ijecs open access www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 6 June, 2014 Page No. 6767-6769

Brief overview of VANET routing protocols and their security attacks

S.I.S.Jaffarvalli, D.Ganesh'

M.Tech student

Computer science and engineering, Aits, Rajampet.

Abstract:

We know that opinion a VANET specialized form of MANET. As we know that a VANET stands for vehicular ADHOC network. a VANET uses every participating car into a wireless node or router ,allowing cars approximately 100 to 300 meters of each other to connect and to form a network with wide range. as car falls out of the signal range ,other cars can join in, connecting vehicles to one other so that a mobile internet is created. However in this research paper I concentrate on classification of VANETS and their security attacks.

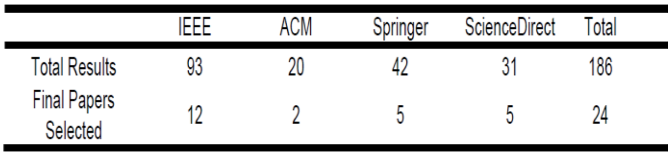
Keywords: MANET, VANET, DOS attack, V2V

1. Introduction:

Vehicular Ad hoc network (VANET) is a class of ad hoc network that consists of vehicles and Road Side Units (RSUs). VANET originally created to enhance safety on the road using cooperative collision warning via Vehicle-to-Vehicle (V2V) communication and Vehicle-to-Infrastructure (V2I). In V2V communication vehicles send and receive messages to and from one to another. These messages can be alert signals about road congestion, accidents ahead or information about traffic on a given route. V2I communications take place between nodes and road side infrastructure and involve finding nearest cheapest gas station, internet services, online toll payment, etc.

2. Security in VANET:

Security plays an essential role in VANET communication due to the fact that message has high level of importance in safety application. Before investigate the security models in VANET, we should identify the threats, challenges and requirements in security. Since wireless is open environment, there exist number of security threats and attacks which are quite non-trivial for VANETs. The safety threats by the attackers are major problems of VANET. The role of the attackers in vehicular network is very important, since they can establish the attacks of different type. Creation of the problems for other users of the network by changing the contents of messages is the aim of the attackers. Sumra et al. (2011) proposed an assortment of attacks in terms of type of attack, their level threat and priority of attack. They categorized them into five groups include: monitoring attack, social attack, timing attack, application attack and network attack. Moreover, Wei et al. (2012) categorized the attacks in VANET into Non-collusion Attack and Collusion Attacks. Also, Raya et al. (2006) categorized the vehicle communication vulnerabilities into six groups include: Jamming, forgery, Traffic Tampering, Impersonation, Privacy Violation and On-board Tampering. According to the special properties of VANET environment, there are various challenges in designing of security model. Razzaque, M., et al. (2013) introduced mobility, privacy, availability, low tolerance, key distribution and cooperation as security challenges in VANET. Furthermore, Papadimitratos et al. (2006) considered Network Volatility, Liability vs. Privacy, Delay-Sensitive



	IEEE	ACM	Springer	ScienceDirect	Total
Total Results	93	20	42	31	186
Final Papers Selected	12	2	5	5	24

3. Various attacks:

1) Denial of Service attack:

This attack happens when the attacker takes control of a vehicle’s resources or jams the communication channel used by the Vehicular Network, so it prevents critical information from arriving. It also increases the danger to the driver, if it has to depend on the application’s information. For instance, if a malicious wants to create a massive pile up on the highway, it can make an accident and use the DOS attack to prevent the warning from reaching to the approaching vehicles [1], [5].

2) Message Suppression Attack,

An attacker selectively dropping packets from then network, these packets may hold critical information for the receiver, the attacker suppress these packets and can use them again in other time[5]. The goal of such an attacker would be to prevent registration and insurance authorities from learning about collisions involving his vehicle and/or to avoid delivering collision reports to roadside access points For instance, an attacker may suppress a congestion warning, and use it in another time, so vehicles will not receive the warning and forced to wait in the traffic.

