International Refereed Journal of Engineering and Science (IRJES)
ISSN (Online) 2319-183X, (Print) 2319-1821
Volume 1, Issue 3(November 2012), PP.09-12
www.irjes.com

An Advanced IDS Approach to Detect Wormhole Attack in VANET

Jagjit Singh, Neha Sharma
Dept. of Electronics & Communication, Amritsar College of Engg & Tech, Punjab, India

Abstract- *Vehicular Ad-hoc network is a particular type of wireless ad-hoc network formed with short range wireless communication devices each represents a vehicle on the road or static device. The problem in VANET due to lack of centralized infrastructure makes it vulnerable to various security attacks. One of such of them most dangerous attack is wormhole attack which mainly occurs least two or more malicious nodes. In this paper we discuses intrusion detection system approach to detect wormhole attack by evaluating decision packets at destination node.*

I Introduction

Communication between vehicles is an aspect highly studied during the past years. Vehicles are equipped with special devices which communicate with each others and with roadside devices. These devices uses short-range wireless connectivity and form a particular type of mobile ad-hoc network, named“Vehicular Ad-hoc Network” or, shortly, VANET. Such a network has several advantages because it provides access to information for users, but also disadvantages Moreover, as the autonomy of self-driving vehicles increases, it becomes more difficult for operators to monitor them closely, and this further exacerbates the difficulty of identifying anomalous states, in a timely manner. In this paper we mainly discuss about the various anomalies associated with in VANET and various type anomaly management systems and their architecture. VANET is basically a technology that uses moving vehicles as nodes to create a mobile network. VANET turns every participating vehicles into a wireless sensor nodes and which allowing vehicles to communicate with each other, create a network with wide range. As vehicle fall out of the signal range they drop out from the network. We mainly understand VANET by taking it subset of MANET. The main aim of VANET is providing safety to passengers. To this end a special electronic device will be placed inside each vehicle which will provide Ad-Hoc Network connectivity for the passengers. This network tends to operate without any infra-structure or legacy client and server communication. Each vehicle equipped with VANET device will be a node in the Ad-Hoc network and can receive and send others messages through the wireless network. Collision warning, road sign alarms and in-place traffic view will give the driver essential tools to decide the best path along the way.

II Vulnerabilities in VANET:

VANET poses some of the most challenging problems in wireless ad hoc and sensor network research. In addition, the issues on VANET security become more challenging due to the unique features of the network, such as high-speed mobility of network entity or vehicle, and extremely large amount of network entities. In particular, it is essential to make sure that “life-critical safety” information cannot be inserted or modified by an attacker; likewise, the system should be able to help establishing the liability of drivers; but at the same time, it should protect as far as possible the privacy of the drivers and passengers. It is obvious that any malicious behavior of users, such as a modification and replay attack with respect to the disseminated messages, could be fatal to other users. In the past few years, considerable effort has been spent in research on VANET networking protocols and applications.Summarizing from the recent researches,VANET security should satisfy the following requirements Message authentication and integrity, message non repudiation, entity authentication, access control, message confidentiality, availability, privacy and anonymity, and liability identification[1]
.

Message Authentication and Integrity: Message must be protected from any alteration and the receiver of a message must corroborate the sender of the message. But integrity does not necessarily imply identification of the sender of the message.

Message Non-Repudiation: The sender of a message cannot deny having sent a message
.

Entity Authentication: The receiver is not only ensured that the sender generated a message, but in addition has evidence of the liveness of the sender.

Access Control: Access to specific provided by the infrastructure nodes, or other nodes, is determined locally by policies. As part of access control, authorization establishes what each node is allowed to do in VANET.

Message Confidentiality: The content of a message is kept secret from those nodes that are not authorized to access it.[2]

Availability: The network and applications should remain operational even in the presence of faults or malicious conditions. This implies not only secure but also fault-tolerant designs, resilience to resource depletion attacks, as well as survivable protocols, which resume their normal operations after the removal of the faulty participants.

Privacy and Anonymity: Conditional privacy must be achieved in the sense that the user related information, including the driver's name, the license plate, speed, position, and traveling routes along with their relationships, has to be protected; while the authorities should be able to reveal the identities of message senders in the case of a dispute such as a crime/car accident scene investigation, which can be used to look for witnesses.[3]

III Attacks on VANET

There are various possible attacks associated with VANET but most commonly occurs tunnel attack and wormhole attack.

