ISSN:0975-9646

# Security Issues on Inter-Vehicle Communications

M.V.B.T.Santhi, K.Deepthi, Ch.Satya Keerthi .N.V.L,P.Lakshmi Prasanna

*IST Department,KL University*
*Vaddeswaram,Guntur Dist,Andhra Pradesh,India.*

***Abstract*-The continuous increase in the number of vehicles in the transportation system calls for an improvement of traffic safety and efficiency of Inter vehicle communication. To achieve this demand, the vehicular communications have been considered to enable various security issues on vehicles is to obtain the traffic safety. Effective implementation of vehicular communication could also improve traffic management system. Inter-Vehicle communications are emerging as a new class of wireless networks enabling mobile users in their vehicles to communicate to the roadside and to each other. Safety related applications require a secure and reliable system. In this paper, we present an overview on the various possible attacks and countermeasures that provide secure communication among vehicles in traffic.**

***Keywords*-Inter-Vehicle Communication, Security, Safety, Traffic, Transport**

## I. INTRODUCTION

Inter-Vehicle Communication (IVC) is attracting a considerable attention from the research community and the automotive industry, where it is beneficial in providing Intelligent Transportation System (ITS) as well as drivers and passengers' assistant services. In this context, vehicular networks are emerging as a new class of wireless networks, spontaneously formed between moving vehicles equipped with wireless interfaces that could be of homogeneous or heterogeneous technologies. The recent advances in wireless technologies and the current trends in ad hoc networks scenarios allow a number of possible architectures for vehicular networks deployment. In this paper, we give a deployment view for vehicular networks illustrating its potential services. We present the possible deployment architectures of these networks and some promising wireless technologies, and we discuss some technical challenges for the deployment of these networks with a main focus on the security problem.

Currently, Inter-Vehicle Communication Systems (IVCS) are widely discussed, attracting a considerable attention from the research community as well as the automotive industry. In this context, vehicular networks are emerging as a new class of wireless networks enabling mobile users in their vehicles to communicate to the roadside and to each other. Vehicular networks are also promising in being a concrete application for ad hoc networks. These networks have special behavior and characteristics, distinguishing them from other types of networks: the nodes' (vehicles') mobility is high and may reach up to 200Km/h, the topology is dynamic but constrained by roads' topology, these networks may scale to a very large number of nodes (vehicles) according to the traffic condition and are expected to have a potentially heterogeneous administration. In this context, we consider that vehicular communication, opposing the wireless mobile communication, does not suffer from resource limitations (energy, CPU, memory, etc.) as vehicles are not tiny nodes and are capable of providing unlimited resources.

Security in Inter-Vehicle communication is a major challenge, having a great impact on future deployment and applications of vehicular networks. Suitable security mechanisms should be in place providing authentication, access control, trust and secure communication between vehicles. In the context of vehicular communication security, we discuss about two terms: Safety and Security. Safety rather concerns people's safety on roads including drivers and passengers, while security concerns the secure data transfer. Consequently, securing Inter-Vehicle Communication should take into account both Safety and Security. Authentication and authorization are important counter-attack measures in vehicular networks deployment, allowing only authorized mobile nodes to be connected and preventing adversaries to sneak into the network disrupting the normal operation or service provision.

## II. RELATED WORK

### A. Existing System

In the Existing architecture there is no security provided among the vehicles in the vehicular networks. Due to this there will be possibility of happening accidents. Sometimes some unsecured vehicle may also come into the networks and intends to do accidents and disturb the vehicular network.

