ISSN:2229-6093

Ajay Wadekar et al , International Journal of Computer Technology & Applications,Vol 8(6),634-639

Improve the efficiency of Detection Technique of different types of attack In VANET:A review paper

Ajay Wadekar, Dr. Kamlesh Namdev (Associate professor),SIRT E ,Bhopal

Sagar Institute of research & technology- Excellence, Bhopal.

Abstract

Vehicular ad hoc network (VANET) has attracted the attention of many researchers in recent years. It enables value-added services such as road safety and managing traffic on the road. Security issues are the challenging problems in this network. Sybil attack is one of the serious security threats that attacker tries to forge some identities. One of the main purposes for creating invalid identities is disruption in voting based systems. In this paper we propose a secure protocol for solving two conflicting goals privacy and Sybil attack in vehicle to vehicle (V2V) communications in VANET. The proposed protocol is based on the Boneh-Shacham (BS) short group signature scheme and batch verification. Experimental results demonstrate efficiency and applicability of the proposed protocol for providing the requirements of privacy and Sybil attack detection in V2V communications in VANET.

Introduction

Introduction of VANET: Vehicular Network (VANET) is a form of Mobile adhoc network, to provide communications among nearby vehicles and between vehicles and nearby fixed equipment, usually described as roadside equipment. It is a cornerstone of the envisioned Intelligent Transportation Systems (ITS). By enabling vehicles to communicate with each other via Inter-Vehicle Communication (IVC) or V2V as well as with roadside base stations via Roadside-to-Vehicle Communication (RVC) or R2V, vehicular networks will contribute to safer and more efficient roads by providing timely information to drivers and concerned authorities. The interesting research area of Vehicular Networks is where ad hoc networks can be brought to their full potential. Both modern high-speed motorways and vehicles that drive upon them are becoming increasingly intelligent. The resulting enhanced situational awareness has the potential to not only facilitate the decision making tasks of the drivers (e.g., trip planning based on traffic congestion on the road), but also to improve highway safety (by bringing information about catastrophic events and road conditions to the driver's attention). Each vehicle equipped with VANET device will be a node in the Ad-Hoc network and can receive and relay 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.

Introduction of attacks: Attacker create problem in the network by getting full access of communication medium. Here we are discussing some properties and capability of

ISSN:2229-6093

Ajay Wadekar et al , International Journal of Computer Technology & Applications,Vol 8(6),634-639

the attackers which has been mentioned in studies [1].The main objective of these attacks is to create problem for legitimate users of network.

Types of Attacks

1) Jamming: The jammer deliberately 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 [2].

Figure: 5.3 Classification of attacks based on Layers

2) Node Impersonation Attack: Each vehicle has a unique identifier in VANET and it is used to verify the message whenever an accident happens by sending wrong messages to other vehicles [2]. Fig 5.2 explains this scenario in which vehicle A involves in the accident at location Z. When police identify the driver as it is associated with driver's identity, attacker changes his/her identity and simply refuses it.

Figure 5.4 Node Impersonation Attack

3) Sybil Attack: Sybil attack [2] so belongs to the first class. In Sybil attack, the attacker sends multiple messages to other vehicles and each message contains different fabricated source identity (ID). It provides illusion to other vehicle by sending some wrong messages like traffic jam message [2]. The objective is to enforce other vehicles on the road to leave the road for the benefits of the attacker.

4) Routing attack: Routing attacks re the attacks which exploit the vulnerability of network layer routing protocols. In this type of attack the attacker either drops the packet or disturbs the routing process of the network. Following are the most common routing attacks in the VANET:

a) Black Hole attack: In this type of attack, the attacker firstly attracts the nodes to transmit the packet through itself. It can be done by continuous sending the malicious route reply with fresh route and low hop count. After attracting the node, when the packet is forwarded through this node, it silently drops the packet.

b) Worm hole attack: In this attack, an adversary receives packets at one point in the network, tunnels them to another point in the network, and then replays them into the network from that point. This tunnel between two adversaries are called wormhole. It can be established through a single long-range wireless link or a wired link between the two adversaries. Hence it is simple for the

adversary to make the tunneled packet arrive sooner than other packets transmitted over a normal multi-hop route.

c) Gray Hole attack: This is the extension of black hole attack. In this type of attack the malicious node behaves like the black node attack but it drops the packet selectively. This selection can be of two types-one is malicious node can drop the packet of UDP whereas the TCP packet will be forwarded. Another is malicious node can drop the packet on the basis of probabilistic distribution.

5) 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.

6) Repudiation: The main threat in repudiation is denial or attempt to denial by a node involved in communication. This is different from the impersonate attack. In this attack two or more entity has common identity hence it is easy to get indistinguishable and hence they can be repudiated.

7) Denial of Service (DOS): 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 [3].