Tunnel attack: Since GPS signals disappear in tunnels, hacker may destroy this temporary loss of positioning information to inject false data once the vehicle leaves the tunnel and before it receives an orginal position update as figure below illustrates. The physical tunnel in this example can also be replaced by an area jammed by the attacker, which results in the same effects.

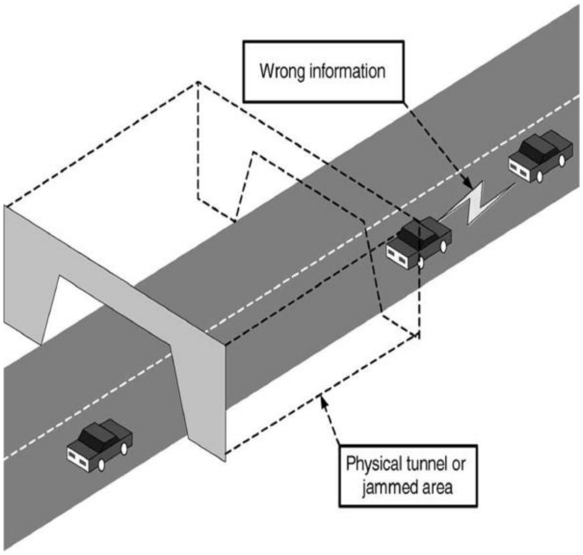
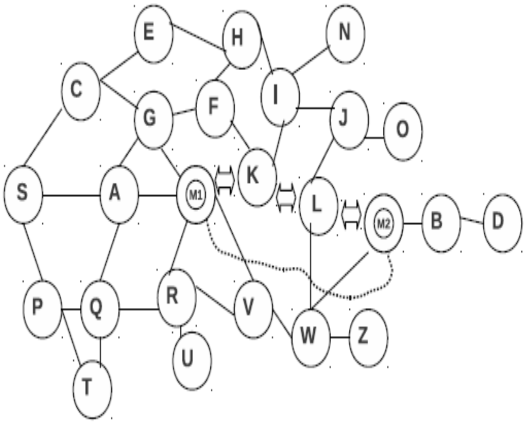


Figure tunnel attack

Wormhole attack: Different types of attacks are possible in case of VANET but the most dangerous is called wormhole attack. It is mostly occurs at least between two or more malicious nodes . In this kind of attack in VANET nodes create own private tunnel among nodes in which message packets comes from them will be move to other path of the malicious nodes by this tunnel and it will broadcast into the network. This will create short path network controlled by these malicious nodes.This attack heavily effected the network operation specially the network that uses the AODV or DSR types of protocols. In VANETs an attacker that controls at least two entities remote from each other and a high speed communication link between them can tunnel packets broadcasted in one location to another, thus disseminating erroneous (but correctly signed) messages in the destination area. [4] Wormhole can be formed using, first, *in-band channel* where malicious node m1 tunnels the received route request packet to another malicious node m2 using encapsulation even though there is one or more nodes between two malicious nodes, the nodes following m2 nodes believe that there is no node between m1 and m2. Second, *out-of-band channel* where two malicious nodes m1 and m2 employ an physical channel between them by either dedicated wired link or long range wireless link shown in Figure



Out of band channel, normal channel, in band channel, malicious nodes

Fig. wormhole attack

When malicious nodes form a wormhole they can reveal themselves or hide themselves in a routing path. The former is an *exposed* or *open* wormhole attack, while the latter is a *hidden* or *close* one. [5]

IV Intrusion detection system

An IDS is a device or software application that monitor network or system activities for malicious activities or policy violations and produce report to a management station. An IDS evaluates a suspected intrusion once it has taken place it also watches for attacks that originate from within system.[6] Vehicular networks are vulnerable to a large variety of attacks. To prevent a network, first and foremost important thing that is helpful is an Intrusion Detection System (IDS). The intrusion detection system of VANET needs to be different from that of the wired networks. Intrusion Detection System is like alarm system of our network that detect unauthorized attempts. The main purpose of Intrusion detection system is to alert network administrator about the possible attacks so that they can be detected in time and hence their effect can be reduced. An IDS differentiates the activities as attacks and normal activities based on their behaviour that is provided to it through certain guidelines. The accuracy of IDS is measured in terms of true positive, true negative, false positive, false negative [7]

V Simulation and results

The results from various simulations shown in the form of graphs.

Positive predictive value: It is actually ratio number of true positive to number of true positives plus number of false positives.

PPV = number of true positives / number of true positive + number of false positives

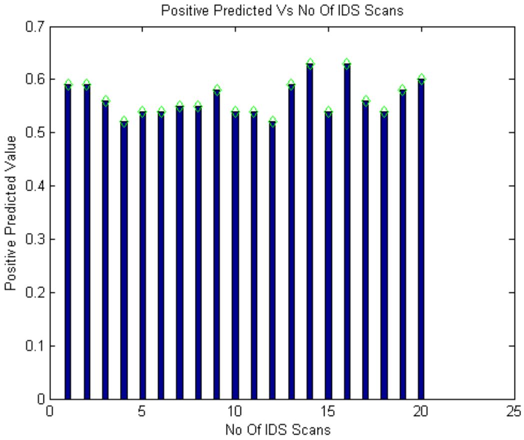


Fig. Positive predictive value

Negative Predictive Value: It is defined as the ratio number of true negatves to the number of true negatives plus number of false postives.

NPV = no. of true negatives / no.of true negatives+ no.of false negatives

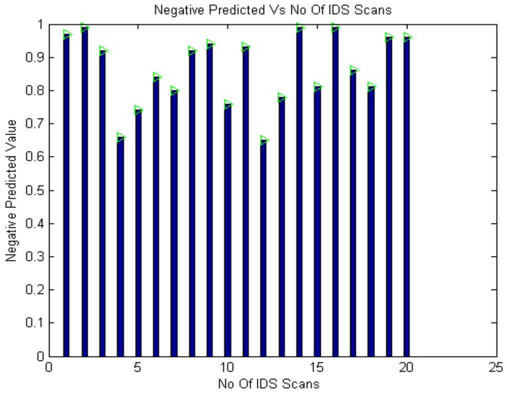


Fig. Negative predictive value

Specificity: Specificity is defined as the ratio of number of true negatives to number of true negatives plus number of false positives.

Specificity = no. of true negatives / no.of true negatives + no. of false positives.

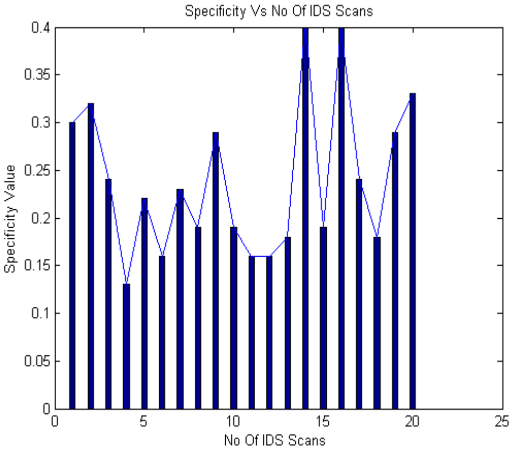


Fig Specificity

VI Conclusion

Safety is a primary concern to many road users. Securing VANET communication is a crucial and serious issue, since failure to do so will delay the deployment of technology on the road. The safety requirements can be powerfully supported by many safety applications, such as traffic report and accidents notifications. Wormhole is very severe attack in adhoc network and it is possible even if the attacker is not compromised ane types of any hosts. The wormhole attack can form a serious threat in wireless networks, especially in adhoc network. We present different methods like PPV, NPV, Specificity to detect these types of attacks.

References:

[1]. K. Amritahmasebi , S.R Jalalina " Vehicular Networks- Security, Vulnerabilities and countermeasures" Goteborg, Sweden ,June 2010.

[2] H. Mustafa, Y. Zhang, "Vehicular Networks, Techniques, Standards and Applications," Auerbach publications, 2009

[3] T. Leinmüller, E. Schoch, C. Maihöfer, "Security requirements and solution concepts in vehicular ad hoc networks," in Proceedings of the 4th Annual Conference on Wireless on Demand Network Systems and Services, 2007, pp. 84–91

[4] Seyed Mohammad Safi Ali Movaghar Misagh Mohammadizadeh. A Novel Approach for Avoiding Wormhole Attacks in VANET. (2009).

[5]. H. Kaur , S. Batish and A.Kakaria, An approach to detect the the wormhole attack in vehicular adhoc network in: International journal of smart sensors and adhoc networks,4,2012.

[6] Y. Zhang and W. Lee, "Intrusion detection in wireless ad-hoc networks,"in Proceedings of the 6th annual international conference on Mobile computing and networking. ACM Press, 2000, pp. 275–283.

[7] Y. Zhang, W. Lee, and Y.-A. Huang, "Intrusion detection techniques formobile wireless networks," Wirel. Netw., vol. 9, no. 5, pp. 545–556, 2003