Secured Geographic Routing Protocol for Vehicular Ad Hoc Networks (VANETs)

Mohammed Erritali[1], Bouabid El Ouahidi[1], and Daniel Bourget[2]

[1] Department of Computer Science
Mohamed V Agdal, University – L.R.I, Faculty of Sciences Rabat, Morocco
mederritali@yahoo.fr, ouahidi@fsr.ac.ma
[2] Telecom Bretagne, France
daniel.bourget@telecom-bretagne.eu

Abstract. A Vehicular ad hoc network called VANETs is a mobile network allowing to vehicles to communicate with each other in the absence of fixed infrastructure, with the aim of improving road safety through the exchange of alerts between neighborhood vehicles or to offer new comfort services to road users. The characteristics of these networks such as: shared wireless medium and the highly dynamic network topology pose a number of nontrivial challenges to security design.

In these networks each vehicle coordinates with every other vehicle in forwarding their packets to reach the destination. Since these vehicles operate in a physically insecure environment; they are vulnerable to different types of attacks such as the blackhole attack, Sybil attack, selective forwarding and altering routing information.

This paper proposes a security solution for VANETs using a pre-existing routing protocol Greedy Perimeter Stateless routing. In this solution, each node in a network has a list of its neighbor nodes including a shared secret key which is obtained by executing a key agreement Diffie Hellman, this key will be used by the AES symmetric encryption algorithm to generate a digital signature, after applying the MD5 hashing algorithm on the non-modifiable data of GPSR packets. Our idea consists that each vehicle verifies the integrity and authenticates the sender in the process of route discovery, Comparing with other recently proposed security routing protocols, our security solution needs less computation times in routing transactions because it use AES and does not need any centralized element in vehicular ad-hoc networks.

Keywords: Attack, Secure routing protocols, VANETs.

1 Introduction

Vehicular networks are a projection of intelligent transportation systems (ITS)[1,2] designating new technologies applied to transportation networks to improve the conduct and bring new services to road users by offering solutions that allow to:

V. Gramoli and R. Guerraoui (Eds.): NETYS 2013, LNCS 7853, pp. 311–315, 2013.

-Reduce road congestion
- Establish a system of traffic management that allows rapid intervention in case of incidents.
- Locate parking
- Report of a pedestrian passageway
-Notify violations of the Stop signal.

From examples of interesting solutions described above we can deduce that the vehicular communication ensures large improvement in terms of road safety, better utilization of resources such as time and fuel and new opportunities for entertainment applications to road users. The services offered in vehicular networks can distinguish several types of communication [2]: Vehicle to Vehicle communication (V2V), vehicle to infrastructure communications (V2I) and hybrid communications derived from the combination of these two types of communications.

Generally networks without infrastructure are called ad hoc networks, which is why V2V communications are called vehicular ad hoc networks (VANETs).

In these networks a successful attack against the road safety alerts could have catastrophic consequences such as loss of human lives. Therefore, making a vehicular communication network secure is not an extension but a primary concern. So far, only a few research efforts have addressed in VANETs security issues, focusing either on identification of their challenges, or proposing secure VANETs architectures.

In VANETs, routing is an important element designed to transmit road safety alerts to all vehicles in neighborhood, so it constitutes an ideal target for attacks which aims to prevent alert messages to reach their destinations.

The routing raises a significant number of problems which are not yet resolved such as packet modification, data injection and the generation of false messages, the rupture of packet forwarding, or deleting packets.

To remedy these vulnerabilities, several secure routing protocols for mobile networks [3, 4] have been proposed in which cryptographic primitives are involved, such as digital signatures, MACs (Message Authentication Code) or asymmetric encryption.

The other sections of the paper are structured as follows:

Section 2 briefly presents possible attack against routing protocols; section 3 describes secure routing protocols. Finally we present our extension to secure greedy perimeter Stateless routing.

