ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)
Vol. 3, Issue 1 (Jan. - Mar. 2015)
International Journal of Advanced Research in Computer Science & Technology (IJARCST 2015)

# Survey: Secure Routing in VANET

[I]Vivek Chand Dubey, [II]Vinod Kumar

**Abstract**
*Vehicular Ad hoc Network (VANET) is an emerging technology since previous some years. It is very important to implement Intelligent Transportation System (ITS). There is some security issues and attacks which are associated with the VANET due to its dynamic nature, like changing topology, lack of infrastructure etc. Our aim is to detect and avoid the attacks and enhance the security. We surveyed in some research paper that there is some possible attacks in the VANET like Sybil attack, Wormhole attack, Sinkhole attack etc. In this paper we try to show that effect of different attacks.*

**Keyword**
*Sybil attack, Sinkhole attack, Wormhole attack, ITS, VANET.*

## I. Introduction

VANET is an ad hoc network in which vehicles act as a node. Some people used to say "Network on Vehicles". Since the mobility of nodes are very fast so its topology is changed rapidly. As we know there are generally three types of communication in VANET. Road Side Unit (RSU) to RSU, vehicles to vehicles and vehicles to RSU. Structure of VANET [1] given in fig. 1 which shows the communication in the VANET.
Each vehicle belongs to the different RSU. If node communicates in the same region then it is called the group communication.

### Why VANET?

We use the VANET instead of Mobile Ad hoc Network (MANET) due to high mobility of the vehicles and we know that MANET does not support high mobility. When the speed of node is fast then the topology and configuration changed rapidly which can not handle by the mobile ad hoc network (MANET) so we need the VANET. It also have some different characteristics from MANET-

- High Mobility
- Unbounded network size
- Rapid changing topology

### Possible application of VANET

The most useful application of VANET is Intelligent Transport System (ITS). ITS is a life safety application which provide the information of one node to another node. Since the path of node is predefined so node cannot move randomly and we can predict the location of nodes after regular time interval on the basis of their respective speed.
Another important and efficient application of VANET is Electronic Toll Collector (ETC). ETC is the process of collecting toll electronically without stopping the vehicles.
Service finder can be another application of the VANET. It can provide the location of nearest filling stations, restaurant, etc.

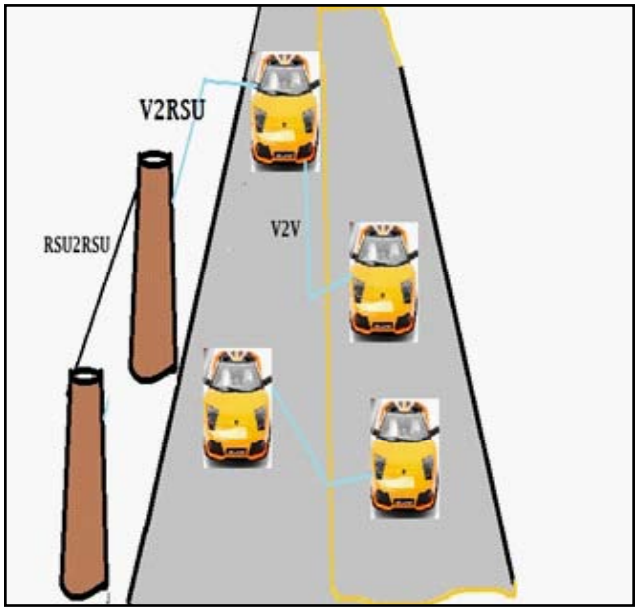


Fig. 1 VANET structure

## II. Routing in VANET

Routing play very important role for packet delivery. Routing basically provide the route to the source to forward the packet to the destination. Source sends the packet to the destination through the intermediate nodes. But here one question is arising that which node will be selected to forward the packet. We can solve this problem by shortest path algorithm.
There are different kinds of routing in VANET based on the different strategies based on the some criteria like proactive, reactive etc. There are some security issues which may cause the problem in routing. If we implement the security on routing then we can obtain secure routing which is most important need of the VANET.

## III. Security in VANET

In modern era, security is major issue to secure any information. Only routing is not sufficient for information exchange but security is also needed for the secure communication. It must satisfy the trust worthiness. In fig.2 it is shown that some vehicles send bogus message to other vehicles for their own profit which is vulnerable [2].

