# Design and Analysis of the Performance of IVC Networks by Using Enhanced Fast Multihop Broadcast Algorithm

**G.Raja Gouthami [#1], Dr. G. Suvarna Kumar[*2], Dr. G. Sandhya Devi [*3]**

M.Tech Scholar [#1], Associate Professor[*2], Assistant Professor[*3]

Department of CSE,
MVGR College of Engineering
Vizianagaram, AP (INDIA).

## Abstract

Now a day's vehicular communication systems were become more and more advantages for communicating the nodes like vehicles and road facets that are present on both sides of road. With these vehicular communication systems, they will exchange the data associated with the traffic to avoid hold up and numerous accidents that takes place in road network. These are getting additional and additional well liked owing to frequent network disruption, continuous topological modification and dynamic nature of vehicles. As these are the various assorted issues that are created by transport networks, there's no mechanism to deliver the data with efficiency. So thus so as to realize this economical knowledge delivery we have a tendency to came with a brand new thought known as as inter vehicular communication (IVC) to significantly contribute to traffic safety and potency. During this purpose of read, there square measure several attainable IVC applications that share the common data like speed of car, direction of car, and position of car in multihop message propagation. In conjunction with this primary data it ought to conjointly capable to spot numerous security attacks that occur throughout knowledge exchange and it ought to ready to offer counter live for those attacks. During this IVC plenty of malicious vehicles invariably try and inject cant into the lay vehicle wireless links that results in plenty of cash losses or to the other type of adversarial stinginess in terms of mis-routing the vehicles. Thus during this paper, we have a tendency to principally developed a quick and secure multihop intervehicular network for communication with no knowledge loss. By conducting numerous experiments on our planned IVC network, results clearly tell that this can be the primary time to implement such a brand new system which may offer counter live fast and fastly for the mortal vehicles that reside in IVC.

## Keywords

**Network Disruption, Traffic Congestion, Adversary Nodes, Inter Vehicular Communication, Efficient Broadcasting.**

## 1. Introduction

As we all know that in the current days, there was a huge increase in number of

© 2016 JCT. All Rights Reserved 

vehicles and growing complexity of the transportation networks. Due to this there were a lot of delay and traffic problems that occur in the current human life.Even though there was a lot of traffic rules and regulations along with traffic signals to guide the vehicle drivers to a proper destination there cause still a huge delay and traffic issues. There was no proper mechanism to make the journey or travel with traffic free with no delay or less delay.

In order to make the journey or travel with traffic free with no delay or less delay, we need to deploy a vehicular network, which is nothing but a number of vehicles all together communicate with each other via a short-range wireless communication. By using this all the vehicles can therefore communicate with each other either directly or through a medium like multi hop transmission. In this network all the vehicles can act as powerful sensors and form mobile sensor networks. Some of the main applications of the vehicular networks constitute driving safety, intelligent transport, infrastructure monitoring, and a lot more monitoring applications.

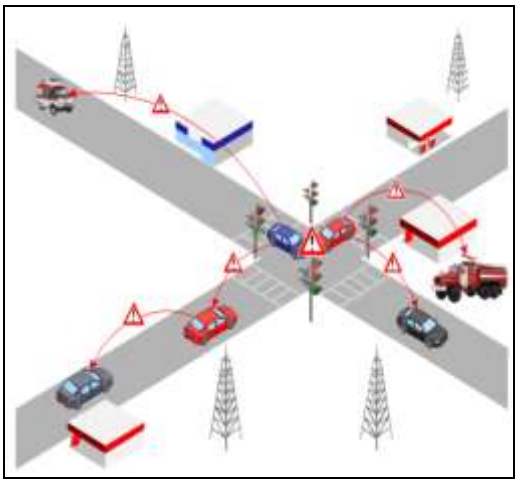

**Figure .1. Represents the Sample Architecture of Vehicular Network**

As we all know that in the current days 3G networks are getting more and more popular and it is very easy to access to 3G in turn. This 3G technology is included in many of the moving vehicles for communicating with each other while driving. The 3G communication has advantage of ubiquitous access and shorter delay. Compared with multi hop inter-vehicle communication, however, communication via 3G has some limitations. First, although 3G communications becomes more and more cheap, the cost of 3G communication is still high.

