Vehicular Communications 13 (2018) 1–12

Contents lists available at ScienceDirect

Vehicular Communications

www.elsevier.com/locate/vehcom

Adaptive trust and privacy management framework for vehicular networks

Thi Ngoc Diep Pham *, Chai Kiat Yeo

School of Computer Science and Engineering, Nanyang Technological University, Singapore

ARTICLE INFO

Article history:
Received 23 October 2017
Received in revised form 14 January 2018
Accepted 13 April 2018
Available online 21 April 2018

Keywords:
VANET
Trust
Privacy
Private Set Intersection
Pseudonym

ABSTRACT

By allowing vehicles to communicate on the roads, vehicular network is becoming a potential solution to improve the traffic safety. Both trust management and privacy protection play critical roles in vehicular network but there needs to be a trade-off between them. Existing works only focus on each issue separately or have not provided a satisfactory solution to both issues. In this paper, we propose a secure and flexible framework for vehicles to manage both trust and privacy. First, we design ALRS – a secure linkability scheme to enable vehicles to recognize either identities or trust levels of other vehicles despite them updating the pseudonyms to protect privacy. The linkability information is kept confidential from external attackers and unauthorized internal nodes using encryption and private set intersection technique. Besides, the linkability can be revoked easily to prevent nodes from being traced by other internal nodes. Second, we design ATMS – a context-aware trust management scheme that allows nodes to evaluate the trustworthiness of received events by considering the entity reputations of the senders. Under the context of privacy, obtaining the entity trust value is challenging. To overcome the challenge, we utilize the linkability information in ALRS and design a decision tree that estimates the entity trust adaptively to the available linkability information. Simulation results demonstrate that our framework helps nodes to simultaneously make accurate decisions towards the data and preserve their privacy in a flexible way.

1. Introduction

Industry and academic research have developed vehicular ad hoc network (VANET) [1,2] to make the traffic safer, more efficient and more convenient. In VANET, vehicles are equipped with on-board units that provide them with computation and communication capabilities. Thus vehicles can send and receive messages with one another and with VANET infrastructure devices at the roadside, thereby enabling various vehicular applications for road safety [3–6], driver assistance and infotainment [7–10]. For example, in cooperative collision warning application [3], vehicles that are aware of road accidents can disseminate the warnings to other vehicles in the vicinity so that they can take actions in advance and avoid the danger.

VANET can only improve the traffic safety if the propagated warnings are assured to be trustworthy. For example, a malicious driver may report a non-existing collision to make the vehicles behind react by braking abruptly, which could possibly cause a chain collision among these vehicles. To deal with such fraudulent messages, drivers need to evaluate the trustworthiness of the entities that send/relay data and the credibility of the data before deciding to believe in them. From now on, we use the term malicious vehicle to indicate the malicious driver, with assumption that each vehicle is attached to a driver for simplification.

While vehicles may enjoy the benefits of VANET applications, they also expose themselves to the threat of location privacy when they cooperate to propagate the messages. Attackers can eavesdrop their messages and infer their location histories for unauthorized tracking. Without privacy-protection schemes, vehicles may be deterred from joining VANET, making it hard to deploy VANET in reality.

Researchers have proposed a number of trust management schemes in VANET. Vehicles evaluate the credibility of the received data by objectively verifying the data against practical and intuitive models [11–16] or fusing the peers' opinion towards the data in consideration of the peers' reputations [17–22]. Existing studies on privacy in VANET suggest vehicles use pseudonyms [23–27] or group signatures [28–30] that are uncorrelated to their real identities to enable them to stay anonymous and authenticated. Unfortunately, these works only handle either trust or privacy without considering both issues jointly.

* Corresponding author.
E-mail address: pham0069@e.ntu.edu.sg (T.N.D. Pham).

https://doi.org/10.1016/j.vehcom.2018.04.006
2214-2096/

Though trust and privacy are both important, there is a trade-off between them. When vehicles change pseudonyms over time to protect privacy, they cannot recognize one another, making it hard to build peer trust. When a node changes pseudonym frequently, other nodes will have insufficient observations of its behaviors to evaluate the entity trust accurately. However, low frequency of pseudonym change allows external eavesdroppers to track vehicles more easily. To enable both trust management and privacy enhancement, [35] proposes a protocol that allows a node to temporarily track a neighbor to update the trust despite the use of pseudonyms. However, the proposal requires vehicles to reveal their identities in plain text to request for tracking. The leakage of this private information enables adversaries to trace the nodes' locations and threaten their privacy.

In this paper, we would like to address the trade-off between trust and privacy in VANET. Our goal is to mitigate the trade-off by enabling vehicles to manage and balance privacy and trust in a flexible manner. Our approach is to adopt pseudonyms for privacy protection but simultaneously letting legitimate vehicles recognize one another to support the entity and data trust management. We propose a trust-privacy framework including two components: Adaptive Linkability and Recognition Scheme (ALRS) and Adaptive Trust Management Scheme (ATMS). ALRS is designed to allow vehicles to grant or revoke selective nodes with the ability to recognize them by identity or trust level. By managing the recognition grant, vehicles can protect their privacy adaptively according to the context, i.e. either hiding identity or trust level when privacy is prioritized or revealing identity when trust management is required. ATMS is designed to utilize the granted recognition information to allow vehicles to verify the data sent by other nodes and update their reputations.

The main challenge to design ALRS is providing flexible recognition in a secure and private manner. Having vehicles exchange their identities when they encounter one another is a simple and straightforward solution to let them recognize one another. However, this process cannot support the selective recognition and the recognition by trust level. To resolve this issue, we suggest that a pair of vehicles confidentially exchange their identities and agree on a shared link value when they first meet. Thereafter, they rely on link values to recognize each other and to grant/revoke the recognizability to selected nodes. