GLANCE over VANET, ATTACKS over VANET and their IDS approaches

Ravi Patel[1], Khushbu Shah[2]
[1]*Department of computer engineering, LJ Institute of Technology, India*
[2]*Assistant Professor, Department of computer engineering, LJ Institute of Technology, India*
[1]*E-mail: ravicpatel@live.com*

***Abstract*- Vehicular Ad-hoc Network (VANET), it is a subclass of Mobile Ad-hoc Networks (MANETs). There are no fix infrastructure of network but relies on vehicles to deliver network functionality. Here, vehicles are equipped with an On-Board Unit (OBU) that makes vehicles to send and receive information from other vehicle or workstation in the Network. Yet, due to high mobility, driver behavior, mobility constraints, VANETS characteristics differs. Security is also critical issue in VANET as attackers can attack in different ways on this life saving vehicular network. Attackers try to compromise node and then provide false information that may mislead the vehicles and causes major accident. Here in this paper we will come across VANET, various classes of attacks in VANET and different Intrusion Detection System (IDS) approaches.**

***Index Terms*- Vehicular Ad-hoc Network (VANET), Intrusion Detection System, Attacks, Ad-hoc Networks, Survey.**

I. INTRODUCTION

In past few years, cyber-crime rate has increased its bound. They are now focusing on making VANET system vulnerable. Today major concern is to provide safety of users and safe their lives in road accidents. Safety and non-safety potential applications of VANET are to ensure the safety of human life on the road. Security is main concern because when data is compromised, the whole system suffers. Security measures must be taken to avoid malicious attacks on the system.

Now, Attackers try to compromise the system according to their need. The do various kind of attacks, some of them are explained in this paper. And research division has also tried to strengthen the system for intruders.

II. VANET

In the recent years, the multi-path ad hoc networks have become an attractive topic. VANET, a subclass of MANETs potential application fields have emerged. Basically, in VANET architecture there is no fix network structure. It has highly dynamic network. In VANET basically, there are two types of communication possible, Vehicle to Infrastructure (V2I) and Vehicle to Vehicle (V2V). Each vehicle are installed with On Board Unit (OBU), which is helpful to communicate with other OBUs and Road Side Units (RSU), which are installed on Road Side to help in communication.[1]

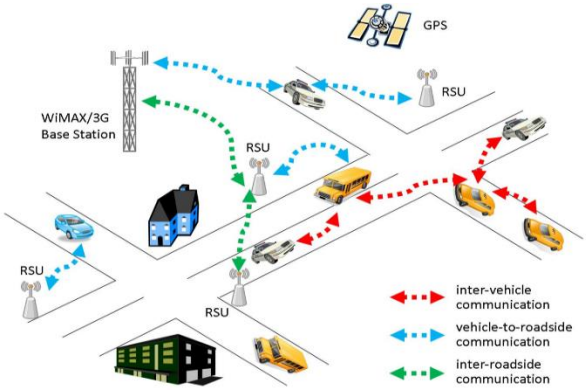

Figure 1: VANET working [12]

III. ATTACKS OVER VANET

Here in this section we will go through some of the attacks carried by intruders on VANET.

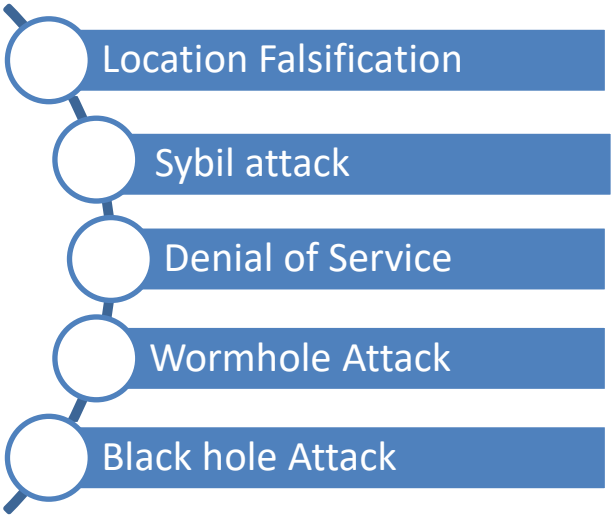

Figure 2: Various attacks on VANET.

