Application areas, Security Issues, Attacks and layer wise solutions of Vehicular Ad Hoc Networks (VANET).

[1]Manasija Bhattacharya, [2]Moumita Mantri , [3]Madhumita Maity

[1,2,3]HALDIA INSTITUTE OF TECHNOLOGY

DEPARTMENT OF INFORMATION TECHNOLOGY

ABSTRACT

Vehicular Ad hoc Networks (VANETs) are the emerging research area to provide safety and reliability not only to the drivers as well as passengers. It becomes the vital support for intelligent transport system. A lot of research works have been proposed and implemented towards it but security issues in VANET is not yet fully implemented. In this article, we have discussed about the VANET, WAVE architecture, challenges, attacks and layer wise possible solution for those problem.

KEYWORDS : *VANET, VANET WAVE architecture, VANET scenario, ARAN, SEAD, SMT, ARIDANE, S-AODV,OSPF*

---

1. Introduction:

One promising application of mobile ad hoc networks is the development of vehicular ad hoc networks (VANET).A MANET is a self forming network, which can function without the need of any centralized control. Each node in an ad hoc network acts as both a data terminal and a router. Another benefit of ad-hoc networks is they can be quickly deployed with no administrator involvement. The administration of a large scale vehicular network would be a difficult task. These reasons contribute to the ad hoc networks being applied to vehicular environments.Traffic fatalities are one of the leading causes of death in the around the world.

The aim of theproject is to enable the driver of a vehicle to receive information about their surrounding environment.

In the future vehicular ad hoc networks will assist the drivers of vehicles and help to create safer roads by reducing the number of automobile accidents. One possible way is to provide the traffic information to the vehicles so that they can use them to analyze the traffic environment. It can be achieved by exchanging the information of traffic environment among vehicles.

2. VANET APPLICATIONS

A classification of applications is also done by as Car to Car Traffic applications, Car to Infrastructure applications, Car to Home applications and Routing based applications**.** Based on the type of communication either V2I or V2V, we are arranging the applications of VANETs into following classes:

2.1 Safety Applications

Safety applications include monitoring of the surrounding road, approaching vehicles, surface of the road, road curves etc. The Road safety applications can be classified as:

1) Co-operative Message Transfer: Slow/Stopped Vehicle will exchange messages and co-operate to help other vehicles. Emergency electronic brake-light is used to avoid potential accidents. This can play an important role in solving the problems such as traffic jams, avoid congestions and in emergency alerts such as accidents, lane changing warning, intersection decision support, cooperative driving (e.g. collision warning, lane merging, etc. [16,17]).

2) Post Crash Notification: In post-crash notification, a vehicle involved in an accident would broadcast warning messages about its position to trailing vehicles so that it can take decision with time in hand as well as pass information to the highway patrol for support

3) Collision Warning: Alerts two drivers potentially under crash route so that they can mend their ways [13].

4) Road Hazard Control Notification: Cars notifying other cars about road having landslide or information regarding road feature notification due to road curve, sudden downhill etc.

2.2 Commercial Applications

The general aim of these applications is to improve passenger comfort and traffic efficiency. The Commercial applications can be classified as:

1) Remote Vehicle Personalization/ Diagnostics: It helps in downloading of personalized vehicle settings or uploading of vehicle diagnostics from/to infrastructure.

2) Internet Access: Future vehicles will be equipped with the capability so that the passages on the vehicles can connect to the Internet.

3) Digital map downloading: Map of regions can be downloaded by the drivers as per the requirement before traveling to a new area for travel guidance. Also, Content Map Database Download acts as a portal for getting valuable information from mobile hot spots or home stations.

4) Real Time Video Relay: On-demand movie experience will not be confined to the constraints of the home and the driver can ask for real time video relay of his favorite movies.

5) Value-added advertisement: This is especially for the service providers, who want to attract customers to their stores. Announcements like petrol pumps, highways restaurants to announce their services to the drivers within communication range. This application can be available even in the absence of the Internet.

