UACEE International Journal of Advances in Computer Networks and its Security – IJCNS
Volume 3 : Issue 2 [ISSN 2250 – 3757]
Publication Date : 05 June 2013

An Approach towards the Analysis of Routing protocols under attack in VANET

Anup P. Dhamgaye, Nekita Chavhan

***Abstract*—Advancement in wireless technology helps to resolve day to day problems in human life and also serves as a life saving application in numerous situations. Its intervention in vehicle offers a priceless opportunity to improve assistance in traffic systems by providing information regarding current traffic environment. VANET (Vehicular Adhoc Network) a, smart network formed by the vehicles provides vehicle to vehicle and vehicle to road side communication which leads to a plethora of automotive applications. For better communication the network should ensure safety and security from different kind of vulnerabilities. Due to open access environment it is vulnerable to different attacks and threats. This paper provides a brief idea about VANET environment, routing protocols and routing attack in VANET eventually a framework which helps in performance assessment of routing protocols under attack is also proposed.**

***Keywords*—VANET, Routing Protocols, AODV, OLSR, MPR, routing attacks**

I. Introduction

In the recent year for improving efficiency and safety of future transportation system, vehicular network has gained a lot of popularity among the industry and academic research community. Pervasive and cheap wireless technology provides several innovative vehicular applications. These applications can be categorized into three major types: road safety, transportation efficiency, and infotainment applications [1]. The main goal of road safety applications is to decrease the number of road accidents. If drivers were provided with warning message, rings etc continuously in every time interval [2] then accident on the road can be avoided. The transportation efficiency can be increases by providing more information to the drivers regarding to choose better routes to reach the destinations. This type of route selection will help in reducing road congestion and maintain a smooth flow of traffic, and increases the capacity of the road. In addition to these applications, infotainment is most widely used and important application in VANETs. It provides additional information or entertainment, which includes advertisement or multimedia, streaming to the passengers. These three types of applications of VANET technology are not completely orthogonal: for example, reducing the number of accidents can in turn reduce the number of traffic jams, which could reduce the level of environmental impact. Vehicular ad hoc networks (VANETs) offer [3] direct communication between vehicles to vehicle and vehicle to roadside units (RSUs). Vehicles can send and receive hazard warnings or information related to the current traffic situation with minimal latency. Vanet has lots of advantage but due to lack of infrastructure and its dynamic nature, it suffers from number of various problems that needs to be resolved before it gets implemented in practical application. These problems are generally associated with security and privacy of VANETs.

The rest of this paper is organized as follows. Section II describes the VANET environment. In section III, the widely used routing protocols are introduced. Section IV provides the detail idea about routing attacks. Proposed Framework is discussed in section V followed by conclusion and future work in section VI.

Anup P. Dhamgaye
Wireless Communication and Computing, Department of CSE,
GHRCE, Nagpur.
India
dhamgaye_100@yahoo.co.in

Nekita Chavhan
Department of CSE,
GHRCE, Nagpur.
India
niki.chavhan@gmail.com

II. Vanet Environment

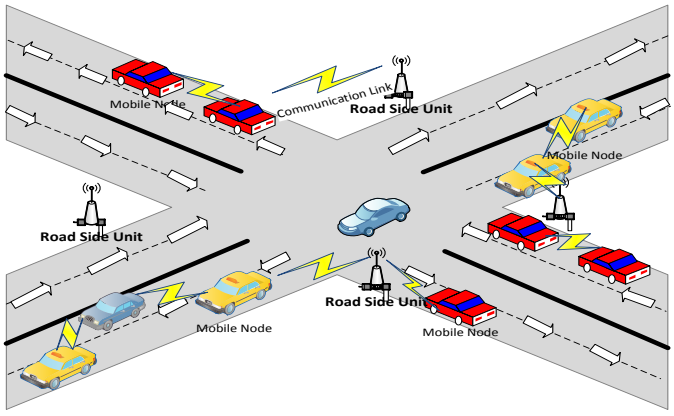

Figure 1. Routing in VANET Environment

VANET generally comprise of sensors [4] and On Board Units (OBU) installed in the car as well as Road Side Units (RSU). Sensors placed in the mobile vehicle collects the data from mobile vehicle comes under the transmission range of