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

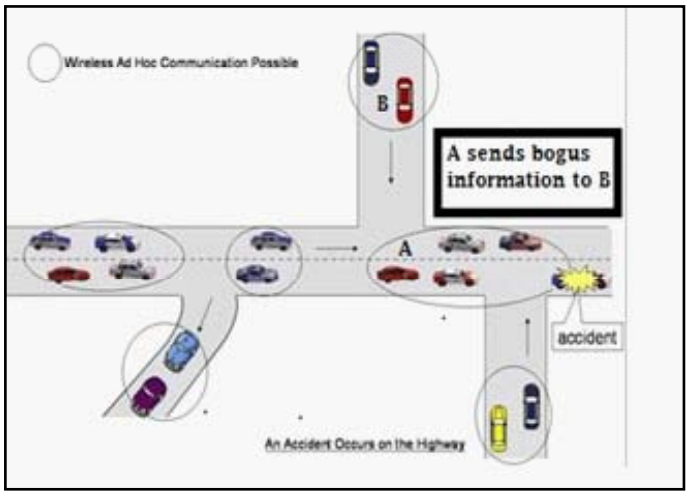



Fig.2: Attack with false information A and B disseminate false information to influence network.

Since the nature of VANET is dynamic and no. of nodes change regularly so any nodes which are unauthorized can enter in the network and try to access the some private information of other nodes. To protect these activities security is necessary.
Attacks in VANET are classified into different layer according to their work. Irshad Ahmed Sumra [6] proposed different kind of attacks layer which are given in the fig. 3

| Monitoring Attacks |
|---|
| Social attack |
| Timing attack |
| Application attack |
| Network attack |

Fig. 3

Under the Monitoring attack those attack come which try to trace the location of the nodes. In social attack one vehicle send some nonsense message to their neighbor vehicles. Fig. 6 shows the example of social attack. Here node D send some nonsense message to the node C.

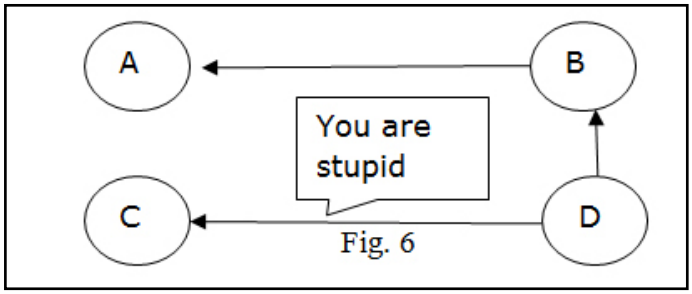
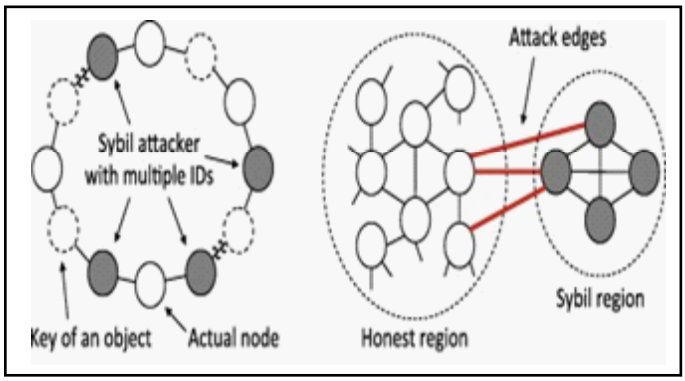



Fig. 6

The aim of Timing attack is to increase the delay between the nodes. This type of attacks is very dangerous because fraction of second is very crucial for life safety application. Application attack includes those attacks which create the problem in the service provided in VANET. Last type of attack is network attack which create problem in the whole network. All the vulnerable attack like Sybil attack, denial of service or node impersonation comes under network attack.
There are many types of attacks [3][10] possible in the VANET which are given below:-

### 1. Sybil attack

In this attack attacker creates multiple ids of same node and send false information to the neighbor nodes. Since other nodes receives message from different ids so they think neighbor node is genuine. Scenario of this attack [4] is given in fig.3 -




### 2. Spamming

In this attack attacker send the spam information for consuming the bandwidth and increasing the delay. It can be any node between source and destination.

### 3. Black hole attack

In this attack all the traffic goes to that node which are not exist. It is also responsible for the data loss.

### 4. Denial of Service (DoS) Attack

The main objective of this attack is to engage the resources and prevent the authenticated node to access the resources. If the resources will be busy then delay will be more which is very critical because the speed of vehicles on highway is very fast which can lead the safety violation.