6) Searching Roadside Locations and vehicle's Direction: For unknown passenger help to find the shopping center, hotels, gas stations, etc., in the nearby area along the road. GPS, sensors and database from the nearest roadside base station are capable of calculating information

2.3 Convenience Applications

Convenience application mainly deals in traffic management with a goal to enhance traffic efficiency by boosting the degree of convenience for drivers. The Convenience applications can be classified as:

1) Route Diversions: Congested Road Notification (CRN) detects and notifies about road congestions which can be used for route and journey planning.

2) Electronic Toll Collection: The toll collection [15] is yet another application for vehicle toll collection at the toll booths without stopping the vehicles. TOLL application is beneficial not only to drivers but also to toll operators.

3) Parking Availability: Parking Availability Notification (PAN) helps to find the availability of space in parking lot in a certain geographical area.

5) Vision Enhancement: drivers are given a clear view of vehicles and obstacles in heavy fog conditions and can learn about the existence of vehicles hidden by obstacles, buildings, and by other vehicles.

4) Driver Assistance: It anticipates the upcoming topography of the road, which is expected to optimize fuel usage by adjusting the cruising speed before starting a descent or an ascent. Secondly, the driver is also assisted [14].

2.4 Productive Applications

Productive application is additional with the above mentioned applications. The Productive applications can be classified as:

1) Time Utilization: If a traveler downloads his email, he can transform jam traffic into a productive task and read on-board system and read it himself if traffic stuck. One can browse the Internet when someone is waiting in car for a relative or friend.

2) Fuel Saving: When the TOLL system application for vehicle collects toll at the toll booths without stopping the vehicles, the fuel around 3% is saved, which is consumed when a vehicles as an average waits normally for 2-5 minutes.

3. Characteristics of VANET

The characteristics of a vehicular ad hoc network are unique compared to other mobile ad hoc networks. The distinguishing properties of a VANET offer opportunities to increase

- **High Mobility:** The nodes in VANETs usually are moving at high speed. This makes harder to predict a node's position and making protection of node privacy [18]. The node motion is constrained by the road topology and layout

- **High Dynamic topology:** In VANETs nodes move with high speed in respect to each other, which results in a very high rate of topology changes.

- **Anonymous Naming:** Most applications in VANETs require identification of the vehicles in a certain region, instead of the specific vehicles. So, anonymous naming system should be followed to protect the privacy of the driver.

- **Unbounded network size:** VANET can be implemented for one city, several cities or for countries. VANETs could involve the vehicles in one city, several cities, or even a country. So the VANETs network should not be dependent on the number of the nodes. This means that network size in VANET is geographically unbounded.

- **Frequent exchange of information:** The ad hoc nature of VANET motivates the nodes to gather information from the other vehicles and road side units. Hence the information exchange among node becomes frequent.

- **Time Critical:** The information in VANET must be delivered to the nodes with in time limit so that a decision can be made by the node and perform action accordingly.

- **No power constraints:** The power in VANET is not a critical challenge as in MANETs, because vehicles have the ability to provide continuous power to the OBU via the long life battery

- **High computational ability:** VANET is designed for the wireless environment where nodes are connected and exchange their information via wireless. In VANET vehicles are nodes & they can be equipped with a sufficient number of sensors and computational resources; such as processors, a large memory capacity, advanced antenna technology and global position system (GPS). These resources increase the

computational capacity of the node, which help obtaining reliable wireless communication and acquiring accurate information regarding its current position, speed and direction

4. VANET Scenario:

1. Special kinds of MANETs, supporting both safety and non-safety applications.
2. Single, short-range dedicated technology (802.11p draft) in basic systems
3. Additional technologies (especially 802.11) in extended systems
4. Peculiarities: a) High mobility b) High number of nodes c) Costs restrictions to allow for high deploy-ability.
5. Internet-based applications a)Beneficial for safety purposes

