Improving Reliability in VANET using Network Coding

Jeet Gandhi[1], Jay Amin[2]

[1] *Student of Master in Engineering, L.J. Institute of Engineering and Technology, Ahmedabad, India.*
[2] *Asst. Professor Computer Department, L.J. Institute of Engineering and Technology, Ahmedabad, India*

ABSTRACT

Vehicular Ad-Hoc Network (VANET) is a wireless connection of network which is formed between the vehicles. In VANET, there is communication between vehicles V2V or between vehicle and road side unit V2R in VANET. The network reliability is very important along with secured communication. The proposed system enhances reliability of the network using linear network coding.

Keyword : *VANET, V2V, V2I, reliability in VANET, network coding*

1. INTRODUCTION

Vehicles are connected to each other through an ad-hoc formation which forms a wireless network called "Vehicular Ad-hoc Network." It infrastructure less, distributed,self-organizing, communication networks. More precisely it is network aiming to improve driving safety and traffic management with internet access. [7] It includes vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) communication in a short range of 100 to 300m. The nodes in the network which are the vehicles communicate to one other by means of North American DSRC (Dedicated Short Range Communication) standard that employs the IEEE 802.11p. It uses 5.850-5.925 GHz band for the use of public safety and private applications [8]. In VANET, the access and the routing protocols are facing several issues like available bandwidth estimation, medium access control, hidden and exposed node problem, high mobility, support of heterogeneous vehicles, fast speed, obstacles and fast handovers. [1] Because of high mobility VANET face challenges in routing protocols. There are numerous routing protocols introduced for the VANET which still faces tremendous challenges like node mobility, limited resources and limited physical security.[1]

Another major concern is the message security in the network. The communication takes place between V2V or V2I so it is easy for any attacker to attack the message and compromise the privacy and security of the node. Hence, there is required secured environment in order to have efficient communication between the nodes.

2. VANET ARCHITECTURE

From the vehicular communication perspective, it can be categorized into: Road-vehicle and the inter vehicle communication. The VANET architecture is as follows:

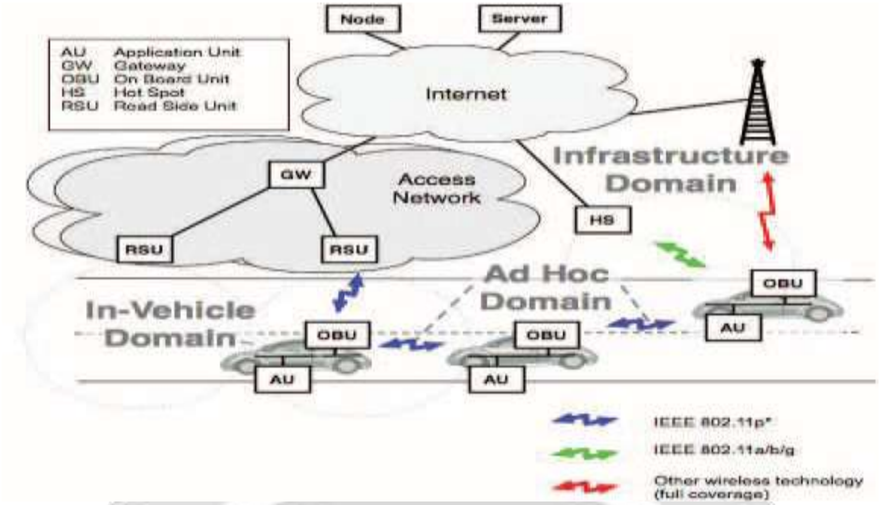


Fig.1 C2C-CC draft reference architecture[8]

There are various components in VANET architecture.

- *On board unit (OBU)*: It is a physical device located in the vehicle. It is responsible for the V2V and V2R communication. AU and OBU are connected by Ethernet. Its two main components are reporter which automatically detects road traffic events and delivers them to the disseminator. And other component is receiver which receives messages from disseminator.

- *Road side Unit (RSU)*: It is a physical device located at fixed positions along roads, highways or dedicated locations.

Application Unit (AU): It is an in-vehicle or road-side entity and runs applications that can utilize the OBU's and RSU's communication capabilities. Its main component is disseminator which aggregates road traffic event reported by clients and propagates them to other receivers.