Here we have basically two way of data forwarding

1. Predefined Route
2. Dynamic Route

Generally in Predefined Routing below attacks may happen [2]

I. Location Falsification
II. Black hole Attack
III. Sybil Attack

And in Dynamic routing below attacks may happen [2]

i. Black hole Attack
ii. Sybil Attack
iii. Wormhole Attack
iv. Denial of Service

3.1 Location Falsification

A node claims a faked position to pretend to be optimal than other candidates [2]

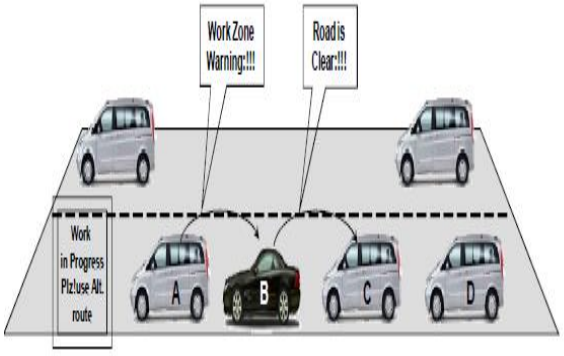

Figure 3: Location falsification [3]

3.2 Sybil Attack

In Sybil attack, the attacker sends multiple messages to other vehicles and each message contains different fabricated source identity. It provides illusion to other vehicle by sending some wrong messages like traffic jam message. The objective is to enforce other vehicles on the road to leave the road for the benefits of the attacker. [3]

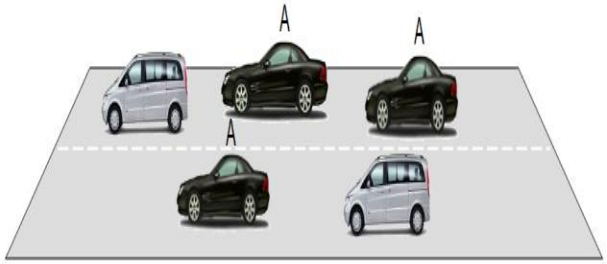

Figure 4: Sybil Attack [3]

3.3 Denial of Service (DOS)

Denial of Service (DOS) is one of the most serious level attacks in vehicular network. In DOS attack, attacker jams the main communication medium and network is no more available to legitimate users. The main aim of DOS attacker is to prevent the authentic users to access the network services. [3]

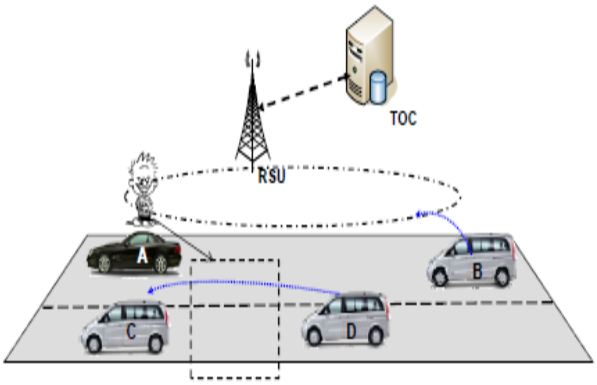

Figure 5: Denial of service [3]

3.4 Wormhole Attack

The wormhole attack consists in tunneling packets between two remote nodes thus disseminating erroneous (but correctly signed) messages in the destination area. [4]

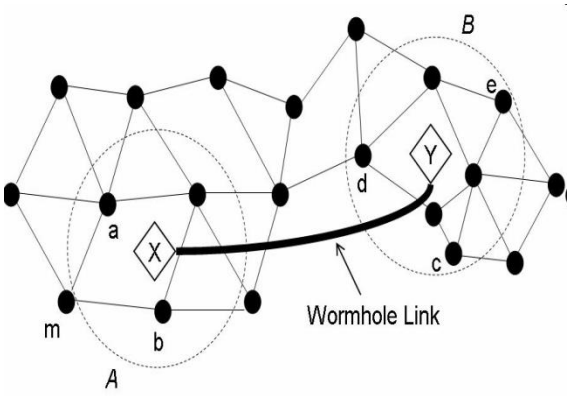

Figure 6: Wormhole Attack[4]

3.5 Blackhole Attack

In Blackhole Attack, a node has the ability to lure all data around an area through itself, then simply discards all data or only forwards portion of received data [2] so it is also called selective forwarding.

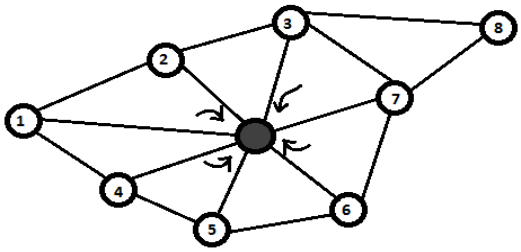

Figure 7: Blackhole Attack

IV. INTRUSION DETECTION SYSTEM (IDS)

In general "Intrusion" means "action that compromise integrity, confidentiality or availability of resource". "Intrusion Detection" means defensive strategy to protect the network systems against the Intrusion detected to minimize the damage or to launch counter blitzes.