3) Fabrication Attack,

An attacker can make this attack by transmitting false information into the network, the information could be false or the transmitter could claim that it is somebody else. This attack includes fabricate messages, warnings, Certificates, identities [5].

4) Alteration Attack,

This attack happens when attacker alters an existing data, it includes delaying the transmission of the Information, replaying earlier transmission, or altering the actual entry of the data transmitted [5]. For instance, an attacker can alter a message telling other vehicles that the current road is clear while the

Road is congested.

5) Replay Attack,

This attack happens when an attacker replay the transmission of an earlier information to take advantage of the situation of the message at time of sending [5].

6) Sybil Attack

Sybil attack *depends on how cheaply identities can be generated, the degree to which the system accepts inputs from entities that do not have a chain of trust linking them to a trusted entity, and whether the system treats all entities identically.* For instance an attacker can pretend and act like a hundred vehicle to convince the other vehicles in the road that there is congestion, go to another rout, so the road will be clear.

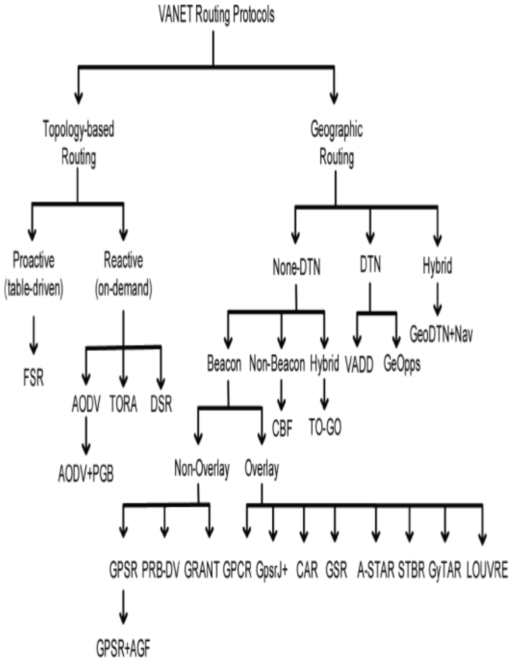
4. Classification of VANET routing protocols:

As shown in Figure 1, there are two categories of routing protocols: topology-based and geographic routing. Topology-based routing uses the information about links that exist in the network to perform packet forwarding. Geographic routing uses neighbouring location information to perform packet forwarding. Since link information changes in a regular basis, topology-based routing suffers from routing route breaks. Despite many surveys already published on routing protocols in MANETs (Mauve, 2001; Mehran, 2004 Giordano, 2003; Stojemnovic, 2004), a survey of newly developed routing protocols specific to VANETs has long been overdue. Li et al. (2007) have made an effort to introduce VANET routing protocols, yet there is still deficiency in a thorough and comprehensive treatment on this subject.

Figure1: Taxonomy of VANET routing protocols

5. VANET network architecture:

According to Figure 2, the architecture of VANETs falls within two categories: pure cellular/WLAN, pure ad hoc. In pure cellular/WLAN architecture, the network uses cellular gateways and WLAN access points to connect to the Internet and facilitate vehicular applications. Vehicles communicate with the Internet by driving by either a cellular tower or a wireless access point.