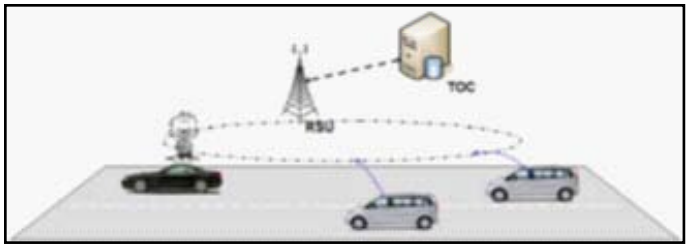



Fig. 4. Jam the channel between vehicle-to-infrastructure [7]

### 5. ID Disclosure

In this type of attack, attackers want to access the Id of the target node by which attacker can access the privacy of the authenticated node.

### 6. Man in the middle attack(MiMA)

As clear from the name, that the middle node create the problem. In this attack message is altered by the intermediate nodes. It is clear that it violate the property of integrity.

### 7. Replay attack

In this attack, attacker resends the previous information which is already sent for taking the advantage.

### 8. GPS Spoofing

In this attack node gives the false location to the neighbor.

### 9. Tunneling attack
In this attack nodes uses the same network in which they exists. They create a private network (tunnel) to connect with distant node which acts as a neighbor node.

## IV. Security Requirement
According to [1][10] there is some security requirement in VANET which are given below:-

### 1. Authentication
The entire node in the network must be authenticated for avoiding different types of attack. If any misbehave is done by any node then we can easily find that which node is responsible for it. It can be achieved by digital signature. Authentication include following attacks-
- Sybil attack
- GPS spoofing
- Position faking
- Tunneling
- Masquerading

### 2. Availability
To reduce the time delay resources must be available for the VANET. If bandwidth consumption is less then availability will be high. It includes the following attacks-
- Denial of service
- Jamming
- Malware
- Spamming
- Black hole attack

### 3. Integrity
Assurance of integrity means secure communication. Real information must not be changed during the communication. It covers these attacks-
- Alteration
- Replay
- Masquerading

### 4. Privacy
Main aim of security is privacy. Privacy of any node in the VANET should not be disclosed. For example node should not know the current location of the node. It covers these attacks-
- Id disclosure
- Location tracing

### 5. Non repudiation
In this attack node deny that they have not sent the message. We have to protect these activities. It includes the attack-
- Loss of event

## V. Related work and solutions
Following solution are given for the above problem and attacks-
Sybil attacks solution is given by Rahbari and Jamali [5]. In this approach cryptography is used. Public key, private key and hashing are the basics of this scheme. It is assume that before the message transmission each vehicles accept an authentication key for signing the message and at the receiver end authentication is checked by the signature verification. Delay in this approach does not depend upon the no. of nodes but it depends upon the no. of message transmission between the intermediate nodes. There is one problem associated with this approach that we can not get the location of the malicious node.
In [7] solution of DoS attack is proposed. It uses the different channel allocation scheme to avoid the DoS problem. It simply categorize the safety and non-safety channel which is given fig. 5

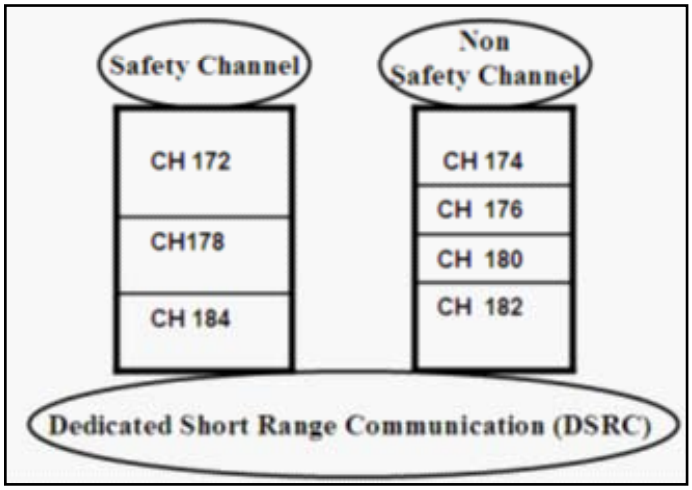


Fig. 5 : Safety and non-safety channel

Let us assume that attackers jams the channel CH172 then information pass through the remaining safety channels in this way we can avoid the DoS attack.
In [8] it is given that how to resolve the problem of replay attack. Since the replay attack uses the old information so if we add the time stamp then we can easily avoid this problem. This method can disclose that when the previous message was sent.
A. Hamieh, J. Ben-othman, and L. Mokdad et al.[9] proposed a solution for the jamming attacks in the VANET. This solution is based on the linear regression.
In [11] author try to solve the problem of wormhole attack by the digital signature technique. This is two step methods, verification done in first step while analysis is done in second step.