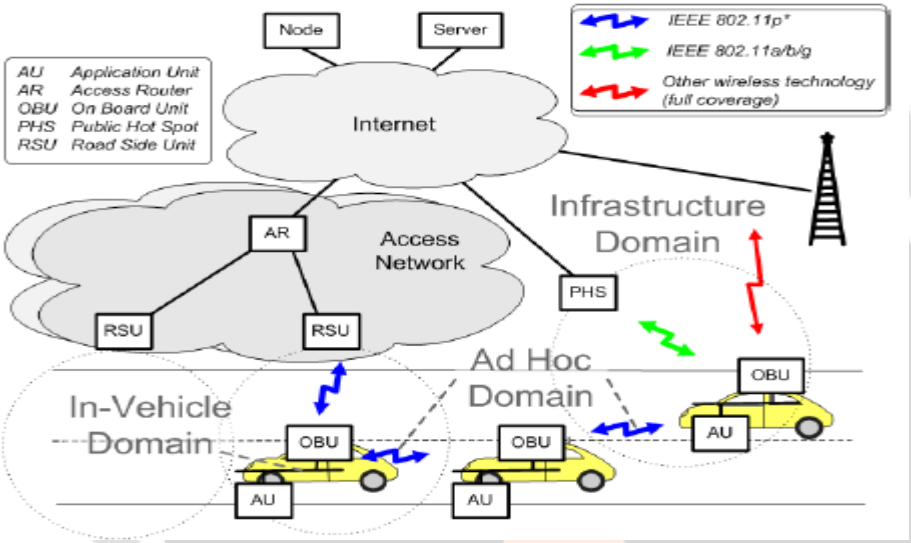

Figure 1: VANET scenario [2]

The aim towards VANET is to provide road safety information among the Nodes (moving vehicles) hence the frequent exchange of such type of data on the network clearly signifies the role of the security. In this work we are concentrated on security challenges and major attacks on VANET and the existing solution for problems.

To establish a VANET, IEEE has defined the standard 802.11p or 802.16 (WiMax). A Dedicated
Short Range Communication (DSRC) is proposed which is operating on 5.9GHz band and uses 802.11 access methods. It is standardized as 802.11p which provides short range communication with low latency.

IEEE introduced a complete protocol stack of 1609 protocol family and named it 'WAVE' (wireless access in vehicular environment) [3]

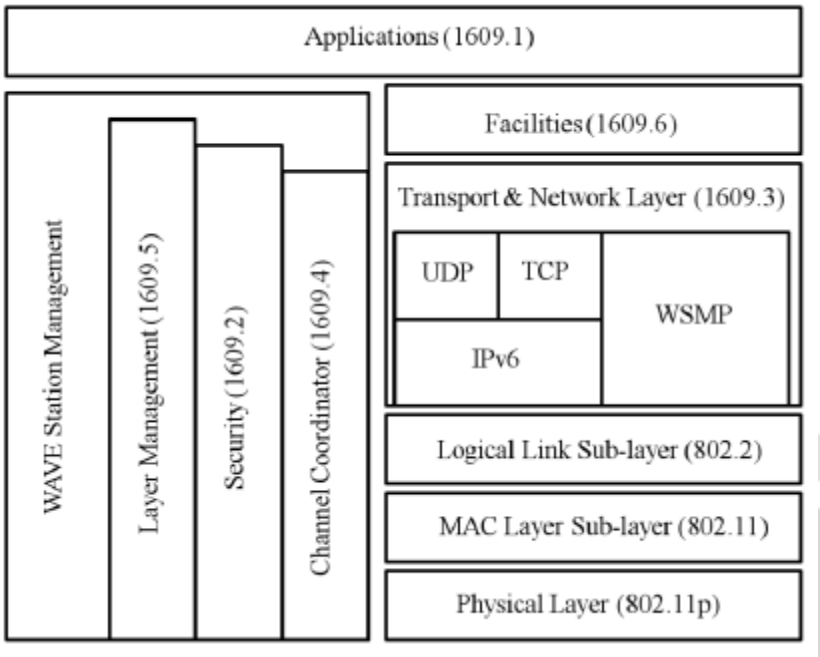

Figure 2:-WAVE architecture

5. Communication types in VANET:

Vehicle-to-Infrastructure (Infrastructure available)
Vehicle-to-Vehicle (Infrastructure available or not)

