Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

Extended 3PAKE authentication scheme for value-added services in VANETs[☆]

R. Muthumeenakshi[a], T.R. Reshmi[b,*], K. Murugan[a]

[a] Anna University, Chennai, India
[b] VIT University, Chennai, India

ARTICLE INFO

Article history:
Received 1 October 2016
Revised 13 March 2017
Accepted 13 March 2017

Keywords:
Authentication
Batch message dispatch
DoS attack
Key generation
Security
3PAKE
Value added services
VANETs

ABSTRACT

An authentication scheme is inevitable for providing secured communication in high-speed networks like Vehicular Ad-hoc Networks (VANETs), where node speed varies between 10 and 40 m/s. The existing authentication schemes providing value-added services in VANETs face many issues such as invalid service requests, Denial of Service (DoS) attacks, verification failures, high transmission overhead and high verification delay. To deal with the exiting issues, an Extended Three Party Password based Authenticated Key Exchange (E-3PAKE) scheme is proposed in the paper. The E-3PAKE has priority based application services that addresses the security and performance issues in existing schemes. The scheme renders a server-client authentication process and batch message dispatch to improve the efficiency of value-added services. The formal analysis done ensures the security enhancement of the scheme and the simulation results prove that the proposed scheme outperforms the existing schemes with respect to transmission overhead, verification and service response delay.

1. Introduction

The Vehicular Ad-hoc Networks (VANETs) are mobile networks consisting of high speed vehicles that can communicate with each other using the built-in wireless interfaces. The Road Side Units (RSUs) acting as intersections for the communication of packets in vehicular nodes are installed at critical points of roads such as traffic intersections, fire stations, etc. to collect and exchange packets for service deliveries. The vehicles out of radio range are communicated through multi-hop communications. The vehicles in networks move at high speed varying between 10 m/s and 40 m/s and RSUs collect the packets from these mobile nodes. The vehicles in VANETs use Dedicated Short Range Communication (DSRC) protocol for their communication with RSUs and other vehicles.

The VANETs ensures road safety by improving the driving experience with safety related applications. The On-Board Units (OBUs) equipped in the vehicles send periodic messages related to traffic updates such as the position, traffic events, speed, direction, current time and acceleration/deceleration. This information exchanges between OBUs and RSUs provides better understanding of the traffic pattern on the road. The value added services are also offered by the VANETs, which are called as non-safety applications. They include services such as Internet access, gaming applications, on-line messenger, news updates, media program streaming, advertisements, etc.

[☆] Reviews processed and recommended for publication to the Editor-in-Chief by Associate Editor Dr. R. Varatharajan.

[*] Corresponding author.
E-mail addresses: muthumeenakshi83@gmail.com (R. Muthumeenakshi), reshmi.tr@vit.ac.in (T.R. Reshmi), murugan@annauniv.edu (K. Murugan).

http://dx.doi.org/10.1016/j.compeleceng.2017.03.011

With the advancement of safety and non-safety applications in VANETs, there emerge several privacy and security challenges that disrupt the proper functioning of the networks. Hence, before providing the service to value added service requests, there is a need to check the identity of the user to ensure authentication and data integrity in the networks. Moreover the private information provided by the users such as a user identity and user location should be preserved confidentially to ensure privacy. Even though, several studies [1,2] addresses the afore-said privacy and security issues, a new authentication scheme is necessary in VANETs for providing value-added services by authenticating the user requests. The RSUs acting as intersection for message/packets from server simultaneously serve as the authentication server. This eventually results in bottleneck problem and paves way to DoS attacks. Hence it is very difficult to ensure efficient and secure value-added services with the existing schemes.

The E-3PAKE is an extended Three Party Password based Authenticated Key Exchange (3PAKE) scheme to overcome the Denial of Service (DoS) attacks by including an additional verification phase. The proposed E-3PAKE addresses the issues in existing schemes and also improves the efficiency in service deliveries with a batch message dispatch method. Following the introduction the paper is presented as given. The Section 2 briefs on the literature survey; Section 3 explains the proposed scheme with design objectives, architecture and its modules. The Section 4 demonstrates the results and analysis and finally the Section 5 gives the conclusions and discusses the future works.

