International Journal of Electrical and Electronic Engineering & Telecommunications

ISSN 2319 – 2518 www.ijeetc.com
Vol. 3, No. 1, January 2014

Research Paper

ANALYSIS OF SECURITY ISSUES IN VEHICULAR AD-HOC NETWORKS

Gunavathi G H[1]* and Bhagyashree R[1]

*Corresponding Author: Gunavathi G H, ✉ gunamitha@gmail.com

The communicating nodes in Ad-hoc networks are dynamic in nature in comparison with the traditional network nodes which appears in any fixed network infrastructure and usually Ad hoc networks are deployed in specific environment to achieve certain goals. Due to these features security challenges also increases in comparison with other traditional networks. We can say that the method used in fixed infrastructure networks cannot be directly applied in the case of Adhoc networks. So a short-range wireless channel has security problems that differ from those of more conventional networks. Vehicular Ad hoc networks (VANETs) are a subgroup of Ad hoc networks with the distinguishing property that the nodes are vehicles. This paper focuses on the security issues concerned with Vehicular Ad hoc-networks which are the most emerging forms of Ad hoc networks now days. Basically security is the main concern under the umbrella in the case of Ad hoc networks because user private data need to be protected by the authorities such that from location profiling and from other attacks on their privacy. Features like system availability and security can be achieved only with the coordination among system operators and vehicle manufacturers so that the faulty units can be identified easily.

Keywords: VANETs, MANETs, GPS, Attacks

INTRODUCTION

An Ad hoc network is a collection of wireless mobile nodes dynamically forming a temporary network without the use of existing network infrastructure or centralized administration. If Ad hoc network consists of mobile node which can be static and wired nodes it will be called (MANETs) and can obtain services offered by the fixed infrastructure. Vehicular Ad hoc Networks (VANETs) are Subgroup of MANETs.

VANETs allow moving vehicles to collectively form a network by allowing the near by nodes to communicate with each other.

SECURITY ISSUES IN VEHICULAR AD HOC NETWORKS

Attacks Categories

- Passive Attacks
- Active Attacks

[1] Department of CSE, A.P.S College of Engineering, Bangalore 560078, India.

Passive Attacks

These are the types of attacks by which any attacker can only monitor the transmission by obtaining messages contents or monitor traffic flows by eavesdropping.

Active Attacks

By active attacks an attacker can cause any serious damage to the data or information like data can be modified, replay previous messages to cause denial of service attack or successfully masquerade of one entity as some other.

External Attacks

These are targeted active attacks which actually damage the routing information or can cause any service so that it can't work properly or even at maximum the specific service can be shut down by these attacks and the most dangerous is that these external active attacks can cause network congestion.

The best way to prevent these types of attack is by applying security mechanism standards like firewalls encryption.

Insider Attacks

They are the more harsh attacks, it is done by the node which already is a trusty node within the network and protected by the security mechanism of that network.

Denial of Service Attack

This attack happens when the attacker takes control of a vehicle resource 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 applications 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.

Message Suppression Attack

An attacker selectively dropping packets from the network, these packets may hold critical information for the receiver, the attacker suppress these packets and can use them again in other time. 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.

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.

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.

Replay Attack

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

Sybil Attack

This attack happens when an attacker creates a large number of pseudonymous, and claims or acts like it is more than a hundred vehicles, to tell other vehicles that

there is jam ahead, and force them to take alternate route.

Eavesdropping

Eavesdropping is the most prominent attack over VANETs against confidentiality. To perform it, attackers can be located in a vehicle (stopped or in movement) or in a false RSU. Their goal is to illegally get access to confidential data. As confidentiality is needed in group communications, mechanisms should be established to protect such scenarios.

Adversaries

Selfish Driver

The general idea for trust in Vehicular Network is that all vehicles must be trusted initially, these vehicles are trusted to follow the protocols specified by the application, some drivers try to maximize their profit from the network, regardless the cost for the system by taking advantage of the network resources illegally.

A Selfish Driver can tell other vehicles that there is congestion in the road, so they must choose an alternate route, so the road will be clear for it.

Malicious Attacker

This kind of attacker tries to cause damage via the applications available on the vehicular network. In many cases, these attackers will have specific targets, and they will have access to the resources of the network.

Pranksters

Include bored people probing for vulnerabilities and hackers seeking to reach fame via their damage. For instance, a prankster can convince one vehicle to slow down, and tell the vehicle behind it to increase the speed.

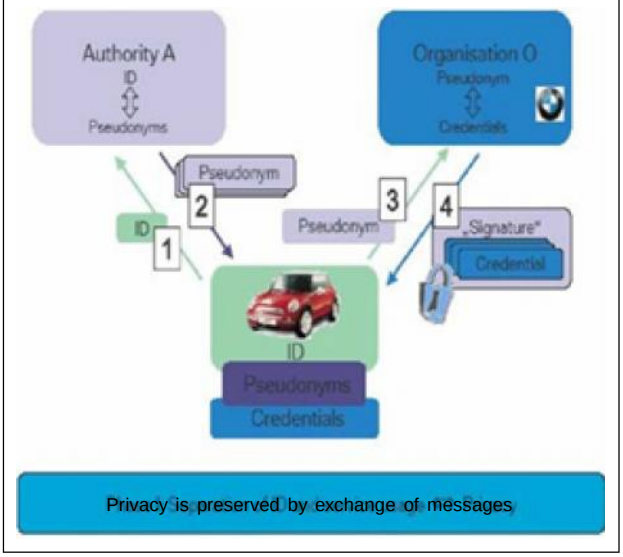
Industrial Insiders

Industrial insiders are those who stays inside the car manufacturing company Attacks from insiders can be very harmful, and the extent to which vehicular networks are vulnerable will depend on other security design decisions.