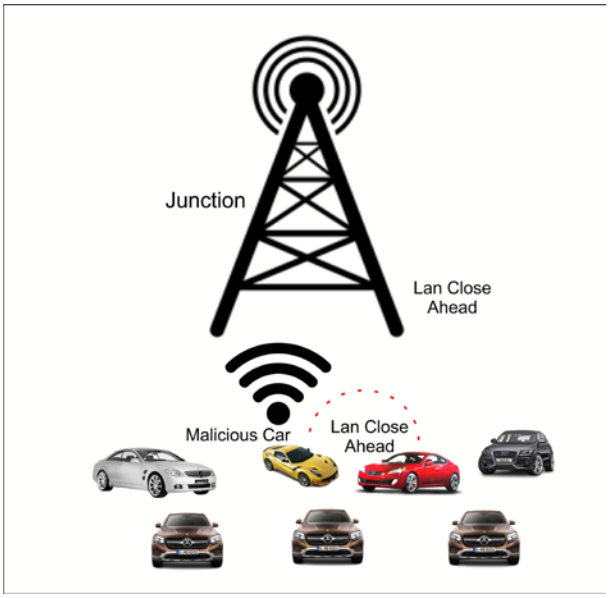

Figure 5.5 Dos Attack

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 jammed.

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. These results too half open connection to handle by a victim node's buffer. As a consequence the legitimate request is discarded.

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

ISSN:2229-6093

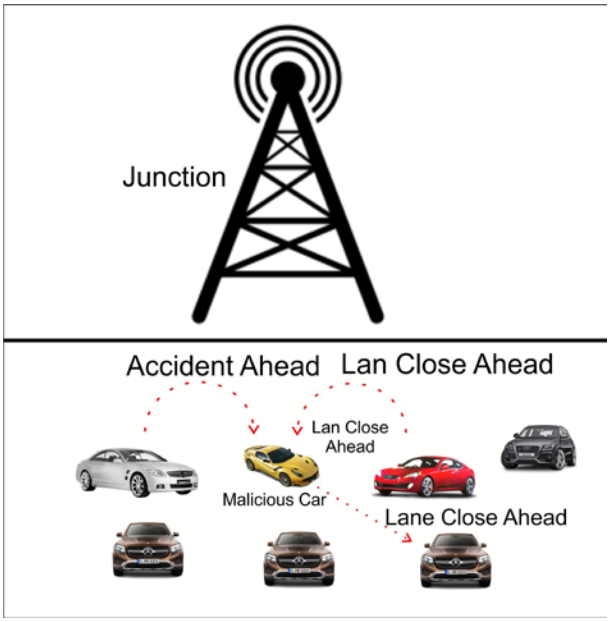

Figure 5.6 DDos attack

RELATED WORK

In VANET it can be expressed by sending numerous intimation messages from one node with numerous identities. When any node creates multiple copies of itself then it creates confusion in the network. So all the illegal and fake IDs and Authority should be Claimed. It can create collision in the network. This kind of situation is known as Sybil attack in the network. A. Cluster-based approaches In, the author proposed the VANET QoS-OLSR protocol to maintain the stability of VANET as well as Stable the Clusters of the communication in the network & overhead minimization. They proposed new Cluster based protocol for VANET called VANET QoS-OLSR. To reduce the stability of cluster they add the parameters including velocity & distance that represent the mobility metrics to the QoS function. select the optimal path, select the MPR nodes so that they broadcast the three message to at maximum 2hop away nodes(Hello, Ant-Hello, Ack). In, Authors have proposed a two phase modelincentive and detection. After cluster formation, misbehavior is detected by aggregating evidences and cooperative decision using Dempster Shafer based cooperative watchdog model. Incentives are in the form of reputation where network services are provided depending on reputation value. Watchdogs are appointed from the nodes in the network that monitor behavior of other nodes in order to ensure vehicles are cooperating with each other.

B. Privacy Preserved Based- Approaches In [6], they propose a security protocol to detect Sybil attacks for position based applications in privacy preserved vehicular ad hoc networks (VANETs). Vehicles in our protocol identify Sybil attacks locally in a cooperative way by examining the rationality of vehicles' positions to their own neighbors. In , it is developed to improve the lightweight Sybil attack detection technique. In lightweight technique there is one disadvantage, the Sybil nodes whose speed is less than 10m/s are also detected as legitimate nodes. To improve this, they enhanced the lightweight Sybil attack detection technique. When new node enters a network its RSS value is checked and it is verified with respect to RSS upper bound value. If received RSS value of node exceeds the RSS upper bound value then that node is recognized as Sybil node otherwise as legitimate node.

Design goals

- **Sybil attack detection:** in vehicular network, a message is broadcasted by more than one vehicle and receiver decides what to do base on the number of incoming messages. So before deciding on the message, the recipient vehicle should check a sender has not been send more than one message in the network. Proposed scheme check re-transmission done by malicious vehicles (in each transmission, it masqueraded itself as one of Sybil identities). This checking can be done non central, by all receivers.

