Wireless Netw (2016) 22:2369–2386
DOI 10.1007/s11276-015-1104-z

Review of vehicular ad hoc network communication models including WVANET (Web VANET) model and WVANET future research directions

M. Milton Joe[1] · **B. Ramakrishnan**[2]

Published online: 31 October 2015

Abstract The most ever growing research field is vehicular ad hoc network. This prominent research field has the widely known communication models such as RoadSide Unit Communication, Vehicle to Vehicle Communication, and Cluster based Communication models. In addition to that M. Milton Joe and B. Ramakrishnan et al. have proposed a new communication model known as WVANET (Web VANET) for vehicular ad hoc network communication. The authors portray that WVANET will be the everlasting research field in future. This WVANET (Web VANET) communication model is fundamentally different from other communication models as it makes use of web signals to disseminate the messages among vehicles. Of course, each communication model in VANET will have its own various pros and cons. This paper provides the overall review of all the existing communication models in VANET and in addition to that WVANET (Web VANET) communication model is also presented. Further this paper discusses the various future research that can be done in WVANET (Web VANET) communication model.

Keywords WVANET · VANET · Web · WiMax · XMPP · XML · OBU · RSU · Cluster

✉ M. Milton Joe
m.miltonjoe@gmail.com

B. Ramakrishnan
ramsthc@gmail.com

[1] Department of Computer Application, St. Jerome's College, Nagercoil, Tamilnadu, India

[2] Department of Computer Science and Research Centre, S.T. Hindu College, Nagercoil, Tamilnadu, India

1 Introduction

Everlasting research field these days are vehicular ad hoc network (VANET) and web technology [1].

1.1 Vehicular ad hoc network

Those days research was on mobile ad hoc network (MANET). The fundamental research on MANET laid the foundation for the new research field known as vehicular ad hoc network (VANET) [1–4]. VANET could be differentiated from MANET by the movements of the nodes. In MANET nodes can move at any directions which may form mesh topology [5]. However, in VANET nodes can move only in the predefined topology (Road) [6]. Another differentiating parameter between MANET and VANET is speed of the nodes. Normally speed of the nodes in MANET is very slow comparing to the nodes of VANET [7–11]. Hence, message dissemination in VANET could be difficult since the nodes are moving at high speed. Researchers have modelled various algorithms to broadcast the messages among nodes in VANET efficiently. In order to send and receive the messages in VANET each vehicles is equipped with On Board Unit (OBU) [12–14]. Message dissemination can be done with the help of protocols. The same protocols used in MANET also can be applied in VANET [15, 16]. As we know the speed of the node in VANET is high, the researchers introduced new protocols to broadcast the message efficiently among the nodes. The fundamental aim of any mobile communication technology is to increase the performance metrics [17, 18]. To achieve high performance efficient routes should be chosen between the source and destination [19]. Wireless sensors are fixed in the vehicles for data collections such as environment monitoring and emergency detection to

disseminate the messages efficiently [20–22]. Research on VANET is carried out in the following communication models namely RoadSide Unit, Vehicle to Vehicle, and Cluster based Communication models so far.

1.2 Web technology

Another prominent research field is web technology which played an important role in people's life [23–25]. It is used to establish communication among the various electronic devices by World Wide Web [26]. Services of World Wide Web (WWW) can be adopted by each electronic device by obtaining the Network address know as IP address. This IP address is used to identify the device in the communication network. The web 2.0 is developed after having much research in web technology and later other technology such as web 3.0 is also developed [27–29]. The various research done on information technology (IT) made the communication possible from anywhere and anytime to connect with one another to exchange the messages [30]. These days most of the time of an individual is spent on the web technology to connect with one another [31]. This web technology becomes popular among the users because this could be the cheap and fastest communication medium forever [31]. Another fundamental advantage of web technology is that message can be disseminated within a fraction of time [31].

From the above views it can be concluded that vehicular ad hoc network and Web Technology are unbeatable research fields. There was no research performed in the combination of VANET and Web Technology. VANET and Web Technology are considered as the different research platform so far. Recently M. Milton Joe and B. Ramakrishnan et al. have proposed a novel communication model known as WVANET (Web VANET) by integrating VANET and web technology.

In this paper all the existing communication models in VANET such as RoadSide Unit, Vehicle to Vehicle, and Cluster based Communication models are reviewed. In addition to that recently introduced WVANET (Web VANET) Communication model is also reviewed and further future research discussions of WVANET (Web VANET) is also presented in this paper.

2 Vehicular ad hoc network communication models

Research on vehicular ad hoc network (VANET) has been carried out in the following communication models.

- RoadSide Unit communication model
- Vehicle to Vehicle communication model
- Cluster based communication model
- Web VANET (WVANET) communication model

2.1 RoadSide Unit communication model

Research in vehicular ad hoc network was started with RoadSide Unit (RSU) communication model [32]. The fundamental architecture of this communication model is fixing the antenna (RoadSide Unit) at the side of the roads and the signal is propagated from it. Each vehicle will get the signal to communicate with other vehicle from the nearby RoadSide Unit (RSU). One of the biggest challenge in vehicular ad hoc network or any other ad hoc network communication is preventing the node from link disconnection as the topology of the network is changed dynamically [33–35]. Data transmission may get failure due to poor quality of wireless links among the nodes and sometimes there may be no links between the source and destination [36–38]. In order to avoid dis-connectivity among the nodes, a Dedicated Short Range Communication (DSRC) is used in VANET communication [39]. This DSRC functions like a wireless protocols which is similar to Wi-Fi.

RoadSide Unit (RSU) communication architecture is represented in Fig. 1. As illustrated in Fig. 1 each vehicle will get the signal from the nearby RSU. Identity of each vehicle will be available at the RSU. All the RSUs will act as the router in vehicular ad hoc network communication scenario. However, this communication architecture has the various kinds of advantages and disadvantages as illustrated below:

2.1.1 Advantages of RSU communication model

- Centralized communication

RSU based communication model is similar to centralized communication. All the nodes in network topology are

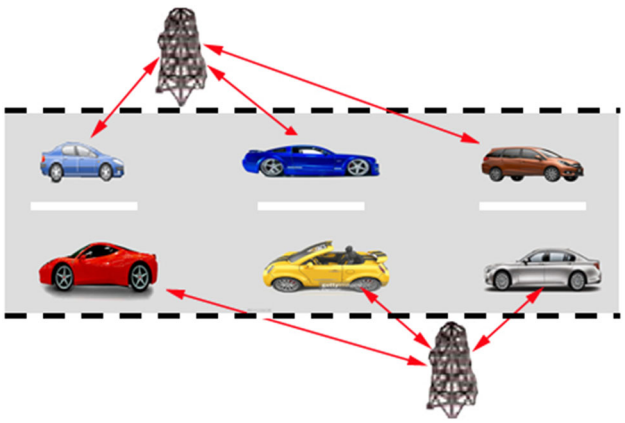

Fig. 1 RoadSide Unit communication model

connected to the nearest RSU where the RSUs are fixed and centralized. As RSUs are centralized the communication can be synchronized and coordinated more efficiently.

- RSUs errors can be fixed easily

As the communication scenario is centralized, it will be easy to fix errors that occur in the RSU. As RSUs are fixed the location of the RSU can be identified quickly and errors occur in the RSU can be rectified sooner.

- Server/client computing model

In RoadSide Unit (RSU) communication model the RSU acts as the server and the nodes act as the clients. All the nodes are connected to the nearest RSU. Since this communication works as a server/client computing model, it will be easy for the RSU to control the nodes and the activities of the nodes can be monitored effectively.

- Less security issues

Every node in this communication architecture is under the control of a RSU and every message transmission can be done only through RSU. If the RSU is alone secured form the various types of security attacks the network communication can be carried out with less security threats.

2.1.2 Disadvantages of RSU communication model

- Many number of RSUs are Needed and More Expensive

The communication range of DSRC is limited to 100–300 m approximately which indicates that many RSUs are obviously needed to establish the comfortable communication among the nodes. Implementing more number of RSUs are highly expensive.

- Link disconnection

Another major drawback of RSU communication model is link disconnection among the nodes. All the nodes should be connected with the DSRC signal to disseminate the messages among the nodes efficiently. As the mobility pattern of VANET nodes are high, the node will be disconnected often from the DSRC signal range.

- Failure of RSU

Any message transmission among the nodes is possible only through RSU. Consider the case, if anyone of the RSU gets failure the entire network will be collapsed. All the nodes under the particular RSU will not be under the coverage and those nodes cannot get any information such as warning alert messages, emerging messages and so on from the other nodes.

- RSU will slow down with multiple service requests

In this communication architecture RSU acts as the server in responding back to the nodes. In high density network topology a single RSU will receive multiple requests from the nodes at the same time. In this case, the working process of RSU will get slow down which will degrade the communication performance among the nodes. With multiple requests at the same time the RSU may not be able to respond back to all the nodes and even some of the service request may be dropped.

- Communication is possible through RSU only

A node can initiate the communication with other node through RSU only. RSU routers the messages to the other nodes and it should be noted that no two nodes can communicate directly. All the communication can be carried out only through RSU which will take more time to deliver the messages among the nodes.

Hence, from the above views it can be identified that RSU communication architecture has various drawbacks. An effective communication model must be needed to overcome the drawbacks exists in RSU communication architecture. Hence, researchers we trying to find out another reliable communication model for vehicular ad hoc network.

