Secure and Reliable Content Distribution Routing Protocol for VANET

Shital Chauhan[1] Hitesh Patel[2]
[1] M. E. Student [2] Asst. Professor
[1, 2]Information Technology Department
[1, 2] Kalol Institute of Technology & research Center, Gujarat, India

Abstract---Vehicular Ad Hoc Networks (VANET) is a kind of special wireless ad hoc network, which has the characteristics of high node mobility and fast topology changes so the content distribution in VANET is very difficult because of the fast topology changes and also VANET has open air medium for sending the packet data so there is less security in content distribution and as well as less reliability in content distribution while using broadcasting protocol. All this difficulty will be overcome in proposed algorithm. open issues are Frequently change connectivity, Open air medium i.e. no security, High mobility so chances of dada delivery is Very less, achieve better throughput, average delivery delay, security and Reliability than existing schemes without compromising on overhead.

Keywords: RSSI (received signal strength indicator), VANET (Vehicular Ad Hoc Networks), Urban Multi-hop Broadcast protocol (UBM), RSA public key cryptography

I. INTRODUCTION

In 1999, Federal Communication Commission (FCC) allocates a frequency spectrum for V2V and V2R wireless communication. In 2003, FCC established Dedicated Short Range Communications (DSRC) use 5.850 – 5.925 GHz band, provide range of 300 m to 1 km with basic data rate of IEEE 802.11p is 3 Mbps for a 10 MHz, also possible higher data rates up to 27 Mbps. These enable vehicles and roadside becomes to form Vehicular Ad Hoc Networks (VANET).VANET is the ad hoc network which provides a spontaneous and direct communication of a car with other cars or with fixed road-side access points [1]This paper introducing the research challenges about As VANET is an emerging area there are lots of issues which are to be addressed. Out of that security issue in content distribution is booming So proposed routing algorithm which is meant for secure and reliable content distribution routing protocol in VANET.

II. OBJECTIVES AND OPEN ISSUES

Objective of this paper is to achieve better throughput, average delivery delay, security and Reliability with existing schemes without compromising on overhead. Issues are Frequently change connectivity, Open air medium i.e. no security, High mobility so chances of dada delivery is Very less these all are open issues today in VANET.

III. BASIC OF VANET

A. *Characteristics of VANET [1]*

major characteristics are as follows:

1) *High mobility and Rapid changing topology:*

Vehicles move very fast especially on highways. Thus, they stay in the communication range of each other just for several seconds, and links are established and broken fast. When the vehicle density is low or existing routes break before constructing new routes, it has higher probability that the vehicular networks are disconnected. So, the previous routing protocols in MANET are not suitable for VANETs.

2) *Geographic position available for vehicles:*

For example, GPS receivers are very popular in cars which help to provide location information for routing purposes so here Vehicles can be equipped with accurate positioning systems integrated by electronic maps.

3) *Mobility modeling and predication:*

The future position of the vehicle can be predicated because Vehicular nodes are usually constrained by prebuilt highways, roads and streets. Vehicles move along pre-defined paths, this provides an opportunity to predict how long routes would last compared to arbitrary motion patterns like the random waypoint model.

4) *Hard delay constraints:*

In VANETs applications, such as the collision warning or Pre-Crash Sensing, the network does not require high data rates but has hard delay constraints, and the maximum delay will be crucial.

5) *No power constraint:*

Since nodes are cars instead of small handheld devices, power constraint can be neglected because of always recharging batteries.

