A Survey of VANET’s Authentication

Khalid Haseeb, Dr.Muhammad Arshad, Dr.Shazia Yasin, Naveed Abbas
Department of Computer Science,
Islamia College Peshawar (Chartered University)
Peshawar, Pakistan
{Khalid.haseeb, Muhammad.arshad,shazia.khalid,Naveed.Abbas}@icp.edu.pk

Abstract - Vehicular Ad hoc networks (VANET’s) must overcome a myriad of security issues to realize their potential. VANET’s are latest research area in network field. VANET’s are deployed in un-trusted and unsecured environments. Consequently, authentication is a forerunner to any secure interactions in these networks. In this paper, survey of VANET’s Authentication is discussed. Different issues regarding to VANET’s Authentication is discussed. This work provides the basis to understand the authentication in VANET’s and to design new more efficient and cost-effective mechanism for authentication in VANET’s.

Keywords: Vehicular ad hoc networks (VANET’s), Vehicular Communications (VC), Security, Authentication, Digital Signatures, Digital Certificates

I. INTRODUCTION

Vehicular ad hoc networks (VANET) have recently drawn the attention of the research community. Vehicular Ad-hoc Networks (VANET’s) represent a rapidly emerging, particularly challenging class of MANETs [1]. Vehicular communications (VC) aim to enhance safety and efficiency of transportation systems. Vehicular applications will provide warnings on environmental hazards, traffic and road conditions and local information. In fact, vehicular networks emerge, among civilian communication systems, as one of the most convincing and yet most challenging instantiations of the mobile ad hoc networking technology. [2]

In VANET’s, being an infrastructure-less networks, nodes will be expected to cooperate to perform essential networking tasks such as routing. In order to provide network-wide connectivity, nodes in a VANET are expected to route data packets on behalf of other nodes in the network that want to reach nodes out of their transmission range. From a security stand point, VANET’s face a number of challenges. The wireless medium has no observable boundaries and is significantly less reliable than wired media. Wireless attacks may come from anywhere and from all directions [3]. The broadcast nature of the transmission medium and the dynamically changing topology add even more complications. Furthermore, the reliance on node collaboration as a key factor of network connectivity presents another obstacle.

In order to provide network security, support for authentication, confidentiality, integrity, non-repudiation and access control should be provided. Authentication is the cornerstone service, since other services depend on the authentication of communication entities [4,5]. Authentication supports privacy protection by ensuring that entities verify and validate one another before disclosing any secret information.

In section II, related works is overviewed. In section III, importance of authentication in VANET’s and how safety message works are discussed. In section IV, different types of authentication are elaborated. In section V, proposed solutions for authentication in VANET’s are overviewed. In section VI, we discussed toolboxes for authentication in VANET’s and in section VII Conclusion and section VIII future Direction is given.

II. RELATED WORK

In VANET’s Security is an important issue for researchers. In [6] Maxim Raya et al. have described the some of problems that characterize the security of vehicular networks and have sketched possible solutions including authentication. El Zarki et al. [8] describe an infrastructure for VC and briefly mention some related security issues and possible solutions including authentication. In [7], the authors give an overview of key security topics in VANET’s. Dotzer discussed privacy issues for vehicle communications in [9].

Hubaux,et al. [10] provided an overview of security and privacy in VANET’s. Weimerskirch et.al. [11] presented a mechanism in which nodes that do not have any additional knowledge to re-recognize themselves when meeting again. This mechanism allows maximum privacy and provides immutable and non-migratable identities. In
[12,13], the authors present a method to derive unique and cryptographically verifiable identifiers from preexisting cryptographic keys.

III. IMPORTANCE OF AUTHENTICATION IN VANET’S

In general, a secure network should have the following attributes: authentication, non-repudiation, confidentiality, data integrity, Access Control and availability[14].

Authentication is the verification of a user’s identity prior to granting access to the network. It can be considered as the first line of defense against intruders.

Non-repudiation is the verification that the data was sent with a user’s credentials so that without denial or repute the data can be associated to the sender.

Confidentiality is the assurance that the data could not have been accessed by any other user than the designated recipient for whom it was meant; thus insuring that the data was untouched until reception. Confidentiality is generally achieved by cryptography techniques.

Data integrity is the assurance that the content of the data was not modified while in transit. It differs from confidentiality in the sense that it allows for detection of data modifications.

Availability is the proportion of time that a system is in a functioning state. Each of these attributes brings its network requirements whose balance and compromises make network security challenging.

Access Control means that user can access which type of resource and what permission user has.

Authentication is the first mechanism for network security and defense against malicious network activity, because if the destination party is not authenticated, then establishing secure channels is not prudent. The importance of authentication in vehicular communications is to ensure that, when a connection is established between two entities without previous knowledge of one another, they are actually communicating securely with their intended destination entity and not an attacker.