From the figure 3, we can clearly find out the architecture of a vehicular network with its signals and communication regions between each and every vehicles. Now a day it is very hard to find the movement of any vehicle also known as vehicle mobility. This is mainly because all the vehicles move at their own and individual wills around the road network and there is no proper device which can identify in which direction they may turn during the riding i.e. It is hard to identify the fore coming status of the vehicle in which way it is going to travel and move along its way. Generally in a vehicular network the routing of packets is monitored and operated by a relay node which will try to decide how long a packet should be kept and which node a given packet should be forwarded to. Our existing study and analysis results shows that it is not possible to find an optimal routing path when the knowledge of future node traces is not available, which is NP-hard problem? It is possible only if we can able to find the knowledge of future node traces, which is almost impractical.

## 2. Related Work

In this section we mainly discuss about the motivation and also the working of a GPS navigation system that is required for implementing this current paper.

© 2016 JCT. All Rights Reserved 

## A) Main Motivation

The main motivation for doing this paper is how efficiently a data can be delivered in an inter-vehicle during transmission over a vehicular networks and this is the main importance for developing this paper. In this paper we focus on such vehicular networks that are sparse and do no assume that all vehicles on the road are member nodes of the vehicular network. Such sparse vehicular networks feature infrequent communication opportunities. Inter-vehicle data delivery may introduce non negligible delivery latency because of frequent topology disconnection of a vehicular network. Thus, we should stress that the inter-vehicle communication in vehicular network are suitable for those applications which can tolerate certain delivery latency. For example, in the context of urban sensing, vehicles continuously collect useful information, such as road traffic conditions and road closures. A vehicle may send a query for a specific kind of information and the one that has the information should respond the querying node with the data. Such communications require multi-hop data delivery in vehicular networks. Other examples of such applications include peer-to-peer file sharing, entertainment, advertisement, and file downloading.

One of the main important components of any intervehicular communication is intelligent transportation system [2], [3], [4], [5]. The information which was gathered from any of the IVC network can able to foster road safety and transportation efficiency. Benefiting from the large capacities (in terms of both space and power) of vehicles, the nodes of these networks can have long transmission ranges and unlimited lifetimes [6].

## B) Global Positioning System

The **Global Positioning System** (**GPS**) is a space-based satellite navigation system that is used to display the location and time information in all weather conditions, anywhere on or near the Earth .The GPS system is mainly used in critical capabilities to military, civil and commercial users around the world. It is maintained by the United States government and is freely accessible to anyone with a GPS receiver [1]. The GPS project was developed in 1973 to overcome the limitations of previous navigation systems, integrating ideas from several predecessors, including a number of classified engineering design studies from the 1960s. GPS was created and realized by the U.S. Department of Defense (DoD) and was originally run with 24 satellites. It became fully operational in 1994.