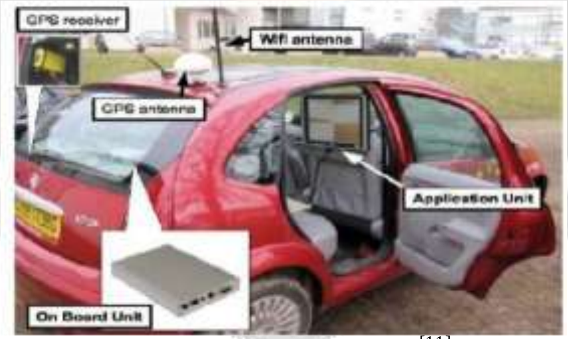


Fig.2 Example of OBU, AU[11]

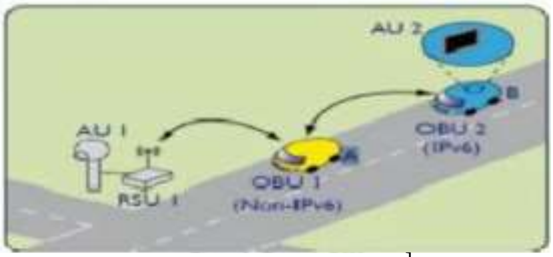


Fig.3 Example of RSU[11]

3. CHARACTERISTICS OF VANET

Vehicular networks have specific characteristics which have to be taken into account while building the architecture. [4][7]

- *High mobility:* The nodes in VANETs usually are moving at high speed. This makes harder to predict a node's position and making protection of node privacy.
- *Continuously changing network topology:* Due to high node mobility and random speed of vehicles, the position of node changes frequently. Hence, network topology in VANETs tends to change frequently.
- *Unbounded network size:* VANET can be implemented for one city, several cities or for countries, which means the network size in VANET is geographically unbounded.
- *Time Critical:* The information in VANET must be delivered to the nodes with in time limit so that a decision can be made by the node and perform action accordingly. [7]
- *Wireless Communication:* VANET is designed for the wireless environment. Nodes exchange their information via wireless network.
- *Better Physical Protection:* The VANET nodes are physically better protected. Thus, VANET nodes are more difficult to compromise physically and reduce the effect of infrastructure attack. [7]
- *Central Authority:* Each and every vehicle in the network has to be registered with a common Centralized Authority and should be assigned an unique identifier for the vehicles security purpose. This hence provides with better security.
- *Power Consumption:* In traditional wireless networks, nodes are power limited and their life depends on their batteries. But Vehicles can provide continuous power to their computing and communication devices. [5]

4. ROUTING PROTOCOLS

There are various routing protocols used in the VANET. The existing routing protocols used are divided into three categories: [2]

- TBR, Topology based routing
- PBR, Position based routing
- Hybrid routing

Among them, the routing protocol based on topology should be divided into pre-active routing protocols and reactive routing protocols, as described in figure which shows the VANET routing protocol classification. The designing on VANET routing protocol referenced the Ad hoc working group on the traditional network DSDV and AODV and other network protocol, and made the comprehensive use of position or velocity information and put forward the GPSR, GPCR and GeoDTN + Nav routing protocols.

The detailed information is provided for the topology based routing protocols:

A. *Proactive routing protocol:* Proactive routing protocols, also known as table-driven protocols, allow every network node to maintain a routing table for storing the route information to all other nodes, every next hop node is maintained in the table entry that comes in the path towards the destination from the source. [9]

- *Destination Sequenced Distance Vector (DSDV) Routing Protocol:* It is based on the distance vector strategy using shortest path algorithm. It implements a single route from source to destination which has been maintained in the routing table. A routing table is maintained for each node containing information of every accessible node in the network and total number of hops needed to succeed those nodes. The destination node initiates a sequence number to every entry in the table. Each node maintains the route reliability by broadcasting their routing table to the neighbouring nodes. DSDV protocol does not allow cyclic routes, reduces control message overhead and excludes extra traffic caused by frequent update. The total size of routing table is reduced as DSDV keeps solely the best possible path to each node instead of multi paths. DSDV is not able to control the networks congestion that decreases the routing efficiency.

