Networks on Road - Challenges in Securing Vehicular Ad hoc Networks

Ramesh Kait[1], R. K. Chauhan[2]
Department of Computer Science & Applications
Kurukshetra University, Kurukshetra
[1]ramesh.kait@gmail.com, [2]rkc.dcsa@gmail.com

ABSTRACT : *The fundamental component for the success of VANET (Vehicular Ad hoc NETworks) applications is routing since it must efficiently handle rapid topology changes and a fragmented network. On demand set up, fault tolerance and unconstrained connectivity are a couple of advantages that why mobile computing continues to enjoy rapid growth.However, it can be expected that security attacks are likely to increase in the coming future due to the more and more wirelss applications being developed and deployed on to the well-known expose nature of wireless medium. Thanks to the substantial research efforts carried out by the community so far, we make the following contribution in this paper. In this paper we are specifically taking real life application of mobile ad-hoc networks i.e. VANET (vehicular ad-hoc networks). We will present a novel infrastructure for vehicle communication on highway and propose some potential security challenges from a driver's perspective and car manufacturer's .We will introduce an exemplary approach to outline various challenges and some possible solution.*

Keywords: *Vehicular Ad hoc NETworks (VANET), security, MANETs, VC, V2V*

1. INTRODUCTION

MANETs consist of mobile/semi mobile nodes with no existing pre-established infrastructure. They connect themselves in a decentralized, self-organizing manner and also establish multi hop routes. If the mobile nodes are vehicles then this type of network is called VANET (vehicular ad-hoc network). One important property that distinguishes MANET from VANET is that nodes move with higher average speed and number of nodes is assumed to be very large.Plummeting cost of electronic components and permanent willingness of manufacturers to increase road safety and to differentiate themselves from their competitors vehicles are becoming “Computer on Wheels” rather than “Computer Networks on Wheels”. Convergence of forces from both the public and private sector implies that in not-too-distant future we are likely to see the total birth of vehicular networks. In 1999, U.S. federal communication Commission (FCC) allocated a block of spectrum in 5.850 to 5.925 GHz band for applications primarily intended to enhance the safety of our networks on roads systems. In fact BMW, Fiat, Renault and some other organizations have united to develop a car-to-car communication consortium, dedicated precisely to impose industry standards for emerging wireless technology [3]. Here is one diagram showing vehicular communication:

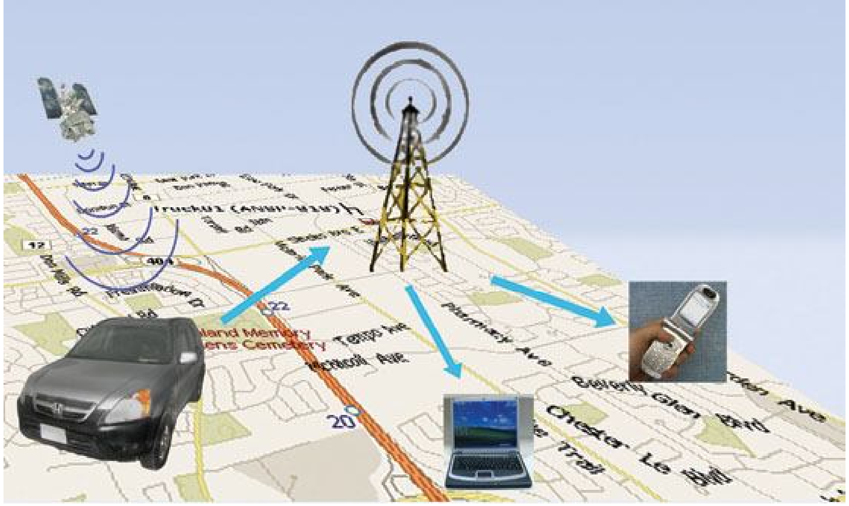

Figure 1: *vehicular communication NETworks on Road*

Manufacturers are able to make a quantum step in this field by letting vehicle communicate with each other. This type of communication results not only enhanced situational awareness which provides the decision making task of drivers but also improve highway safety. Considering the tremendous benefits expected from VANET, it is clear that car-to-car communication is likely to become most relevant realization of mobile ad-hoc networks. But besides the benefits such communication raises various formidable challenges.