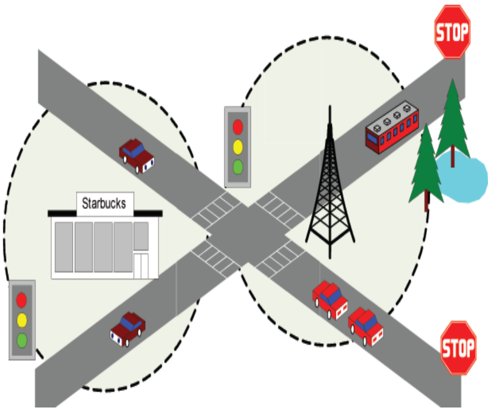
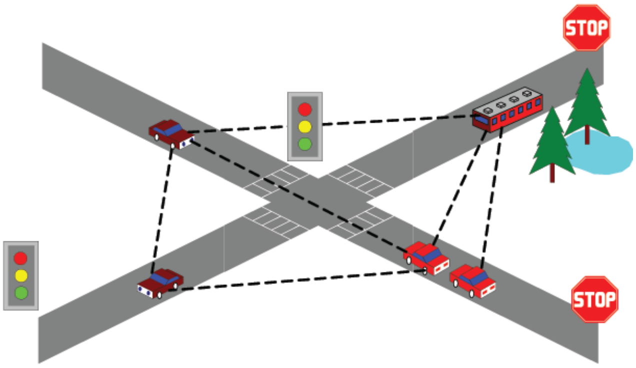


Figure2:

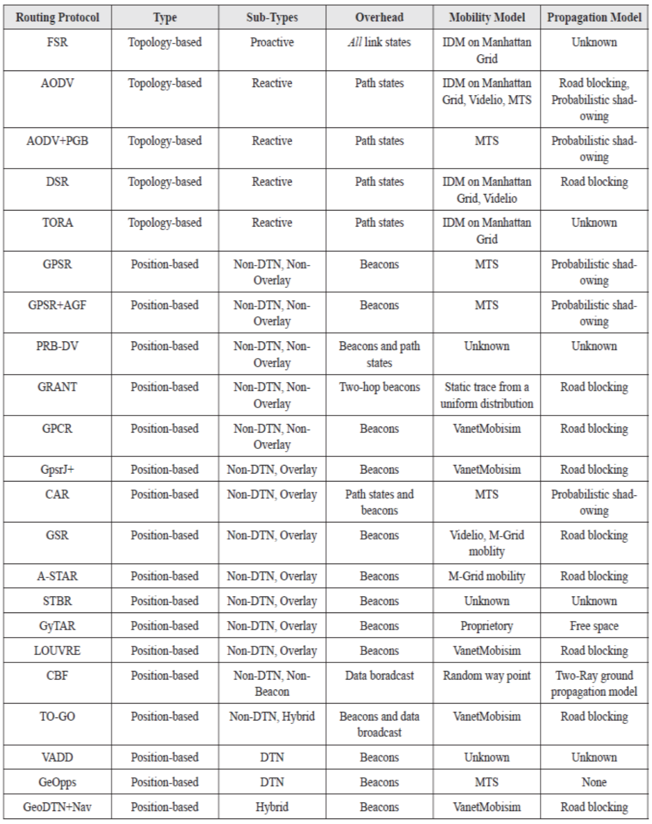
A) WLAN cellular



B) ADHOC

The infrastructure-less network architecture is in the pure ad hoc category where nodes perform vehicle-to-vehicle communication with each other. Similar to mobile ad hoc networks (MANETs), nodes in VANETs self-organize and self-manage information in a distributed fashion without a centralized authority or a server dictating the communication. In this type of network, nodes engage themselves as servers and/or clients, thereby exchanging and sharing information like peers. Moreover, nodes are mobile, thus making data transmission less reliable and suboptimal .Apart from these characteristics, VANETs possess a few distinguishing characteristics, presenting itself a particular challenging class of MANETs

The following figure shows the topology of various VANET protocols.