2.2 Vehicle to Vehicle communication model

Various research made on vehicular ad hoc network found the new communication model known as Vehicle to Vehicle (V2V) Communication Model. In this V2V Communication architecture each vehicle is manufactured with On Board Unit (OBU), which is capable of sending and receiving the messages among vehicles [40–42]. This network architecture removed the limitations exist in RoadSide Unit communication model. Especially fixing of RSUs at the side of roads are completely eliminated and direct vehicle to vehicle communication is made possible [43]. Each node in V2V model functions as the router to transmit/receive the messages. The V2V communication model is depicted in the Fig. 2. As shown in the Fig. 2 each vehicle will get connected with other vehicle through the DSRC signal. This V2V

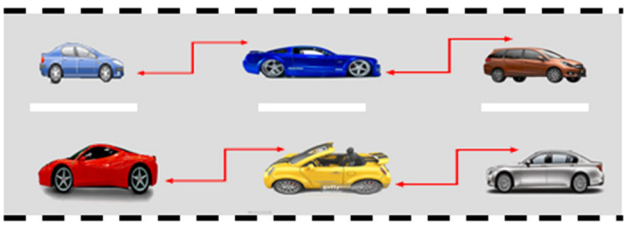

Fig. 2 Vehicle to Vehicle communication model

communication is much used to deliver the warning messages and emergency messages. Later this communication was improved to respond to the service requests received from the nodes. Though this communication model is better than the RSU model, it has certain advantages and disadvantages as described below.

2.2.1 *Advantages of Vehicle to Vehicle communication model*

- Less installation cost as RSU is removed

The main advantage of this communication model is less installation cost as RSU is replaced by On Board Unit (OBU).

- Network failure may be reduced

As the communication is carried out vehicle to vehicle, the failure of a vehicle will not lead to the entire network failure. If one vehicle gets failure the process of that particular vehicle can be carried out by another vehicle.

- Efficient routing process can be determined

As each vehicle in this communication model acts as the router an efficient and shortest routes can be chosen to deliver the data to the destination. Efficient routing protocol to determine the route discovery can be modelled based on the behaviors of the nodes.

2.2.2 *Disadvantages of Vehicle to Vehicle communication model*

- Multi-hop communication model

This V2V communication model is also known as Multi-hop communication architecture. That is, communication between the source and destination is possible only through intermediate vehicles. In highway environment, if there is no intermediate vehicles between source and destination, the message cannot be routed to the intended recipient [44]. Ultimately the message transmission delay will be high.

- Link disconnection

Another problem of DSRC signal propagation model is link disconnection among the nodes. The range of DSRC is approximately 100–300 m. The nodes within the city environment will get connected with the signal as the mobility pattern of the node is slow. However in the highways the mobility pattern of the nodes are high which will lead to link disconnection often.

- Authentication of nodes

In this V2V communication model each vehicle acts as the router in transmitting the messages among the nodes. In this case each vehicle in the network topology should be trust worthy. For the same, each vehicle should be authenticated efficiently. False authentication or spoofing of the identity will cause in spreading of the false messages among the nodes and the entire communication will be collapsed.

- Duplication of data

Though efficient authentication mechanism are applied to authenticate the nodes, it is also possible to duplicate the data with the wrong data. It cannot be trusted always that forwarding node forwards the data that it has received from its neighboring node. The attacker may change the data while sending the data to the next hop or may not forward the data to the next hop.

- Message transmission time

As discussed earlier message transmission is possible with the help of intermediate vehicles. There will be many number of intermediate vehicles to select the next hop. Next hop selection algorithm should be modelled efficiently so that the message can be routed efficiently. The selected next hop node should be trust worthy otherwise the message may be dropped. There are many factors that need to be considered and monitoring of each node will lead to high overhead. When a message is transmitted through multi-hop nodes the message transmission time will be a little more than sending of the messages directly between the nodes.

- Weak security

VANET network topology is being changed rapidly. Monitoring each node in the network architecture is a difficult task. In this V2V communication model all the processes are given to the nodes itself which will lead to the security threat always. In this V2V communication architecture, we cannot trust all the nodes and some nodes may misbehave. Misbehaving nodes will degrade the communication performance in the network. The malicious node will change the data and even it can spread out the false information to the network and so on. In this case, a secure algorithm should be modelled for identifying the malicious nodes to prevent the network from the various attacks [45].

2.3 Cluster based communication model

After considering the drawbacks of the previous communication models in vehicular ad hoc network, researcher proposed a novel communication architecture know as Cluster Based Communication Model. The illustration of Cluster based communication model is shown in Fig. 3. As

demonstrated in Fig. 3 all the vehicles are grouped into various number of clusters depending on the density of the vehicles [41]. One vehicle is chosen as the cluster head for each cluster by considering the various parameters [41]. This architecture is similar to client/server model. That is, cluster head will act as the server and all the nodes under a cluster head will act as the clients. All the cluster heads are interconnected in such a way that it would be easy to disseminate the messages to other cluster heads [41]. This communication model eliminated the concept of multi-hop communication environment by employing cluster heads. Cluster head will store all the acquired data in its database and it will distribute the data to its clients as it is requested by the nodes. A special procedure called synchronization algorithm is executed at a regular periodical interval in such a way that all the cluster heads will update the data with one another [41, 46, 47].

2.3.1 Advantages of cluster based communication model

- Network topology is defined for effective communication

In VANET communication another type of distributed communication architecture is defined as clusters. Cluster based communication will have the control over the nodes in VANET architecture and the effective communication can be carried out.

- Multi-hop communication is reduced

The main drawback of vehicle to vehicle communication model is multi-hop communication methodology which will degrade the communication performance when the distance between the source and destination is long. In cluster based communication this multi-hop structure is somewhat reduced and it leads to better communication performance in the V2V communication architecture.

- Server/client communication architecture

Here, cluster heads act as the server and all the other nodes under the cluster heads act as the clients. This mechanism provides a control among the nodes. Cluster head can monitor its client nodes and the misbehaving nodes can be identified effectively.

- Non-infrastructure based RSUs

In cluster based communication architecture all the cluster heads are acting as the RSU. However, here all the cluster heads are not fixed which will lead to less link disconnection among the client nodes and a better communication performance can be achieved.

- Network failure may be reduced

In cluster based communication model all the cluster heads are connected with one another. If a cluster head gets failure the process of that cluster head will be taken over by the nearest cluster head and immediately new cluster head will be elected. This prevents the network failure and enhances the communication performance.

- Synchronization procedure call

In cluster based communication model synchronization procedure call is executed at the regular periodical time. When a node gets a new information, it is sent to the cluster head immediately and the cluster head keeps the information to serve the other nodes upon request. During the synchronization procedure call execution each cluster head updates the newly received information with other cluster heads which makes sure that the new information is available to all the nodes in the network topology.

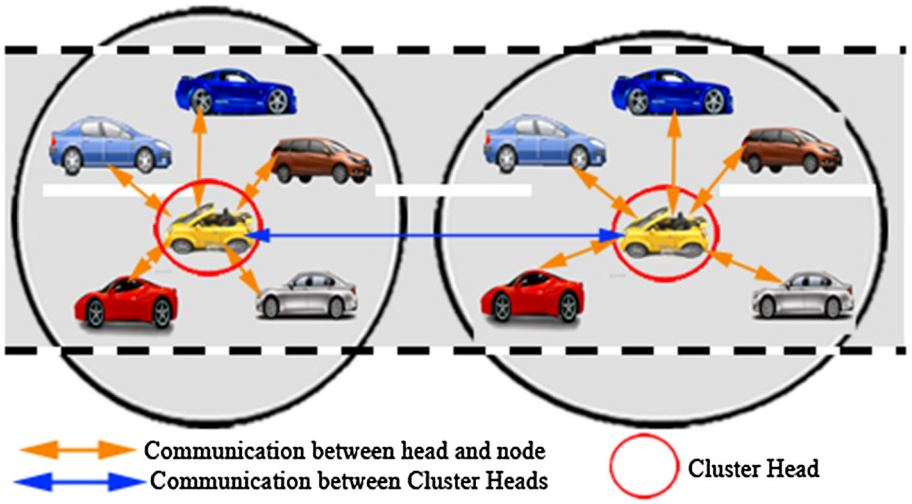

Fig. 3 Cluster based communication model

2.3.2 Drawbacks of cluster based communication model

- Cluster head election overheads and switching overheads

Based on the density of the vehicles in the network topology various numbers of clusters are created. In highway environment network topology will change rapidly which will lead to election of new cluster heads. Election of new cluster head and switching of the control form the previous cluster head to the new cluster head will lead to high overheads. This situation is applicable to all the cluster heads that are exist in the network environment.

- Poor memory utilization

In the cluster based communication model all cluster heads store the data that have been received from its client nodes. A special procedure called synchronization algorithm is executed to update the data with other cluster heads which ensures that all the cluster heads will have the same data at a regular periodical time. It must be noted that all the cluster heads retain the redundant data in it which leads to poor memory utilization.

- Transferring of data

In this communication model as soon as a new cluster head is elected the data of the old cluster head should be transferred to the new cluster head. This process takes certain time to exchange the database depending upon the size of the data. Meanwhile the communication will be delayed because the data exchange process is not yet completed and also it requires extra overheads for data transferring.