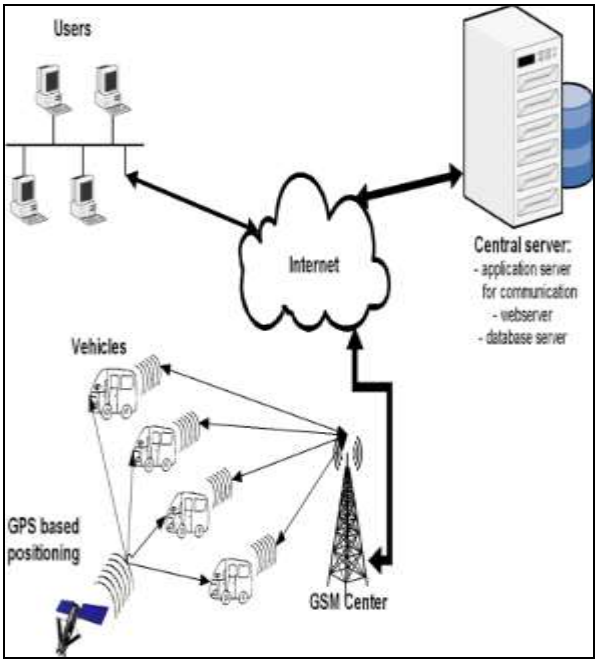


**Figure .2. Represents the Architecture of GPS System over Vehicular Network**

© 2016 JCT. All Rights Reserved 

From the figure 2, we can clearly identify the GPS route navigation system which was used in a vehicular network for identifying the position and traffic of the vehicles and this was send to the central server or service provider with the help of internet.Here there will be a set of users who try to access the information that was hosted through the internet and they all try to connect the network over GSM center which will collect all the vehicles information and try to sense that information through internet.

In the literature, there was several multihop broadcast algorithms have been proposed. These algorithms generally share the set of common properties mentioned in previous sections, thus falling into a single class of solutions. Unfortunately, they have all been developed without security in mind, whereas security is a fundamental problem in this context that should not be overlooked [13]. Indeed, attackers might run malicious actions to inject false information or alarm, thus rendering the safety application ineffective [14]–[20].

# 3. Proposed Enhanced Fast Multihop Broadcast Algorithm

In this proposed mechanism we proposed an enhanced fast multihop Broadcast algorithm where this was used effectively in IVC networks to communicate with each other without any communication loss between the vehicles. This algorithm has achieved the concept of Revoke at the time of any vehicle route failure. Now let us look some of the preliminaries that are used for this application. They are as follows:

To simplify the discussion, we have made the following assumptions about the general model that we are considering.

**1)** We suppose that at most one malicious vehicle is on the network.
**2)** There are no obstacles and no buildings in the road.
**3)** The hearing communication range is symmetric. It means that, if a vehicle *V* hears a vehicle *P*, then we assume that *P* can also hear *V* .
**4)** We suppose that there are *N* vehicles arranged in the platoon. A platoon can be looked at as a collection of nodes/vehicles that are connected by a wireless local area network and are engaged in longitudinally following each other.
**5)** A vehicle *V* does not know its transmission range.
**6)** The verifier node *V* directly communicates with the verified node *P*.
**7)** Each vehicle knows its own location, e.g., using GPS, which provides accurate information about time and position.
**8)** All the vehicles belong to a public key infrastructure (PKI) ; i.e., each vehicle has a public/private pair of keys and a unique identity certified by a certification authority. We assume that the certification authority corresponds to the government agency that is responsible for assigning license plates: a vehicle can be used only if it is provided with a unique license plate, a PKI certificate that is associated to its plate ID, and the public key of the certification authority. We assume that certificate revocation lists are updated at a given time interval (e.g., daily) by the vehicle and stored in a local memory.1
**9)** The power and computational resources are supposed largely adequate for our application's requirements.
**10)** The network is loosely time synchronized.

© 2016 JCT. All Rights Reserved 

## Enhanced Fast Multihop Broadcast Algorithm (EFMBA)

The main aim of EFMBA is to reduce the time that is required by a message to propagate from the source to the farthest vehicle in a certain area of interest. To achieve this goal, EFMBA exploits a distributed mechanism for the estimation of the communication range of vehicles. These communications range estimations are obtained by exchanging a number of *Hello* messages among the vehicles and are then used to reduce the number of hops that an alert message has to traverse to cover a certain area of interest. This leads to a decrease in the number of transmissions and the time that is required by a broadcast message to reach all the cars that follow the sender within a certain distance [7]-[9].