B.*Reactive routing protocols*: Reactive routing protocols, also known as on-demand routing protocols. They are called so because on requirement of a route that does not exist from source node to destination node, the route discovery starts. Flooding of the network helps in route discovery mechanism by sending a route request message. Any node existing on the route towards the destination on receipt of the request message, sends back a route response message to the source node using unicast communication. [9]

- *Ad-hoc On-demand Distance Vector (AODV) Protocol:* AODV protocol reduces flooding in the network and gives low network overhead comparing to the proactive protocols. This routing protocol minimizes the routing table by creating a route when a node needs to send information data packets to other nodes in the network, hence reducing the memory size required. The routing table keeps the entries of the recent active nodes and the next hop node of the route instead of keeping the whole route. AODV uses destination sequence numbers (DesSeqNum) for route discovery which eliminates looping in routes and provides dynamic updates for adapting the route conditions. AODV is more suitable for large networks and network having high dynamic topology. This protocol causes delay in route discovery process. When route failures occur, new route discovery is required causing additional delays thus decreasing the data transmission rate and increasing the network traffic. This causes more bandwidth consumption that is increased due to increasing number of nodes in the network which causes collision leading to packet loss problem.
- *Dynamic Source Routing (DSR) Protocol:* DSR routing protocol is a reactive protocol which implements routing process using low overhead and quick reaction to frequently changing topology to ensure successful packet delivery even if change in network happens. DSR is a multi-hop routing protocol decreases the network traffic by decreasing periodic messages. DSR provides two processes that are the route discovery mechanism and route maintenance process.

5. Literature Review

Sr. No.	Paper Title	Method Used	Advantage	Disadvantage
1.	Rethinking Vehicular Communications: Merging VANET with Cloud Computing	VANET Cloud Architecture	Computing, communication, physical resources can be dynamically allocated to users	Privacy and security challenges
2.	Implementing Authentication Mechanism using Extended Public Key Cryptography in Wireless Network	Cryptography RSA+AES	Encryption is faster as the non-symmetric key cryptography is used	Time taken by RSA algorithm is comparatively greater
3.	VANET-CLOUD: A GENERIC CLOUD COMPUTING MODEL FOR VEHICULAR AD HoC NETWORKS	Cloud-VANET Architecture	Provides digital services such as software, computational infrastructures, and platforms to VANET users at a reduced cost.	Communication and coordination between VANET-Cloud, Security and privacy issues
4.	CPAV: Computationally Efficient Privacy Preserving	Anonymous Authentication	The CPAV authentication	Unable to provide batch

	Anonymous Authentication Scheme for Vehicular Ad Hoc Networks	Scheme	scheme is providing the anonymous authentication with low certificate and signature verification cost	authentication with low computational cost in an efficient way
5.	Dynamic Key based Authentication Scheme for Vehicular Cloud Computing	Dynamic key distribution authentication	The proposed system aims to detect malicious vehicles in the network and maintain overall trust between the vehicles	More complexity

6. PROPOSED WORK

- **Steps for proposed solution:**
- Sender requests for key co-efficient from cloud: key distribution as a service.
- KDaaS (i.e. from cloud) generates key co-efficient.
- KDaas (i.e. from cloud) encrypts key co-efficient.
- It sends encrypted key co-efficient to sender and destination.
- Sender decrypts key co-efficient.
- Sender encodes data by key co-efficient using Linear Network Computing.
- Receiver receives data.
- It decrypts key co-efficient.
- It then decodes the data using key co-efficient