- Message transmission time is high

In a cluster range all the nodes are connected under a cluster head. All the communication process will be controlled by the cluster head. Even if two neighboring nodes within a cluster range need to exchange the messages with each other that can be done through the cluster head. Instead of sending the messages directly the message is routed through the cluster head which takes more time to transfer the data among the nodes.

- Link disconnection among the cluster heads

In this communication architecture cluster heads play a vital role. All the data dissemination process is controlled by the cluster heads. If link disconnection between the cluster head and its client nodes occur the communication will be collapsed. Similarly all the cluster heads are connected with one another. In this case, link between the cluster heads may be disconnected due to long distance. Link disconnection may be one of the drawbacks which need to be addressed in cluster based communication model.

2.4 Mobility models and standards used in VANET

Research in vehicular ad hoc network was carried out in the following three mobility models [48].

- Highway mobility model
- Manhattan mobility model
- Freeway mobility model

2.4.1 Highway, Manhattan and Freeway mobility models

Normally there will be of two lanes in highway mobility model where vehicles can move in both the directions respectively. Mobility pattern of nodes in highway model will be high and there will be not much obstacles to prevent the DSRC signal transmission. As the speed of the nodes are high in this model, the network architecture will change often.

Manhattan mobility model is used in the city environments where the streets are arranged in a predefined manner [49]. In this mobility model the mobility speed of each node will be slow compared to the Highway mobility model. As Manhattan mobility model represents city environment, there will be obstacles such as buildings, trees and so on to prevent DSRC single transmission. These obstacles will lead to link disconnection often.

In Freeway mobility model there will of multiple lanes where the nodes can choose any lane to reach its destination. Very limited research was carried out in this mobility model. It may be said that there will be no obstacles and the nodes will move at high speed in Freeway mobility model.

In Roadside Unit model the RSU acts as the router in transferring the data whereas in vehicle to vehicle communication model each vehicle acts as the router in exchanging the messages among the nodes. Similarly in Cluster based communication model cluster head acts as the router in forwarding messages among nodes. The change of network topology and communication performance will differ one mobility model to another mobility model.

There are two standards available for vehicular ad hoc network communication. They are standards 802.11 and 802.11p [3]. The earlier research in VANET was carried out with 802.11. This standard 802.11 is much suitable for mobile ad hoc network (MANET) where the mobility speed of nodes will be of slow. In VANET the speed of the nodes are high and the standard 802.11 is not suitable and the usage of 802.11 will lead to link disconnection among

the nodes often. The advanced version of 802.11 is 802.11p. This advanced standard 802.11p will support for high mobility nodes network topology. Usage of standard 802.11p in VANET will bring better communication performance than the usage of the standard 802.11 [3].

2.5 Protocols used in VANET

Routing protocols play an important role in vehicular ad hoc network communication [50–54]. Designing a network protocol must be appropriate for the network design to ensure high performance [55–58]. Messages among the vehicles need to be disseminated efficiently without delay. Emergency messages should be transmitted in time so that it would be helpful to the passengers and drivers to take necessary actions according to the situation [59]. Various routing protocols have been developed for vehicular ad hoc network communication and all are listed in Fig. 4 [60].

2.5.1 Topology based routing protocol

Route selection is the rapid task in sending messages between source and destination. In topology based routing, it considers how the route is selected for establishing the link between source and destination to transfer the data. This topology based routing protocols can be classified into proactive and reactive.

2.5.1.1 Proactive routing In proactive routing scheme each node in the network topology maintains one or more routing

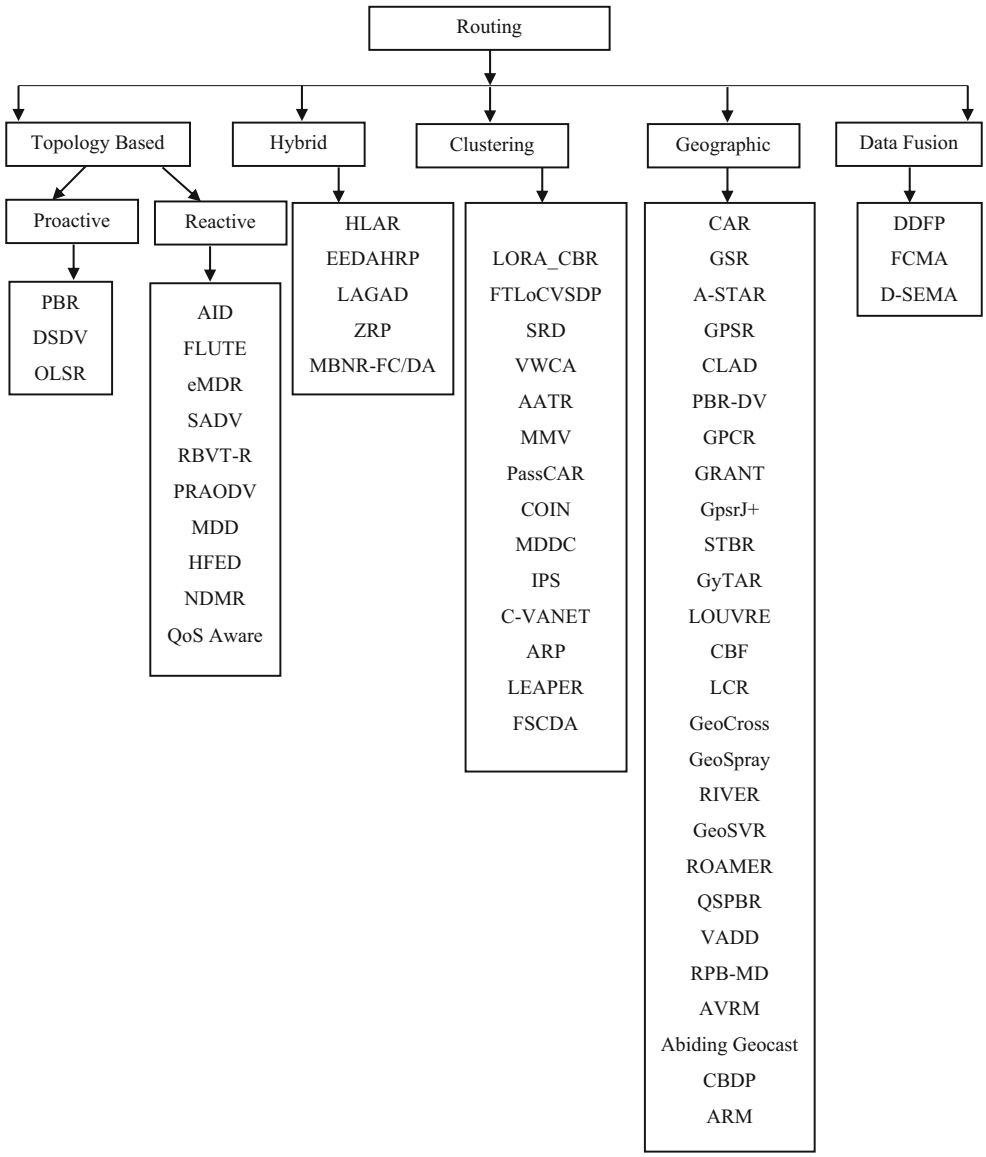

Fig. 4 Routing protocols for vehicular ad hoc network

tables which are updated at a regular periodical interval. In order to maintain the fresh routing table information each node broadcasts a message to the entire network topology to identify if there is any change in the network. The various list of available proactive routing protocols are listed in Fig. 4.

However, this routing information has the following disadvantages.

- It takes extra overhead cost to maintain the up to date information.
- Throughput of the network may be affected.
- Slow reaction on restructuring and failures.

2.5.1.2 Reactive routing In reactive routing scheme each node discovers or maintains route based on demand. This routing methodology floods a control message by global broadcast during discovering a route. As soon as route is discovered then the available bandwidth is used to transfer the messages. The fundamental advantage of this routing scheme is it needs less routing information. The various list of available reactive routing protocols are listed in Fig. 4.

However, it has the following disadvantages.

- It produces huge control packets during route discovery when network topology is changed.
- High latency time in route finding.
- Excessive flooding can lead to network clogging.

2.5.2 Hybrid routing

Hybrid routing scheme is the combination of both proactive and reactive routing schemes. In this routing scheme, the route is initially established with the proactive routing concepts and later the route may be established with the reactive routing concepts based on the demand. The various list of available hybrid routing protocols are listed in Fig. 4.

This hybrid routing has the following disadvantages.

- Advantage depends on number of other nodes activated.
- Reaction of traffic demand depends on gradient of traffic volume.

2.5.3 Clustering routing

In cluster based routing entire network topology is divided into various number of clusters based upon the density of the nodes in the topology. For each cluster, one node is chosen as the cluster head (CH). Cluster head controls the flow of message transmission among the nodes in its cluster group. All the other nodes are connected to the cluster head. Any message transfer can be done through the cluster head only. Whenever the cluster head reaches the cluster boundary the new cluster head should be elected and then all the control and data of the old cluster head need to be transferred to the new cluster head. The various list of available clustering routing protocols are listed in Fig. 4.

This clustering routing has the following disadvantages.

- Cluster head election and switching are extra overhead cost
- Poor memory utilization as all the cluster heads are storing the redundant data.
- Communication is only possible through cluster head.

2.5.4 Geographic routing

Geographic routing is also known as georouting or position-based routing. This routing uses the principle of geographic position information. Here, the source sends a message to the geographic location of the destination instead of using network address. In this routing scheme each node should be able to determine its own location and the source should be aware of the location of the destination. Using the geographic location, a message can be routed to the destination without knowledge of network topology or a prior route discovery. Position of each node can be identified by GPS or through periodic beacon messages. The various list of available geographic routing protocols are listed in Fig. 4.

2.5.5 Data fusion routing

Data fusion can be distributed into network and executed on nodes which reduce data from redundant nodes. It fuses the information from complementary nodes to get complete view from cooperative nodes. Consequently only the inference of interest is sent. The various list of available data fusion routing protocols are listed in Fig. 4.

3 WVANET (Web VANET) communication model

M. Milton Joe and B. Ramakrishnan et al. proposed a novel communication architecture for vehicular ad hoc network known as WVANET (Web VANET) as shown in the Fig. 5 [1]. The proposed WVANET is the integration of the technologies such as vehicular ad hoc network and web technology [1]. All the previous communication models in VANET used Dedicated Short Range Communication (DSRC) to exchange the messages with one another. In the WVANET communication model messages can be disseminated through web [1]. WiMAX towers are fixed at the side of the roads to propagate the web signals [1]. As we

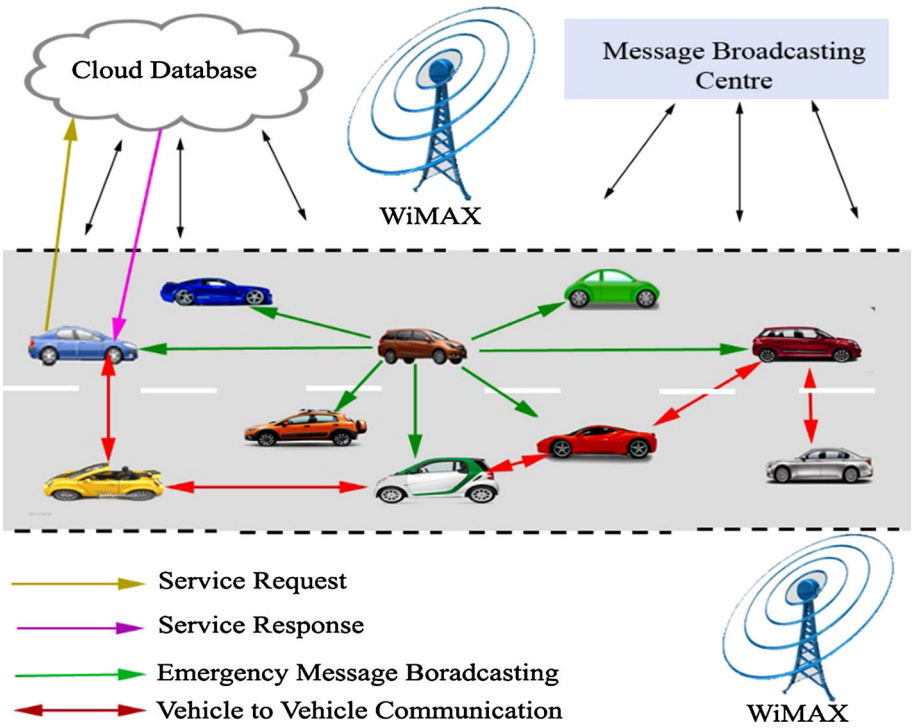

Fig. 5 WVANET communication model

know the range of the WiMAx is long in distance very few towers are enough to establish the fair network communication. All the vehicles will be connected with one another through web [1]. In WVANET communication model Extensible Messaging and Presence Protocol (XMPP) is used to disseminate the messages among nodes. In this network architecture each vehicle must be manufactured with WiMAX receiver and Global Positioning System (GPS) [1]. GPS is used to identify the current location of the vehicles. Once the current location of each vehicle is identified, the communication panel of each vehicle will be updated with the list of nearest passing vehicles and this list will be updated in a periodical interval based on the location statistics of the particular vehicle [1]. Three types of communication modes are proposed in the WVANET model as listed below [1]:

- Car to Car communication
- Broadcasting of messages
- Service discovery

Once list of nearby passing vehicles are listed in the communication panel, any node can choose any other node to communicate with it [1]. As web technology is integrated in VANET the message can be transmitted within a fraction of time. Broadcasting of messages in WVANET is the crucial application to enhance the safety of the passengers [1]. In the proposed WVANET a single message can be disseminated to all the nearby vehicles within a fraction of time. As a vehicle is moving in the highways it may be in need of some sort of service information [1]. The process of requesting and getting back the response for the requested service is known as service discovery [1]. Multimedia services are also one of the services of WVANET. In the other existing communication models multimedia contents can be provided to the nodes through Cognitive Radio Networks with cloud storage [61–65] whereas in the proposed WVANET model multimedia contents can be provided to the nodes through web more quickly and effectively.

The proposed WVANET is always much better than the other communication models exist in vehicular ad hoc network [1]. The founders of WVANT communication model portray that WVANET architecture will lead the future research in vehicular ad hoc network.

The proposed WVANET communication model should be carried out for further research developments in various aspects. Future research developments should enhance the communication performance as well as security constraints.

3.1 Advantages of WVANET communication model

- Single hop communication

In WVANET communication architecture, the network is similar to Peer to Peer to network. That is, any source can send the message to any destination with a single hop. When a message is transmitted with a single hop, the data can be delivered to the destination faster and it will take less time to reach the intended recipient.

- Very less link disconnection

As WVANET functions with the web signal, there is very less possibility for a node to get disconnected form the network topology. Web signal is propagated from the WiMAX towers and we know that the range of the WiMAX is miles of distance. When the signal strength is available for long distance, it ensures that the nodes will be under coverage forever.

- Transmission time

The main advantage of WVANET communication model is less message transmission time. Here, the communication model is single hop communication which leads to quick transmission. In the previous communication models, the network topology is multi-hop which will take more time to transmit the messages between the source and destination. In WVANET model, the message can be transmitted directly between the source and destination without intermediate node. Hence, every message can be delivered faster in WVANET communication model.

- Multimedia and entertainment clips from the web

People will be interested in multimedia and entertainment clips while travelling for a long distance. As web technology is integrated in VANET any type multimedia and entertainment contents can be accessed from the web.

- Cloud database

In the proposed WVANET communication model, cloud environment is used to store the data. When cloud database is used, the stored data can be accessed at anytime from anywhere which ensures that the stored data can be available to all the nodes at anytime.

- Live traffic monitoring to avoid collision

These days all the city environments have the live traffic monitoring system at the side of the roads. These live traffic monitoring system can be streamed to the vehicles to identify the current traffic conditions of the particular locations. So that the vehicle can choose its destination routes according to the traffic conditions.

- Data loss can be avoided

Implementation of cloud database stores the data at multiple servers, which prevents the data loss. All the stored data will be available to the nodes always without any difficulties.

4 Future research directions of WVANET

Research directions of WVANET can be turned towards various ways. However, here we review some of the key research directions of WVANET.

- Research on communication
- Research on multimedia communication
- Research on security issues

4.1 Research on communication

Any communication model in vehicular ad hoc network needs to be enhanced for better communication performance. In such a way the proposed WVANET communication model should be researched further to obtain the best communication performance. The fundamental aim of vehicular ad hoc network communication is to save the passengers during the emergency situations. For the same a secure and efficient protocol must be developed to disseminate the messages within a fraction of time to all the nodes.

4.1.1 Efficient protocol

It has been portrayed by the researchers of WVANET that it could be the everlasting research field in vehicular ad hoc network. Message can be disseminated within a fraction of time to all the nodes in WVANET compared to the other communication models exist in VANET. However, to broadcast the messages during emergency situations a secure and efficient protocol is must. Hence, future research direction of WVANET can be turned towards modelling of a novel protocol to disseminate the messages efficiently. The following parameters must be considered, while developing a novel protocol for WVANET.

- Density of the vehicles
- Speed of each node
- Time factor
- Directions of the nodes
- Internet traffic

The above listed are the some of the key parameters that should be considered while developing a novel protocol for WVANET communication model. Of course, the modelling protocol should be secure enough. When there is an emergency event occurs, the modelled novel protocol should be capable of identifying the other vehicles that are nearby. As soon as the nearby nodes are known the emergency message should be broadcasted to all the nodes in such a way the nodes can take the alternative route to reach the destination.

The proposed WVANET communication model makes use of web signals to exchange messages among vehicles. The internet protocol suite is abstracted into four layers as shown in Fig. 6.

Here, the link layer comprises of communication technologies for a single network segment. The fundamental

function of link layer is to move the packets between the internet layers of the hosts within same link. Function of internet layer is connecting nodes across independent networks which establishes the internetworking. This layer functions to send the packets across multiple networks through internet working. This process is called as routing. Node to Node communication is achieved through transport layer. Process to Process application data exchange can be achieved through application layer.

In WVANET communication architecture data exchange between two processes can be done in the application layer. Hence, a novel and secure protocol as discussed above should be developed for the application layer communication. There are various protocols do exist for the web based communication in the application layer such as BGP, DHCP, DNS, FTP, HTTP, IMAP, LDAP, MGCP, NNTP, NTP, POP, RTP, RTSP, RIP, SIP, SMTP, SNMP, SSH, XMPP and so on. In the proposed WVANET model XMPP protocol is used to exchange the data among vehicles. It must be noted that XMPP is designed for the web based applications. In order to achieve a better communication performance in WVANET a special protocol need to be designed for WVANET communication architecture. The protocol should disseminate the messages efficiently and it should be secure enough. Hence, modelling a novel emergency message broadcasting protocol will have high impact in WVANET communication model.

4.2 Research on multimedia communication

Another prominent research area in web vehicular ad hoc network (WVANET) is multimedia communication. Multimedia communication can be live streaming of videos and even gamming. In the proposed WVANET architecture all the nodes are connected to the internet. Nodes can capture the live videos and they could be shared with the other nodes possibly the nodes should be connected to the internet. Even the captured live vides can be stored in the cloud database and later those videos can be viewed by other nodes as it is needed from the cloud data centers.

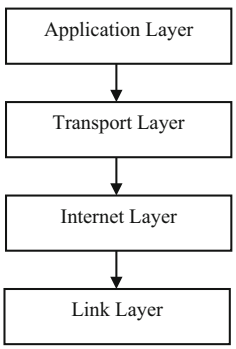

Fig. 6 Internet protocol suite

These kind of multimedia communication in WVANET will be a prominent research field that can be carried out further. As we know, most of the roads these days have the camera to monitor the traffic conditions at the corresponding locations. Those videos can be streamed to the vehicles based on the demand. With these type of streaming, the moving vehicles can come to know the traffic conditions at the desired location and based on the traffic condition the vehicle can choose the apt path to reach the destination. This type of multimedia communication in WVANET will reduce time delay waiting at the collision area. On the other hand entertainment videos will entertain the passengers during the travel time. Entertainment videos also can be watched live from the cloud database though the internet as web communication is integrated in the proposed WVANET communication model.

In future, the research can be carried in WVANET in such a way the vehicles can be used to transmit the secure information to the destinations. For instance, hiding confidential data in an image and video can be transmitted through the vehicles. A novel and secure protocol is needed to provide live streaming and to transfer the confidential data in WVANET efficiently.

4.3 Research on security issues

The broadest research in vehicular ad hoc network communication is security issues. Similarly the proposed WVANET communication model should prevent the various security threats. It should be noted that all the internet attacks are also possible in WVANET communication model as web technology is integrated in vehicular ad hoc network. Here, we would like to discuss some of the key security concerns of WVANET model.

4.3.1 Authentication

Authentication is the process of making sure that all the nodes within the network are verified. Each node that enters the communication network must be authenticated efficiently [66]. In WVANET architecture each node is communicating through the internet technology which could be attackable by the unauthorized nodes to exchange the false messages within the network. These kinds of unauthorized nodes may create accidents and collision among the nodes. Hence, each node that enters the WVANET architecture must be authenticated. Here, the list of available web based authentication mechanism are reviewed.

- Password based authentication
- Privacy question based authentication

- Mobile and E-mail authentication

4.3.1.1 Password based authentication Password based authentication is the mostly used validation mechanism in web based services. This password can be created by the user at the time of account creation with the combination of alphanumeric characters. It should be noted that purely character based password can be attacked by the hackers easily. Highly complicated passwords need to be created to avoid hacking. These complicated password may not be remembered always for the original user also. There are many techniques that are attempted by the attackers to crack the passwords such as password guessing attack, cracker programs, Brute force attack or dictionary attack. Even the malicious software known as keylogger can be injected into a node to monitor the key stroke of a victim to hack the password.

From the above views, it can be concluded that the password based authentication mechanism cannot be the apt one for WVANET communication model. Hence, a novel authentication mechanism need to be developed specially for WVANET.

4.3.1.2 Privacy question based authentication Another way of authenticating a user in the web based application is privacy question based authentication mechanism. In this approach a privacy question and its answer are set by the user at the time of profile creation. Special care need to be taken in framing answer to the question as the answer could be easily guessable. As described in the previous section various cracking and keylogger software can be used to hack the answers. Hence, this authentication mechanism is also not sufficient enough to get adopted in WVANET communication model.

4.3.1.3 Mobile and E-mail authentication Mobile and E-mail based authentication mechanism are proposed to validate the user originality at the time of suspicious unauthorized access. When unauthorized access is suspected for an account, the account will be locked temporarily and the lock will be released after the successful verification of the user. In order to verify the user originality the generated random number either will be sent to the mobile number of the user added in the profile at the time of account creation or to the E-mail account that is registered with the user profile. However, this mechanism has the various limitations when we try to adopt this mechanism into WVANET communication model.

- This authentication procedure completely depends on Mobile and E-mail service provider and it will not depend on WVANET service provider.
- This mechanism does not make use of any of the WVANET communication data to authenticate the node.
- Depending on another service provider will be always a security threat and the WVANET communication architecture cannot function independently.

From the above observation it is clear that a secure authentication mechanism is needed to authenticate nodes in WVANET communication model and the authentication mechanism should be under the characteristics of WVANET.

4.3.2 Sybil attack

Sybil Attack is the process in which a vehicle claims to be in different positions at a same time with different identities. This attack will damage the entire network topology and it will take more bandwidth consumption. In this attack model a vehicle transmits multiple messages with different identities to the other vehicles. All the other vehicles assumes that there is a heavy network traffic ahead.

Figure 7 represents the Sybil attack. As shown in the Fig. 7 the vehicle A claims to be at different locations at the same time and it sends multiple messages to the other vehicles with different identities. There were three types of defense mechanisms proposed against Sybil attack namely registration, position verification and radio resource testing. The mechanism registration is not sufficient enough as the malicious nodes can create multiple identities by means of stealing. If strict registration is introduced that would lead to privacy risks. In position verification mechanism position of each node is verified. The aim is to make certain that each physical node refers to one and only one identity. In radio testing it is assumed that all the physical nodes are limited in resources.

This Sybil attack is also possible in WVANET architecture and this attack will increase the network bandwidth heavily in WVANET. This attack will damage the network topology and the connections among the nodes. A secure algorithm must be developed to avoid Sybil attack in

Fig. 7 Sybil attack

WVANET and the modelling algorithm should minimize the network traffic.

4.3.3 Bogus information attack

This attack is attempted by the nodes for personal advantages. Node sends the false (Bogus) message to the other nodes such as "heavy traffic is ahead take diversion" in order to divert the nodes to the other routes so that the route is clear to the attacker. This attack will create heavy network traffic in certain areas which will make the network busy and the communication process will slow down. The illustration of bogus information attack is shown in the Fig. 8.

As represented in the Fig. 8 the colluding attackers A and C disseminate the bogus information to affect the decision of other vehicles (D). After the receipt of false information the vehicle D assumes that the received information is correct and it takes the alternative route and the route is clear for the attacker (E). This bogus information attack will lead to many type of security problems and it will affect the network topology. These kind of attack will also create collision which will lead to unexpected accidents. A special care must be shown in detection and prevention of this type of attack. In WVANET architecture this bogus information attack need to be prevented and for the same a secure algorithm need to be developed to monitor the behavior of the nodes in the network topology.

4.3.4 Impersonation attack

In ad hoc network each node can be identified with the help of its IP and MAC address. Similarly in WVANET architecture each node is uniquely identified with IP and MAC address. However, these two identities are not sufficient enough to authenticate the nodes in the network topology. A malicious node can spoof the IP and MAC addresses in order to get the identity of the other nodes so that it can hide itself in the network. The malicious node can make use of the identity of other nodes to communicate with other nodes. In this attack the malicious node can broadcast the false information such as heavy traffic, accidents and so on with the identity of other nodes. For instance, a malicious node can spoof the identity of an emergency vehicle and it can request for the priority lane and even it can demand the RSU to turn the green signal on. An efficient algorithm need to be developed to identify the malicious nodes that has the spoofed identity. Moreover, attempting a strict authentication will lead to privacy issues because the driver of the vehicle has the right to prevent the disclosure of his driving routes. A novel and secure algorithm is needed obviously to defend the impersonation attack in WVANET communication model.

4.3.5 Timing attack

The fundamental aim of vehicular ad hoc network communication is to prevent the accidents. For the same emergency messages need to be broadcasted as the right time to avoid the accidents. However, in this attack mode when the attacker receives an emergency message does not forward the message at the normal time rather adds more time slots in order to create delay. Thus, the nearby vehicles of the attacker receives the message after the moment when they should receive the message actually. If the vehicle receives the message at the right time it may take different lane to avoid the accidents. This type of attack is known as Timing Attack. The Fig. 9 depict the timing attack that is attempted by the attacker.