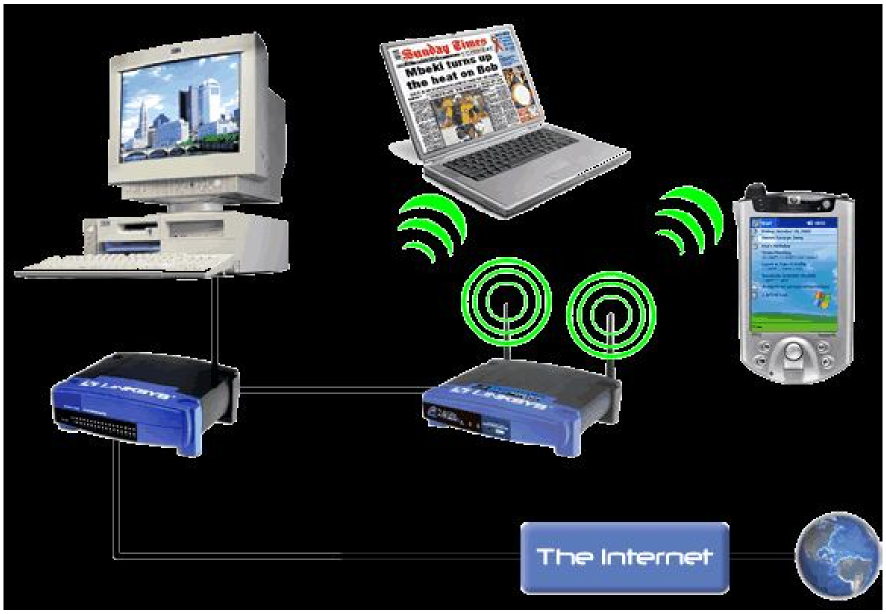

Figure 2: Mobile Adhoc Networks

In this paper we start the discussion with the introduction then in the **section 2** of this paper contain some potential safety related applications of VANETs and various challenges that vehicles that it faces on road. The **section 3** gives detail why VANET is need of more security and what kind attack may happens on such networks. **Section 4** gives detail of security architectural concepts about VANET that what are the devices we have to make secure from security point of views.

2. APPLICATIONS

Over the years tremendous work is done in mobile ad-hoc networks. Now vehicular communication networks are a new technology that has drawn the attention of industry and academia. The main goal of VANET is providing safety and comfort for passengers. We categorizes the applications in two parts:[5]

2.1 Entertainment related application

- Internet access
- Road side service (fast food, shopping mall, fuel section, toll collection etc)

2.2 Challenges in Vehicular Communication

- **Scale:** For a network to be established on road, we assume the numbers of nodes are very large. And a technically convincing solution is a pre-requisite for any security architecture.
- **Dynamic Movements:** Since the number of nodes in this networks are vehicles and it is assumed that various vehicles are dynamically joining and leaving the network at high speed. So on a large scale to maintain the data becomes a crucial task.
- **Real Time Sensitivity:** Many applications demand strict deadline for delivery of messages. So security mechanism must consider these real time constraints.
- **Heterogeneity**: Heterogeneity in vehicular communication is additional challenge where nodes/vehicles are possibly equipped with GPS, cellular transmitter/receiver. Interoperability amongst these heterogeneous nodes is a critical task.

3. WHY SECURITY IN VANET IS NEEDED?

Apart from numerous advantageous features it is obvious that such kind of services face various adversarial attacks.[2,3,5,6,7,8] .We outline some of the threats against security.

- **Denial of services:** When an attacker is malicious and active and wants to bring down the network by denying the service. It may cause accidents and even more fatal disastrous action could happen.[4]
- **Attacker Forgery:** Attackers maliciously sends fake messages about traffic jams and give suitable direction and hence divert the drivers the node to other routes clearing his way. A single attacker forges and transmits false information and hazard warnings and local danger warning[7,8]
- **On-board Tampering:** An attacker may select to tinker with the data, tampering with the on-board sensing and other hardware. It may be easier to replace or bypass real time clock or wiring of the sensor. Any hacker can have the total access control of that board.[5,7]
- **Need for Secure Protocol:** The protocols designed so far for routing in ad-hoc networks are AODV (ad-hoc on demand distance vector) routing,

DSR (dynamic source routing), DSDV (destination sequenced distance vector routing)[9] But these protocols face some security challenges. A critical evaluation is needed in security when actually implemented on road.