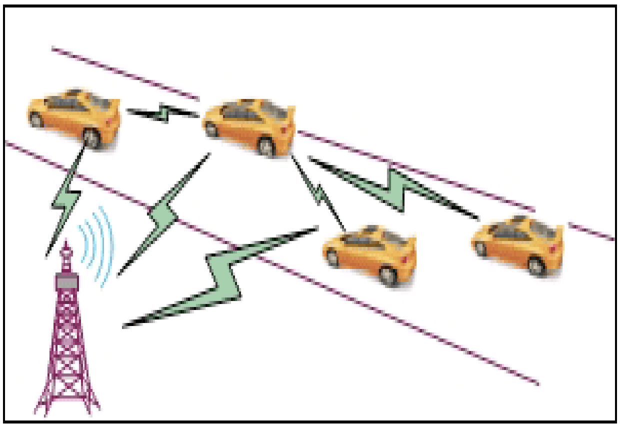


**Fig 1 Existing architecture in vehicular networks**

### B. Proposed System

In the proposed architecture only authenticated vehicles can enter into the network and vehicles go in a secure path and which is also authenticated .If two vehicles send packets at the same time i.e., when collision occurs then the drops the packets of one of the source according to the protocol.

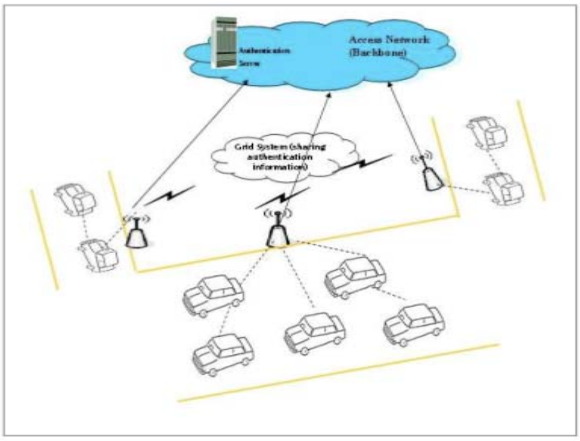


**Fig 2 Proposed architecture for inter vehicle communication**

The main aim for vehicular communication systems is security and eliminating the excessive cost of traffic collisions. Departing vehicles can inform other vehicles that they intend to depart the highway and arriving cars at intersections can send warning messages to other cars traversing that intersection. Although the main advantage of vehicular networks is safety improvements, there are several other benefits. Vehicular networks can help in avoiding congestion and finding better routes by processing real time data. This in return saves both time and fuel and has significant economic advantages. The main objective of this paper is to provide counter measures for various attacks in traffic to provide secure communication among vehicles in traffic.

## III. SYSTEM DESIGN

### A. Overview of the Security Issues on Inter-Vehicle Communications

Inter-Vehicle Communication (IVC) is attracting a considerable attention from the research community and the automotive industry, where it is beneficial in providing Intelligent Transportation System (ITS) as well as drivers and passengers' assistant services. In this context, vehicular networks are emerging as a new class of wireless networks, spontaneously formed between moving vehicles equipped with wireless interfaces that could be of homogeneous or heterogeneous technologies. The recent advances in wireless technologies and the current trends in ad hoc networks scenarios allow a number of possible architectures for vehicular networks deployment. In this paper, we give a deployment view for vehicular networks illustrating its potential services. We present the possible deployment architectures of these networks and some promising wireless technologies, and we discuss some technical challenges for the deployment of these networks with a main focus on the security problem.

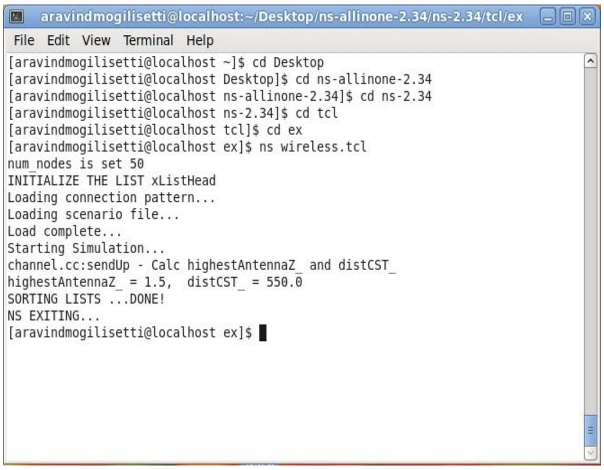
Security in Inter-Vehicle communication is a major challenge, having a great impact on future deployment and applications of vehicular networks. Suitable security mechanisms should be in place providing authentication, access control, trust and secure communication between vehicles. In the context of vehicular communication security, we discuss about two terms: Safety and Security. Safety rather concerns people's safety on roads including drivers and passengers, while security concerns the secure data transfer. Consequently, securing Inter-Vehicle Communication should take into account both Safety and Security. Authentication and authorization are important counter-attack measures in vehicular networks deployment, allowing only authorized mobile nodes to be connected and preventing adversaries to sneak into the network disrupting the normal operation or service provision.