As depicted in the Fig. 9 there is an accident between the vehicles A and B and the vehicle D was informed about this accident. However, the vehicle D did not forward the message in time to the other vehicle F by adding extra time slots to delay the message. If the node F received the message in time it would have taken the different lane but due to the delay it received the message after it has received the accident position. This attack model is known

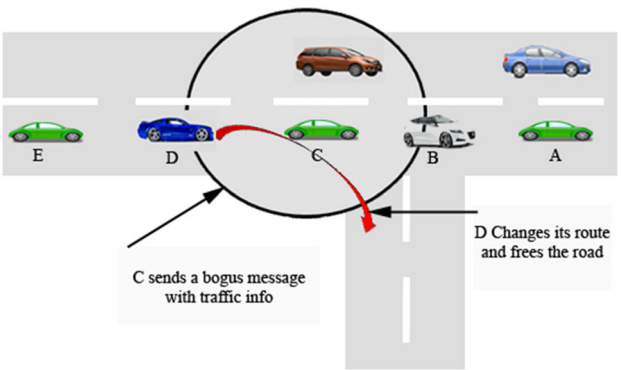

Fig. 8 Bogus information attack

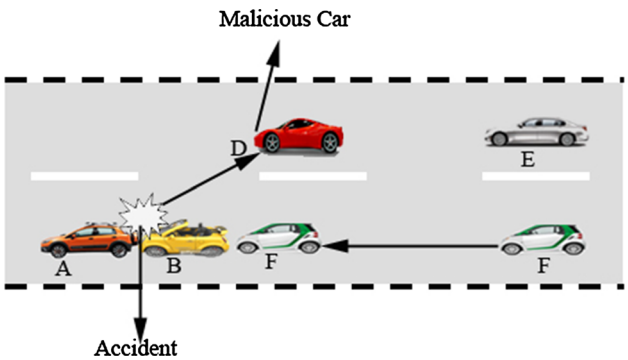

Fig. 9 Timing attack model

as timing attack. This attack collapses the entire communication process of the vehicular ad hoc network communication. As we know the fundamental aim of VANET communication is to disseminate the emergency messages in time. This timing attack will be the biggest challenge to the researchers. In WVANET every message should be transmitted in time without further delay to achieve the better communication performance. For the same an effective algorithm need to be modelled to prevent the timing attack in WVANET architecture.

4.3.6 Illusion attack

In this attack model the attacker attaches sensors to produce the wrong sensor readings regarding the traffic information. The traffic monitoring system may receive the incorrect traffic information because of the wrong senor readings and those incorrect traffic information can be broadcasted to the nodes. This type of attack model is known as illusion attack. In vehicular ad hoc network communication scenario many types of data are received form the vehicles and those data are disseminated to the other nodes as it is requested by the nodes. When a node sends a data to the server that data must be trust worthy because those data are going to be used by other nodes. Attaching wrong sensors at the vehicles will send the incorrect information to the server and will be the security threat forever. Those incorrect data will be broadcasted to the other nodes and believing the received data the nodes may take different routes. This may lead to collision at the particular location and it will also create accidents. These kind of illusion attack must be prevented to provide trust worthy communication among the nodes. All the data received at the server end need to be checked for its trust worthy. However, checking all the data received at the server end will lead to extra overhead and it will be a difficult task to complete it. Hence, this illusion attack also need to be prevented in WVANET communication model and to do so an efficient algorithm need to be modelled.

4.3.7 ID disclosure

Malicious node reveals the identity of the neighboring nodes so that the vehicles can be tracked to know its current location. Once the identity of the vehicle is revealed, the particular vehicle can be misused for various malicious activities. Attacker sends a malicious virus to the list of nodes to identify the target node. Once a node is attacked by the virus it will send the ID of the victim node to the attacker. Once the identity of the node is revealed the traveling route of the victim can be traced by the attacker and the victim node can be misused widely. Attacker can make use of the victim's identity to broadcast the false information among the nodes. These kind of ID disclosure will also lead to privacy issues. Identity of each node should not be revealed. If identity is revealed that identity can be used by malicious nodes to collapse the vehicular ad hoc network communication. In the proposed WVANET communication architecture this type of attack should be avoided and for the same a secure algorithm should be developed.

4.3.8 Denial of Service (DoS) and Distributed Denial of Service (DDoS)

Denial of Service (DoS) is the process in which a node sends many dummy messages from different identities to the server as well as to other nodes. When the server receives multiple dummy messages continuously, the server will become busy and the performance of the network will be slow. Due to this, the server may not be able send the required information to the legitimate users. Similarly sending many dummy messages like "Lane is closed ahead" to the legitimate vehicle causes the vehicle to take alternate route. The Denial of Service (DoS) is represented in the Fig. 10.

As shown in the Fig. 10 the malicious car sends many dummy messages with different identities to the legitimate car and to the server. The aim is to prevent the legitimate vehicle not to get the service form the server. When the server gets many dummy messages it will become busy as well as the efficiency of entire network will be poor. This Denial of Service (DoS) attack is the most harmful attack to every network communication architecture.

Distributed Denial of Service (DDoS) attack is more advanced than the DoS attack. In this DDoS attack number of malicious vehicles attack a legitimate node from different locations at different time slots in a distributed manner. The Fig. 11 illustrates distributed denial of service (DDoS) attack.

As demonstrated in the Fig. 11 malicious three vehicles attack a target legitimate vehicle A by sending many dummy messages such as "Accident Ahead", "Lane

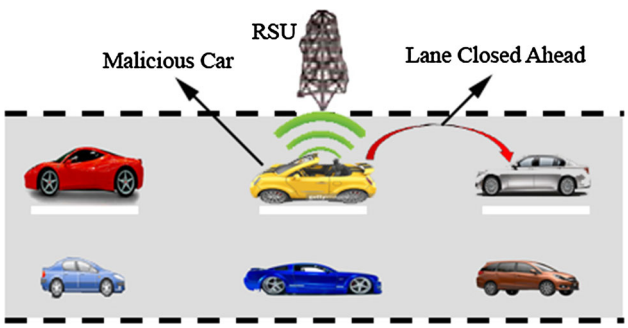

Fig. 10 Denial of Service attack

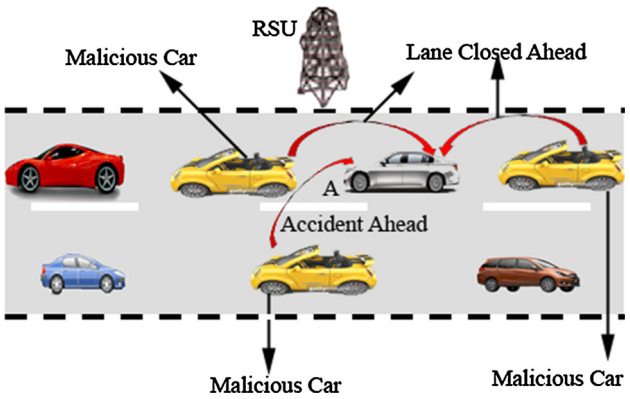

Fig. 11 Distributed Denial of Service (DDoS) attack

Closed Ahead" from different locations and timeslots. The aim of this attack is to stop the victim vehicle not to communicate with the other vehicles. The victim vehicle will be isolated form the network communication due to this attack. A novel and secure algorithm should be modelled to prevent the DoS and DDoS attacks in WVANET communication architecture.

4.3.9 Virus attack

Virus is a malicious software program which is more harmful to any network communication architecture. In VANET, this virus is spread out from one vehicle to another vehicle when the user sends or downloads the information in the network architecture. In the WVANET architecture all the vehicles are connected to the internet and the communication is carried out through the web. When the user sends a data from one vehicle to another vehicle or when the user downloads a data from the internet this virus can attach itself in the existing program and it can move to the particular vehicle to infect it. Virus program needs an existing program to move from a node to another node. If a node is vulnerable in the network then the victim will be infected by virus and the communication will be collapsed. Once a node is infected by virus in the network architecture it is also possible for other nodes to get infected by virus as the nodes receives the files form the infected node. All the nodes in the WVANET communication architecture should not be vulnerable to avoid virus infection. In WVANET communication all the communication is carried through internet and every vehicle will upload and download the information form the server. Hence, it is possible for a node to get infected by the virus attack. A secure virus attack detection and prevention algorithm must be developed to enhance the communication performance of WVANET communication architecture.

4.3.10 Worm attack

Worm is another type of malicious software code which is more damageable to the network. Worm does not need an existing program to propagate from a node to another node like virus. Worm will scan for the vulnerable nodes in the network architecture. As soon as a victim is found the worm will propagate to the victim node to infect it. After infecting a node, it will start the scanning process to find out the other vulnerable nodes in the network. Once another victim is found, it will propagate to the victim and infects it. Similarly, the worm propagates to all the vulnerable nodes in the network architecture. This type of worm propagation will infect and collapse the entire network communication process. All the nodes in the network must not be vulnerable to avoid worm attack. Normally these worm will be silent during the scanning process. So that the worm cannot be identified by the worm scanning process. In the proposed WVANET architecture this worm attack will be the biggest challenge. Any malicious user in the network can spread out the worm in order to collapse the entire network communication. An effective and secure worm propagation detection and prevention algorithms should be developed to enhance the WVANET communication model.

4.3.11 Trojan attack

The Trojan attack is derived from the Greek mythology. Trojan looks like harmless at the beginning. However it will leave a node unprotected in the network architecture. It will enable the hackers to steal the sensitive information from a node. Initially the Trojan will look like a useful information to the nodes so that the node will install it. This will be similar to the social engineering attack. In WANET communication process the attacker may send the Trojan to the list of neighbors to attack them. Once a node is attacked by the Trojan it will leave the node unprotected and it will transfer the control of the victim node to the attacker. The attacker can steal the sensitive information of node and those information can be misused for various nuisance activities. Normally a Trojan can perform the following actions.