2 Attack against Routing Protocols

Vehicular Ad hoc networks are dynamic and self-organized so any node can participate in routing and also uses a shared wireless medium to send packets .therefore there are no barriers to ensure that a malicious node cause disturbances in the circulating traffic. In the following section we will present some type of attack [9, 10, 11, 12] against routing protocols:

1- Blackhole attack: The black hole attack consists to insert a malicious node in the network. This node, by various means, will modify the routing tables to force the maximum of neighboring nodes to pass information through it. Then like a black hole in space, all the information that will go in it will never be retransmitted.

2- The type of attack Denial of Service DOS: The attacker sends an excessive amount of data to overload the network for the purpose to overflow the routing table of relay nodes.

3- Insertions of infinite loops: An attacker will modify the network routing mechanism with one or more nodes malicious, so that packets will be routed in infinite loops and will therefore consume network bandwidth.

4- Sybil attack: The "Sybil attack" consists that a malicious vehicle is masquerading as several vehicles. Thus it modifies the routing table that will become invalid. For example a malicious node witch pretend to be multiple nodes can gain a significant advantage for an election of master node.

5- Identity spoofing: A malicious node usurps address of a legitimate node as the source address in order to disseminate its messages on the VANETs network.

6- Wormhole attack: The attack of the wormhole requires the insertion of at least two malicious nodes A and B .These two nodes are connected by a link A-B. The goal of this attack is to trick the neighboring nodes about distances. Because in general a routing protocol seeks the shortest path in number of hops.

7- The alteration/modification of routing packets: A malicious node will retrieve a package and alter it, by adding false information (about the recipient, the sender or the data).

3 Secure Routing Protocols

SRP [6] is based on DSR protocol and requires a pre-existing secured association between source node and the destination node (secret key exchange) and it uses a MAC to ensure the confidentiality of the route learned from the source to the destination. These authors propose a mechanism to detect malicious behavior neighborhoods (Neighbor Lookup Protocol) and a mechanism for secure data transmission (Secure Message Transmission Protocol).

ARIADNE [7] is also based on DSR (Dynamic Source Routing) and it is used to authenticate messages routing with three mechanisms. The first is the use of a shared secret key between each pair of nodes, the second combines a secret shared between the nodes and the broadcast authentication (TESLA), and the third is the use of a digital signature.

SAODV [5] secures the modifiable routing data as the number of hops, which can for example be decremented by an attacker, and authenticates the fields that should not be changed using an RSA digital signature.

Figure 1 illustrates these secure routing protocols with used cryptographic techniques.

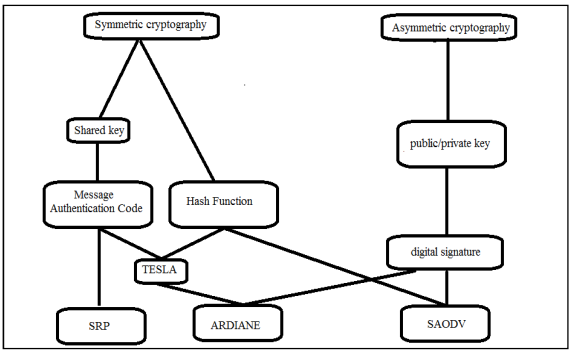

Fig. 1. Secure routing protocols with used cryptographic techniques

4 Adding Security Aspect in Greedy Perimeter Stateless Routing

Geographical routing protocols of vehicular networks have been developed without considering the security aspects against routing attacks. In this section we present our contribution to secure GPSR or generally geographical routing like it.

4.1 1st Extension: Establish Secret Keys

Our first contribution in this work is to propose an approach that allows to establish secret keys Diffie-Hellman between two neighboring vehicles (in a hop) when exchanging beacons packets to build direct neighbors tables of Greedy Perimeter Stateless Routing protocol [8]. The idea is to have neighbor's tables that contain secret keys that will be used as a symmetric encryption key.

