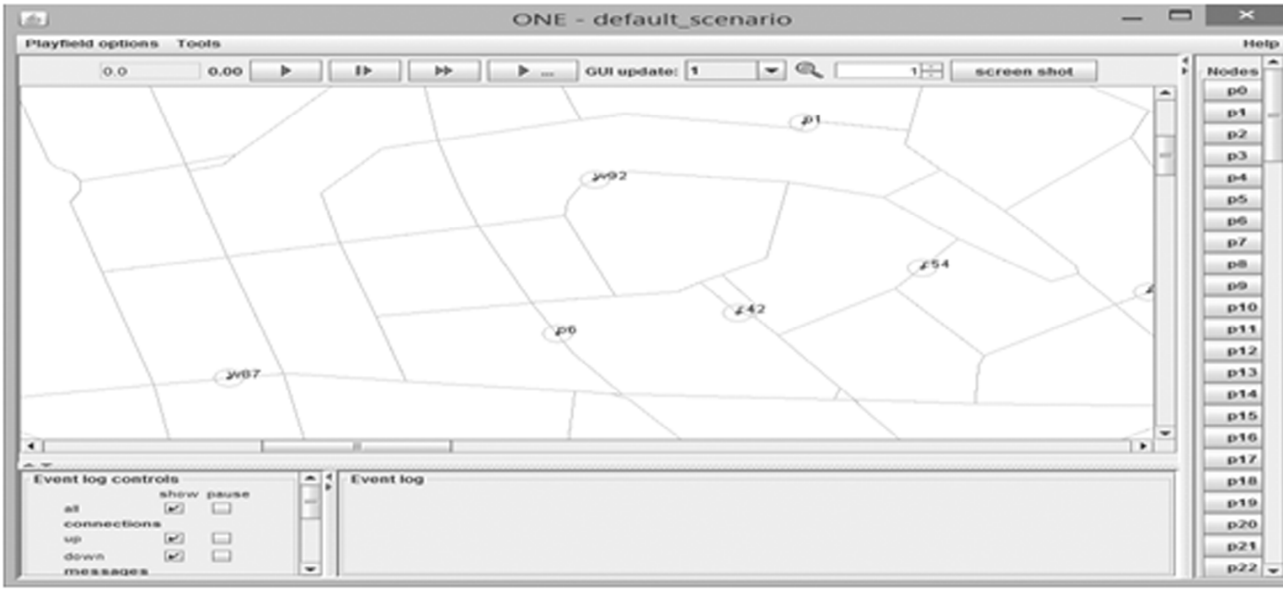

Figure 3: Graphic user Interface of ONE Tool

based on java. It supports assessing tests by intermutual perception and post-handling apparatuses. Using this simulator we can create our own layout using distinctive movement models and real world fragments for implementation of routing and application protocols.

6. RESULTS

When we have conducted the simulation in one_1.5.1-RC2 ; we found these outcomes of the proposed work and also we have compared these results values with the existing work values, which have shown better results than earlier.

6.1. Delivered Packets

The higher the delivery of packets in the network the more efficient your network will be.Our proposed strategy shows that the delivery of packets is more in it as compared to existing technique.

6.2. Over-Head Ratio

Overhead is one of the crucial issue of VANET, below we mention the graph and table shows that propose overhead is less compare to existing.