mobile vehicle, this collected data by the sensors can be displayed with in vehicle using OBU(On board unit) to the driver of the receiving vehicle. Depending on the nature and importance of data it sent to the RSU or even broadcasted to the other vehicles. The RSU(Road side unit) is a static unit which is placed beside the road which is used to distributes received data from the mobile vehicle ,traffic control centers, etc and transmits this information to another vehicles and also provides commercial services such as parking space booking, Internet access and gas payment. VANET uses some routing protocols for communication purpose. Routing protocols are used for V2V or V2I communication. In VANET the routing protocols are divided into different types depending upon their application. Figure 1. shows a routing in VANET environment.

III. Routing Protocols in VANET

Routing Protocols in VANET is broadly classified [5] into five types are as follows: topology based, position based, cluster based, broadcast based and geocast based. This classification is based on area/application where they are most suitable. Figure 2. gives the classification routing protocol in VANET.

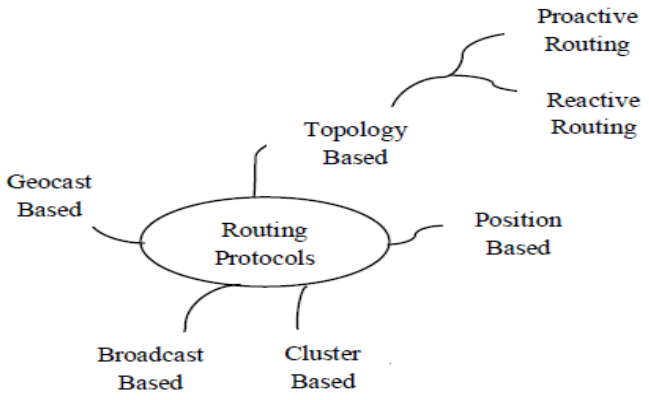

Figure 2. Routing Protocols in VANET

In VANET environment topology based routing protocol is most widely used to find the route for data transfer between the vehicles.

A. *Topology based routing protocol*

The topology based routing protocol [6] is further classified into two categories as follows: Proactive (Table Driven) and Reactive protocols (On-Demand). These routing protocols concerned about the link information during the data packet transmission.

- ***Proactive Routing***

It maintained the next forwarding hop in background regardless of communication requests. In order to maintain the paths or the link states between any pair of nodes it broadcast or flood control packets among the nodes. After that a table is constructed within node such that each entry in the table indicates the next hop node toward a certain destination. Since it maintained the table there is no route discovery required also it provides low latency for real time applications. The various types of proactive routing protocols are: FSR, DSDV, OLSR, CGSR, WRP, and TBRPF.

- ***Reactive Routing***

It usually constructs the route whenever necessary for a node to communicate. Therefore it maintains the routes that are currently in use, and hence reducing the load of the network. Reactive routings typically have a route discovery phase where query packets are flooded into the network in search of a path. The phase completes when a route is found. The various types of reactive routing protocols are AODV, PGB, DSR, TORA, and JARR.

IV. Routing Attacks in VANET

In VANET the malicious node can interrupt the communication by sending fake messages several times using fake routing information and it also advertise fake links for disturbing routing operations in the communication network. In the following subsection we will discuss briefly about current routing attacks.

A. *Flooding attack*

In this type of attack the attacker consume nodes resources such as battery power, and also uses the bandwidth which ultimately reduces the network performance. For example, in AODV protocol, an attacker node [7, 8] sends large number of RREQs in a very short span of time to that node which is not present in the network and all nodes accept the packet but no one will responds to it which causes exhaustive consumption of nodes resources and this leads to the denial of service (DOS).In this way this attack leads to the unwanted disruption of communication and also consumes precious resources.