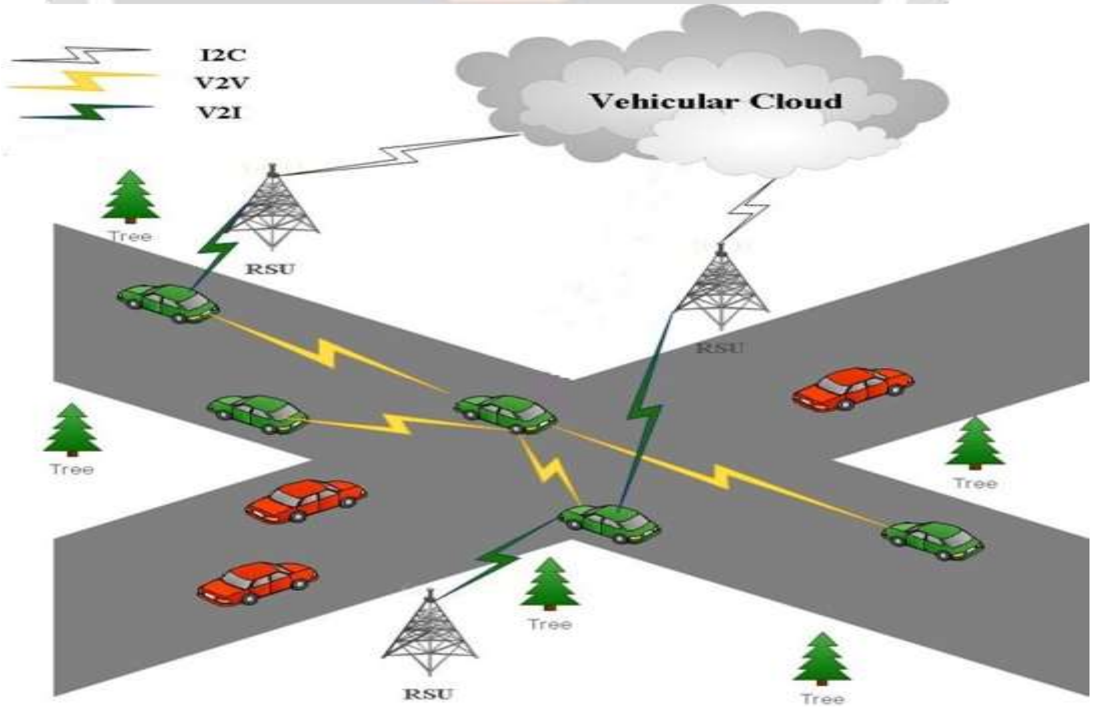
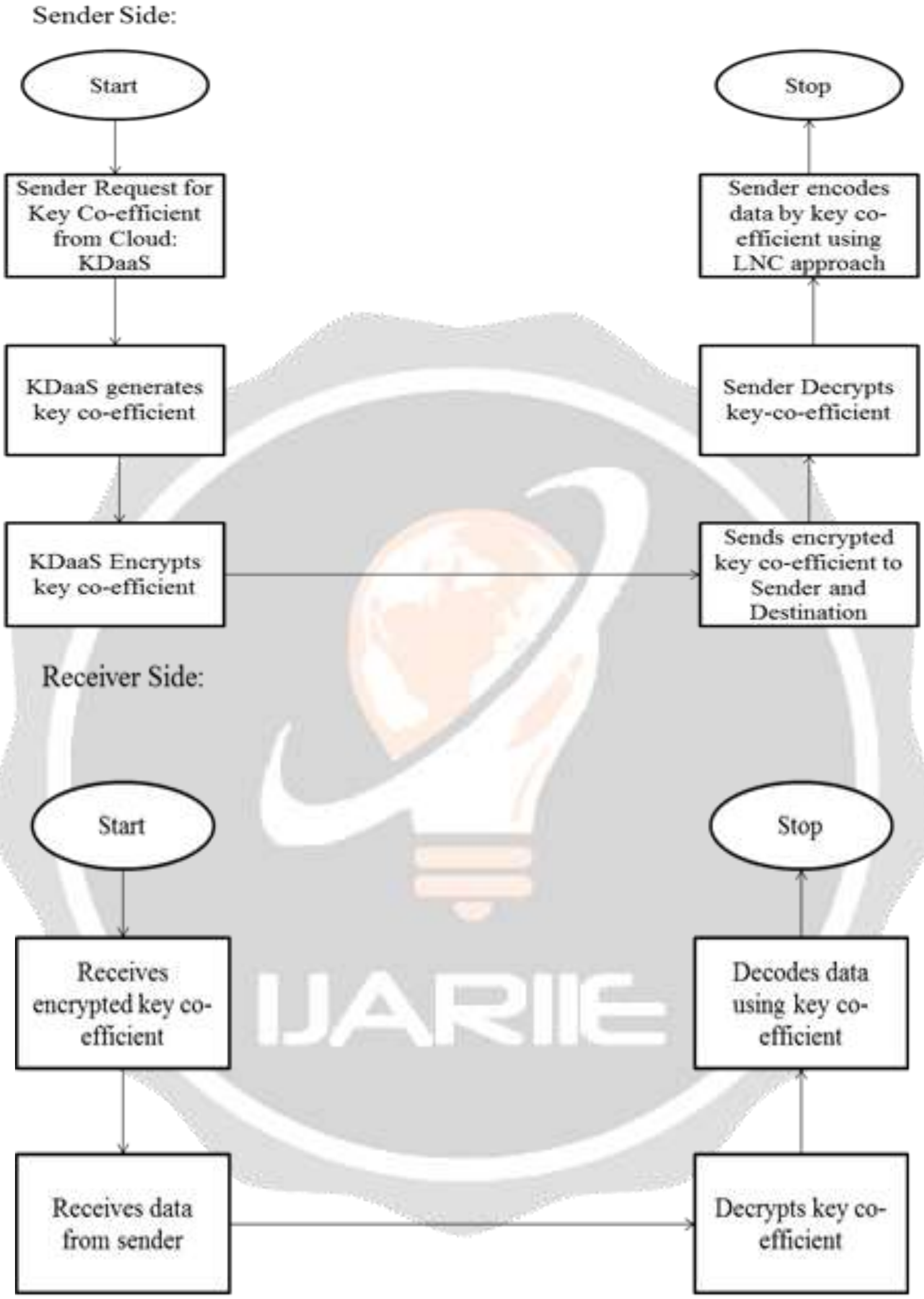