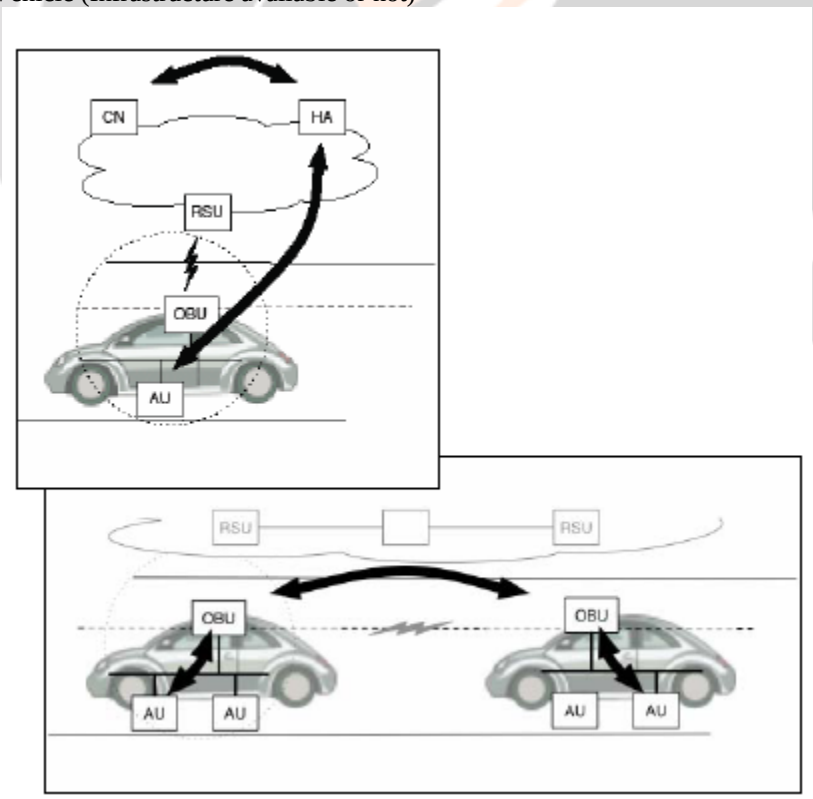

Figure3: VANET connectivity diagram (RSU:-Road side unit, HA: - Home agent, OBU: - On board unit, AU:-Application Unit)[2]

6. Challenges Creating Ad Hoc Networks and VANET

- Topology of the network changes rapidly and Vehicles have a high degree of mobility. (As the vehicles moves from one point to other duration of a connection last very less, thus we need to disseminate information very fast to individual vehicles)[1,4,5]
- Wireless communication is unreliable. The error rate in wireless network is much higher than on the Ethernet.
- ***Network Scalability:*** The scale of this network in the world approximately exceeding the 750 million nodes [6], and this number is growing, another problem arise when we must know that there is no a global authority govern the standards for this network [7], [8], [9], for example: the standards for DSRC in North America is deferent from the DSRC standards in Europe, the standards for the GM Vehicles is deferent from the BMW one.
- ***Bootstrap****:* At this moment only few number of cars will be have the equipment required for the DSRC radios, so if we make a communication we have to assume that there is a limited number of cars that will receive the communication, in the future we must concentrate on getting the number higher, to get a financial benefit that will courage the commercial firms to invest in this technology [8].
- ***Security:*** Security for this application must be imposed otherwise system can crash.

7. SECURITY ISSUES, and attacks in VANET

Security issues are derived from challenges from ad-hoc network. VANET security must to satisfy the following needs:-

- **Message Authentication and Integrity:** Authentication ensures that the message is generated by the authenticated user. In VANET two or more vehicle can communicate with each other hence authentication is necessary more over message should be protected from any alternation..
- **Message Non-Repudiation:** once a node send a message it can't deny about this.
- **Access Control:** control over a line must be ensured.
- **Message Confidentiality:** unauthorized access must be prevented.
- **Privacy and Anonymity**: Conditional privacy should be achieved within the sense that the user connected info, as well as the driver's name, the license plate, speed, position, and traveling routes at the side of their relationships, has got to be protected; whereas the authorities ought to be ready to reveal the identities of message senders within the case of a dispute like a crime/car accident scene investigation, which may be accustomed hunt for witnesses.
- **Liability Identification:** Users of vehicles are legally responsible for their deliberate or accidental actions that disrupt the operation of other nodes, or the transportation system. Several attacks are known which will be classified depending on the layer the attacker uses. At the physical layer and data link layers and network layer the attacker will disturb the system either by jamming or overloading the channel with messages. Flooding false messages or rebroadcasting a recent message is also an attainable attack.
- **Jamming:** The jammer intentionally generates interfering transmissions that prevent communication within their reception range. In the VANET scenario, an attacker can relatively easily partition the network, without compromising cryptographic mechanisms and with limited transmission power.