This scheme is composed of the following two phases: 1) the estimation phase and 2) the broadcast phase. The former phase is continuously active and is meant to provide each vehicle with an up-to-date estimation of its transmission range. The latter phase is performed only when a message has to be broadcast to all vehicles in the sender's area of interest [10]. To forward a packet, each receiver has to compute its waiting time before attempting to forward the message. This waiting time is expressed through a contention window (CW), which is computed using

$$CW = \left| \frac{(MaxRange - d)}{MaxRange} \times (CWMax - CWMin) + CWMin \right|.$$

**TABLE 1**
**Represents the Notations That Are Used In Proposed EFMBA**

| Symbol | Definition |
|---|---|
| $CMBR$ | Current Maximum Back Range |
| $CMFR$ | Current Maximum Front Range |
| $LMBR$ | Latest-Turn Maximum Back Range |
| $LMFR$ | Latest-Turn Maximum Front Range |
| $MaxRange$ | How far the transmission is expected to go backward before the signal becomes too weak to be intelligible |
| $d$ | Distance between two vehicles |
| $CW$ | Contention Window |
| $CWMax$ | Maximum Contention Window |
| $CWMin$ | Minimum Contention Window |
| $Hello$ | Hello message transmitted by a vehicle in the estimation phase to update the transmission range |
| $drm$ | declared transmission range in the $Hello$ message |
| $P$ | The prover vehicle |
| $V$ | The verifier vehicle |
| $R$ | The geographical region |

When a car has to send or forward a broadcast message, it computes the *MaxRange* value in the broadcast message as the maximum between *LMBR* and *CMBR* values. To avoid unnecessary transmissions, all vehicles between the original sender and the current forwarder abort their attempt to forward the message, whereas all vehicles behind the current forwarder compute a new CW for the next hop[11],[21].

In this below algorithm we mainly focus on the procedure of sending a *Hello* message (Algorithm 1). In every turn, each vehicle determines a random waiting time (lines 1 and 2). After this waiting time, if neither other transmission is heard nor a collision happened (line 6), it proceeds with transmitting a *Hello* message. This *Hello* message includes the *vehicle_ID* (line 7), the *timestamp* (line 9), the *vehicle_position* (line 8), the *declared_max_range* (line 10), and the list of neighbors and their two-hop neighbors *list_neigh_S* (line 11). Furthermore, the sender uses its private key to generate a signature to the message (line 12), and then, it transmits the message (line 13).

© 2016 JCT. All Rights Reserved 

## Algorithm 1: Sending Hello Message Algorithm (Executed by Sender Vehicle say X)

1 Input: *list_neighbors*: list of neighbors of $V$,
*vehicle_X*: the identity of the sender $X$,
*position_X*: the sender position,
*current_Time_X*: current time of the sender,
$LMFR$, $CMFR$, *list_neigh_X*: the list of neighbors of $X$,
$K^X_{private}$: private key of the sender $S$,
$H$: hash function;
2 Output: *Hello* message ;
3 For each turn ;
4 *sending_time* := *random*(*turn_size*);
5 wait (*sending_time*);
6 **if** *not* (*heard_Hello_msg*() *or heard_collision*()) **then**
7 *Hello_msg.vehicle_ID*:= *vehicle_X*;
8 *Hello_msg.vehicle_position*:= *position_X*;
9 *Hello_msg.timestamp*:= *current_Time_X*;
10 *Hello_msg.declared_max_range*:= $max(LMFR, CMFR)$;
11 *Hello_msg.list_neighbor*:= *list_neigh_X*;
12 *Hello_msg.signature*:= $K^X_{private}$
(H(*Hello_msg.vehicle_ID*, *Hello_msg.vehicle_position*,
*Hello_msg.timestamp*,
*Hello_msg.declared_max_range*,
*Hello_msg.list_neighbor*)) ;
13 transmit (*Hello_msg*);
14 EndFor

Now we discuss an algorithm for receiving Hello Message by a list of intermediate vehicles in the each and every individual zone (Say V).This was clearly explained in the algorithm 2.