- Deleting data
- Blocking data
- Modifying data
- Copying data
- Disrupting the performance of the networks

In WVANET communication model every node will store many data in it and those data can be used for the various communication purposes. This Trojan will delete the information stored on the victim node. Once the data is

deleted the victim node may not be able to communicate in the network topology. Similarly the Trojan can block the data that is being sent from a node to another node. Trojan will block the emergency message that is being disseminated in the network. Emergency messages should be broadcasted at the correct time without delay but the Trojan may block the information that is being broadcasted in the network. Another serious issue of Trojan is modifying the data. That is, the Trojan can change the original data with the false information and the false information will be sent to the nodes in the network which will collapse the network communication. All the data stored in a node should be kept secret and that should not be copied without the consent of the authorized user. However, the Trojan will copy the data stored on a node without notifying the user and it will send the sensitive information the attacker. This Trojan will disrupt the communication performance of the entire network in WVANET communication model. A secure and effective algorithm should be developed to protect the proposed WVANET communication model from Trojan attack.

4.3.12 Spyware attack

The Spyware is installed on a node without the consent of the node when a file is downloaded. The aim of Spyware is to monitor and gather the information about the node and report it to the attacker. This Spyware would reset the auto signature, read and delete the files of a node. Even this Spyware will format the data storage (hard drive) of a node. Vehicle to Vehicle communication depends on huge amount of data. However, this Spyware would read the secret data of the node and then sends those information to the attacker and even the files exist on the victim node can be deleted by this Spyware. In addition to that, the Spyware can format the data storage (hard drive) of a node. Once the hard drive of the node is formatted, the node will be isolated and the communication in the particular network will be collapsed. This Spyware attack will be real task to the defenders to defend against them. In WVANET, this Spyware needs to be prevented to secure the communication among the nodes.

4.3.13 Spam attack

The spam attack is similar to E-mail spam attack. In this attack a malicious node sends more unwanted messages to the network which consumes more network bandwidth. Also this type of attack will create latency in the network scenario. This spam attack will make the server busy and the server will be slow in responding to the legitimate nodes. Sending unwanted data to a node will divert the communication of a node and even the unwanted data will contain malicious viruses to infect the node. This attack will consume more network bandwidth and the network performance will be reduced obviously. In WVANET communication architecture, this attack will degrade communication performance. Hence, a secure algorithm should be modelled to prevent these kind of attacks.

So far, we have reviewed the various types of security attacks that are possible for WVANET communication model. Recently introduced WVANET communication model should prevent the various security attacks that are aimed by the attackers.

5 Conclusions

Research in vehicular ad hoc network has been carried out in RoadSide Unit (RSU) Vehicle to Vehicle (V2V), Cluster Based (CBVANET) Communication models so far. However, recently researchers introduced a novel communication model known as Web VANET (WVANET). The WVANET communication architecture is the integration of Web Technology and Vehicular Network Technology. In WVANET communication model all the nodes are communicating with other nodes through web which is completely different from other communication models. This paper has provided the review of all the communication models available in vehicular ad hoc network including WVANET communication model. In addition to that this paper has also provided the future research directions of WVANET architecture.

References

1. Joe, M. M., & Ramakrishnan, B. (2015). WVANET: Modelling a novel web based communication architecture for vehicular network. *Wireless Personal Communications*, 1–15. doi:10.1007/s11277-015-2886-0.
2. Xiong, H., Chen, Z., & Li, F. (2012). Efficient and multi-level privacy-preserving communication protocol for VANET. *Computers & Electrical Engineering, 38*, 573–581.
3. Ramakrishnan, B., Rajesh, R. S., & Shaji, R. S. (2010). Performance analysis of 802.11 and 802.11p in cluster based simple highway mode. *International Journal of Computer Science and Technologies, 1*(5), 420–426.
4. Ramakrishnan, B., Joe, M. M., & Nishanth, R. B. (2014). Modeling and simulation of efficient cluster based manhattan model for vehicular communication. *Journal of Emerging Technologies in Web Intelligence, 6*(2), 253–261.
5. Duarte, P. B. F., Fadlullah, Z. M., Vasilakos, A. V., & Kato, N. (2012). On the partially overlapped channel assignment on wireless mesh network backbone: A game theoretic approach. *IEEE Journal on Selected Areas in Communications, 30*(1), 119–127.
6. Sandonis, V., Calderon, M., Soto, I., & Bernardos, C. J. (2013). Design and performance evaluation of a PMIPv6 solution for geonetworking-based VANETs. *Ad Hoc Networks, 11*, 2069–2082.

7. Wahab, O. A., Otrok, H., & Mourad, A. (2013). VANET QoS-OLSR: QoS-based clustering protocol for vehicular ad hoc networks. *Computer Communications, 36*, 1422–1435.
8. Hongseok, Y., & Dongkyun Kim, K. (2011). Repetition-based cooperative broadcasting for vehicular ad-hoc networks. *Computer Communications, 34*(15), 1870–1882.
9. Isaac, J.-T., Camara, J.-S., Zeadally, S., & Marquez, J.-T. (2012). A Secure vehicle-to-roadside communication payment protocol in vehicular ad hoc networks. *Computer Communications, 31*(10), 2478–2484.
10. Yousefi, S., Altman, E., El-Azouzi, R., & Fathy, M. (2008). Improving connectivity in vehicular ad hoc networks: An analytical study. *Computer Communications, 31*(9), 1653–1659.
11. Lim, S., Yu, C., & Das, C.-R. (2012). Cache invalidation strategies for internet-based vehicular ad hoc networks. *Computer Communications, 35*(3), 380–391.
12. Shieh, W.-Y., Lee, W.-H., & Shen, L. (2006). Analysis of the optimum configuration of roadside units and onboard units in dedicated short-range communication systems. *IEEE Transactions on Intelligent Transportation Systems, 7*(4), 565–571.
13. Joe, M. M., Shaji, R. S., & Thulasi, R. (2013). Modeling Network Communication in VANET using Bluetooth Technology. *International Journal of Advanced and Innovative Research, 2*(3), 643–651.
14. Joe, M. M., Ramakrishnan, B., & Shaji, R. S. (2014). Modeling GSM based network communication in vehicular network. *IJCNIS, 6*(3), 37–43. doi:10.5815/ijcnis.2014.03.05.
15. Tuteja, A., Gujral, R., & Thalia, S. (2010). Comparative performance analysis of DSDV, AODV and DSR routing protocols in MANET Using NS2. In *International conference on ACE* (pp. 330–333).
16. Joe, M. M., Shaji, R. S., & Ashok Kumar, K. (2013). Establishing inter vehicle wireless communication in vanet and preventing it from hackers. *IJCNIS, 5*(8), 55–61. doi:10.5815/ijcnis.2013.08.07.
17. Wang, X., et al. (2012). A survey of green mobile networks: Opportunities and challenges. *MONET, 17*(1), 4–20.
18. Rahimi, M. R., Venkatasubramanian, N., & Vasilakos, A. V. (2013). MuSIC: Mobility-aware optimal service allocation in mobile cloud computing. In *IEEE CLOUD* (pp. 75–82).
19. Meng, T., Wu, F., Yang, Z., Chen, G., & Vasilakos, A. V. (2015). Spatial reusability-aware routing in multi-hop wireless networks. *IEEE Transactions on Computers*, *PP*(99), 1–13. doi:10.1109/TC.2015.2417543.
20. Yao, Y., Cao, Q., & Vasilakos, A. V. (2013). EDAL: An energy-efficient, delay-aware, and lifetime-balancing data collection protocol for wireless sensor networks. In *Mobile ad-hoc and sensor systems (MASS), 2013 IEEE 10th international conference on 14–16 Oct* (pp. 182–190). Hangzhou: IEEE.
21. Wei, G., Ling, Y., Guo, B., Xiao, B., & Vasilakos, A. V. (2011). Prediction-based data aggregation in wireless sensor networks: Combining grey model and Kalman Filter. *Computer Communications, 34*(6), 793–802.
22. Liu, X.-Y., Zhu, Y., Kong, L., Cong Liu, Y., Vasilakos, A. V., & Min-You, W. (2015). CDC: Compressive data collection for wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems, 26*(8), 2188–2197.
23. Vasilakos, A. V., Li, Z., Simon, G., & You, W. (2015). Information centric network: Research challenges and opportunities. *Journal of Network and Computer Applications, 52*, 1–10.
24. Yang, M., Li, Y., Jin, D., Zeng, L., Xin, W., & Vasilakos, A. V. (2015). Software-defined and virtualized future mobile and wireless networks: A survey. *MONET, 20*(1), 4–18.
25. Sheng, Z., et al. (2013). A survey on the IETF protocol suite for the internet of things: Standards, challenges, and opportunities. *IEEE Wireless Communications 20*(6), 91–98.
26. http://en.wikipedia.org/wiki/Web_service.
27. Joe, M. M., Ramakrishnan, B., & Shaji, R. S. (2013). Prevention of losing user account by enhancing security module: A facebook case. *Journal of Emerging Technologies in Web Intelligence, 5*(3), 247–256.
28. Shehab, M., Squicciarini, A., Ahn, G.-J., & Kokkinou, I. (2012). Access control for online social networks third party applications. *Computers & Security, 31*, 897–911.
29. Joe, M. M., & Ramakrishnan, B. (2014). Enhancing security module to prevent data hacking in online social networks. *Journal of Emerging Technologies in Web Intelligence, 6*(2), 184–191.
30. Yin, H., Fu, Q., Lin, C., Lin, C., Ding, R., Lin, Y., et al. (2006). Mobile police information system based on web services. In *Tsinghua science and technology* (Vol. 11(1), pp. 1–7), ISSN 1007-0214 01/21.
31. Joe, M. M., & Ramakrishnan, D. B. (2014). A survey of various security issues in online social networks. *International Journal of Computer Networks and Applications, 1*(1), 11–14.
32. Shivaldova, V., Paier, A., Smely, D., & Mecklenbräuker, C. F. (2012). On roadside unit antenna measurements for vehicle-to-infrastructure communications. In *23d IEEE international symposium on personal, indoor and mobile communications* (*PIMRC*).
33. Kumar, N., Chilamkurti, N., & Rodrigues, J. J. P. C. (2014). Learning automata-based opportunistic data aggregation and forwarding scheme for alert generation in vehicular ad hoc networks. *Computer Communications, 39*, 22–32.
34. Zhang, X. M., Zhang, Y., Yan, F., & Vasilakos, A. V. (2015). Interference-based topology control algorithm for delay-constrained mobile Ad hoc networks. *IEEE Transactions on Mobile Computing, 14*(4), 742–754.
35. Yen, Y.-S., Chao, H.-C., Chang, R.-S., & Vasilakos, A. (2011). Flooding-limited and multi-constrained QoS multicast routing based on the genetic algorithm for MANETs. *Mathematical and Computer Modelling, 53*(11–12), 2238–2250.
36. Li, P., Guo, S., Yu, S., & Vasilakos, A. V. (2014). Reliable multicast with pipelined network coding using opportunistic feeding and routing. *IEEE Transactions on Parallel and Distributed Systems, 25*(12), 3264–3273.
37. Spyropoulos, T., Rais, R. N. B., Turletti, T., Obraczka, K., & Vasilakos, A. (2010). Routing for disruption tolerant networks: Taxonomy and design. *Wireless Networks, 16*(8), 2349–2370.
38. Li, P., Guo, S., Yu, S., & Vasilakos, A.V. (2012) CodePipe: An opportunistic feeding and routing protocol for reliable multicast with pipelined network coding. In *INFOCOM* (pp. 100–108).
39. Xiang, X., Qin, W., & Xiang, B. (2014). Research on a DSRC-based rear-end collision warning model. *IEEE Transactions on Intelligent Transportation Systems, 15*(3), 1054–1065.
40. Ramakrishnan, B., Rajesh, R. S., & Shaji, R. S. (2010). An efficient vehicular communication outside the city environments. *International Journal of Next-Generation Networks (IJNGN), 2*(4), 1.
41. Ramakrishnan, B., Rajesh, R. S., & Shaji, R. S. (2011). CBVANET: A cluster based vehicular ad hoc network model for simple highway communication. *International Journal of Advanced Networking and Applications, 2*(4), 755–761.
42. Viriyasitavat, W., Boban, M., Tsai, H.-M., & Vasilakos, A. V. (2015). Vehicular communications: Survey and challenges of channel and propagation models. *IEEE Vehicular Technology Magazine, 10*(2), 55–66.
43. Zhou, L., Zhang, Y., Song, K., Jing, W., & Vasilakos, A. V. (2011). Distributed media services in P2P-based vehicular networks. *IEEE T. Vehicular Technology, 60*(2), 692–703.
44. Zeng, Y., Xiang, K., Li, D., & Vasilakos, A. V. (2013). Directional routing and scheduling for green vehicular delay tolerant networks. *Wireless Networks, 19*(2), 161–173.
45. Nishanth, R. B., Ramakrishnan, B., & Selvi, M. (2015). Improved signcryption algorithm for information security in networks.