- **Privacy preserving:** in this scheme, checking for retransmission is without revealing the sender identities. So a privacy-aware scheme is proposed.

ISSN:2229-6093

Comparison between different detection techniques

All of these localization techniques studied have their pros and cons. Table 2 briefly compares these techniques. As we can see from the table, although several interesting solutions have been reported in the literature, basically none of them satisfy all the requirements of critical applications at the same time, such as being available anywhere and anytime, with highly accurate and reliable Position computations. For these reasons, one of the most appealing problems to be solved by VANETs is how to provide an anytime, anywhere, fine-grained, and reliable localization system to be used by vehicles in a VANET for critical safety and emergency
applications. An anytime requirement means That the localization system must be free of delays when computing the current positions

Table: 02

Required localization accuracy for some VANet applications

Technique	Localization Accuracy		
	Low	Medium	High
Routing	X	–	–
Data Dissemination	X	–	–
Map Localization	X	–	–
Coop. Adapt. Cruise Control	–	X	–
Coop. Intersection Safety	–	X	–
Blind Crossing	–	X	–
Platooning	–	X	–
Vehicle Col. Warn. System	–	–	X
Vision Enhancement	–	–	X
Automatic Parking	–	–	X

of the vehicles (e.g., no startup delay). This requirement is critical, since the high mobility of VANETs means that slightly outdated position information cannot be used and could even be dangerous. To be available anywhere is also a challenge in a VANET localization system. It means that the localization system cannot rely only on satellite infrastructure, since it would then not work in environments without direct visibility to satellites. Also, it cannot rely only on local infrastructure localization techniques, since it would not be available in places without this infrastructure. Finally, a fine-grained localization system ensures a low localization error for vehicles, which enables most critical VANET applications to have some degree of confidence. As shown in Table, it is clear that a single technique will not be enough to provide a localization system with all of the features requested by critical VANET applications. As a result, ways to combine different localization techniques and protocols in a single localization system will be required. Data-fusion techniques, which will be studied in the next section, are the natural choice for technique combinations aimed at acquiring improved data

Conclusion

In this paper, Localization Systems were studied from the viewpoint of Vehicular Ad Hoc Networks (VANETs). We showed how GPS receivers, the most common source of localization information in VANETs, can become erroneous or unavailable in a number of situations. We then discussed how these localization inaccuracies can affect most VANET applications, especially critical ones. A number of other localization systems are available to be used by vehicles to estimate their positions: Map Matching, Dead Reckoning, Cellular Localization, Image/Video Processing, Localization Services, and Relative Distributed Ad Hoc Localization. All of these techniques have their pros and cons. In this paper we argue that future localization systems for VANETs are likely to use some kind of Data Fusion technique in order to provide position information for vehicles that is accurate and robust enough to be applied in VANET critical applications. We then show how Data Fusion techniques can be used to compute an accurate position based on a number of relatively inaccurateposition estimations.

References

[1] Vehicular Ad Hoc Networks: A New Challenge for Localization-Based Systems | Azzedine Boukerche a, Horacio A.B.F. Oliveira, Eduardo F. Nakamura, Antonio A.F. Loureiro

[2] Megha Nema1, Prof. Shalini Stalin2, Prof. Vijay Lokhande3, 2014, *"Analysis of Attacks and Challenges in VANET"* , International Journal of Emerging Technology and Advanced Engineering, Volume 4, Issue 7

[3] D.Jiang,V.Taliwal, A.Meier, W.Holfelder and R.Herrtwich;2006,"Design of 5.9GHz DSRC based vehicular safety communication", IEEE Wireless Communication Magazine , Vol.13, No.05, pp:36-43.

[4] Pratibha Tomar , Brijesh Kumar Chaurasia2 and G . S. Tomar;2010 , " State of the Art of Data Dissemination in VANETs" , International Journal of Computer Theory and Engineering , l.2,No.6

[5] Nisha K.Warambhe and Dr. S.S. Dorle;2012, "Implementation of Protocol for Efficient Data Storage And Data Dissemination in VANET", International Journal of Advanced Research in Computer Science and Electronics Engineering, ISSN: 2277 – 9043, Volume 1, Issue 2

[6] Pratibha Tomar, Munesh Chandra; 2010, " An Application of Routing Protocols for Vehicular Ad- hoc Network", IEEE , International Conference on Networking and Information Technology, Volume 2, No. 12

[7] Dr.Kamlesh Namdev,Dr. Prashant Kumar, IEEE, 2015 International Conference on Communication Networks (ICCN)

[8] J. W. Cresswell ; 2002, "Research Design: Qualitative, Quantitative and Mixed Methods Approaches", 2nd. Ed. California: Sage Publications, PE-WASUN '04 Proceedings of the 1st ACM international workshop on Performance evaluation of wireless ad hoc, sensor, and ubiquitous networks page 77-86.

[9] http://www.msr-waypoint.net/pubs/70463/tr-2007-90.pdf