Fig.4 Proposed Architecture

- **Flowchart:**

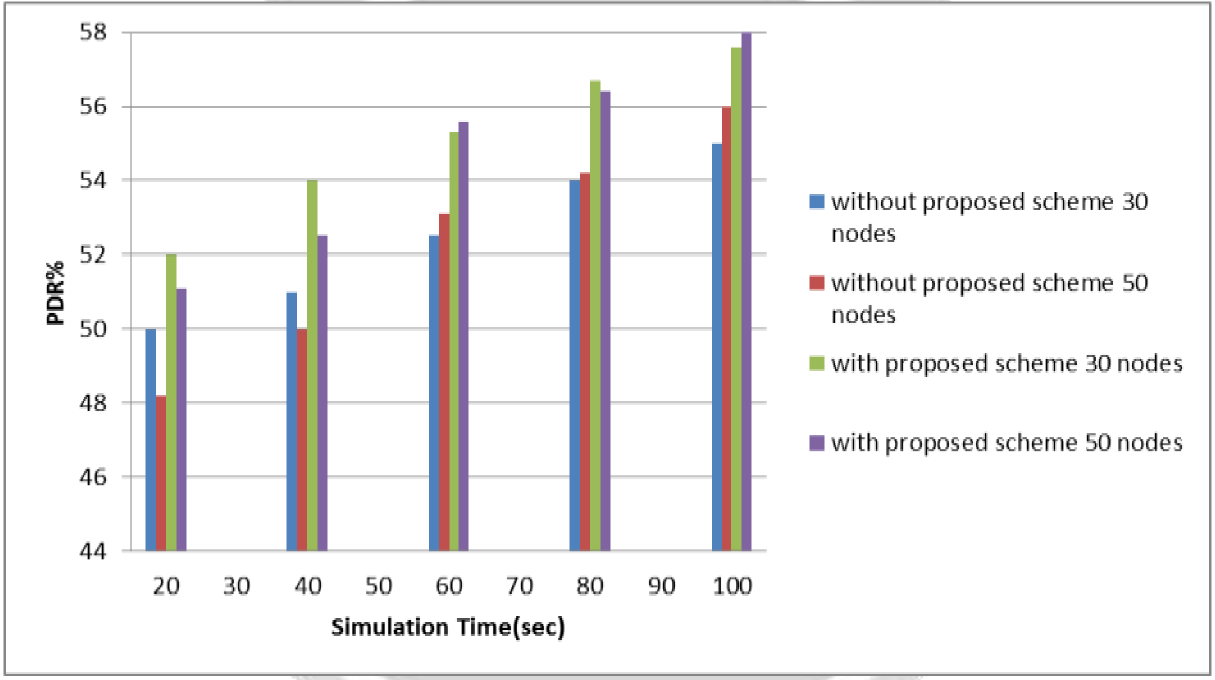

Sender Side:
Start
Sender Request for Key Co-efficient from Cloud: KDaaS
KDaaS generates key co-efficient
KDaaS Encrypts key co-efficient
Sends encrypted key co-efficient to Sender and Destination
Sender Decrypts key-co-efficient
Sender encodes data by key co-efficient using LNC approach
Stop
Receiver Side:
Start
Receives encrypted key co-efficient
Receives data from sender
Decrypts key co-efficient
Decodes data using key co-efficient
Stop

7. SIMULATION RESULT

The simulator used is ns-2. The Amazon web service is used to get the linear network coding parameters. The simulator parameters are as follows:

Simulator Parameters	
Number of Nodes	30 and 50
Speed	20m/s
Area	652*752m
Simulation Time	20-100s

The graph of proposed solution as compared to the existing technique is as follows:



Graph 1: PDR% vs Simulation Time(sec)

8. CONCLUSION

Vehicles are becoming a part of the global network. The proposed work uses linear network coding to send the packets. The network coding matrix is obtained from cloud which is secured and delivered to sender and receiver. They could benefit from spontaneous wireless communications in a near future, making VANET a reality. Vehicular networks will not only provide safety and life saving applications, but they will become a powerful communication tool for their users. Hence, there is required a powerful reliability in VANET environment in order to have efficient and successful communication.

9. REFERENCES

[1] Kalkundri Ravi, Kalkundri Praveen, “AODV Routing in VANET for Message Authentication Using ECDSA”, IEEE, ISBN:978-1-4799-3357-0, April 2014, pp. 1389-13893.