A. How safety messaging protocol works

To better understand the importance of authentication, understanding the working of simple safety messaging protocol is necessary. In [15] authors defines specifications of safety messaging. Inspired from [15], the basics of safety message protocol are as under:

In compliance with the DSRC specifications [16], we considered that:

- Each vehicle V periodically sends messages over a single hop every 300 ms
- The range of the messages is of 10 s travel time i.e. the minimum range is 110 m and the maximum is 300 m.
- The inter-message interval drops to 100 ms and the range to 15 m if the vehicles are very slow or stopped (i.e., their speed is less than 10 miles/h or16 km/h).
- Vehicles take decisions based on the received messages and may transmit new ones. For example, if V receives an emergency warning from another vehicle W and, based on their mutual positions, estimates that it is also in danger, it sends out its own warning messages.

IV. AUTHENTICATION VANETS

There are certain requirements for authentication in VANET’s, which must be met for secure and authenticated vehicular communication.

1. Computation overhead: the amount of cryptographic operations a node has to compute for an authentication request in CPU time, for example, the time needed for verifying a digital signature.
2. Control overhead: the bandwidth overhead (in bytes per second) for an authentication request, for example, exchanging cipher keys or certificates.
3. Latency: the time needed to respond to an authentication request.
4. Initialization time: the time needed to initialize the authentication system, for example, setting up a certificate authority and key distribution.
5. Strong authentication: Authentication in VANET’s should be strong.
6. Scalable: Authentication should be scalable.
7. Support for re-authentication and revocation procedures.

V. AUTHENTICATION METHODS

There are different methods are used to authenticate nodes in VANET’s.

Node level authentication means that the message is proven to originate from certain node.

Group level authentication means that the message is proven to originate from a certain group of nodes.
**Unicast authentication** means the message is sent to only one node. Sometimes special messages are sent to specified node in vehicular ad hoc networks.

**Multicast authentication** means the message is sent to many nodes. Sometimes messages are sent not to all nodes in the vehicular ad hoc.

**Broadcast authentication**: means the message is sent to all nodes in the network.

**VI. TOOLKit FOR AUTHENTICATION IN VANET’S**

Digital signatures have been proposed for achieving authentication in vehicular ad hoc networks. There are some shortcomings in using digital signatures without certificates. So certificates are used with digital signatures to overcome the shortcoming.

**A. Digital Signature**

Cryptographic digital signatures are applied to messages or hashes over messages to provide authenticity, integrity protection and non-repudiation. Digital message signatures are commonly using public-private key cryptography. Messages or hashes over the respective messages are signed with the message originators’ private keys. By using private key, it is guaranteed that the messages originate from nodes holding the required cryptographic key material and the messages have not been altered by intermediate forwarding nodes. The message receiver verifies the integrity and authenticity of the messages, by using the corresponding public keys. The node cannot be impersonated because the node only knows private key.

In VANET’s, any message sent by a vehicle should be digitally signed specially safety messages or warning messages. Furthermore, messages that serve as input or triggers to the safety system could also be signed.

The main advantage is the requirements for digitally signature are very small i.e. the nodes need a possibility to receive or create and store cryptographic key pairs. They need the processing power for creating and verifying message signatures.

Main disadvantage is Message forging and denial of service (DoS) attacks are possible.

**B. Digital Signatures with Digital Certificates**

The signatures can be combined with digital certificates provided by a trusted third party. The basic assumption with certificates is that nodes, which include certificates in their messages, are trusted by other nodes that are able to verify the certificates. Certificates are provided by trusted third party.

In VANET’s, Digital Signature provides Data integrity. The distribution of certificates is limited to valid VANET nodes, e.g. communication systems inside vehicles or roadside equipment. Since nodes having obtained a valid certificate can only create new valid active safety messages, this excludes outside attackers. Obviously, this statement holds only, if we can assume that those attackers have no certified keys and if they are unable to extract any from valid nodes. Owner identification might also be used for other legal aspects, not directly linked to active safety application, which is out of scope for this document.

The advantages of the digital signature with certificate are:

- The possibility to exclude external attackers from the system,
- The ability to remove malicious or defective nodes.

**VII. CONCLUSION**

The fundamental security functions in VC will consist in authenticating the origin of a data packet. Authentication and the inherent integrity property counter the in-transit traffic tampering and impersonation vulnerabilities. Authentication helps also to control the authorization levels of vehicles. In this paper, requirements and methods of authentication in VANETS are discussed. Digital signatures and Digital Certificates have been discussed comprehensively. Working, advantages and disadvantages of digital signatures with digital certificates have been discussed.

**VIII. FUTURE DIRECTION**

The future direction requires studying different possible authentication types for vehicular network. And Design an efficient, Reliable and cost-effective mechanism for authentication in vehicular ad hoc

**REFERENCES**


