Journal of Computer and System Sciences 81 (2015) 1042–1058

Contents lists available at ScienceDirect

Journal of Computer and System Sciences

www.elsevier.com/locate/jcss

An intelligent approach for building a secure decentralized public key infrastructure in VANET

Neeraj Kumar [a,*], Rahat Iqbal [b], Sudip Misra [c], Joel J.P.C. Rodrigues [d,e]

[a] Department of Computer Science and Engineering, Thapar University, Patiala (Punjab), India
[b] Department of Computing and Digitial Environment, Coventry University, Coventry, UK
[c] School of Information Technology, Indian Institute of Technology, Kharagpur (West Bengal), India
[d] Instituto de Telecomunicações, University of Beira Interior, Portugal
[e] ITMO University, St. Petersburg, Russia

ARTICLE INFO

Article history:
Received 14 May 2014
Received in revised form 9 August 2014
Accepted 5 September 2014
Available online 19 December 2014

Keywords:
Vehicular Ad Hoc networks
Learning Automata
Security
Bayesian Coalition Game

ABSTRACT

This paper proposed an efficient decentralized public key infrastructure (PKI) using the concepts of Bayesian Coalition Game (BCG) and Learning Automata (LA). LA are assumed as the players in the game, which coordinate among one another for information sharing. To preserve the confidentiality and integrity of the messages, dynamic coalition among the players of the game is formulated using symmetric key encryption and hash-based message authentication. Also, privacy preservation and certificate revocation are included in the proposed scheme to defend against the misbehaving vehicles. For each action taken by an automaton, its action may be rewarded/penalized by the environment in which it operates. LA update their actions probability matrices by getting the reinforcement signal from the environment. The performance of the proposed scheme is evaluated with respect to various metrics in comparison to the other state-of-the-art existing schemes. The results obtained prove the superiority of the proposed scheme.

1. Introduction

Vehicular Ad Hoc Networks (VANET) have emerged as a new powerful technology due to its usage for applications in intelligent transportation systems (ITS), surveillance systems, and safety alerts on the road [1–3]. Vehicles on the road communicate with one another with/without the existing infrastructure support. Modern vehicles may contain some specialized units such as On Board Units (OBUs), and Application Units (AUs). These units can be used for communication with the nearest Road Side Units (RSUs) which provide infrastructure support to the moving vehicles. The communication between OBUs and AUs is performed by utilizing OBUs communication capabilities, where an AU can communicate with an OBU using wired/wireless technology, while OBUs communicate with RSUs using wireless standards such as IEEE 802.11p/WAVE or 802.11 a/ b/g. [1–3].

Vehicles in VANETs generally have OBUs installed on board of the vehicles, which can be used for providing communication among other OBUs or with RSUs. Moreover, OBUs also provide communication with AUs. OBUs are used for congestion control, IP mobility management, data collection, and processing [1–3]. RSUs are deployed as fixed units alongside the road

* Corresponding author.
E-mail addresses: neeraj.kumar@thapar.edu (N. Kumar), r.iqbal@coventry.ac.uk (R. Iqbal), smisra@sit.iitkgp.ernet.in (S. Misra), joeljr@ieee.org (J.J.P.C. Rodrigues).

http://dx.doi.org/10.1016/j.jcss.2014.12.016
0022-0000/

in an optimized manner so as to preserve the coverage and connectivity to all the vehicles. These can provide communication to the vehicles using Dedicated Short Range Communication (DSRC) with IEEE 802.11p/WAVE standards [1–5].

As vehicles are widely used for dissemination of safety related information to users, so any change or alteration in disseminated information by any misbehaving node can be a threat to secure data dissemination to other vehicles in VANETs. To avoid such incidents, a strong PKI needs to be developed in which certificates are issued to the communication parties for a particular duration only. If any misbehavior is observed from any node in the network, then the issued certificate is revoked and Certificate Revocation List (CRL) is constructed for all such nodes [6]. For efficient operation of PKI in VANETs, CRLs need to be updated continuously. But due to high mobility and temporary certificates with vehicles called as pseudonyms, creation and maintenance of dynamic CRLs is also another challenging task in this environment [6].