In particular, a vehicle that receives a ***Hello*** message in line 2 generates the public key (line 3) using *f*(*sender_id_X*), where *f* is a hash function. In line 4, the receiver verifies the signature of *Hello* message. Then, it checks for the freshness of the message (line 6). This check is performed by verifying the coherence between the time that was inserted in the message by the claiming vehicle (the sender of the *Hello* message) and the current time of the receiver.

## Algorithm 2: Receiving Hello Message Algorithm (Received by Vehicle say V)

1 Input: *list_neighbors*: list of neighbors of $V$,
*current_Time_V*: the current time of $V$,
*sender_id_X*: the identity of the sender,
*sender_position_X*: the field corresponding to sender position,
*currentTime_X*: current time of the sender included in the message,
*drm_X*: the declared maximum range received, *list_neigh_X*: the list of neighbors in the received message,
*signedHelloMsg_X*: the received signature ;
2 < *sender_id_X*, *sender_position_X*, *currentTime_X*, *drm_X*, *list_neigh_X*, *signedHelloMsg_X* > ;
3 $K^{Pub}_X \leftarrow f(sender\_id\_X)$;
4 **if** $H(sender\_id\_X, sender\_position\_X, currentTime\_X, drm\_X, list\_neigh\_X) \neq K^{Pub}_X(signedHelloMsg\_X)$ **then**
5 handle this exception ;
6 **if** *IsNotCoherent* (*current_time_X*, *current_time_V*) **then**
7 handle this exception ;
8 **if** *IsNotPresent* (*list_neighbors*, *sender_id_X*) **then**
9 add(*list_neighbors*, < *sender_id_X*, *sender_position_X*, *currentTime_X*, *drm_X*, *list_neigh_X*, *signedHelloMsg_X* >) ;
10 *mp* := *my_position*() ;
11 *sp* := *sender_position* ;
12 *drm* := *declared_max_range* ;
13 *d* := *distance*(*mp*, *sp*) ;
14 **if** (*received_from_front*(*Hello_msg*)) **then**
15 $CMFR := max(CMFR, d, drm)$ ;
16 **else**
17 $CMBR := max(CMBR, d, drm)$ ;

For each message that passes the previous checks, the receiver extracts the information (*sender_id_X*) and checks whether this is the first received *Hello* message that carries the *sender_id_X*. Then, the receiver stores (*sender_id_X, sender_position_X, declared_max_range, timestamp, list_neighbor_X*) in its list of neighbors (line 9), extracts from the *Hello* message the estimation of the maximum transmission range (line 11) and the *sender_position* (line 12), and

© 2016 JCT. All Rights Reserved 

determines its own position (line 12) and the distance from the sender (line 13).

If the *Hello* message is received frontward, the value of *CMFR* is updated (lines 14 and 15); otherwise, *CMBR* is updated (lines 16 and 17). In both cases, the new value is obtained as the maximum among the old ones, the distance between the considered vehicle and the *Hello* message sender, and the sender's transmission range estimation provided by the *Hello* message [12].

# 4. Implementation Modules

Implementation is the stage where theoretical design is converted into practical design. Here we divide the application into various modules and then decide the flow of the application in a modular fashion. The following are the 5 modules for this application.

1) IVC Module
2) Sender/Server Module
3) Client Module
4) Revoke Module
5) Public Key Certification Module

## 1) IVC Module

In this module the IVC acts major role for this Inter vehicular communication. Here this will monitor all the vehicles status during the data transmission between server/sender to the destination. Here the vehicles will be changed its states from one region to other region randomly and the fllowing are the states which will be changed they are as follows: Initially all the nodes will be in active state where this is known as vehicular node with normal mode. Once if the nodes are started for data communication then some nodes will be converted as transmission nodes. At the time of any node absence this will be converted as Revoke state where at that situation node should check for an alternate best path.