- **Attack using impersonation:** Spoofing occurs when a node misinterprets its identity in the n/w such as by altering MAC/IP address.[4]
- **Masquerade:** An attacker actively pretends to be another vehicle by using false identity.

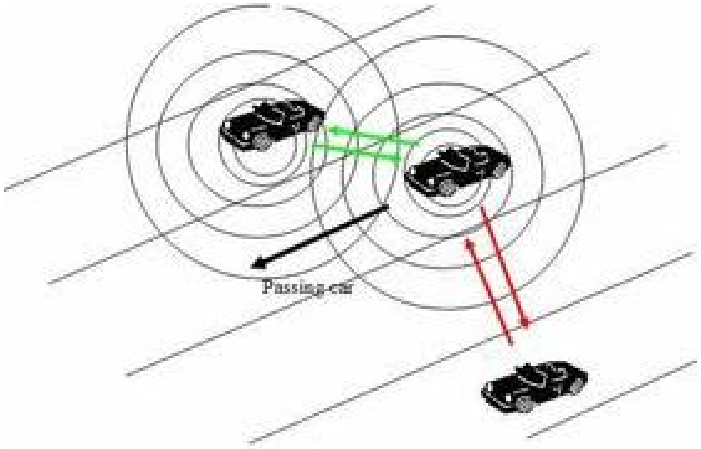

Figure 3: *Vehicle Tracing*

4. SECURITY ARCHITECTURAL CONCEPTS

Against a wide range of threats, we present various architectural components needed to protect.

- **Hardware**

To avoid on-board tampering, two network modules must be installed for security namely EDR-event data recorder and TPD-Tampering proof device. EDR is responsible for recording vehicle critical data such as position, time, and speed. This data is helpful in investigating accident. TPD will take care of storing all the cryptographic material and performing cryptographic operations i.e. verifying messages.

- **Message Authentication**

Fundamental security function in vehicular communication will consist of authenticating the origin of data packet. Authentication also helps to control the authorization level of vehicles.

- **Vehicle Authentication**

This is related to security from car's manufacturers. Certification Authorities will issue certified public/private key pairs to vehicles. Different Certification Authorities (CA) will have to be cross certified so that vehicles from different regions /different manufacturers can authenticate each other.

- **User Authentication**

Each user of a vehicular communication system has a unique identity and a pair of private and public cryptographic keys i.e. a certificate issued by an authority for a user. The user is bound to its credential.

Taking various issues and security threats into account, we simply provide the following notable solution features.

- **Time stamp:** All vehicles in the communication network must add sequence number as well as time stamps. Because the components are equipped with GPS. And GPS is a time service.

Digital Signatures as building block: Message legitimacy is mandatory to protect VANET. Exchange of safety messages needs authentication not encryption. So in this context digital signatures are assumed to be a better option because these messages are stand alone

- **Tamper-proof device:** To avoid on-board tampering, device should be tamper –proof. This device is responsible for signing outgoing messages. To reduce the task of any kind of attack, the device should be restricted to authorize people. Tamper proof device use revocation protocol to send secure messages.[5]
- **Authenticated Routing Protocol:** Popular ad-hoc routing protocols are subject to a variety of attacks. These protocols have the problem that they allow attackers to influence a victim's selection of routes or enable denial of service. One protocol ARAN (authenticated routing for ad-hoc network), provides secure routing for open environment. ARAN is a simple protocol that does not require any additional work from nodes within a group.[4]

4.0 Proposed Solution model to Attack:

The proposed model gives the solution to the all above attack of attackers and the model uses On-Board-Unit(OBU). This is the device which is fitted in all the vehical node, for making the decision for determining the attacks and the processing unit suggest the OBU to switch channel, technology or to use the frequency hopping techniques. As depicted in the **figure 4.0** bellow.