2. Related works

The VANETs uses information exchanged through OBUs equipped with each vehicles for requesting service applications. To provide a better driving experience the periodic information related to traffic such as traffic events, speed, direction, acceleration, current time and position are periodically sent by the OBUs. In VANETs each and every node (vehicle) establishes communication for accessing services from other nodes or internet. The authentication of session keys and establishment of connections between OBUs and RSUs are very important to overcome the security issues in service applications. Based on the survey [3], the VANETs are more exposed to the DoS attacks due to limitations in the existing authentication schemes.

There are several message authentication schemes proposed to overcome the threats in service deliveries. These methods are not robust and hence pave way to security attacks. In [3], the authors presented a new authentication scheme to improve the security in vehicles and service provider communication. The scheme called as ABAKA is a value-added service in VANETs which authenticate many requests using batch authentication method. It uses a single verification operation and generates session keys based on Elliptic Curve Cryptography (ECC). These keys are distributed to the vehicle using broadcast messages. The scheme suffers excessive transmission overhead due to the broadcast messages and is proven to face DoS attacks. The scheme also faces more delay in group authentication. A new identity method using the anonymous public key generation and Public Key Infrastructure (PKI) is proposed in [4]. The public key certificate introduces more communication overhead and key management issues causing more storage constraints. A scheme for allowing the vehicles to distribute the messages to all vehicles through multi-hop communication is proposed in [5]. These messages are signed and verified for authentication. The characteristics of vehicle are not revealed for satisfying the privacy requirements. A software oriented solution is used to generate the signature, and bloom filter technique and binary search method are used for message verification. Although the scheme induced low communication overhead and was used for verifying the group requests in VANETs, the scheme was not robust. The proposal of the work in [6] to support authentication and key establishment in vehicle and service provider communication uses a blind signature technique. The technique uses a randomly generated signature and allows the vehicles to access the service provided by roadside infrastructure. The authors in [7] acknowledged that the existing PKI security methods are not appropriate for VANETs application and proposed an authentication scheme which authenticates messages within intra and inter RSU and supported handoff between RSUs. The method uses a hierarchical method that causes computational and communication overhead.

The Authenticated Key Exchange (AKE) protocol is responsible for authenticating the users with each other and also establishes the secret session keys which protect their subsequent communication. A type of AKE protocol called Password based Authenticated Key Exchange (PAKE) where more than one user with an easy and low-entropy password, high-entropy secret session key, and a weak key tries to authenticate the nodes. The two party setting (2PAKE) protocol is most suitable for the Client-Server architecture. However, it is not convenient to use these protocols in very large scale client-to-client communication environments. As each client requires password for peer to peer communication, it consumes excess client memory. To overcome these problems, the 3PAKE [8] was proposed. The trusted server of 3PAKE acts as a mediator between the communicating nodes and each client node needs only one password to authenticate it to the authentication server. There were many security flaws identified in the 3PAKE and to make the scheme more secured and practicable, many modifications are proposed and awaiting standardization.

In this paper, we limit our focus to 3PAKE [8] protocol. This scheme neither requires the server public keys nor symmetric cryptosystems for authentication. However, the work in [9,,10] proved that 3PAKE protocol is efficient but suffers security threats. And also, the authors in [11] demonstrated the share attack on 3PAKE protocol. These conclusions on 3PAKE paved way to the improved 3PAKE protocol using server based public key exchanges [12]. But the scheme generated more overhead packets and hence it initiated the design of a new 3PAKE protocol [13] for reducing the communication overhead packets without using the public keys. To overcome many of the proven threats the improved schemes working on server public keys were proposed in [14,15]. An efficient authentication scheme based on verifiers for resisting the dictionary attacks