Computers and Electrical Engineering 000 (2018) 1–18

Contents lists available at ScienceDirect

Computers and Electrical Engineering

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

Extending security horizon through identification authentication and tracking services in hierarchical vehicular networks☆

Atanu Mondal[a,*], Sulata Mitra[b]

[a] Department of Computer Science and Electronics, Ramakrishna Mission Vidyamandira, Howrah, India
[b] Department of Computer Science and Technology, Indian Institute of Engineering Science and Technology, Shibpur, India

ARTICLE INFO

Article history:
Received 14 March 2016
Revised 4 January 2018
Accepted 16 January 2018
Available online xxx

Keywords:
VANET
Identification
Authentication
VIN
Centralized
Distributed

ABSTRACT

The inter-vehicle communication in vehicular ad hoc network must be protected from unauthorized message injection and message alteration of unauthentic vehicles. A lightweight scheme for identification, authentication and tracking of vehicles in hierarchical vehicular ad hoc network is proposed in the present work. This work aims to preserve the basic security features such as authentication, confidentiality, and integrity in presence of attackers whose operational capability is in between mote-class attacker and laptop class attacker. In the present scheme the communication among the different levels of the hierarchical vehicular ad hoc network is in encrypted form to protect the network from the access of attackers. The performance of the scheme is evaluated qualitatively and quantitatively. Both the qualitative and quantitative performance of the proposed scheme is compared with the existing schemes.

1. Introduction

The vehicular ad hoc network (VANET) allows inter-vehicle communication for improving road traffic safety. The vehicles in VANET can effectively guide and supervise other vehicles to provide secure and reliable information services. But the adversaries may misuse the resource by generating and communicating message with other vehicles. The unauthentic vehicles may jeopardize the safety of other vehicles, drivers, passengers as well as efficiency of the transportation system by generating false message like to clear the road for selfish reason. Hence identification and authentication of vehicles are essential to protect VANET from unauthorized message injection and message alteration. It is also essential to track the vehicles at various check points within a boundary or premises in high mobility VANET to manage the security and safety of vehicles in case of theft or any unwanted incident.

In this work a secured vehicle identification, authentication and tracking scheme is proposed. It is an extension of the previous works [1,2]. Both the schemes [1,2] consider hierarchical VANET. The hierarchical VANET can track and also can provide service to a lot of high velocity vehicles due to its increased coverage area. A centralized scheme for the identification, authentication and tracking of a vehicle using vehicle identification number (VIN) [3] is proposed in [1]. The centralized scheme is implemented in a centralized hierarchical VANET in which the certifying authority (CA) is at the root level, base

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Area Editor Dr. G. Martinez Perez.

* Corresponding author.
E-mail addresses: atanumondal@vidyamandira.ac.in (A. Mondal), sulata@cs.iiests.ac.in (S. Mitra).

https://doi.org/10.1016/j.compeleceng.2018.01.020
0045-7906/

Table 1

Schemes	[1]	M_1	[16]	[17]
$COMM\_OH_v$ (bit)	888	4606	6144	23,760
STO_OH_v (bit)	888	3918	16,170	67,152
$COMP\_OH_v$ (cc)	84,362	84,407	87,235	86,214

stations (BSs) are at the intermediate level and vehicles are at the leaf level. But this centralized scheme provides service to a fixed number of vehicles like other existing centralized schemes (discussed in Section 2). Moreover due to high velocity a vehicle may go out of the coverage area of such centralized VANET. Hence the proposed centralized scheme [1] is extended in a distributed scheme [2] for accommodating more vehicles in VANET. The distributed scheme [2] is implemented in a distributed hierarchical VANET in which CA is at the root level (R_CA) and also at the first level (F_CA), BSs are at the second level and vehicles are at the leaf level. The F_CAs in the first level of the hierarchy increase the coverage area of VANET which in turn helps to accommodate more vehicles in [2] than [1].

But the communication channel between the different levels of the hierarchy is not secure in both the schemes [1,2]. An attacker can access the message by sensing such insecure channel. Hence the existing schemes [1,2] are modified in the present work to ensure security of the communication channel among the different levels of the hierarchy. M_1 is the modified version of [1] and M_2 is the modified version of [2]. The list of parameter is mentioned in APPENDIX. The present work is a lightweight security scheme as it uses symmetric key cryptography. The secret key of symmetric key cryptography is shared among the communicating nodes in encrypted form. It needs less complex computation than public key cryptography and hence it is suitable for a high mobility network like VANET. Moreover it needs less communication, computation and storage overhead than existing schemes as shown in Table 1. It deals with securing the network at every step of communication within the network. The qualitative performance of M_1 and M_2 is measured in terms of security analysis and overhead analysis. The quantitative performance of M_1 and M_2 is also studied through simulation taking VIN processing time per vehicle per BS, percentage of authentic vehicles per BS, packet loss per BS, service block per BS and rate of tracking of vehicles per BS as performance metrics. Both qualitative performance and quantitative performance are compared with the existing schemes and [1,2].The security analysis shows that the cracking of data by the attacker is of no use in the present work. The overhead analysis shows the significant improvement of the present work in terms of communication, computation and storage overheads over the existing schemes. The results of simulation experiment show the improved performance of the present work in terms of the minimization of authentication delay and packet loss with minimum block of service at a BS. The authentication delay is measured using the parameter VIN processing time.

The rest of the paper is organized as follows. Section 2 deals with related works. In Section 3 network and system assumptions are described in details. The present work is elaborated in Section 4. Performance analysis of the present work along with a detailed comparative study is done in Section 5. Section 6 concludes the work and also highlights the future scope of the work.

2. Related work

Several vehicle authentication schemes have been reported so far for centralized VANET. A 3-tier architecture having trusted authority at the root level, road side unit (RSU) at the intermediate level and on board unit (OBU) at the leaf level is proposed in [4]. The trusted authority issues a token to each authentic OBU within its coverage area. Each OBU sends this token along with the message to its parent RSU. The RSU verifies the authentication of the received token. If the received token is authentic the RSU issues another token that contains safety message signature and a valid time period to the OBU. Now the OBU can broadcast the message to other OBUs using this safety message signature during the valid time period. The OBU leaves the safety message signature after moving into the coverage area of a new RSU. But the method of verifying the authentication of RSUs and OBUs by the trusted authority is not mentioned. The assignment of a new safety message signature by the RSU to all the OBUs within its coverage area incurs extra computation and communication overhead. Moreover the performance of the proposed scheme is not studied by increasing the number of OBUs within the coverage area of the RSU continuously. A pseudonymous authentication based conditional privacy protocol is proposed in [5] for vehicular authentication. In this protocol the vehicles register themselves with trusted motor vehicle department using its identity such as vehicle's license plate number; owner's address etc. and get a ticket or signature. The vehicle uses this ticket to obtain token from the neighbour vehicles. The token is used by the vehicle to generate pseudonyms for anonymous message broadcasting. The sender vehicle broadcasts its pseudonym to its neighbours during anonymous communication. The receiver vehicle uses this pseudonym to encrypt their message before transmission. But the attacker can also receive the pseudonym which is broadcasted by the sender vehicle and can jeopardize the security of the VANET. A proxy based authentication scheme is proposed in [6]. Each vehicle is equipped with a tamper proof device. The device has three preloaded secret master keys. Each vehicle uses the secret keys to generate its identification and privacy key. Each vehicle also transmits the identification and privacy key to its parent RSU. The RSU uses the privacy key as the verifier of the identification. The vehicle is authentic if the verification of its identification is successful. But the authentication of a vehicle is verified using a new identification and privacy key when it enters into the coverage area of a new RSU which incurs extra communication and

Please cite this article as: A. Mondal, S. Mitra, Extending security horizon through identification authentication and tracking services in hierarchical vehicular networks, Computers and Electrical Engineering (2018), https://doi.org/10.1016/j.compeleceng.2018.01.020