B. *VANET Structure [2]*

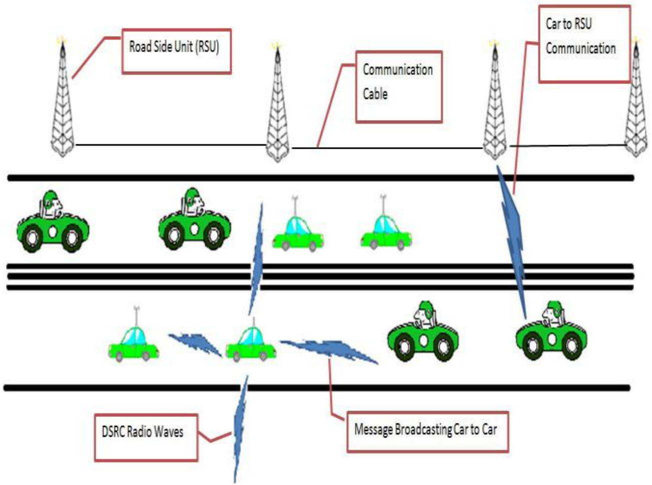

Fig. 1:VANET Structure **[2]**

C. Reference Architecture of VANET [1]

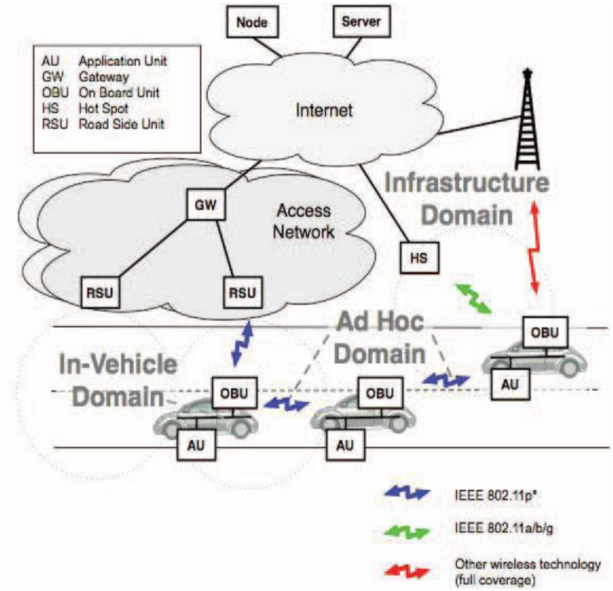

Fig. 2: Reference Architecture [1]

D. Component of Reference Architecture

1. OBU (on board unit)
2. RSU (road side unit)
3. AU (application unit)

1) OBU (on board unit) [3]

V2V and V2R communications are possible by A Physical device located in a vehicles.OBU has IPv6 GeoNetworking and an AU that contains regular IPv6 stack. Two communication are possible 1st is Station-internal Communication between AU and OBU is done by regular Ethernet and 2nd is station-external communication between OBU and other OBU/RSU is done by WLAN. Client application consists of two main components which are: Reporter, Receiver and HMI.

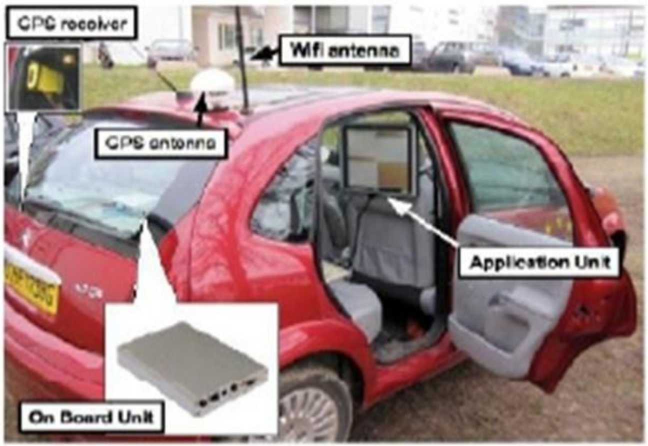

Fig. 3: Example of OBU, AU [3]

2) RSU (Road-Side Unit) [3]

For support both IPv6 Geo Networking and regular IPv6 routing RSU unit is used. A physical device located at fixed positions along roads, highways or dedicated locations. If RSU does not cover the necessary range for delivering GeoBroadcast packets, the packets is forwarded by nearby vehicles thanks to the multihop communication mechanism in IPv6 over C2Cnet.