## IV. IMPLEMENTATION

### A. User-Interface Design

User Interface design is the design of computers, appliances, machines, mobile communication devices, software applications, and websites with the focus on the user's experience and interaction. The goal of user interface design is to make the user's interaction as simple and efficient as possible, in terms of accomplishing user goals—what is often called user-centered design. Good user interface design facilitates finishing the task at hand without drawing unnecessary attention to it. Graphic Design may be utilized to support its usability. The design process must balance technical functionality and visual elements (e.g., mental model) to create a system that is not only operational but also usable and adaptable to changing user needs.

Interface design is involved in a wide range of projects from computer systems, to cars, to commercial planes; all of these projects involve much of the same basic human interactions yet also require some unique skills and knowledge. As a result, designers tend to specialize in certain types of projects and have skills centered around their expertise, whether that be software design, user research, web design, or industrial design.

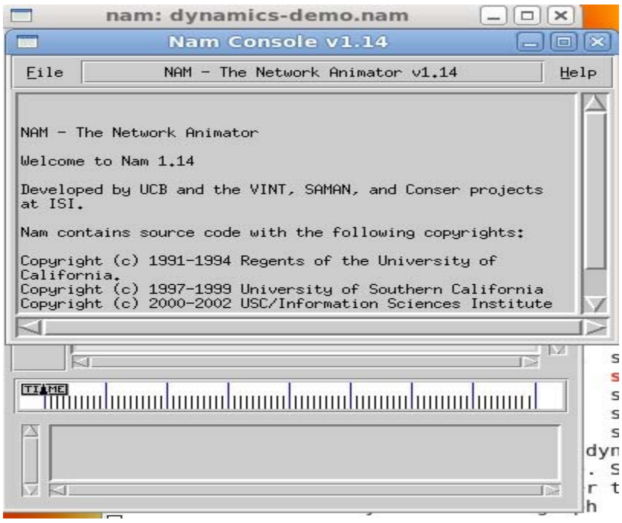

aravindmogilisetti@localhost:~/Desktop/ns-allinone-2.34/ns-2.34/tcl/ex
File Edit View Terminal Help

```
[aravindmogilisetti@localhost ~]$ cd Desktop
[aravindmogilisetti@localhost Desktop]$ cd ns-allinone-2.34
[aravindmogilisetti@localhost ns-allinone-2.34]$ cd ns-2.34
[aravindmogilisetti@localhost ns-2.34]$ cd tcl
[aravindmogilisetti@localhost tcl]$ cd ex
[aravindmogilisetti@localhost ex]$ ns wireless.tcl
num_nodes is set 50
INITIALIZE THE LIST xListHead
Loading connection pattern...
Loading scenario file...
Load complete...
Starting Simulation...
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 550.0
SORTING LISTS ...DONE!
NS EXITING...
[aravindmogilisetti@localhost ex]$ 
```

**Fig 3 User-Interface of Terminal**

### *B. Network Animator Design*

Nam is a network animator that provides packet-level animation, protocol graphs; traditional time-event plots of protocol actions, and scenario editing capabilities. Nam benefits from a close relationship with ns, which can collect detailed protocol information from a simulation. The authors describe how nam uses preprocessing to visualize data taken directly from real network traces. They also feel that visualization tools such as nam make protocol design and debugging easier.