Table 1
For Delievered Packets

Number of nodes	*AES*	*ECC*
5	38	214
10	141	54
15	328	88

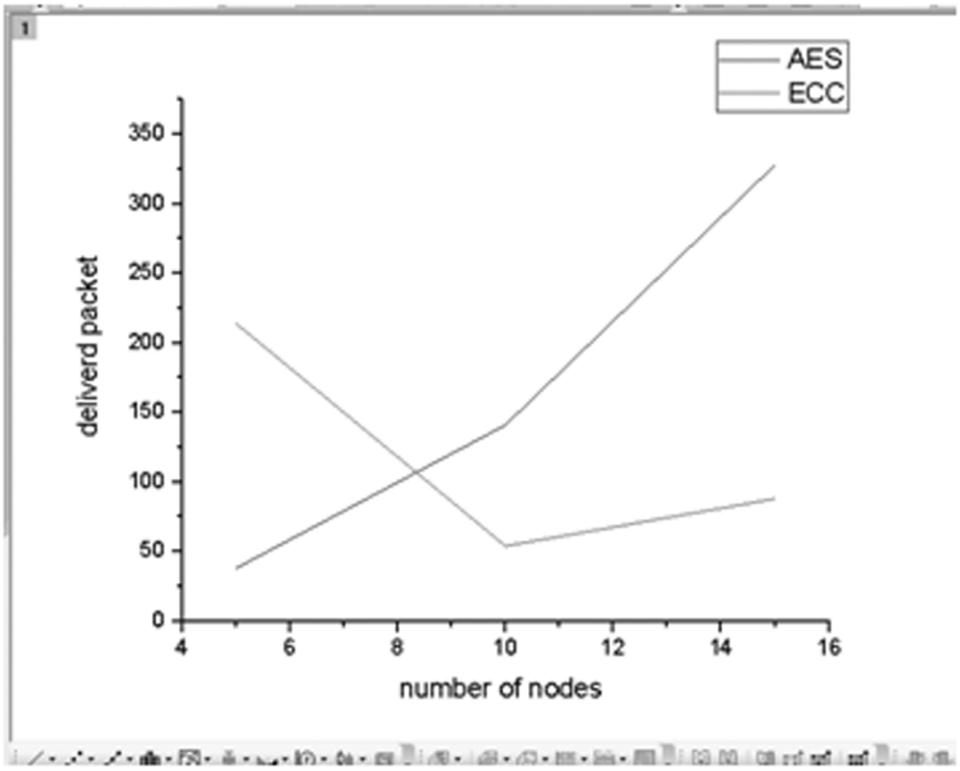

Figure 4: Comparison of Delivered Packets

Table 2
For Over-Head Ratio

Number of nodes	*AES*	*ECC*
5	0.5789	12.2150
10	0.8014	2.1111
15	1.1890	4.2159

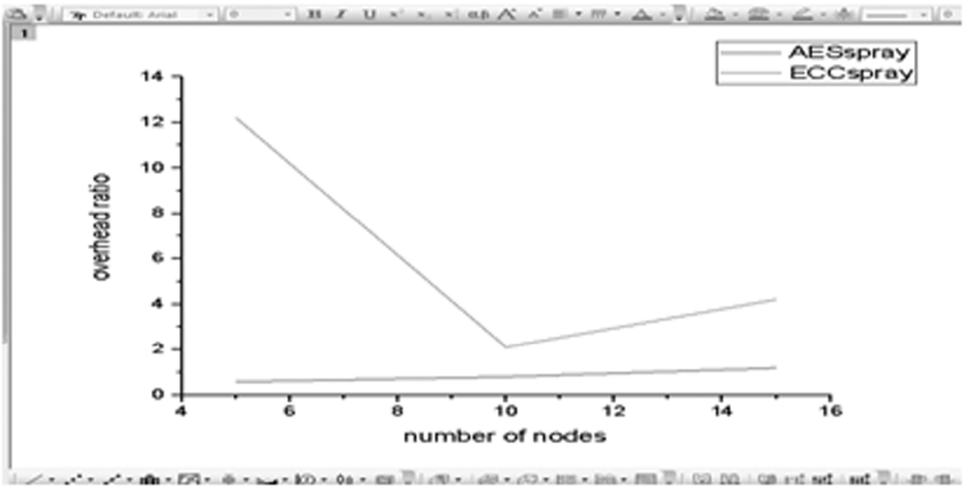

Figure 5: Comparison of Over-Head Ratio

6.3. Relay

Relay is described as number of hop count. On the basis of our result we see that our hop count is less compare to existing technique by reducing hopcount we also reduce overhead which we already discuss above.