## 2) Server/Sender Module

In this module, the server will browse the Image as input file and initialize the nodes, then select a client Ip Address & send to the particular end user. Server node will send their image file to IVC router and in that IVC it will be verifying all the nodes region by region and finally it will come to a final fourth region through which it can be received by the destination. Once data has been received successfully it will be handovered to the client.

## 3) Client Module

In this module, there will n-number of 'n' number of end users available in the IVC network (say A, B, C and D). The end user can receive the data file from the server via IVC router. The end user will receive the file by without changing the File Contents. Users may receive particular data files within the router only.

## 4) Revoke Module

This is a module which is available in this application in order to identify the available best node with normal state to transfer the data from one region to other region. This module will be invoked when any vehicle loses its normal state and it became in active then automatically revoke will be initiated and then it will identify the best nodes which are available alternatively from the failure node. This is very important module in the current application.

## 5) Public Key Certification Module

In this module we will be identifying the vehicles which are valid for communication between server and client and if any node which is not having valid authority by the PKC,then it is treated as absence vehicle and then it will not be allowed to send the data through this node to the destination. This acts

© 2016 JCT. All Rights Reserved 

like a authentication server which is used to authenticate the nodes during transmission.

# 5. Conclusion

In this paper, we for the first time have proposed a novel mechanism to identify the attack vehicles during the broadcasting in inter vehicular communication networks. We have implemented a enhanced fast Multihop broadcast algorithm in order to provide high security for the vehicular communication either there was any attack / revoke occur during communication. This paper has scratched the surface of what is promising to be a new and fertile area of research in IVC security. We have elaborated on security issues in IVC, considering a general class of applications based on Multihop broadcast; we have chosen a representative case study for this class, FMBA, to concretely discuss issues and solutions.

# 6. References

[1] G. Karagiannis, O. Altintas, E. Ekici, G. Heijenk, B. Jarupan, K. Lin, and T.Weil, "Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 4, pp. 584–616, 4th Quart., 2011.

[2] F. Qu, F.-Y. Wang, and L. Yang, "Intelligent transportation spaces: Vehicles, traffic, communications, and beyond," *IEEE Commun. Mag.*, vol. 48, no. 11, pp. 136–142, Nov. 2010.

[3] Sena, M.L., 2006. Cartographic presentation in navigation and route guidance systems. 18th ICA/ACI International Cartographic Conference, 2: 909-916.

[4] L. Li, J. Song, F.-Y. Wang, W. Niehsen, and N. Zheng, "New developments and research trends for intelligent vehicles," *IEEE Intell. Syst.*, vol. 20, no. 4, pp. 10–14, Jul./Aug. 2005.

[5] T. L. Willke, P. Tientrakool, and N. F. Maxemchuk, "A survey of intervehicle communication protocols and their applications," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 2, pp. 3–20, 2nd Quart., 2009.

[6] J. Luo and J.-P. Hubaux, *A Survey of Research in Intervehicle Communications*. New York, NY, USA: Springer-Verlag, 2006, pp. 111–122, Embedded Security in Cars–Securing Current and Future Automotive IT Applications.

[7] Y.-W. Lin, Y.-S. Chen, and S.-L. Lee, "Routing protocols in vehicular ad hoc networks: A survey and future perspectives," *J. Inf. Sci. Eng.*, vol. 26, no. 3, pp. 913–932, May 2010.

[8] A. Broggi, P. Cerri, S. Ghidoni, P. Grisleri, and H. G. Jung, "A new approach to urban pedestrian detection for automatic braking," *IEEE Trans. Intell. Transp. Syst.*, vol. 10, no. 4, pp. 594–605, Dec. 2009.

[9] M.-T. Sun, W.-C. Feng, K. Fujimura, T.-H. Lai, H. Okada, and K. Fujimura, "GPS-based message broadcasting for intervehicle communication," in *Proc. ICPP*, Aug. 2000, pp. 279–286.