8. ATTACKS IN VANET:

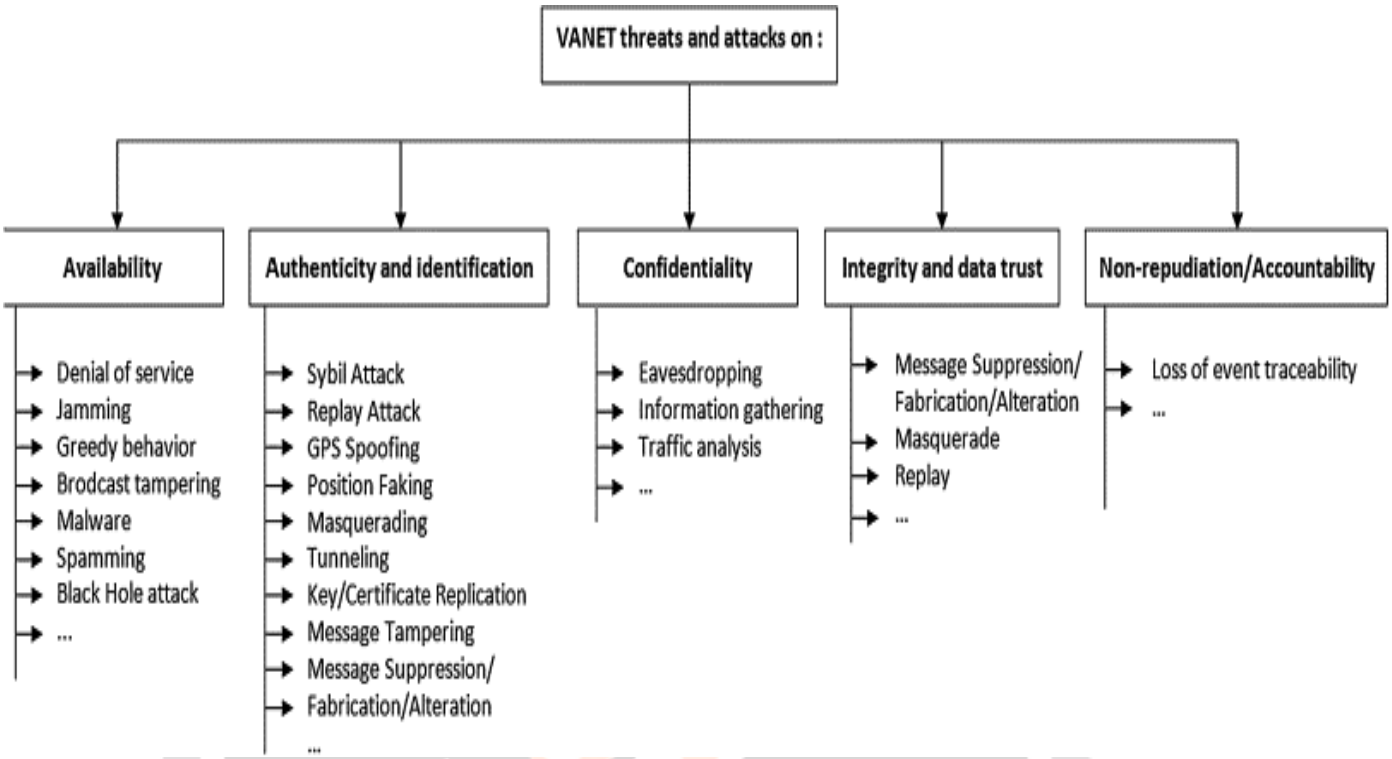

Figure 4

In VANET, there are some problematic issues most of which are flied around security issues such as data integrity, privacy, and confidentiality. Moreover, there are some issues which can influence the efficiency of VANET such as unpredictable temporary situations (e.g. creating traffic jam because of an accident). The security of VANETs is one of the most critical issues because their information transmission is propagated in open access environments.
Due to the nature of open wireless medium used in VANET, there are a different type number of possible attacks by that the VANET is exposed to. Some of the attacks are mentioned below.

