INTELLIGENT VEHICULAR COMMUNICATION SYSTEM FOR COLLISION AVOIDANCE AND EVALUATION METRICS

Vijeta Verma[1], Vidha Sharma[2]

[1]*Software Engineer, Nescant Info Systems Pvt. Ltd, Delhi, (India)*

[2]*M.Tech (CSE), D.I.T.M.R, Faridabad, Haryana, (India)*

ABSTRACT

Adhoc networks consider vehicals as their prime area of development and many projects are already running for investigation of number of application areasincluding traffic and travel information systems.

In this paper we present conceptual model of intelligent networks and the general concept of intelligent ad hoc vehicular network for Collision Avoidance and later we describe the logical framework auto sensing of traffic information in vehicular ad hoc networks. Collaborative Signal and Information Processing is utilized to allow this higher level information to be generated by collaboration between nodes.

Efficient traffic alerts and updated information about traffic incidents will reduce traffic jams, increase road safety and improve the drivingin the city.

This scheme is application specific and requires some knowledge of the topology of the road network. At this stage we have assumed this information can be obtained from a digital map.

Keywords: Gps, Manet, Traffic & Travel Information Systems, Vanet , Vehicular Networks, Wireless Technology

I. INTRODUCTION

Vehicular Ad Hoc Networks (VANET) are a form of MANETs used for communication among vehicles and between vehicles and roadside equipment.

InVANET is an Intelligent Vehicular AdHoc Networking and uses WiFi IEEE 802.11 and WiMAX IEEE 802.16 for easy and effective communication between vehicles with dynamic mobility. Effective measures such as media communication between vehicles can be enabled as well methods to track automotive vehicles. InVANET is not foreseen to replace current mobile (cellular phone) communication standards.

1.1 Mobile Ad-Hoc Network (MANET)

A mobile ad-hoc network (MANET) is a kind of wireless ad-hoc network, and is a self-configuring network of mobile routers (and associated hosts) connected by wireless links – the union of which form an arbitrary topology. The routers are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger Internet.

Many commercial field forces deploy a ruggedized portable computer such as the Panasonic Tough book 29 with their fleet of vehicles. This requires the units to be anchored to the vehicle for driver safety, device security, and user ergonomics. The rugged laptops are rated for severe vibration associated with large service vehicles and off-road driving, and harsh environmental conditions of constant professional use such as in EMS, fire and public safety.

Within an ad hoc network, although each node (vehicle) is an independent device, by coordinating their sensing, processing and communication to acquire information about their environment, it is possible to accomplish high level tasks. This collaboration makes nodes more autonomous and as a whole, forms a novel type of distributed sensor network.

II. INTELLIGENT NETWORKS

2.1. The Need for Intelligence

Integration of 3G solutions isn't the only step mobile operators must take to support today's and tomorrow's subscribers and services.

They must deploy systems that utilize leading technologies to the fullest advantage. The new systems must provide two key areas of System intelligence. The interaction with subscribers, services, and transport mechanisms. The service flexibility, which is the ability to enable subscribers to choose how they access the network and their services.

2.1.1. Interaction

The level of interaction requires the advanced ability to inspect packets from individual transactions in great detail, which will provide the mobile operator with a greater understanding of its subscribers. With this vital capability, mobile operators can determine subscriber usage patterns, and then make intelligent decisions regarding deployment of customized services and service billing.

In order to capture this information, mobile operators must deploy an intelligent mobile gateway at the edge of the packet core that will perform deep packet inspection to determine the subscriber's service level and align it with applications, location, portal access, community.

Services or other criteria. It can then examine the network status and conditions. When the intelligent mobile gateway understands all the dynamics of the subscriber session, it can intelligently shape the session using quality of service (QoS), bandwidth allocation, and flow control. This allows operators to actively shape and manage traffic flows, improving the mobile subscribers' experience, and appropriately charging the subscriber.