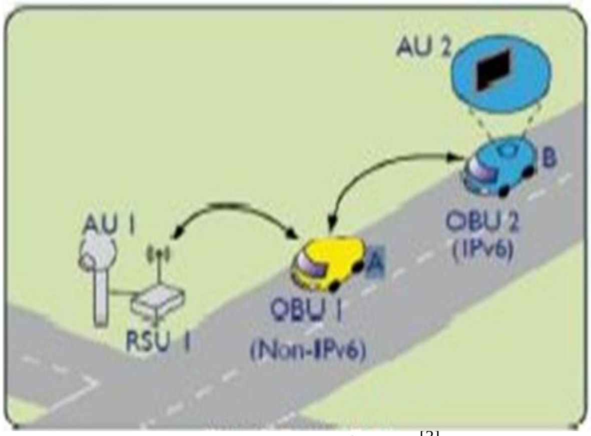

Fig. 4: Example of RSU [3]

3) AU (Application Unit) [3]

In-vehicle or road-side entity to runs applications that can utilize the OBU’s or RSU’s communication capabilities for that AU connected to the Internet. Server application has one main component and one support component: Disseminator, HMI.

E. Classification of routing protocol for VANET [4]

(1) Topology based routing protocols
(2) Position based routing protocols
(3) Cluster based routing protocols
(4) Geocast routing protocols
(5) Broadcast routing protocols

IV. TOPOLOGY BASED ROUTING PROTOCOLS

A. Proactive routing protocols

Proactive protocol is divided in two routing protocols.

1. Destination – Sequenced Distance – Vector Routing [DSDV]: Destination maintain all the successful path , and periodically exchange it with neighbours.

2. Fisheye state routing [FSR]: Maintains a TOPOLOGY TABLE (TT) based upon last information received from neighbouring and periodically exchanges it with local neighbours.

B. Reactive / Ad hoc based routing protocols

Reactive/Ad hoc based routing protocol is divided in four routing protocols.

1. Ad Hoc On Demand Distance Vector [AODV]:
This protocol has main three part:
-Route Requests (RREQs)
-Route Replies (RREPs)
-Route Errors (RERRs)
2. Temporally Ordered Routing Algorithm [TORA]: Creates DAG (Direct Acyclic Graph)
3. Dynamic Source Routing Protocol [DSR]: Flooding Route Request packets in the network
4. Junction - based Adaptive Reactive Routing [JARR].

V. POSITION BASED ROUTING PROTOCOLS

Position based routing protocol is divided in three routing protocols.

1. Connectivity Aware Routing Protocols [CAR]-Maintains the cache of Successful route between various source and destination.
2. Movement Based Routing [MORA]
See the direction of the neighbours
3. Street Topology Based Routing [STBR] Computing road connectivity at Junction nodes.

VI. Cluster Based Routing Protocols

Cluster based routing protocol is divided into two protocols.
1. Cluster Based Location Routing [CBLR]: A group of nodes identifies themselves to be a part of cluster and a one node is designed as cluster head will broadcast the packet to cluster. Provide good scalability but Increase Network delay & overhead Clustering for Open IVC Network [COIN] Proved inter vehicle communication (IVC).
Hierarchical Cluster Based Routing [HCB] is two layer Communication:
Layer -1: Single radio interface for communication with each other
Layer -2: Super node can communicate with node of other Cluster

VII. Geocast Routing Protocols

Geo cast routing is basically a position based multicast routing. Each node knows it's own & neighbour node geographic position by position determining service like GPS.
This protocol divided into two protocols:
1. Robust Vehicular Routing [ROVER] protocol: In this protocol only control packets are broadcast and Data packets are unicast.
2. Inter-Vehicle Geocast [IVG]:This is Timer based mechanism for message forwarding and Periodic broadcasts are used to overcome network fragmentation Distributed Robust Geocast [DRG] Improve the reliability of message forwarding by defining the zone of forwarding (ZOF)

VIII. Broadcast Routing Protocols

Broadcast routing protocol is divided into two protocols
1. BROADCOMM Routing Protocol: BROADCOMM is based on hierarchical structure for highway network. In this protocol highway is divided into virtual cells which move like vehicles.
2. Urban Multi-hop Broadcast protocol [UMB]
This protocol is designed to overcome the interference, packet collision and hidden node problem Sender node try to select the furthest node in the broadcast direction for forwarding and acknowledging Secure Ring Broadcasting [SRB] It is to minimize the Retransmission messages Classifies nodes into three groups: Inner Nodes, Outer Nodes , Secure Ring Nodes.