## VI. Summary
Up to this we discuss about the VAANET its characteristics, routing and different security issues and attacks related with the VANET. We also discussed related works. Now we try to summarize all the work mentioned above.
In this part we try to categorize the attacks means which attack cover which types of security issue. Here we are considering issues like integrity, availability and confidentiality etc. Table 1 shows the categorization of attacks.

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

Table : 1

| | Integrity | Authentication | Communication type | Non-Repudiation | Availability | Confidentiality | Solution techniques |
|---|---|---|---|---|---|---|---|
| Sybil Attack | | ✓ | V2V V2R SU | | ✓ | ✓ | Group signature and encryption decryption, digital signature |
| Jamming | | | V2V | | ✓ | | Group signature, linear regression |
| MiMa | ✓ | | V2V | ✓ | | ✓ | Encryption decryption and digital signature |
| Replay | ✓ | | V2V | | | | digital signature |
| ID Disclosure | | ✓ | NO IDEA | | | ✓ | Encryption decryption |
| DoS | | | NO IDEA | | ✓ | | Group signature |
| Black hole | | | V2V | | ✓ | | Group signature |

## VII. Conclusion

Thus, we are seeing that there are different techniques to achieve security. We will have to apply many techniques to cover all the security issues which increase the time delay. There is a requirement of more efficient algorithms and techniques to achieve the security.

## Reference


[1]. *G.Samara, Wafaa A.H. Al-Salihy, R.Sures "Security Analysis of Vehicular Adhoc Network", 2010 Second International Conference on Network Applications, Protocols and Services.*

[2]. *M.K. Nasir, A.S.M. Delowar Hossain, Md. Sazzad Hossain, Md. Mosaddik Hasan, Md. Belayet Ali " Security Challenges And Implementation Mechanism For Vehicular Ad Hoc Network", International Journal Of Scientific & Technology Research Volume 2, Issue 4, April 2013*

[3]. *Vinh Hoa LA, Ana Cavalli, "Security Attacks And Solutions in Vehicular Adhoc Networks: A Survey" International Journal on AdHoc Networking Systems (IJANS) Vol. 4, No. 2, April 2014*

[4]. *A. Rawat, S. Sharma, R. Sushil, "VANET: Security Attacks And Its Possible Solutions" , Journal of Information and Operations Management ISSN: 0976–7754 & E-ISSN: 0976–7762 , Volume 3, Issue 1, 2012, pp-301-304*

[5]. *M. Rahbari and Mhd. Ali Jabreil Jamali "Efficient Detection of Sybil Attack Based On Cryptography in VANET", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011*

[6] *I.A. Sumra, I. Ahmad, H. Hasbullah, J. Ab Manan, "Classes of attacks in VANET", in Tenth International Conference on Wireless and Optical Communications Networks (WOCN), pp 1 - 5, 2013.*

[7]. *H. Hasbullah, I. A. Soomro, J.A. Manan, "Denial of Service (DOS) Attack and Its Possible Solutions in VANET", World Academy of Science, Engineering and Technology Vol:4 2010-05-25*

[8]. *S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, A. Hassan, "Vehicular ad hoc networks (VANETs): status, results, and challenges", Telecommun. Syst. 50 (4) (2012) 217–241.*

[9]. *A. Hamieh, J. Ben-othman, and L. Mokdad, "Detection of radio interference attacks in VANET," 2009 IEEE Global Telecommunications Conference,doi:10.1109/ GLOCOM.2009.5425381.*

[10]. *M.N. Mejri, J. Ben-Othman, Mohd. Hamdi "Survey on VANET security challenges and possible cryptographic solutions", www.elsevier.com/locate/vehcom*

[11]. *Anil Kumar Fatehpuria, SandeepRaghuwanshi "An Efficient Wormhole Prevention in MANETS through digital signatures " International journal of Emerging Technology And Advance Engineering (IJETAE) Vol 3 Issue march 2013*