Furthermore, deep packet inspection functionality provides much more flexibility for operations, such as subscriber classification and billing. With this ability, mobile operators can account and bill for services based on criteria, such as time, location, per usage, service level, destination, application, and other parameters, while employing billing techniques like pre-paid, reverse charge, push service billing, and many others.

2.1.2. Service Flexibility

An intelligent mobile gateway positioned at the edge of the network not only efficiently handles the traffic, it has the processing power and memory required for a resource intensive transaction, such as streaming audio or video, that would ordinarily overburden a mobile device. In such transactions, the information can be cached at the edge of the network where it can be appropriately processed, managed, and streamed to the subscriber, reducing the impact on the mobile device and network, thereby enhancing the subscriber's capabilities.

2.2. Conceptual Model of The Intelligent Network

The IN standards present a conceptual model of the Intelligent Network that model and abstract the IN functionality in four planes shown in "Fig. 1" –

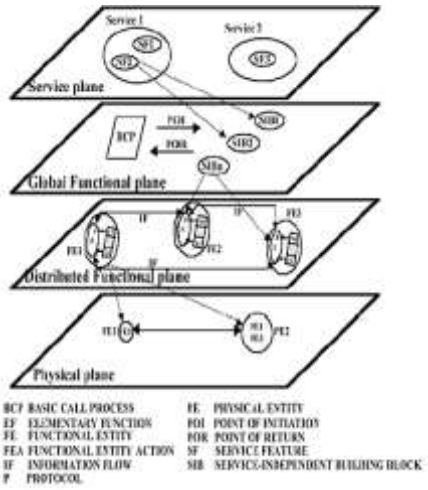

Figure 1: IN Conceptual Model

The **Service Plane (SP):** This plane is of primary interest to service users and providers. It describes services and service features from a user perspective, and is not concerned with how the services are implemented within the network.

The **Global Functional Plane (GFP):** The GFP is of primary interest to the service designer. It describes units of functionality, known as service independent building blocks (SIBs) and it is not concerned with how the functionality is distributed in the network. Services and service features can be realised in the service plane by combining SIBs in the GFP.

The **Distributed Functional Plane (DFP):** This plane is of primary interest to network providers and designers. It defines the functional architecture of an IN-structured network in terms of network functionality, known as functional entities (FEs). SIBs in the GFP are realised in the DFP by a sequence of functional entity actions (FEAs) and their resulting information flows.

The **Physical Plane (PP):** Real view of the physical network. The PP is of primary interest to equipment providers. It describes the physical architecture for an IN-structured network in terms of physical entities (PEs) and the interfaces between them. The functional entities from the DFP are realised by physical entities in the physical plane.

III. CONCEPT OF INVANET

InVANET is an Intelligent Vehicular AdHoc Networking and uses WiFi IEEE 802.11 and WiMAX IEEE 802.16 for easy and effective communication between vehicles with dynamic mobility. Effective measures such as media communication between vehicles can be enabled as well methods to track automotive vehicles. InVANET is not foreseen to replace current mobile (cellular phone) communication standards.

"Older" designs within the IEEE 802.11 scope may refer just to IEEE 802.11b/g. More recent designs refer to the latest issues of IEEE 802.11p (WAVE, draft status). Due to inherent lag times, only the latter one in the IEEE 802.11 scope is capable of coping with the typical dynamics of vehicle operation.

Automotive vehicular information can be viewed on electronic maps using the Internet or specialized software. The advantage of WiFi based navigation system function is that it can effectively locate a vehicle which is inside big campuses like universities, airports, and tunnels. InVANET can be used as part of automotive electronics, which has to identify an optimally minimal path for navigation with minimal traffic intensity. The system can also be used as a city guide to locate and identify landmarks in a new city.