To secure the VANET, first we have to discover who are the attacker, their nature, and capacity to damage the system.

Sybil Attack*:* In this type of attack, an attacker use different identities at the same time.

Node Impersonation: Impersonation is an endeavor by a node to send a changed version of a message received from the $64000 mastermind for the incorrect purpose and claim the message has come back from the mastermind. To beat this downside, a novel symbol is appointed to every vehicle node in VANET, which can be wont to verify the $64000 message mastermind. Police might use it to spot the motive force because it is related to driver's identity [11, 12] It's necessary to guard this symbol in order that it cannot be misused by the assaulter.
ID Disclosure: Generally a driver is itself owner of the vehicles hence getting owner's identity can put the privacy at risk.

Location Tracking*:* The location of a given moment or the path followed along a period of time can be used to trace the vehicle and get information of driver.

Session hijacking: Most authentication process is done at the start of the session. Hence it is easy to hijack the session after connection establishment. In this attack attackers take control of session between nodes.

Denial of service (DOS) attack: DoS attacks are most prominent attack in this category. In this attack

attacker prevents the legitimate user to use the service from the victim node. DoS attacks can be carried out in many ways [1,10].

a) Jamming: In this technique the attacker senses the physical channel and gets the information about the frequency at which the receiver receives the signal. Then he transmits the signal on the channel so that channel is jam.

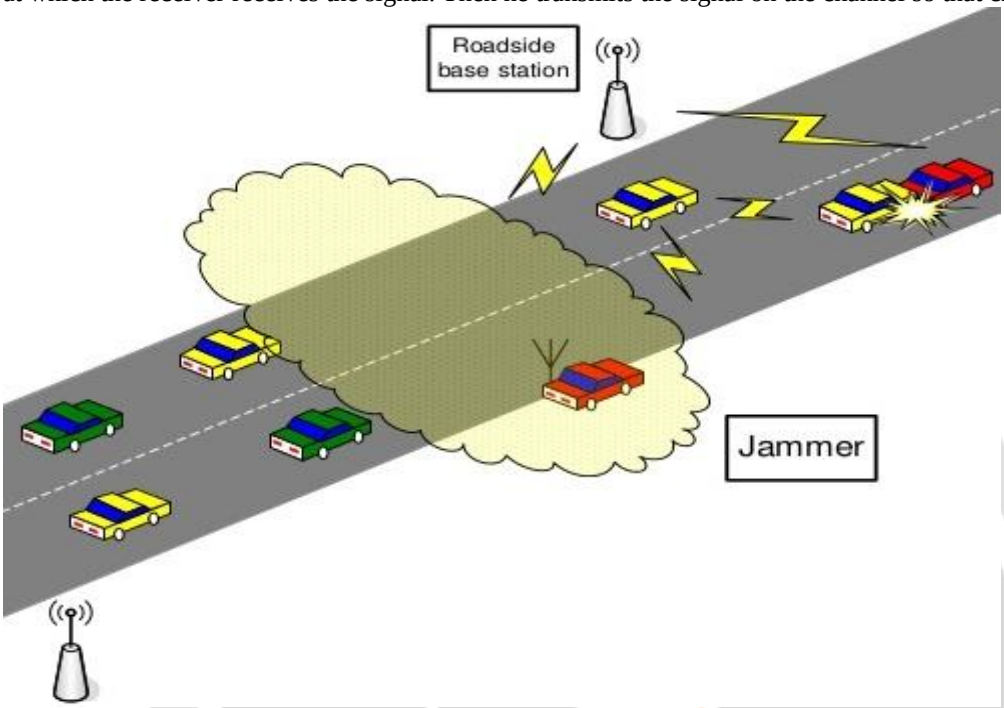

Figure 4: Jamming

b) SYN Flooding: In this mechanism large no of SYN request is sent to the victim node, spoofing the sender address. The victim node send back the SYN-ACK to the spoofed address but victim node does not get any ACK packet in return. This result too half opens connection to handle by a victim node's buffer. As a consequence the legitimate request is discarded.

c) Distributed DoS attack*:* This is another form Dos attack. In this attack, multiple attackers attack the victim node and prevents legitimate user from accessing the service.