B. *Blackhole attack*

In black hole attack [9], a malicious node pretends to have optimum route for the destination node, and indicates that packet should route through this node. When the malicious node will receive the data packet, it can misuse or discard the traffic. This attack may be caused either RREQ or RREP packets in AODV routing protocol by simply modifying the sequencing number.

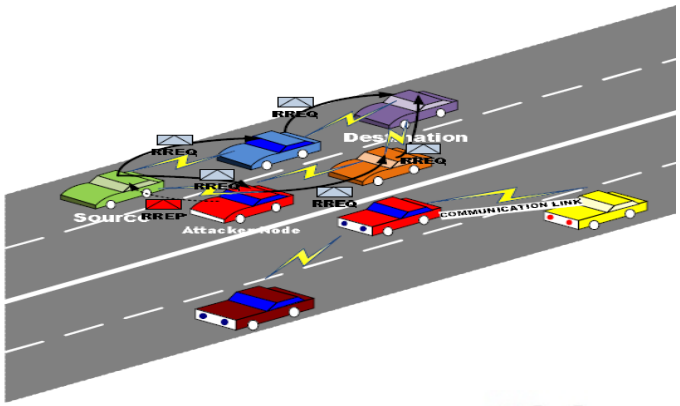

Figure 3. Blackhole attack on AODV

This attack can be more harmful in dynamic network like VANET where the traffic information and other necessary information will not be received by the driver. This attack is shown in figure 3.

C. *Link spoofing attack*

In this attack [7] an attacker disrupts the routing operation by advertising the fake link information with the non-neighbors node. This attack is more clearly explained by considering OLSR routing protocol. In this protocol an Attacker advertises a fake link with targets two-hop neighbors; due this a target node select an attacker node to be its MPR (Multipoint Relay) and an attacker node can easily manipulate data or routing traffic.

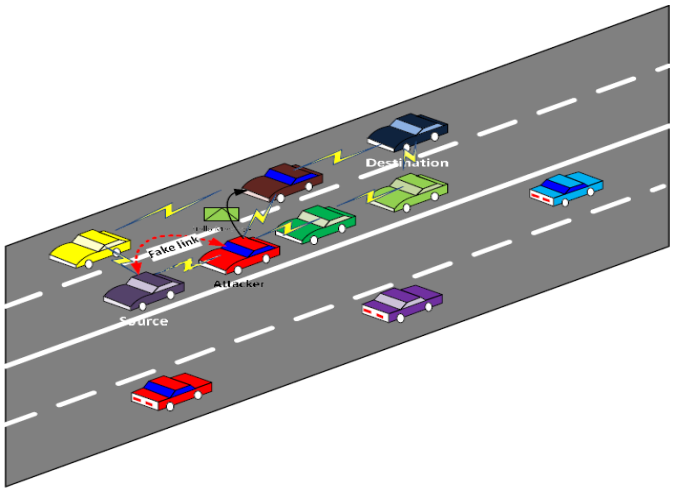

Figure 4. Link spoofing attack

This attack is also more vulnerable in VANET as it can modify or drop the lifesaving routing traffic. Figure 4. shows an example of the link spoofing attack in OLSR routing protocol.

D. *Wormhole attack*

The wormhole attack [10] is more severe attack in VANET environment.