Communication capabilities in vehicles are the basis of an envisioned Intelligent Vehicular AdHoc Network (InVANET) or Intelligent Transportation Systems (ITS). Vehicles are enabled to communicate among themselves (vehicle-to-vehicle, V2V) and via roadside access points (vehicle-to-roadside, V2R). Vehicular communication is expected to contribute to safer and more efficient roads by providing timely information to drivers, and also to make travel more convenient. The integration of V2V and V2R communication is beneficial due to the fact that V2R provides better service sparse networks and long distance communication, whereas V2V enables direct communication for small to medium distances/areas and at locations where roadside access points are not available.

Providing vehicle-to-vehicle and vehicle-to-roadside communication can considerably improve traffic safety and comfort of driving and traveling. For communication in vehicular ad hoc networks, position-based routing has emerged as a promising candidate. For Internet access, Mobile IPv6 is a widely accepted solution to provide session continuity and reach ability to the Internet for mobile nodes. While integrated solutions for usage of Mobile IPv6 in (non-vehicular) mobile ad hoc networks exist, a solution has been proposed that, built upon on a Mobile IPv6 proxy-based architecture, selects the optimal communication mode (direct in-vehicle, vehicle-to-vehicle, and vehicle-to-roadside communication) and provides dynamic switching between vehicle-to-vehicle and vehicle-to-roadside communication mode during a communication session in case that more than one communication mode is simultaneously available.

3.1. Ipv6

Mobile IPv6 is a version of Mobile IP - a network layer IP standard used by electronic devices to exchange data across a packet switched internetwork. Mobile IPv6 allows an IPv6 node to be mobile—to arbitrarily change its location on an IPv6 network—and still maintain existing connections.

IV. INTELLIGENT TRANSPORTATION SYSTEM NETWORK ARCHITECTURE

The ad hoc network will comprise two node types: mobile nodes (vehicles) and fixed nodes deployed at the roadside. The number of fixed nodes in the network will be small relative to the number of mobile nodes. A subset of these fixed nodes will be connected to external networks. Each vehicle participating in the ITS will be equipped with a telemetric platform interfaced to on-board systems through a CAN bus. Through this platform data will be collected and analyzed from on-board sensors. These sensors may include,

- Anti-Lock Braking System (ABS)
- Automatic Traction Control (ATC)
- Speedometer
- Airbag and crash sensors.

It is assumed that vehicles are able to obtain positional information from on-board GPS receivers. All nodes are equipped with a processor, memory and digital communication equipment. Nodes organize themselves into a number of local ad hoc networks (or clusters). At this local level, a proactive routing scheme is adopted so that

communication between nodes in the same cluster is responsive. Nodes advertise their presence to their immediate neighbors by transmitting periodic beacons.These beacons are essentially empty packets with information contained only in the packet header. Information in the packet header is shown in Table 1;

Field Name	*Description*
Node ID	Unique identifier.
Time-stamp	Time packet was transmitted.
Destination	ID of destination node
Location	Geographical location of originating node.
Velocity	Velocity of originating node.
Heading	Navigational heading of node.

Table 1: Summary of packet header

On receipt of a beacon message, the 'node id' of the originating node is added to a list of neighbors. Nodes regularly scan this list to determine link states. If no beacon message is received from a node in the list, after a given period of time the neighbor is considered lost. This process enables link-state information to be constructed and maintained for the local ad hoc network.

4.1 Collaborative Signal and Information Processing

Collaborative signal and information processing (CSIP) [Kumar et al, 2002] provides the data representation and control mechanisms to allow nodes in the ad hoc network to collaboratively process and store sensor information, respond to external events and report results [Liu et al, 2002].

Traffic information is generated in the network by means of task requests. Task requests may be issued by individual nodes or they may be 'injected' into the network through a fixed node with a connection to an external network. Task requests are divided into types with each relating to some well-known traffic phenomenon, for instance one task request may be to detect "ice on the road". Each task request type is associated with one or more of the available onboard sensors which may be sampled to determine the existence of the phenomenon. Taking the "ice on the road" task request as an example, it may be associated with the ABS, ATC and an external thermometer. Particular readings from each of these sensors can be interpreted to indicate that there is "ice on the road".