Table 3
For Realy Packets

Number of nodes	*AES*	*ECC*
5	60	2828
10	254	168
15	718	459

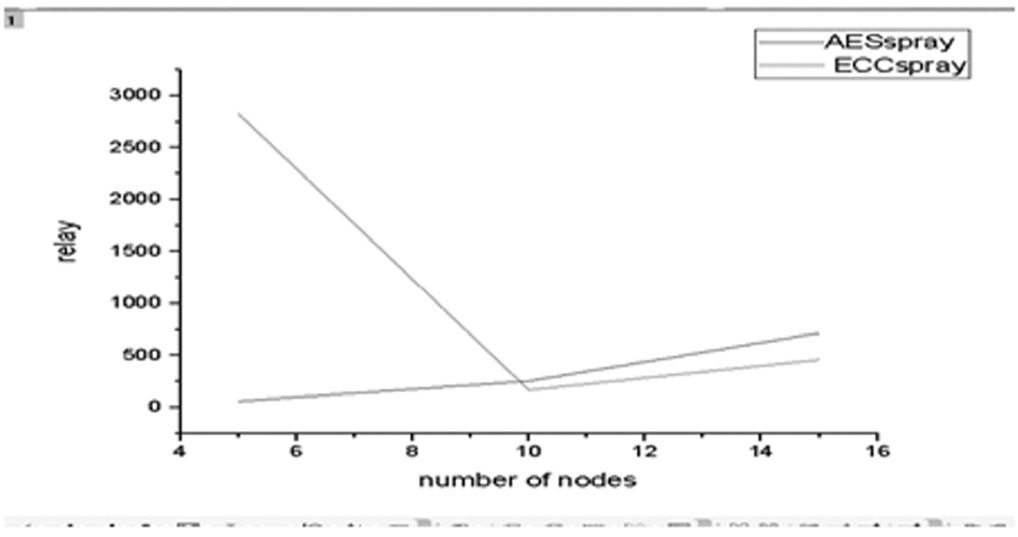

Figure 6: Comparison of Realy Packets

6.4. Aborted

In simulation time, how many packets are dropped due to destination not found or neighbor does not meet are known as aborted packets. Below table shows that aborted packet are less compared to existing technique.