4.2 2nd Extension: Adding a Symmetrical Digital Signature

In VANETs the digital signature will be the mechanism to ensure the integrity and the authentification of packets exchanged between two direct GPSR neighbors. Indeed, the mobility of nodes requires a minimal time of routing packet from the source to the destination, which is why we propose to use the AES encryption algorithm.

Figure 2 illustrates the process of creation of the digital signature.

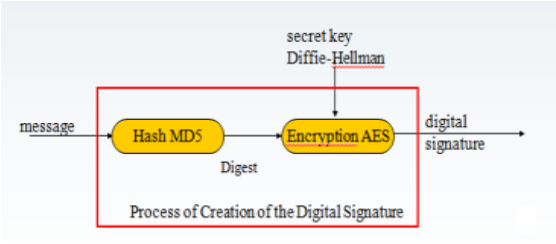

Fig. 2. GPSR digital signature

5 Conclusion and Perspectives

The problematic of communication and security in vehicular ad hoc networks attract more and more attention from research groups. Indeed, the ease of deployment of vehicular ad hoc networks and their spontaneous nature make them a compelling solution for the safety of drivers and their passengers. However, these networks require that all users work together to route information of other users on the same VANET network .This hypothesis and several other characteristics (mobility, bandwidth) make the problems of routing and security of communications in these networks a capital axis of research. In this paper we have presented GPSR protocol extensions. As perspectives of this work we will use to study how to define a level of trust between nodes and how to implement an intrusion detection system in a vehicular ad hoc network.

References

1. Khalfallah, S., Jerbi, M., Cherif, M.O., Senouci, S.-M., Ducourthial, B.: Expérimentations des communications inter-véhicules, Colloque Francophone sur l'Ingénierie des Protocoles (CFIP). Les Arcs, France (2008)
2. Jerbi, M.: Protocoles pour les communications dans les réseaux de véhicules en environnement urbain: Routage et GeoCast basés sur les intersections. Thèse, France (2008)
3. Idjiwa, A., Radhouane, B., Rebecca, B., Laurent, G.: Protocole de routage ad hoc sécurisé dans une architecture clusterisée, http://idjiwa.free.fr/wordpress/?cat=3
4. Hu, C., Perrig, A., Johnson, D.B.: Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols (2003)
5. Zapata, M.G.: Internet draft. In: Secure Ad hoc On-Demand Distance Vector (SAODV) Routing (September 15, 2005)
6. Papadimitratos, P., Haas, Z.J., Samar, P.: The Secure Routing Protocol (SRP) for Ad Hoc Networks (December 2002)
7. Hu, Y.-C., Perrig, A., Johnson, D.B.: Ariadne: A Secure On Demand Routing Protocol for Ad Hoc Networks
8. Karp, B., Kung, H.T.: Greedy Perimeter Stateless Routing for Wireless Networks. In: Proceedings of the Sixth Annual ACM/IEEE International Conference on Mobile Computing and Networking, MobiCom 2000, Boston, MA (August 2000)
9. Douceur, J.R.: The Sybil Attack. In: Druschel, P., Kaashoek, M.F., Rowstron, A. (eds.) IPTPS 2002. LNCS, vol. 2429, pp. 251–260. Springer, Heidelberg (2002)
10. Hu, Y.C., Perrig, A., Johnson, D.B.: Wormhole Detection in Wireless Ad Hoc Networks. Technical Report TR 01- 384, Department of Computer Science, Rice University (June 2002)
11. Karlof, C., Wagner, D.: Securing Routing in Wireless Sensor Networks: Attacks and Countermeasures. In: Proceedings of First IEEE International Workshop on Sensor Network Protocols and Applications, Anchorage, AK, USA, pp. 113–127 (May 2003)
12. Zhou, Z., Yow, K.C.: Geographic Ad Hoc Routing Security: Attacks and Countermeasures. Ad Hoc & Sensor Wireless Networks, 235–253 (March 2005)