[10] M. Roccetti and G. Marfia, "Modeling and experimenting with vehicular congestion for distributed networks"New York, NY, USA: Springer-Verlag, 2010, pp. 1–16.

[11] L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, "A scalable robust authentication protocol for secure vehicular

© 2016 JCT. All Rights Reserved 

communications," *IEEE Trans. Veh. Technol.*, vol. 59, no. 4, pp. 1606–1617, May 2010.

[12] B. Mishra, P. Nayak, S. Behera, and D. Jena, "Security in vehicular ad hoc networks: A survey," in *Proc. ICCCS*, Feb. 2011, pp. 590–595.

[13] Q.Wu, J. Domingo-Ferrer, and Ú. González-Nicolás, "Balanced trustworthiness, safety and privacy in vehicle-to-vehicle communications," *IEEE Trans. Veh. Technol.*, vol. 59, no. 2, pp. 559–573, Feb. 2010.

[14] S. Basagni, M. Conti, S. Giordano, and I. Stojmenovic, *The Next Paradigm Shift: From Vehicular Networks to Vehicular Clouds*. Hoboken, NJ, USA: Wiley, 2013, pp. 645–700.

[15] P. Papadimitratos, L. Buttyan, T. Holcze, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, "Secure vehicular communication systems: Design and architectures," *IEEE Commun.Mag.*, vol. 46, no. 11, pp. 100–109, Nov. 2008.

[16] A. Weimerskirch, J. J. Haas, Y.-C. Hu, and K. P. Laberteaux, "Data security in vehicular communication networks," in *VANET: Vehicular Applications and Internetworking Technologies*, K. P. Laberteaux, Ed.Chichester, U.K.: Wiley, Nov. 2009, ch. 9.

[17] L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, "A scalable robust authentication protocol for secure vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 59, no. 4, pp. 1606–1617, May 2010.

[18] B. Mishra, P. Nayak, S. Behera, and D. Jena, "Security in vehicular ad hoc networks: A survey," in *Proc. ICCCS*, Feb. 2011, pp. 590–595.

[19] G. Calandriello, P. Papadimitratos, J. P. Hubaux, and A. Lioy, "On the performance of secure vehicular communication systems," *IEEE Trans.Dependable Secure Comput.*, vol. 8, no. 6, pp. 898–912, Nov./Dec. 2011.

[20] M. Raya and J.-P. Hubaux, "The security of vehicular ad hoc networks," in *Proc. ACM SASN*, Nov. 2005, pp. 11–21.

[21] A. Aijaz, B. Bochow, F. Dötzer, A. Festag, M. Gerlach, R. Kroh, and T. Leinmüller, "Attacks on intervehicle communication systems—An analysis," in *Proc. Workshop Intell. Transp.*, Mar. 2006, pp. 1–11.

# 7. About the Authors

**G.RAJA GOUTHAMI** is currently pursuing her 2 years M.Tech in Department of Computer Science and Engineering at MVGR College of Engineering Vizianagaram, AP, India. Her area of interest includes Computer Networks.

**DR. G. SUVARNA KUMAR** is currently working as an Associate Professor in Department of Computer Science and Engineering at Department of Computer Science and Engineering at MVGR College of Engineering Vizianagaram, AP, India. He has more than 14 years of teaching experience in various engineering colleges.His research interest includes Machine Learning (Image Processing) and Computer Networks.

© 2016 JCT. All Rights Reserved 

**DR. G. SANDHYA DEVI** is currently working as an Assistant Professor in Department of Computer Science and Engineering at Department of Computer Science and Engineering at MVGR College of Engineering Vizianagaram, AP, India. She has more than 8 years of teaching experience in various engineering colleges.Her research interest includes Image Processing, Programming and Computer Networks.

© 2016 JCT. All Rights Reserved 