nam: dynamics-demo.nam

Nam Console v1.14

File NAM - The Network Animator v1.14 Help

```
NAM - The Network Animator

Welcome to Nam 1.14

Developed by UCB and the VINT, SAMAN, and Conser projects
at ISI.

Nam contains source code with the following copyrights:

Copyright (c) 1991-1994 Regents of the University of
California.
Copyright (c) 1997-1999 University of Southern California
Copyright (c) 2000-2002 USC/Information Sciences Institute
```

Fig 4 View of the Network Animator

### *C. Vehicular Network Design*

The design of the Vehicular network is developed using the simulator by writing code in TCL language, and with the help of the present library files which generates the scenario. We have used the scenario file to develop an architecture consisting of 5 nodes out of which 2 are source and 3 are destinations. The Scenario file sets up a CBR connection among the nodes. The co-ordinates of the nodes are specified in the scenario files, based on these co-ordinates the position of the nodes are finalized. The following figure will provide a clear idea of about how the mesh network is designed.

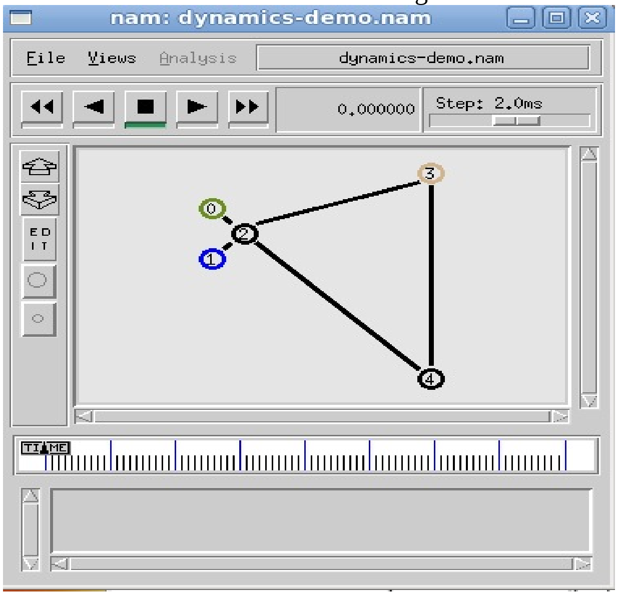


Fig5 Initial position of vehicular network

### *D. Communication Between sender and the reciever*

Initally we considered five nodes namely 0,1,2,3 and 4. We considered the nodes 0,1 as the sender cars i.e., 0,1 cars are sending packets to the destination.The main aim of the sender nodes 0,1 is to send the packets to node 3.The two nodes 2,4 will act as the mediater nodes i.e., the nodes 0,1 send packets to node 3 via 2,4 nodes.To deistinguish between the nodes 0,1 i.e., to know which node is sending packets we have represented with two different colors blue and green,blue for node1, green for node 0.

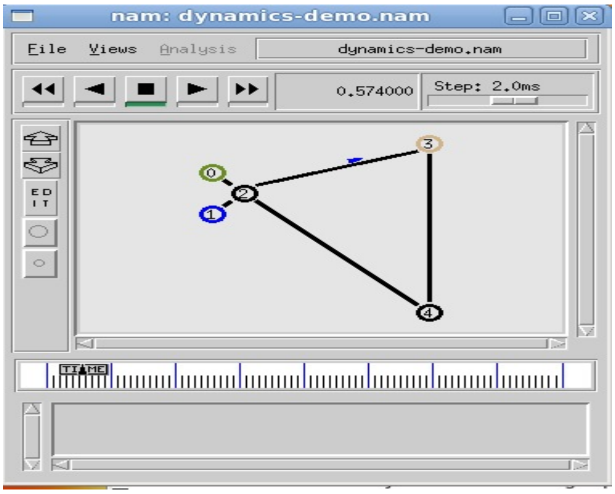
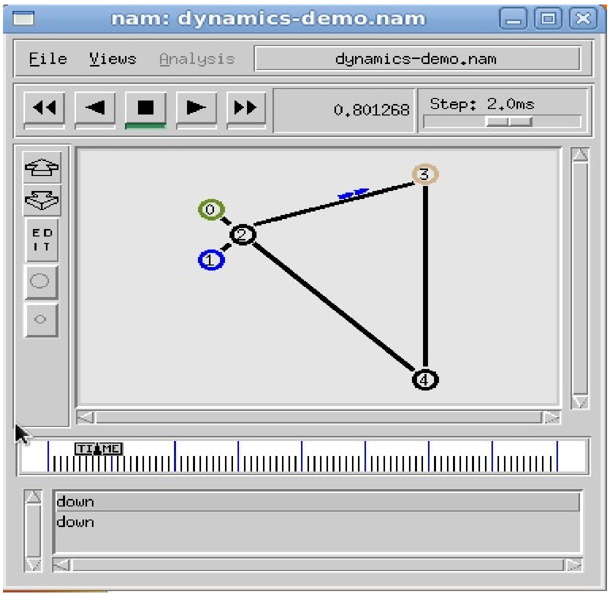