There exist many solutions in the literature for managing the key revocation process in PKI infrastructure [7–9]. In these solutions, authors have either used short lived certificates or compressed CRLs, but these strategies may generate large overhead due to the maintenance of CRLs at different locations and verifying each generated certificate. To reduce load, some techniques [10–12] also exist which circulate the status of certificate to vehicles at regular intervals. Certificate revocation in these schemes was constantly updated using caching/hashing-based techniques.

Keeping in view of all the above issues and challenges, in this paper, we propose a new efficient decentralized PKI infrastructure in VANETs using the concepts of BCG and LA. Following are the contributions in this paper. A new LA and BCG based certificate revocation scheme is proposed for the construction of decentralized PKI infrastructure. Message authentication and confidentiality among the players of the game is preserved by the construction of hash chain-based Merkle tree. Each player in the coalition game decides its action (move forward, stay in the current position, or move backward) according to the feedback received from the environment and updates its action probability vector.

The rest of this paper is organized as follows. Existing related works are briefly reviewed in Section 2. Section 3 discusses the background and preliminaries about LA and BCG. Section 4 illustrates the network model and problem formulation. Section 5 describes the proposed approach in detail. Section 6 provides the performance analysis of the proposed scheme. Finally, Section 7 concludes the paper with future insights.

2. Related works

Carlos et al. [6] proposed privacy preserving mechanism with certificate revocation in VANETs. The proposed scheme in addition to preserving the user's identity also maintains the confidentiality and unforgeability about the certificate status issued to the vehicles. The performance of the proposed scheme was found better than the other schemes of its category. Plobl et al. [13] proposed a privacy-aware secure infrastructure for VANETs. Authors proposed symmetric and asymmetric based cryptographic solution for preserving the user's privacy. The scheme was efficient in comparison to other schemes with respect to computation complexity and bandwidth requirements. Daeinabi et al. [14] proposed advanced security scheme based on clustering and key distribution in VANETs. Vehicles are divided in to different clusters in the proposed scheme and cluster heads are elected based upon the trusty nodes. Authors have used proxy blind signature, hash message authentication and symmetric key encryption to secure end-to-end communication. Raya et al. [15] proposed a new technique in which authors have used anonymous certificates to hide the identity of the users, but the scheme had large storage overhead, as many key pairs are required for storage of keys. Wasef et al. [16] proposed a novel signature and certificate verification scheme for VANETs. In this scheme, vehicles simultaneously sign and verify the certificates issued to them, but this scheme generates large overhead, as multiple operations such as signing and verification are to be executed simultaneously.

Lu et al. [17] proposed an efficient privacy preservation scheme in which vehicles get the certificates from the nearest RSUs. Vehicles again contact nearest RSUs as soon as the old certificates expire. Zhang et al. [18] proposed an efficient RSU-based message authentication scheme for moving vehicles, but this scheme has disadvantage because if some of the RSU are collapsed, then whole authentication process would be destroyed. Zhang et al. [19] proposed a new authentication protocol for providing secure communication in VANETs. The authors have divided the vehicles in different zones with each zone was managed by one of the vehicles which may act as a cluster head node. Group signature scheme is used to reduce the complexity of authentication in this scheme.

Hao et al. [20] proposed a distribution framework using efficient key distribution for secure message authentication in VANETs. In this scheme, RSUs are assumed to be trusted as key distribution servers which are used to control the authenticated message transfer between vehicles and RSUs. Wasef et al. [21] proposed an efficient mechanism for certificate revocation in VANETs. The proposed scheme is quite effective in detecting misbehaving nodes and can be integrated with any existing PKI infrastructure. Wu et al. [22] proposed an efficient mechanism for secure V2V communication. Using the group signature [22] and ID-based signature [23] schemes, authors designed conditional privacy preserving scheme for VANETs. All the vehicles communications are authenticated using a single centralized authority with a group signature. Li et al. [24] proposed an efficient and secure communication scheme with key establishment in VANETs, but this scheme may not be applicable to generate safety alerts generated in VANETs.

As a computational intelligence technique, BCG and LA are used for taking adaptive decisions in various applications, e.g., LA select their optimal action based on past experiences from the given environment. This technique has been recently adopted to wireless communication networking areas and applied to solve various issues such as – call admission control