2FLIP: A TWO-FACTOR LIGHTWEIGHT PRIVACY PRESERVING AUTHENTICATION SCHEME FOR VANET

ABSTRACT

Authentication in vehicular ad hoc network (VANET) requires not only secure and efficient authentication with privacy preservation but also applicable flexibility to handle complicated transportation circumstances. In this paper, we proposed a TWO-Factor Light weight Privacy preserving authentication scheme (2FLIP) to enhance the security of VANET communication. 2FLIP employs the decentralized certificate authority (CA) and the biological password based two factor authentication (2FA) to achieve the goals. Based on decentralized CA, 2FLIP only requires several extreme lightweight hashing process and a fast MAC operation for message signing and verification between vehicles. Furthermore, any certificate revocation list (CRL) related overhead on vehicles is avoided. 2FLIP makes the scheme resilient to Denial of Service (DoS) attack in both computation and memory, either caused by deliberate invading behaviors or jammed traffic scenes. The proposed scheme provides strong privacy preservation that the adversaries can never succeed in tracing any vehicles even with all RSUs compromised.
INTRODUCTION

Vehicular ad hoc network (VANET) has been subject to extensive research efforts from government, academia and industry in recent decades. In VANET, every vehicle is equipped with an onboard unit (OBU), through which it could communicate wirelessly with other vehicles and roadside units (RSUs) over one or more hops. Thus, a large scale wireless network could be constructed, which utilizes dedicated short-range communications (DSRC) to realize high-speed reliable data exchange of vehicle-to-vehicle (V2V) and vehicle-to-roadside unit (V2R), simultaneously achieving features of mobile ad hoc and communicatively opportunistic.
EXISTING SYSTEM

Privacy preserving authentication (PPA)

➢ Large quantity of PPA schemes for VANET is proposed, some of which are based on public key infrastructure (PKI) and are employing traditional digital signature technique to authenticate messages.

Disadvantages

➢ Vulnerable availability due to effortless DoS attack.

➢ Collapse of scheme caused by high packet loss ratio.

➢ The utilization of digital signature and corresponding certificate significantly adds the size of an actual on-the-fly message, leading to a heavy burden on wireless communicating bandwidth.

➢ This might cause that some important messages in a life-or-death VANET application, would be dropped.
PROPOSED SYSTEM

- A two-factor Lightweight Privacy preserving (2FLIP) Authentication Scheme for VANET which introduces the idea of two-factor authentication technique to VANET mainly by utilizing message authentication code (MAC) and hash operations for improving the security and privacy of VANET.

- Moreover, a tamper-proof device (TPD) is embedded in OBU to store system key and to sign/verify messages.

- To secure communications of V2V and V2R, 2FLIP only requires several extreme lightweight one-way hash operations and a MAC generation operation for message signing, a hash function along with one fast MAC regeneration for verification.

- Digital signature verification process is only launched when vehicle needs system key updating, which would not affect the performance.

Advantages

- 2FLIP is the first authentication scheme which achieves both strong privacy preservation and DoS resilience for secure VANET

- Does not employ symmetric or asymmetric key mechanism, additionally it is also the first authentication scheme trying to authenticate multiple users of one single vehicle, conditionally trace each one of them in post-event investigation.
SYSTEM ARCHITECTURE

Deploy OBU

Deploy Vehicle

Create connection

Initialization message

Certificate authority

Assign secret key/pass

OBU

Vehicle

Key update

Login/ authentication
MODULES

- Node initialization
- Certificate authority
- Vehicle login
- System key update
- Message tracing

HARDWARE REQUIREMENTS

Processor : Any Processor above 500 MHz.
Ram : 128Mb.
Hard Disk : 10 Gb.
Compact Disk : 650 Mb.
Input device : Standard Keyboard and Mouse.
Output device : VGA and High Resolution Monitor.

SOFTWARE SPECIFICATION

Operating System : Win2000/XP / Linux 9.0
Programming Package : TCL coding
Tools : VM ware Workstation