Table 4
For Aborted Packets

Number of nodes	*AES*	*ECC*
5	10	525
10	40	40
15	92	97

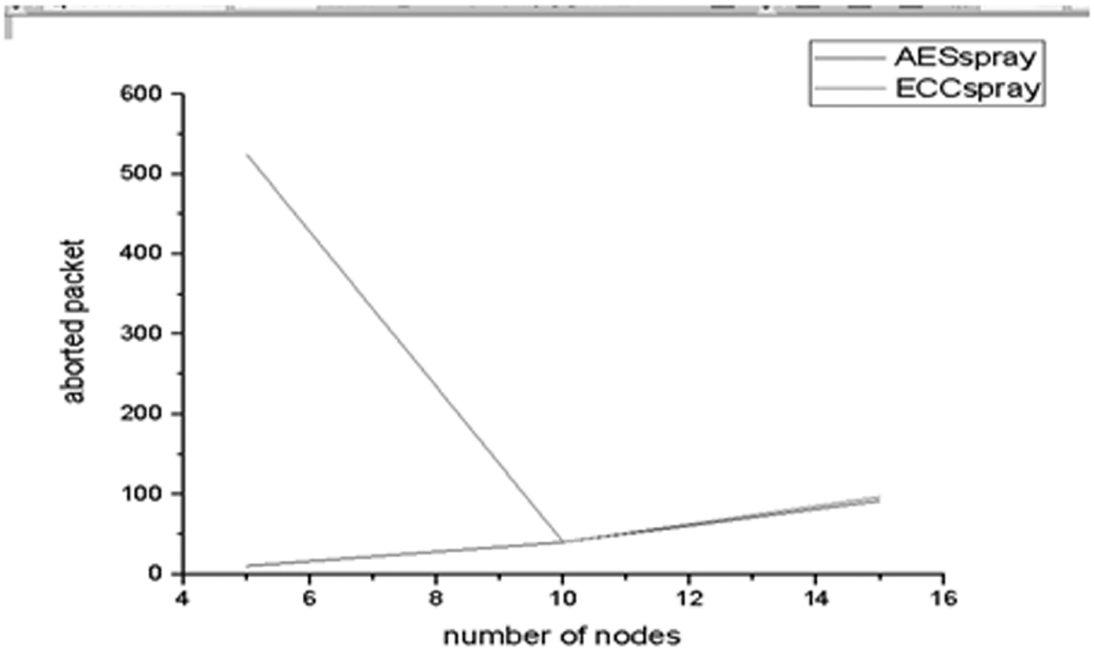

Figure 7: Comparison of Aborted Packets

7. CONCLUSION

VANET is a emerging region of research;as we know that the essential information at correct time is so crucial, so keeping that perspective in mind we have proposed this strategy so that quickly information can be sended and received securely.In this paper we have implemted AES cryptographic algorithm. Our simulation and result shows that our proposed scheme gives better result in terms of delivered packets, overhead ratio, number of packet relay and aborted packets, which in a way or another advances the security.

REFERENCES

[1] Patil S, Chillerge G.”Delay Tolerant Networks – Survey Paper”, .Int.Journal of Engineering Research and Applications,4(2):21-25,2014

[2] Suryawanshi Y, Kapur A, Chawhan M.”Analysis of Symmetric Key Cryptosystem in VANET”, Int. J. on Recent Trends in Engineering and Technology,7(2):63-67,2012

[3] Guo S, Zhao X, Zhang F, Wang T, Shi ZJ, Standaert FX, Ma C.”Exploiting the incomplete diffusion feature: A specialized analytical side-channel attack against the AES and its application to microcontroller implementations”, IEEE Transactions on Information Forensics and Security,9(6):999-1014,2014

[4] Liu K, Ng JK, Lee VC, Son SH, Stojmenovic I.”Cooperative data scheduling in hybrid vehicular ad hoc networks: VANET as a software defined network”.

[5] Jayapal C, Roy SS.”Road traffic congestion management using VANET”, In 2016 International Conference on Advances in Human Machine Interaction (HMI), IEEE, pp. 1-7,2016

[6] El Brak S, Bouhorma M, Boudhir AA, El Brak M, Essaaidi M.”Voice over VANETs (VoVAN): QoS performance analysis of different voice CODECs in urban VANET scenarios”, International Conference In Multimedia Computing and Systems (ICMCS), IEEE, pp. 360-365,2012

[7] Wei YC, Chen YM. “Adaptive decision making for improving trust establishment in VANET”,16th Asia-Pacific InNetwork Operations and Management Symposium (APNOMS), IEEE, pp. 1-4,2014

[8] Liu Z, Xiang Y, Sun W. “GeoSVR: A Geographic Stateless VANET Routing”, InConference Anthology, IEEE, pp. 1-7,2013

[9] Horng SJ, Tzeng SF, Pan Y, Fan P, Wang X, Li T, Khan MK.”b-SPECS+: Batch verification for secure pseudonymous authentication in VANET”, IEEE Transactions on Information Forensics and Security,8(11):1860-75,2013

[10] Bondre V, Dorle S. “Design and performance evaluation of AOMDV routing protocol for VANET”, International Conference In Computer, Communication and Control (IC4), IEEE, pp. 1-4,2015

[11] Wu C, Ohzahata S, Ji Y, Kato T. “Joint MAC and Network Layer Control for VANET Broadcast Communications Considering End-to-End Latency”, In 28th International Conference on Advanced Information Networking and Applications, IEEE, pp. 689-696,2014

[12] Chen L, Tang H, Wang J.”Analysis of VANET security based on routing protocol information”, Fourth International In Intelligent Control and Information Processing (ICICIP), IEEE, pp. 134-138,2013

[13] Mudigonda S, Fukuyama J, Ozbay K. “Efficient Data Broadcast for Generic Applications Using a Scalable Dynamic VANET Algorithm”, In International Conference on Connected Vehicles and Expo (ICCVE), IEEE, pp. 274-281,2012

[14] Timpner J, Schürmann D, Wolf L.”Trustworthy Parking Communities: Helping Your Neighbor to Find a Space”, IEEE Transactions on Dependable and Secure Computing, IEEE,13(1):120-32,2016