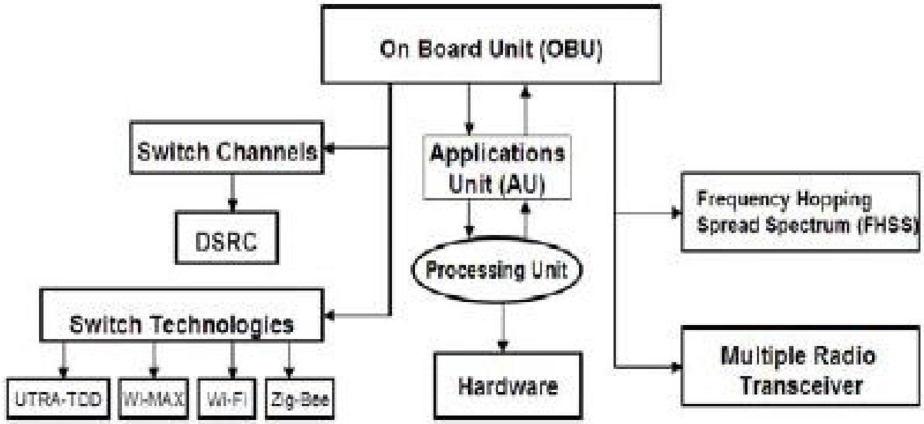

***Figure 4.0 :** Proposed Model for Solution*

4.1 Channel Swtching:

Dedicated short ranege Communications (DSRC) provides multiple channels and hence it devided into sevenchannels in which three channel(CH 172, Ch178 and CH184) are having safety parameteres and all other having the Non Safety Channels(CH 174, CH176, Ch180 and Ch182). In tthis case if attackers Jams the one Channel the the node can communicate with the other channel

4.2 technology Swtching:

There are so many communications technology are available that works with the netork and these technology(Wi-MAX, Wi-Fi,Zigg-Bee and Ultra-TDD i.e. Time Division Duplex) facilitate the node to move from one techno to another

4.3 Frequency Hoping Spread Spectrum:

This technology is very much famous and used in GSM,Bluetooth, 3G and 4G and this is having the facility of expanding the band width of a signal by adding some keys/codes so that the packets can be transmitted over a set of ifferent frequency range. And hence whenever the jammer jams the network then the node having the facility to mi=ove from one frequency to another.

4.4 Multi Radio Transceivers:

It is also possible for OBU to have multiple transceivers for sending and receiving messages using some based on Design Principles.

Discussion and Conclusion

Safety is the primary concern to many road user and safety requirement are powerfully supportted by many safety applicationsIn terms of communication we have provided a feature that captures the distinctive characteristics of Vehicular Communication (VC), Vehicular-to-Vehicular (V2V) communication through a careful survey of literature. We find that we have probably come out with the some possible threats against vehicular communication. And this is important as one can't anticipate in details against any protocol. [1] The presented list of challenges and attacks could also grow. Our focus is on VC which emerges as a promising technology that draws world wide support and has potential for large scale deployment. While this paper presents no technical results but we believe this paper can be helpful for future designer in VC.

References

[1] Holger Fubler,Sascha Schnaufer,Matthias Transier,Wolfgang Effelsberg, "Vehicular Ad-hoc Network from Vision to Reality and Back", In Proc.of 4th Annual IEEE/IFIP Conference on Wireless on Demand Network Systems and Services (WONS), Obergurgl,Austria,January 2007.

[2] Magda El Zarki, Sharad Mehrotra, Gene Tsudik and Nalini Venkatasubramanian, "Security Issues in a Future Vehicular Network",Eurowireless,Feb-02.

[3] Bryan Parno, Adrian Perrig, "Challenges in Securing Vehicular Networks", Poster presented at USENIX Security Symposium,August-04.

[4] Kimaya Sanzgiri, Daniel LaFlamme, Bridget Dahill, "Authenticated Routing for Ad hoc Networks", Proc. Of IEEE Journal on selected area in communication 23.3(2005):598-610.

[5] Maxim Raya and Jean Pierre Hubaux," The Security of Vehicular Ad Hoc Networks", Proceeding of 3rd ACM workshop on security of adhoc and sensor network, 2005.ISBN1-59593-227-5

[6] P. Papadimitratos,V.Gligor, J-P Hubaux, " Securing Vehicular Communication –Assumptions ,Requirement and Principles", Proc. Of workshop on embedded security in cars(ESCAR),Nov-2006.

[7] Maxim Raya, P.Papadimitratos,Jean-Pieree Hubaux, "Securing Vehicular Communication", Proc. of IEEE wireless communication magazine ,special issue on inter vehicular communication,Oct-2006.

[8] Florian Dötzer, "Privacy Issues in Vehicular Ad Hoc Networks", Privacy Enhancing Technologies Pg.197-209.

[9] C.K.Toh, "Adhoc mobile wireless network: Protocol and Systems", (January 2002).