When a sensing task is generated, it is added to the task list of the originating node. Each entry in the task list contains a number of name-value pairs The node then transmits the task request to its immediate neighbors. On receipt of the task request, the receiving node checks if there is a corresponding entry in its own task list. If a task request of equal priority and of the same origin is not found in the task list, the new task request is added. The node then directs its subsystems to begin sampling each of the on-board sensors that has indicated by the type of the task request. Samples are then compared with the ranges specified and combined to determine if the event type given in the task request is also occurring at that location. These results are summarized in a task response message and transmitted to the node identified as the origin of the task request When task requests are forwarded, the forwarding node adds their own 'node ID' to the task request i.e., they become the originator of that task request. This process enables task requests to propagate through the network. If an individual node's task list grows too large, task requests with the lowest priorities are removed. Any task request which has expired will also be removed. As task responses are generated, they will propagate back to the originator of the

task request. This node will have a number of responses associated with a single request. These responses are then combined to localize traffic phenomenon i.e., the locations of responses giving high confidence levels can be used to produce a boundary for the traffic phenomenon detailed in the original request. The task response message at the originating node may then be distributed.

4.2 Information Distribution

Traffic information is most likely to influence drivers' decisions when it relates to the immediate area or when they are likely to enter into that area. To maximize information gain in the network whilst keeping the consumption of network resources to a minimum, traffic information (i.e., task response messages) will only be transmitted to a node if that information is relevant in terms of the nodes likely route. Consider the scenario shown in Fig. 2; at time *t1*, a node belongs to cluster 1 and is involved in CSIP to detect a particular event in the traffic network and a task response message is generated. The node's heading changes and the links to nodes in cluster 1 are destroyed. Later, at time *t2*, the node comes into communication range of a second cluster.

Links between the node and others in the local ad hoc network are established through the neighbor discovery protocol outlined in section 3.1. As new neighbors are discovered, the node receives beacon messages with positional information included in the packet headers (see Table 1). This positional information is combined with information about the structure of the road network (e.g., a digital map) to determine the likely route of each neighbor. Using this information, the receiving node examines the list of task response messages for any that relate to possible routes of each neighbor. Relevant traffic information is transmitted to that neighbor.

This method of information distribution is novel in that the movement patters of a node are used to determine when it should be provided with traffic information. We anticipate that this method will reduce bandwidth consumption whilst increasing information gain, outweighing any cost associated with the additional processing necessary.

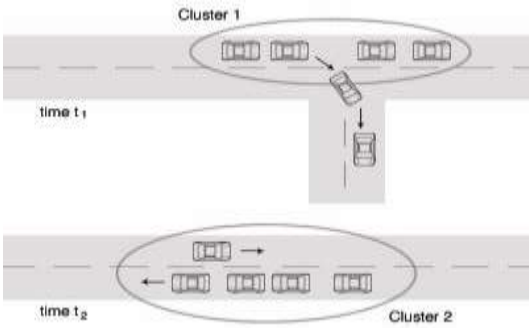

Figure 2: A Task Response Message Is Stored In A Mobile Node and Distributed To Another Ad Hoc Cluster.

V. ROUTING METHODOLOGY

In VANETs, wireless communication has been a critical technology to support the achievement of many applications and services. However, due to the characteristics of VANETs such as high dynamic topology and intermittent connectivity, the existing routing algorithms in MANETs are not available for most application scenarios in VANETs.