In this paper mainly focus on
1. How to find Neighbour Information
2. How to reduce broadcast.
3. How to protect packet data form attacker.
For above problem the proposed algorithm is designed.

- *How to finding neighbour information:*

Broadcasting messages can lead to frequent contention and collisions in transmission among neighbour vehicles. This problem is known as a broadcast storm.
For this problem tow scheme are there:
(1) Neighbour Information-based Broadcast Scheme (NIBS)
(2) Slotted p-persistence scheme

A. Neighbour Information-based Broadcast Scheme (NIBS)[5]*:*

In this scheme two things are done.
1st is Exchange of hello message and 2nd is building a neighbour table.
NIBS assume that every vehicle has a Global Positioning System (GPS) and knows its geographical position and velocity. Every vehicle periodically sends a hello message includes a geographical position and a vehicle ID. All the vehicles build their own neighbour tables which consist of vehicle IDs and the positions of vehicles based on the received hello messages. The neighbour tables are then used to select the best rebroadcasting vehicle for an emergency message.

Selection of rebroadcasting vehicle. NIBS is based on the slotted p-persistence scheme.

1) Slotted p-persistence scheme[5]:
upon receiving a message, a vehicle checks the message ID and relative distance between the sender and itself. The vehicle then knows which slot it belongs to and rebroadcasts the message at the time assigned to its slot, unless the vehicle overhears a duplicate message during the waiting time. However, the slotted p-persistence scheme has major two problems. In a sparse network, there may be an empty slot without any Vehicles, causing unnecessary waiting time. Meanwhile, in a dense network, too many vehicles can converge on one slot. This causes frequent contention and collisions leading to a broadcast storm.[5]

It Compares NIBS and slotted p-persistence scheme in terms of their end-to-end delay and collision ratio using an ns-2 simulator [5]
1) Simulation Environment.
2) Performance metrics.
3) Simulation results.

2) How to reduce broadcasting:
RSSI-Voting Algorithm [6]*:*
An asymmetric link problem is a considerable effect in vehicular network. Most of researches concerning this problem are extensions on unicasting routing protocols which have a primary route of data transmission. However, reliable broadcasting protocols such as Density-Aware Reliable Broadcasting protocol (DECA) have no exact route for sending data but do data dissemination therefore, making a solution for broadcasting protocols. For this problem design a method to select the most efficient preferred node with broadly transmission range and vastly neighbour coverage. RSSI-Voting algorithm as a new node selection algorithm. Each node votes a neighbour who has the highest Received Signal Strength Indicator (RSSI). When a sender wants to broadcast a message, it will select a preferred forwarder node who gains a majority vote. The simulation

results show that our mechanism can improve protocol performance up to 17% and decrease its retransmission overhead up to 28%.

Existing System:

In Existing System have protocols for security in VANET but in which public-private key based cryptography mechanisms are used which creates overhead.

Also in Existing system work is done on AODV but it will increase the traffic due to lots of Route Requests (RREQ) packets. So protocol has to be redesign in such a way so that it can overcome this issue and also supports the high mobility.

Proposed System:

In our proposed System, protocol for security as well as reliability in VANET for applications like content distribution which in result will increase the probability of delivery in Delay Tolerant Network. Like VANET.

Open Issues:

Content distribution in VANET is a challenge due to network dynamics and high mobility

In Proposed Algorithm:

Solution Approach:

1. Use Urban Multi-hop Broadcast protocol (UBM) for proposed algorithm.
2. Store-Carry-Forward paradigm.
3. RSSI (Received Signal Strength Index).
4. RSA public key cryptography method for security purpose.

