Distributed Trust Based Authentication Scheme in a Clustered Environment Using Threshold Cryptography for Vehicular Ad Hoc Network

S. Sivagurunathan, Thiagarajar College of Engineering, India
V. Mohan, Thiagarajar College of Engineering, India
P. Subathra, Thiagarajar College of Engineering, India

ABSTRACT

A Vehicular Ad-Hoc Network, or VANET, is a form of Mobile Ad-Hoc Network to provide communications among nearby vehicles and between vehicles and nearby fixed equipments. Security has become a prime concern in providing communication between these vehicles. Unlike wired networks, the characteristics of Vehicular Ad Hoc Networks (VANETs) pose a number of non-trivial challenges to security design. In this paper, the authors present a threshold security mechanism with a mobility based Clustering. Nodes that have a similar moving pattern are grouped into a cluster, and unlike other clustering algorithms, it takes the moving pattern of the vehicles into consideration with the driver’s intention. The stability of clusters is estimated based on relative mobility of cluster members. A threshold cryptographic scheme is employed on top of the clusters to protect routing information and data traffic. To ensure distributed trust in the clustered environment, the private key \( k \) is divided into \( n \) pieces in such a way that \( k \) is easily reconstructable from any \( p \) number of pieces.

Keywords: Clustering, Mobility, Threshold Cryptography, Threshold Security Mechanisms, Vehicular Ad-Hoc Networks

1. INTRODUCTION

Vehicular Ad-Hoc Network (VANET) is an important application of MANET (Munoz & Syracuse, 2002). Vehicular Networks are an en-...
by providing timely information to drivers and concerned authorities.

The main applications of VANETs are: SOS services, stolen vehicle tracking, map download/update, intersection collision warning, vehicle based road condition warning, emergency vehicle signal preemption and work zone warning. The main focus of this paper is on the ability of VANET to provide safety and comfort for 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 relay others messages through the wireless network (Park et al., 2009). Collision warning, road sign alarms and in-place traffic view will give the driver essential tools to decide the best path along the way (Plobi et al., 2006). This helps the drivers to react and prepare against sudden traffic events in advance.

Vehicles can also drive collaboratively to speed up the flow of traffic. Security of these messages exchanged is a prime concern. This paper provides an easy way for vehicle assisted secure information exchange without any additional roadside infrastructure and special technologies. The fundamental vulnerability of VANET comes from open peer to peer architecture. Unlike wired networks that have dedicated routers, each vehicle in VANET may function as a router and forwards packets to other nodes. The wireless channel is accessible to both legitimate network users and attackers. The attack may range from passive eavesdropping to active impersonation. Since compromising a vehicle is possible, trust relationship among them is very important in case of co-operative driving. As a result there is no clear line of defense in VANETs from the security design perspective. The salient features of VANETs pose both challenges and opportunities in achieving the above security goals.

Apart from routing the messages exchanged in VANET also influence the behavior of the drivers. Depending on the information they get, they will, e.g., drive very carefully and slowly in case of a glaze warning or choose an alternate route in the case they are informed about the traffic jam on their desired route. Adversaries could exploit this by injecting wrong messages and slowing down traffic or getting a vehicle free road. To prevent this kind of misuse security is very important in VANETs (Plobi et al., 2006).

In this paper section 2 focuses on the state of the art for VANET security Section 3 discusses the techniques adopted for clustering and security. Section 4 throws light on the mobility based clustering algorithm for VANET. Section 5 deals with routing security, key management services and the system model. Section 6 explains the concepts of threshold cryptography and its usage in key management. Section 7 provides the simulation results and section 8 concludes the paper.

2. LITERATURE REVIEW

VANETs aim at enhancing safety and efficiency in transportation systems. They comprise network nodes, that is, vehicles and Road side Infrastructure Units RSU, equipped with on-board sensory, processing, and wireless communication modules. Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication can enable a range of applications. Among these, primarily safety will be enabled, as numerous research and development initiatives indicate, by vehicles frequently beaconing their position, along with warnings on their condition or environment. Nonetheless, VANETs can be vulnerable to attacks and jeopardize user’s privacy. For example, an attacker could inject beacons with false information, or collect vehicle’s messages, track their locations, and infer sensitive user data. To thwart such attacks, security and privacy enhancing mechanisms are necessary or, in fact, a prerequisite for deployment.

The most prominent industrial effort in this domain is carried out by Car 2 Car Communication Consortium, the IEEE 1609.2 working group, the NoW project and the
Interference Management in Heterogeneous Networks
[www.igi-global.com/chapter/interference-management-in-heterogeneous-networks/172202?camid=4v1a](www.igi-global.com/chapter/interference-management-in-heterogeneous-networks/172202?camid=4v1a)

Next-Generation Strategic Business Model for the U.S. Internet Service Providers: Rate-Based Internet Subscription
[www.igi-global.com/chapter/next-generation-strategic-business-model/52180?camid=4v1a](www.igi-global.com/chapter/next-generation-strategic-business-model/52180?camid=4v1a)