International Journal of Computer Networks and Applications (*IJCNA*), *2*(3), 151–157.
46. Ramakrishnan, B., Rajesh, R. S., & Namesh, C. (2010). A study on service procedure in clustered vehicular communication. *International Journal of Advanced Research in Computer Science, 1*(4), 535–542.
47. Ramakrishnan, B. (2010). Analytical study of cluster and sans cluster vehicular adhoc network communication. *International Journal of Computer Engineering and Information Technology, 25*(1), 01–11.
48. Ramakrishnan, B., Nishanth, R. B., Joe, M. M., & Shaji, R. S. (2015). Comprehensive analysis of highway, Manhattan and Freeway mobility models for vehicular ad hoc network. *International Journal of Wireless and Mobile Computing, 9*(1), 78–89.
49. Ramakrishnan, B. (2013). Analysis of Manhattan mobility model without RSUs. *IOSR Journal of Computer Engineering* (*IOSR-JCE*), *9*(5), 82–90.
50. Ramakrishnan, B., Rajesh, R. S., & Shaji, R. S. (2011). Analysis of routing protocols for highway model without using roadside unit and cluster. *International Journal of Scientific & Engineering Research, 2*(1), 1–9.
51. Ramakrishnan, B., Rajesh, D. R. S., & Shaji, R. S. (2010). An intelligent routing protocol for vehicle safety communication in highway environments. *Journal of Computing, 2*(11), 65–72.
52. Ramakrishnan, B. (2009). Performance analysis of AODV routing protocol in Vehicular ad-hoc network service discovery architecture. *Network, 13*(14), 15.
53. Ramakrishnan, B., Sreedivya, S. R., & Selvi, M. (2015). Adaptive routing protocol based on cuckoo search algorithm (ARP-CS) for secured vehicular ad hoc network (VANET). *International Journal of Computer Networks and Applications (IJCNA), 2*(4), 173–178.
54. Busch, C., Kannan, R., & Vasilakos, A. V. (2012). Approximating congestion + dilation in Networks via "Quality of Routing" games. *IEEE Transactions on Computers, 61*(9), 1270–1283.
55. Xiao, Y., Peng, M., Gibson, J., Xie, G. G., Ding-Zhu, D., & Vasilakos, A. V. (2012). Tight performance bounds of multihop fair access for MAC protocols in wireless sensor networks and underwater sensor networks. *IEEE Transactions on Mobile Computing, 11*(10), 1538–1554.
56. Vasilakos, A., et al. (2012). *Delay tolerant networks: Protocols and applications*. Boca Raton: CRC Press.
57. Youssef, M., et al. (2014). Routing metrics of Cognitive Radio Networks: A survey. *IEEE Communications Surveys and Tutorials, 16*(1), 92–109.
58. Vasilakos, A., et al. (1998). Evolutionary-fuzzy prediction for strategic QoS routing in broadband networks. In *The 1998 IEEE international conference on fuzzy systems proceedings* (Vol. 2, pp. 1488–1493).
59. Selvi, M., & Ramakrishnan, B. (2015). Prioritized and secured data dissemination technique in VANET based on optimal blowfish algorithm and signcryption method. *International Journal of Computer Networks and Applications (IJCNA), 2*(4), 165–172.
60. Dua, A., Kumar, N., & Bawa, S. (2014). A systematic review on routing protocols for vehicular ad hoc networks. *Vehicular Communications, 1*, 33–52.
61. Jiang, T., Wang, H., & Vasilakos, A. V. (2012). QoE-driven channel allocation schemes for multimedia transmission of priority-based secondary users over Cognitive Radio Networks. *IEEE Journal on Selected Areas in Communications, 30*(7), 1215–1224.
62. Shen, Z., Luo, J., Zimmermann, R., & Vasilakos, A. V. (2011). Peer-to-peer media streaming: Insights and new developments. *Proceedings of the IEEE, 99*(12), 2089–2109.
63. Jiau, M.-K., et al. (2015). Multimedia services in cloud-based vehicular networks. *IEEE Intelligent Transportation Systems Magazine, 7*(3), 62–79.
64. Zhou, J., et al. (2015). Secure and privacy preserving protocol for cloud-based vehicular DTNs. *IEEE Transactions on Information Forensics and Security, 10*(6), 1299–1314.
65. Zhou, L., et al. (2010). Context-aware middleware for multimedia services in heterogeneous networks. *IEEE Intelligent Systems, 25*(2), 40–47.
66. Attar, A., et al. (2012). A survey of security challenges in Cognitive Radio Networks: Solutions and future research directions. *Proceedings of the IEEE, 100*(12), 3172–3186.

M. Milton Joe received his B.Sc. Computer Science degree from Bharathidasan University, India and MCA degree from Anna University, India. Presently he is working as Assistant Professor at St. Jerome's College in Nagercoil, India. He has 4 years of research experience and authored many research papers in reputed international journals. His research interests include Web VANET (WVANET), Web Security, Vehicular Network and Social Network Security.

Dr. B. Ramakrishnan is currently working as Associate Professor in the Department of Computer Science and research Centre in S.T. Hindu College, Nagercoil. He received his M.Sc. degree from Madurai Kamaraj University, Madurai and received M.Phil. (Comp. Sc.) from Alagappa University Karaikudi. He earned his Doctorate degree in the field of Computer Science from Manonmaniam Sundaranar University, Tirunelveli. He has a teaching experience of 28 years. He has twelve years of research experience and published more than forty research articles in reputed international journals. His research interests lie in the field of Vehicular networks, mobile network and communication, Cloud computing, Green computing, Ad hoc networks and Network security.