An IDS is composed of three phases [5]: first is data collection then it is followed by analysis phase then finally phase that tries to counter the effect of intrusion.

IDS can be classified according to detection techniques used into three categories [5]:

- Signature based system [6]: Here, system cross verifies system behavior with the malicious behavior of node from the database
- Anomaly detection system [7]: Here, system monitors behavior of system from normal behavior and detects if behavior seems to be deviates from standard pre-established behavior of system it triggers alarm.
- Specification based system [8]: Set of protocols or condition of programs is pre-defined. Attack is alarmed if protocol or program condition is breached.

IDS architectures are classified into three categories [5]:

- Stand-alone IDS [5]: Here in this architecture, every node individually collect data from other node and detects intrusion using local resources. Each node has no information of the potion of other nodes and no alerts cross the network.
- Co-operative and distributed IDS [9]: Here, cooperation is established among the neighbors to detect intrusion. Neighboring nodes exchange alerts and regarding information.
- Hierarchical IDS [10,11]: To overcome the lack of cooperation among different IDS approaches for ad hoc networks, this approached was proposed as here, network is divided into set of groups (clusters) contain leader in each cluster. Hierarchical IDS try to reduce cooperation among the nodes by dividing network into clusters. Here, leader is administrator and monitors and generate alerts if intrusion detected.

V. CONCLUSION

This paper presents the VANET infrastructure, attacks over VANET and to overcome the attacks various IDS approaches. VANETs are extremely vulnerable to attacks, as they share the wireless medium and the absence of traditional security architecture. So proper security approaches should be introduced in this life saving system. However Intrusion Detection System with their approaches improves the network security in VANET. But there is necessary in improving the IDS further for increasing efficiency. As some times false positive ratio of detection is more in current IDS system.

REFERENCES

Papers

[1] Yousefi, Saleh, Mahmoud Siadat Mousavi, and Mahmood Fathy. *"Vehicular ad hoc networks (VANETs): challenges and perspectives."* ITS Telecommunications Proceedings, 2006 6th International Conference on. IEEE, 2006.

[2] Xu, Yufei, X. Wu, and D. Teng. *"Secure Routing in WSNs and VANETs: Security Improved Geographic Routing and Implicit Geographic Routing."*
[3] Sumra, Irshad Ahmed, et al. *"Classes of Attacks in VANET."* Electronics, Communications and Photonics Conference (SIECPC), 2011 Saudi International. IEEE, 2011.
[4] Singh, Er Jagjit. *"Wormhole Attack Detection by using Intrusion Detection System in VANET."*
[5] Erritali, Mohammed, and Bouabid El Ouahidi. *"A review and classification of various VANET Intrusion Detection Systems."* Security Days (JNS3), 2013 National. IEEE, 2013.
[6] Anjum, Farooq, Dhanant Subhadrabandhu, and Saswati Sarkar. *"Signature based intrusion detection for wireless ad-hoc networks: A comparative study of various routing protocols."* Vehicular Technology Conference, 2003. VTC 2003-Fall. 2003 IEEE 58th. Vol. 3. IEEE, 2003.
[7] P. C. Kishore Raja, DLSuganthi.M, R.Sunder, *"WIRELESS NODE BEHAVIOR BASED INTRUSION DETECTION USING GENETIC ALGORITHM"*, Ubiquitous Computing and Communication Journal, 2006.
[8] Ping, Yi, et al. *"Distributed intrusion detection for mobile ad hoc networks."* Journal of systems engineering and electronics 19.4 (2008): 851-859.
[9] Zhang, Yongguang, and Wenke Lee. *"Intrusion detection in wireless ad-hoc networks."* Proceedings of the 6th annual international conference on Mobile computing and networking. ACM, 2000.
[10] Anantvalee, Tiranuch, and Jie Wu. *"A survey on intrusion detection in mobile ad hoc networks."* Wireless Network Security. Springer US, 2007. 159-180.
[11] Sen, Jaydip. *"An intrusion detection architecture for clustered wireless ad hoc networks."* Computational Intelligence, Communication Systems and Networks (CICSyN), 2010 Second International Conference on. IEEE, 2010.

Web Sites
[12]
http://www.cs.nthu.edu.tw/~jungchuk/research.html