VANETs NETWORK MODEL

Communication among the VANETs networks will be done by two nodes or entity one will be obviously vehicles while the second entity can be base station. In the case of vehicles the communicating node either base station or vehicle could belongs to private individual as well as government organization as illustrates in (Figure 1).

Figure 1: A VANET Setup Describing Primarily Safety Messages Exchanges to the Drivers



The communicating nodes in VANETs are either vehicles or base stations. Vehicles can be private (belonging to individuals or private companies) or public (i.e., public transportation means, e.g., buses, and public services such as police cars). Base stations can belong to the government or to private service providers.

We assume a communication channel supported by an IEEE 802.11-like technology.

Because in VANETs the network totally dependent on the basic communicating node that is vehicles so therefore the two main factors will be involved due to the high speeds movement of vehicles will be mobility and short connection times between neighbors at the time of takeover.

The features of power generation and computation as well as power consumption are the advantages which differentiate Adhoc network with the traditional networks. VANETs can support huge number of microprocessor Devices like EDR (Event data recorder) and GPS (Global Positioning System).So by the use of GPS devices is not only the solution for security support in VANETs; we have also describe alternative options.

The scale of VANETs is another feature that sets them apart. With hundreds of millions of nodes distributed everywhere, VANETs are likely to be the largest real-world mobile ad hoc network. But communication in this network will be mainly local, thus partitioning the network and making it scalable.

HOW TO SECURE VANETs

In the next sections, we propose a set of security solutions to be deployed in vehicular networks. We attempt to consider all the possible options but take into account both the current state of the art and the long-term viability of these networks.

Requirements

A security system for safety messaging in a VANET should satisfy the following requirements:

- Authentication: Vehicle reactions to events should be based on legitimate messages (i.e., generated by legitimate senders). Therefore we need to authenticate the senders of these messages.
- Verification of data consistency: The legitimacy of messages also encompasses their consistency with similar ones (those generated in close space and time), because the sender can be legitimate while the message contains false data.
- Availability: Even assuming a robust communication channel, some attacks (e.g., DOS by jamming) can bring down the network. Therefore, availability should be also supported by alternative means.
- Non-repudiation: Drivers causing accidents should be reliably identified; a sender should not be able to deny the transmission of a message (it may be crucial for investigation to determine the correct sequence and content of messages exchanged before the accident).
- Privacy: People are increasingly wary of Big Brother enabling technologies. Hence, the privacy of drivers against unauthorized observers should be guaranteed.
- Real-time constraints: At the very high speeds typical in VANETs, strict time constraints should be respected.

Digital Signatures as a Building Block

As emphasized in the above section, message legitimacy is mandatory to protect VANETs from outsiders, as well as misbehaving insiders. But since safety messages will not contain any sensitive information confidentiality is not required.

As a result, the exchange of safety messages in a VANET needs authentication but not encryption. Symmetric authentication mechanisms usually induce less overhead per message (not counting the handshake needed to establish a shared key) than their asymmetric counter parts. But digital signatures are a better choice in the VANET setting, because safety messages are typically standalone.

In addition, given the huge amount of network members and the sporadic connectivity to authentication servers, a Public Key Infrastructure (PKI) is the most suitable way for implementing authentication.

Tamperproof Device

The use of secret information such as private keys incurs the need for a tamper-proof device in each vehicle. In addition to storing the secret information, this device will be also responsible for signing outgoing messages. To reduce the risk of its compromise by attackers, the device should have its own battery, which can be recharged from the vehicle, and clock, which can be securely resynchronized, when passing by a trusted roadside base station. The access to this device should be restricted to authorized people.

CONCLUSION

In this paper, we have explained why Vehicular Ad hoc networks need to be secured, and why this problem requires a specific approach. We have proposed a model that identifies the most relevant communication aspects. We have also identified the major threats.

In terms of future work, we intend to further develop this proposal. In particular, we intend to explore in more detail the respective merits of key distribution by the manufacturers or by governmental bodies; we will also perform numerical evaluations of the solutions.

REFERENCES

1. Hassinen M, Hyppönen K and Haatajam K (2006), “An Open, PKI-Based Mobile Payment System”, in Emerging Trends in Information and Communication Security, International Conference (ETRICS’ 2006), pp. 86-100.
2. http://www.webopedia.com/TERM/S/security.html
3. Kevin C Lee, Uichin Lee and Mario Gerla (2009), “Survey of Routing Protocols in Vehicular Ad Hoc Networks”, RoutingBook ChapterKLULMario.pdf
4. Parno B and Perrig A (2005), “Challenges in Securing Vehicular Networks”, *Proc. of HotNets-IV*.
5. Yue Liu, Jun Bi and Ju Yang (2009), “Research on Vehicular Ad Hoc Networks”, *Chinese Control and Decision*.