Depending on the number of senders and receivers involved, routing approaches can be divided into three types: geocast/broadcast, multicast, and unicast approaches.(i) Geocast/Broadcast- With the requirement of distributing

messages to unknown/unspecified destinations, the geocast/broadcast protocols are necessary in VANETs. The current message broadcast protocols on vehicular ad hoc networks, such as a spatially aware packet routing algorithm (which predicts the permanent topology holes and conducts the geographic forwarding), SADV (which finds the best path to forward the packet), an interference aware routing scheme (which equips the node with a multichannel radio interface and switches the channels based on the SIR evaluation), FROV (which selects the retransmission spans further node to rebroadcast a message), and a multihop broadcast protocol (which divides the road into segments and chooses the vehicle in the farthest nonempty segment). (ii)Multicast- Multicast is necessary to communications among a group of vehicles in some vehicular situations, such as intersections, roadblocks, high traffic density, accidents, and dangerous road surface conditions. The multicast protocols have been categorized into two main types. One is topology-based approaches, such as ODMRP (which generates a source-based multicast mesh and forwards based on the group address), MAODV (which generates a group-based multicast tree), and GHM (which generates group-based multicast meshes). The other one is location-based approaches, such as PBM (which is based on positions of all one-hop neighbors and positions of all individual destinations), SPBM (which introduces hierarchical group membership management), LBM (which uses a multicast region as destination information for multicast packets), and RBM and IVG (which define a multicast scope for safety warning messages). (iii) Unicast- The unicast communication protocols for VANETs have three approaches- greedy: nodes forward the packets to their farthest neighbors towards the destination, like improved greedy traffic-aware routing (GyTAR); opportunistic: nodes employ the carry-toward technique in order to opportunistically deliver the data to the destination, like topology-assist geo-opportunistic routing; and trajectory based: nodes calculate possible paths to the destination and deliver the data through nodes along one or more of those paths, like trajectory-based data forwarding (TBD)

VI. EVALUATION METRICS

Metrics have been designed for evaluating the performance of VANET at application and Network Layer. The major factors of evaluation metrics are shown in the Table 2.

Factors of evaluation	**Description**
Delay Time	Compared to ideal time vehicle would take in absence of signals and other vehicles
Estimation Error	Accuracy of information availaible in the range specified
Transmission delay	Average delay of a packet when the packet is generated, until the time it gets successfully received by all neighbors
Packet delivery ratio	Ratio of the number of messages received by the destination to the number sent by the sender
Jitter	Jitter is the variation in the end-to-end delay between packets arriving at the destination
Connection duration	To monitor a meaningful interaction between different parties
Load on the network	Number of packets sent, received and dropped
Awareness percentage	Fraction of nodes passing the location that had information about the location before entering it

Table 2: Performance factors evaluation metrics of VANET at Application and Network Layer

VII. CONCLUSION

In this research paper we have presented the general concept of intelligent ad hoc vehicular network for Collision Avoidance. Also here we have presented the logical framework auto sensing of traffic information in vehicular ad hoc networks.

It also deals with efficient traffic alerts and updated information about traffic incidents will reduce traffic jams, increase road safety and improve the driving in the city, but in spite of having all the measures it suffers with few minor issues like delay jitter, network load which we will be addressing in our next research work.

REFERENCES

[1]. Wang, J., & Yan, W. (2009). RBM: a role based mobility model for VANET. In Proceedings of international conference on communications and mobile computing January 2009.

[2]. Chen, Y., Lin, Y., & Lee, S. (2010). A mobicast routing protocol for vehicular ad hoc networks. ACM/Springer Mobile Networks and Applications

[3]. What is the Best Achievable QoS for Unicast Routing in VANET ?Mate Boban, Geoff Misek, and Ozan K. Tonguz 2009 IEEE

[4]. J. Freebersyser, B. Leiner, "A DoD Perspective on Mobile Ad Hoc Networks", In "Ad Hoc Networking", edited by Charles E. Perkins, chapter 2, pp. 29-51, Addison-Wesley, 2001.

[5]. M. THOMAS et al.:"Auto-sensing" Intelligent Simulation and Modeling GroupSchool of Computing and Informatics, Nottingham Trent University, Burton Street, Nottingham NG1 4BU. UK

[6]. "The basics of the GSM technology platform"GSM World focus 1996 , published by "Mobile Communications International"

[7]. "Wireless Data" IEEE Communications Magazine - January 1995

[8]. J. Schiller "Mobile Communication", Addison Wesley.