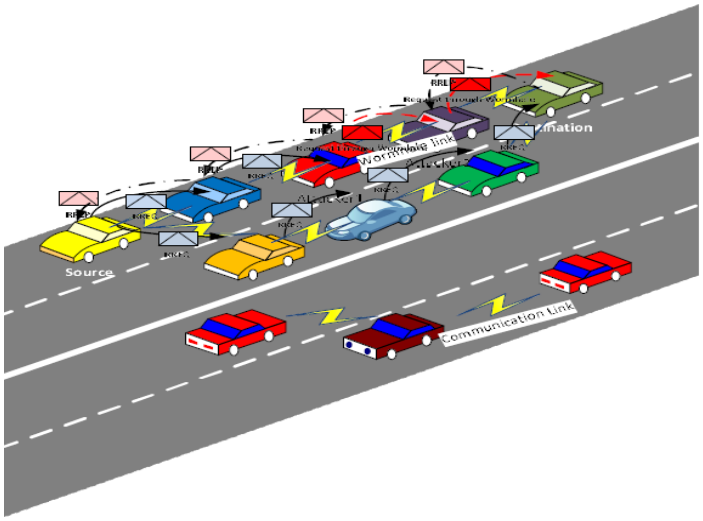

Figure 5: Wormhole attack on reactive routing

In this attack the attacker node record packets at one location and replay at another location, using private high speed network and hence a source to destination communication is proceed through this attacker nodes. Figure 5. shows an example of the wormhole attack on reactive routing protocol. This attack is more serious as it launches against any kind of communication that provide authenticity and confidentiality.

E. *Colluding misrelay attack*

In this attack multiple attackers [11] work in collusion whose intention is to modify or drop routing packets which leads in disruption of normal communication process. This attack is more difficult to detect. Figure 6. shows an example of colluding misrelay attack.

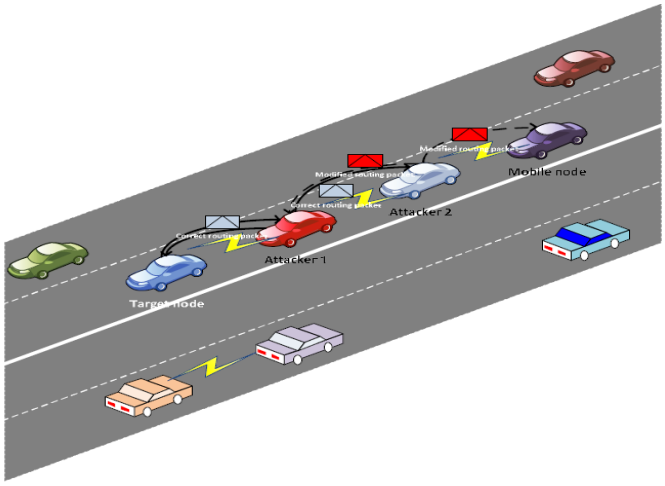

Figure 6. Colluding misrelay attack

V. Proposed Framework

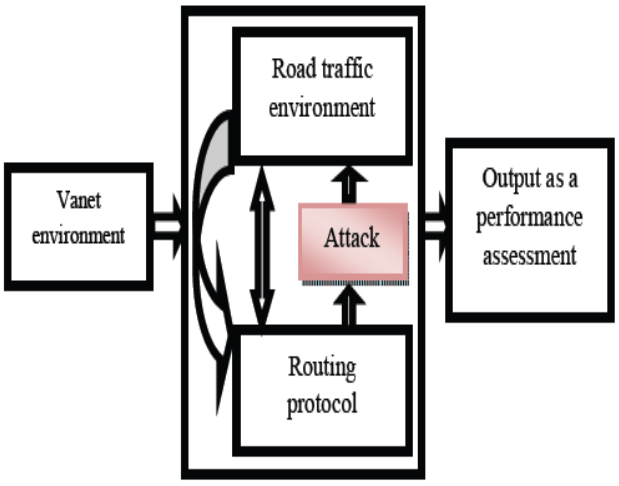

Figure 7: Proposed plan for performance assessment of routing protocols with and without attack

As we have discussed in earlier section the VANET environment, routing protocols used in VANET and the possible attacks in routing protocol. The performance of the network is depends upon the routing therefore the choice of

routing protocol should be design in such way that it should provide a efficient routing in any condition like under attack also. To analyze the performance of these routing protocols we are providing a proposed plan for it. Figure 7 shows framework of proposed plan. It consists of VANET environment, various possible attacks in routing and output unit. In this propose plan VANET environment is avail with any of the routing protocol which is suitable according to their application. Then, we will first analyze the network performance without attack by using some metric like network load, throughput and packet delay. Same metric will be used to analyze the performance of routing protocol under attack and then we compare the result using the obtained metrics to analyze which of these protocols are more vulnerable under any of the routing attack.