Fig 6 Communication between sender and receiver

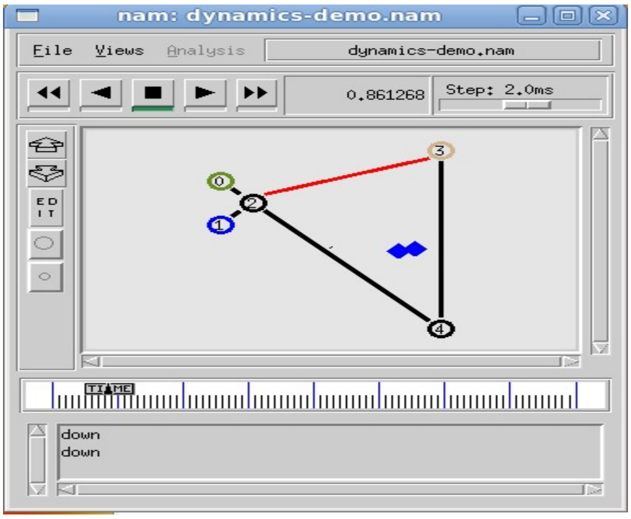
In the figure 7 transfer of packets is done between node1 and node 3.To represent that node 1 is sending data we have shown the packet transfer in blue color. Every time size of packet may or may not change. Node1 is sending packets to node3 via the node2.



```
down
down
```

Fig 7 Transfer of packets between node1 and node 3

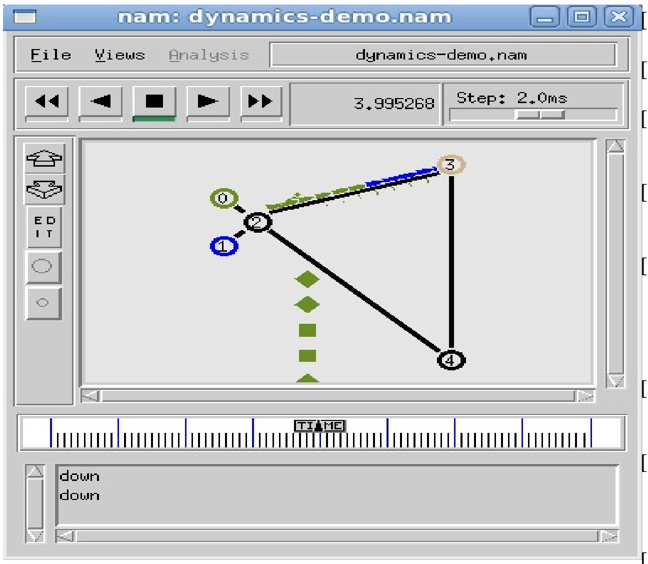
In the figure 8 the node1 wish to send packets to node 3 via node 2.But the route between node 2 to node 3 is not secured so it is not safe if the messages go between the route node 2 and node 3. So the packets are dropped in the middle of the transfer only.



```
down
down
```

**Fig 8 Dropping of packets**

In the figure 9 collision of packets is taking place. Node 1 and Node 0 are sending packets at the same time so collision occurred. One of the packets needs to be dropped that's why the packet from the node 0 is been dropped.



```
down
down
```

**Fig 9 Packet Drop due to collision**

## V. CONCLUSION

This paper addresses about vehicular communication security, presenting some important security requirements. The problem of authentication, authorization and access control in these networks is discussed. Security is one of the significant challenges impacting vehicular networks. In this paper we present an overview on the various possible attacks and countermeasures that provide secure communication among vehicles in traffic.