[2] Lu Chen, Hongbo Tang, Junfei Wang, "Analysis of VANET Security Based on Routing Protocol Information", IEEE, June 2013, pp. 134-138.

[3] Rasheed Hussain, Junggab Son, Hasoo Eun, Sangjin Kim and Heekuck Oh, "Rethinking Vehicular Communications: Merging VANET with Cloud Computing", IEEE, ISBN: 978-1-4673-4510-1/12, 2014, pp.606-609.

[4] Ravinder Kaur, Dr. Neeraj Sharma, "A Node Authentication Mechanism to Enhance the Security in VANETs", IJETER Vol.1 Issue 2, ISSN: 2454-6410, July 2015, pp. 16-22.

[5] Manish Kumar Sharma, Rasmeet S. Bali, Arvinder Kaur, "Dyanimc Key based Authentication Scheme for Vehicular Cloud Computing", IEEE, ISBN:978-1-4673-7910-6/15, 2015, pp.1059-1064.

[6] SALIM BITAM, ABDELHAMID MELLOUK, AND SHERALI ZEADALLY, "VANET-CLOUD: A GENERIC CLOUD COMPUTING MODEL FOR VEHICULAR AD HOC NETWORKS", IEEE, ISBN: 1536-1284/15, 2015, pp.96-102.

[7] Ram Shringar Raw, Manish Kumar, Nanhay Singh, "SECURITY CHALLENGES, ISSUES AND THEIR SOLUTIONS FOR VANET", IJNSA Vol.5 No.5, Sept. 2013, pp. 95-105.

[8] Yue Liu, Jun Bi, Ju Yang, "Research on Vehicular Ad Hoc Networks", IEEE, 2009, pp. 4430-4435.

[9] Shilpi Dhankhar, Shilpy Agrawal, "VANETs: A Survey on Routing Protocols and Issues", IJIRSET Vol.3 Issue 6, ISSN: 2319-8753, June 2014, pp. 13427-13435

[10] Amandeep Kaur Gill, Charanjit Singh, "Implementation of NTRU Algorithm for the Security of N-Tier Architecture", IJCSIT Vol. 5 No. 6, ISSN: 0975-9646, 2014, pp. 7631-7636.

[11] DEESHA G. DEOTALE & UMA NAGARAJ, "SURVEY OF VEHICLE AD-HOC NETWORK", IJCNS Vol. 1 Issue 4, ISSN: 2231-1882, 2012, pp. 86-90.