VI. Conclusion and future work

In this paper the various routing protocols and the possible routing attack that can hamper the network communication of VANET environment are discussed. The performance of routing protocol will vary with or without attack. To select a better routing protocol for communication an analysis must be done before implementing it in the vanet application. Hence to analyze the performance of routing protocol a framework is proposed in this paper. In future this framework will be implemented for analyzing the performance of various VANET routing protocol with or without attack.

References

[1] H. Hartenstein and K. P. Laberteaux, "A tutorial survey on vehicular ad hoc networks," IEEE Commun. Mag., vol. 46, no. 6, pp. 164–171, Jun. 2008.

[2] Y. Toor, P. Muhlethaler, and A. Laouiti, "Vehicle ad hoc networks: applications and related technical issues," IEEE Commun. Surveys & Tutorials, vol. 10, no. 3, pp. 74-88, 2008.

[3] Chandrasekaran, Gayathri. "VANETs: The Networking Platform for Future Vehicular Applications." Department of Computer Science, Rutgers University(2008).

[4] Abdalla, Ghassan MT, Mosa Ali Abu-Rgheff, and Sidi Mohammed Senouci. "Current trends in vehicular ad hoc networks." Ubiquitous Computing and Communication Journal (2007).

[5] Zeadally, Sherali, et al. "Vehicular ad hoc networks (VANETs): status, results, and challenges." Telecommunication Systems (2010): 1-25.

[6] Sharma, Yatendra Mohan, and Saurabh Mukherjee. "A Contemporary Proportional Exploration of Numerous Routing Protocol in VANET." International Journal of Computer Applications (0975–8887) Volume (2012).

[7] Ngadi, Md, Rasheed Hafeez Khokhar, and Satria Mandala. "A review current routing attacks in mobile ad-hoc networks." International Journal of Computer Science and Security 2.3 (2008): 18-29.

[8] Yi, Ping, et al. "Flooding attack and defence in ad hoc networks." Journal of Systems Engineering and Electronics 17.2 (2006): 410-416.

[9] Tseng, Fan-Hsun, Li-Der Chou, and Han-Chieh Chao. "A survey of black hole attacks in wireless mobile ad hoc networks." Human-centric Computing and Information Sciences 1.1 (2011): 1-16.

[10] Hu, Yih-Chun, Adrian Perrig, and David B. Johnson. "Wormhole attacks in wireless networks." Selected Areas in Communications, IEEE Journal on 24.2 (2006): 370-380.

[11] Kannhavong, Bounpadith, et al. "A survey of routing attacks in mobile ad hoc networks." Wireless Communications, IEEE 14 5 (2007): 85-91.

About Author (s):

Anup P. Dhamgaye received B.E. degree from Kavikulguru Institute of Technology and Science, Ramtek, Dist. Nagpur, State-Maharashtra. He is pursuing Master of Engineering (M.E.) in Wireless Communication and Computing from G. H. Raisoni College of Engineering, Nagpur, Maharashtra, India. His research area includes Wireless network security, Vehicular Adhoc Network.

Nekita Chavhan received Master of Engineering (M.E) in Wireless Communication and Computing from G. H. Raisoni College of Engineering Nagpur, Maharashtra India. She is working as Assistant Professor in G.H. Raisoni College of Engineering, Nagpur. Her research area includes Ad-hoc Wireless networks, Wireless sensor networks and Mobile Technology.