## VI. FUTURESCOPE

The basic architecture of inter-vehicle communication is implemented. We can even extend this paper by proving many vehicles communication among them. We have shown that the packet will not accept if that particular node is not authenticated. Like this way we can even provide some other security issues in the architecture. We shown four cars as four nodes, but we can even increase the number of cars and show the communication among them.

## REFERENCES

[1]H. Hartenstein, B. Bochow, A. Ebner, M. Lott, M. Radimirsch, D.Vollmer: Position-Aware Ad Hoc Wireless Networks for Inter-Vehicle Communications: The Fleetnet Project, ACM Symposium on Mobile Ad Hoc Networking and Computing, MobiHoc, 2001.

[2]C. Tchepnda, H. Moustafa, H. Labiod, G. Bourdon: Securing Vehicular Communications: An Architectural Solution Providing a Trust Infrastructure, Authentication, Access Control and Secure Data Transfer, ACM Autonet 2006 workshop in conjunction with Globecom 2006.

[3] J. P. Hubeaux, S. Capkun, J. Luo: The Security and Privacy of Smart Vehicles, IEEE Computer Society, 2004.

[4] P. Golle, D. Greene, J. Staddon: Detecting and Correcting Malicious Data in VANETs, ACM VANET, October 2004.

[5] M. Raya, J. P. Hubaux: The Security of Vehicular Ad Hoc Networks, ACM SASAN, 2005.

[6] M. Uhm: Making the Adaptivity of SDR and Cognitive Radio Affordable, DSP Magazine, May 2006.

[7] L. Zhou, Z. Haas: Securing Ad hoc Networks, IEEE Network Magazine, 13(6):24-30, 1999.

[8] M. Raya, J. P. Hubaux: The Security of Vehicular Networks, ACM Workshop on Security of Ad hoc and Sensor Networks, SASN05, 2005.

[9] X. Yang, J. Liu, F. Zhao, N. Vaidya: A vehicle- to-vehicle communication protocol for cooperative collision warning, MobiQuitous, August 2004.

[10] H. Moustafa, G. Bourdon, Y. Gourhant: AAA in Vehicular Communication on highways using Ad hoc Network Support: a proposed Architecture, Proceedings of the second ACM workshop on VANETs 2005, in conjunction with MobiCom 2005, SEP05.

[11] I. Chakeres, J. Mackers, T. Clausen: Mobile Ad hoc Network Architecture, I-D draft-ietf-autoconf- manetarch-06, October 2007

[12] E. Bacelli, K. Mase, S. Ruffino, S. Singh: Address Autoconfiguration for MANET: Terminology and Problem Statement, I-D draft-ietf- autoconf-statement-01, August 2007 (work in progress).

[13] Car2Car Communication Consortium Manifesto, work in progress, May 2007.

[14] IEEE P802.11p: Draft Amendment to STANDARD FOR Information technology Telecommunications and information exchange between systems

[15] J. Ott, D. Kutscher: The "Drive-thru" H. Moustafa, G. Bourdon, Y. Gourhant: AAA in Vehicular Communication on highways using Ad hoc Network Support: a proposed Architecture, Proceedings of the second ACM workshop on VANETs 2005, in conjunction with MobiCom 2005, September 2005.

[16]H. Moustafa, G. Bourdon, Y. Gourhant: Providing Authentication and Access Control in a Vehicular Network Environment, IFIPSEC 06, 2006.