IX. Proposed Algorithm

Sender_or_Intermediate_node()

1. Set timer in fixed interval.
2. Divide message into n packets.
3. Encode each packet using RSA public key cryptography method//for security
4. Until the timer expires each adjacent node calculates the velocity of node from RSSI value.
5. Set new relay node as node with lowest RSSI value //reduced network overhead.
6. If node with lowest RSSI value is nearer to radio range radius.
7. Then select new relay node equal to the node with next lowest RSSI value//to avoid packet loss
8. Above steps repeat until the timer expire.
9. If timer expire and no adjacent nodes with lowest 10. RSSI then blindly forward packet to the any adjacent node.
11. This process is repeat until the destination node is note found. proposed Algorithm which is somehow based on Urban Multi-hop Broadcast protocol (UBM).

A. Urban Multi-hop Broadcast protocol (UBM)

1) UBM is designed to overcome the interference, packet collision and hidden node problems during message distribution in multi hop broadcast.

2) In UMB the sender node tries to select the furthest node in the broadcast direction for forwarding and acknowledging the packet without any prior topology information.

3) UMB protocol performs with much success at higher packet loads and vehicle traffic densities.

4) In proposed algorithm RSSI (Received Signal Strength Index) for finding relay node to broadcast packet data.

5) In proposed algorithm RSA (Public key cryptography method) for encrypt packet data to achieve security. Use store-carry-forward paradigm.

X. Conclusion

As VANET is an emerging domain, there are lots of issues which are to be addressed. Out of that security issue in content distribution is booming so in proposed algorithm which is meant for Secure and Reliable Content Distribution in VANET.

References

[1] Yue Liu,Jun Bi, Ju Yang,“Research on Vehicular Ad Hoc Networks” ,CCDC (2009).

[2] Ghassan Samara, Wafaa A.H. Al- Salihy and R. Sures “Security Issues and Challenges of VANET”, University Sain Malaysia, IEEE (2010).

[3] Deesha G. Deotale & Uma Nagaraj,“ Survey of Vehicle Ad – Hoc Network” , IJCNS, vol-1 (2012).

[4] A.Chinnasamy, Dr. S. Prakash, “Chronicles of Routing Protocols for Vehicular Ad-Hoc Networks”,IJERA, Vol. 3, Iss. 2 (2013).

[5] Jae-Seung Bae, Dong-Won Kum, Jae-Choong Nam, Jae-In Choi, and You-Ze Cho “Neighbor Information-based Broadcast Scheme for VANET” ,IEEE (2012).

[6] Nattavit Kamoltham, Kulit Na Nakom, Kultida Rojviboonchai , “Improving Reliable Broadcast over AsymmetricVANETs Based on a RSSI-Voting Algorithm” ISPACS (2011).

[7] Uma Nagaraj, Poonam Dhamal, “Broadcasting Routing Protocols in VANET”, ISSN, Vol 1, No.2 (2011).

[8] Rong-Hou Wu, Yang-Han Lee, Hsien-Wei Tseng, Yih-Guang Jan, and Ming-Hsueh Chuang,“Study of Characteristics of RSSI Signal” , IEEE (2008).

[9] Pradeep B, Manohara Pai M.M , M. Boussedjra, J. Mouzna ,“GlobalPublic Key Algorithm for secure location service in VANET” ,IEEE (2009).

[10] Khalid Haseeb, Dr.Muhammad Arshad, Dr.Shazia Yasin, Naveed Abbas, “A Survey of VANET’s Authentication” ISBN- (2010).

[11] Anup Dhamgaye, Nekita Chavhan, “Survey on security challenges in VANET” , IJCSN-volume2 (2013).

[12] Mostofa Kamal Nasir, A.K.M. Kamrul Islam, Mohammad Touhidur Raman and Mohammd Khaled Sohel,“Taxonomy of Security in Vehicular Ad-Hoc Network” ,IJSRP, Vol-3 (2013).