Black Hole Attack: This is one type of routing attack. In this all the traffic of the network gets redirected towards a specific node which is actually doesn't exist which results in data lost. The attacker firstly attracts the nodes to transmit the packet through itself. After attracting the node, when the packet is forwarded through this node, it silently drops the packet.

9. Possible SOLUTION FOR ATTACKS

Defense against Attack [19, 23]:

Attack	**Targeted Layer in the protocol Stack**	**Proposed Solution**
Warm hole Attack	Physical and MAC	FHSS, DSSS
Black hole Attack	Network	Packets Leashes
Resource Consumption	Network	SEAD[19]
Information Disclosure	Network	SMT[19]

Location Disclosure	Network	SRP[19], NDM[19]
Network	Network	SRP[19], SEAD[19]
Repudiation	Application	ARAN[19]
DOS	Multi-Layer	SEAD[19],ARIDANE[19]
Impersonation	Multi-Layer	ARAN[19]

Security Features in Some of the Routings Protocols in Ad Hoc Networks [20, 21, 22]

Protocols	***Security Positives***	***Security Negatives***
SRP	Fabricated, compromised or replay route replies rejected; No online CA; guaranteed acquisition of correct topological information in a timely manner; No complete knowledge of keys By all nodes	Security association as a requirement; possible attack when nodes collude during the two phase of a single route discovery; each SRP query can only discover routes should be set up to ensure robustness
SAR	Can be easily incorporated on different routing protocols; Defines different trust levels	Requirement for different keys for different level of trust (large number of keys); dynamic key
SEAD	Implements one-way hash chain which is a cheaper solution; uses Access node authentication; overcomes the DOS attacks	Sensitive to wormhole attacks
ARAN	Uses cryptographic certificates and robust against modifications, fabrication and Impersonation	Requires preliminary certification process; costly protocol due to asymmetric cryptography, not immune to wormhole attacks
ARIDANE	Uses symmetric cryptography and is based on authentication (Shared key, MAC and authentic route discovery chain); guarantees that the target node of a route discovery authenticates the source	Needs mechanism to bootstrap authentication keys; only the enhanced version protects against a wormhole attack
S-AODV	Public key cryptography used	High overhead; possible route Discovery corruption; compromise of IP portion
Sec-AODV	Uses SUCV, provides on-demand trust establishment	Sensitive to DOS attacks
SMT	Guarantees integrity, replay protection and origin authentication; interoperability with accepted procedures such as Source routing; symmetric key cryptography used	Limited protection against compromised topological information
OSPF	Flooding the information least dependency; hierarchy routing and information hiding; two authentication methods; a simple password scheme and a cryptographic message digest	Age field not protected by digital signature; internal routers can generate incorrect routing information; public key cryptography very expensive and will slow performance of the router

10. CONCLUSION:

In this paper, Security is the most important feature in VANET. In this article we study VANET applications, characteristics, implementation architecture and scenario, challenges to create VANET, security issues, attacks and possible solution for those attacks. Here we mainly concentrated about security issues, attacks and layer wise proposed solution for that problem. Through this study of different aspects of VANET we can conclude that there is wide scope of research is still required in the area of security issues and solutions. We hope that the article presented in this paper to be useful and helpful to students and researchers in the field of VANET.