Routing Protocol	Type	Sub-Types	Overhead	Mobility Model	Propagation Model
FSR	Topology-based	Proactive	*All* link states	IDM on Manhattan Grid	Unknown
AODV	Topology-based	Reactive	Path states	IDM on Manhattan Grid, Videlio, MTS	Road blocking, Probabilistic shadowing
AODV+PGB	Topology-based	Reactive	Path states	MTS	Probabilistic shadowing
DSR	Topology-based	Reactive	Path states	IDM on Manhattan Grid, Videlio	Road blocking
TORA	Topology-based	Reactive	Path states	IDM on Manhattan Grid	Unknown
GPSR	Position-based	Non-DTN, Non-Overlay	Beacons	MTS	Probabilistic shadowing
GPSR+AGF	Position-based	Non-DTN, Non-Overlay	Beacons	MTS	Probabilistic shadowing
PRB-DV	Position-based	Non-DTN, Non-Overlay	Beacons and path states	Unknown	Unknown
GRANT	Position-based	Non-DTN, Non-Overlay	Two-hop beacons	Static trace from a uniform distribution	Road blocking
GPCR	Position-based	Non-DTN, Non-Overlay	Beacons	VanetMobisim	Road blocking
GpsrJ+	Position-based	Non-DTN, Overlay	Beacons	VanetMobisim	Road blocking
CAR	Position-based	Non-DTN, Overlay	Path states and beacons	MTS	Probabilistic shadowing
GSR	Position-based	Non-DTN, Overlay	Beacons	Videlio, M-Grid moblity	Road blocking
A-STAR	Position-based	Non-DTN, Overlay	Beacons	M-Grid mobility	Road blocking
STBR	Position-based	Non-DTN, Overlay	Beacons	Unknown	Unknown
GyTAR	Position-based	Non-DTN, Overlay	Beacons	Proprietory	Free space
LOUVRE	Position-based	Non-DTN, Overlay	Beacons	VanetMobisim	Road blocking
CBF	Position-based	Non-DTN, Non-Beacon	Data boradcast	Random way point	Two-Ray ground propagation model
TO-GO	Position-based	Non-DTN, Hybrid	Beacons and data broadcast	VanetMobisim	Road blocking
VADD	Position-based	DTN	Beacons	Unknown	Unknown
GeOpps	Position-based	DTN	Beacons	MTS	None
GeoDTN+Nav	Position-based	Hybrid	Beacons	VanetMobisim	Road blocking

Fig: 3 Topology of VANETS

Conclusion:

Vehicular Ad Hoc Networks is promising technology, which gives abundant chances for attackers, who will tryto challenge the network with their malicious attacks. In summary, the open issue in VANET routing is then whether there is any benchmark tool for evaluating these protocols. IP version 6has been proposed for use in vehicular networks. Cars should be able to change their IP addresses so that they are not traceable, however it is not clear how this will be illustrated. In future work I try to prove this statement.

References

[1] M Raya, P Papadimitratos, JP Hubaux, "Securing Vehicular Communications", IEEE Wireless Communications, Vol13, October 2006.

[2] H Fussler, S Schnaufer, M Transier , W Effelsberg ,"Vehicular Ad-Hoc Networks: From Vision to Reality and Back", Proc. Of IEEE Wireless on Demand Network Systems and Services, 2007.

[3] GMT Abdalla, SM Senouci "Current Trends in Vehicular Ad Hoc Networks", Proceedings of UBIROADS workshop, 2007.

[4] M Raya, D Jungels, P Papadimitratos, I Aad, JP Hubaux,"Certificate Revocation in Vehicular Networks " , Laboratory for computer Communications and Applications (LCA)
School of Computer and Communication Sciences ,EPFL, Switzerland, 2006.

[5] B. Parno and A. Perrig, "Challenges in Securing Vehicular Networks", Proc. of Hot Nets-IV, 2005.

[6] Cheng, P. C., Weng, J. T., Tung, L. C., Lee, K. C.,Gerla, M., & Härri, J. (2008). GeoDTN+NAV: A Hybrid Geographic and DTN Routing with Navigation Assistance in Urban Vehicular Networks. In Proceedings of the 1st International Symposiumon Vehicular Computing Systems (ISVCS'08), Dublin, Ireland. M.E.E. Najjar, P. Bonnifait, A road-matching method for precise vehicle localization using belief theory and kalman filtering, AutonomicRobots 19 (2) (2005) 173–191.