References:

1. Ram Shringar Raw, Manish Kumar, Nanhay Singh ,"SECURITY CHALLENGES, ISSUES AND THEIR SOLUTIONS FOR VANET" International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.5, September 2013
2. C2C-C Requirements for Usage of NEMO in VANETsC2C, empowered by NEC
3. Sajjad Akbar, Mohammad, Asim Rasheed, Amir Qayyum "VANET Architectures and Protocol Stacks: A Survey" Center of Research in Networks and Telecom (CoReNeT), Mohammad Ali Jinnah University (MAJU) Islamabad, Pakistan
4. Hannes Hartenstein et al., "A tutorial survey on vehicular Ad Hoc Networks" , IEEE Communication Magazine, June 2008, pp. 164-171
5. B. Parno and A. Perrig, "Challenges in Securing Vehicular Networks", Proc. of HotNets-IV, 2005.
6. M Raya, D Jungels, P Papadimitratos, I Aad, JPHubaux,"Certificate Revocation in Vehicular Networks " ,Laboratory for computer Communications and Applications (LCA)School of Computer and Communication Sciences ,EPFL,Switzerland, 2006 .
7. M Raya, P Papadimitratos, JP Hubaux, "Securing VehicularCommunications", IEEE Wireless Communications, Vol 13, October 2006 .
8. B. Parno and A. Perrig, "Challenges in Securing Vehicular Networks", Proc. of HotNets-IV, 2005.
9. I Aad, JP Hubaux, EW Knightly, "Impact of Denial of Service Attacks on Ad Hoc Networks", Networking, IEEE/ACM Transactions on Volume 16, August, 2008.
10. Murthy, C. S. R.,Manoj, B. S.: Ad Hoc Wireless Networks: Architectures and Protocols. PEARSON,ISBN 81-317-0688-5, (2011).
11. P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, M. Zhendong, F. Kargl, A. Kung, J-P Hubaux, "Secure vehicular communication system : Design and Architecture Communications" IEEE Magazine, November 2008,vol. 46, pp. 100-109.
12. Ayonija Pathre1 ,Chetan Agrawal2, Anurag Jain3 "IDENTIFICATION OF MALICIOUS VEHICLE IN VANET ENVIRONMENT FROM DDOS ATTACK" Ayonija Pathreet al, Journal of Global Research in Computer Science, Volume 4 No 6, 30-34
13. X. Yang, L. Liu and N. Vaidya, "A vehicle-to-vehicle communication protocol for cooperative collision warn-ing," 1st Annual International conference on Mobile and Ubiquitous Systems: Networking & Services, MOBIQ-UITOUS'04, pp. 114-123.
14. www.scania.com
15. T. ElBatt, S. Goel, G. Holland, H. Krishnan, J. Parikh, "Cooperative Collision Warning Using Dedicated Short Range Wireless Communications", 3rd ACM International Workshop on VANETs, Los Angeles, California, USA, 2006.
16. Qian, Yi, Nader Moayeri. "DESIGN SECURE AND APPLICATION-ORIENTED VANET", National Institute of Standards and Technology. Apr 2009: http://w3.antd.nist.gov/pubs/Yi-Paper7.pdf.
17. H. Wu, R. Fujimoto, R. Guensler, M. Hunter, "MDDV: A Mobility-Centric Data Dissemination Algorithm for Vehicular Networks," in 1st ACM workshop on vehicular ad hoc networks, Oct. 2004, pp. 47 – 56.
18. Hannes Hartenstein et al., "A tutorial survey on vehicular Ad Hoc Networks" , IEEE Communication Magazine, June 2008, pp. 164-171
19. C.Siva Ram Murthy & B.S Manoj, "Mobile Ad Hoc Networks- Architectures & Protocols", Pearson Education, New Delhi, 2004.

20. Aura T. and maki, S, "Towards a Survivable Security Architecture for Ad-hoc Network", Springer-Vverlag, 2001.
21. Hoeper , K. and Gong, "Models of Authentication in Ad Hoc Networks and their Related Network Proreties" CACR2004-20003.
22. Ajay Jangra1, Nitin Goel2, Priyanka3& Komal Bhatia4 "Security Aspects in Mobile Ad Hoc Networks (MANETs): A Big Picture" International Journal of Electronics Engineering, 2(1), 2010, pp. 189-196
23. Danesh, A. and Inkpen K., "Collaborating on Ad Hoc Wireless Network", at www.parc.xerox.com/sl/projects/ ubicomp-workshop/positionpapers/danessh.pdf.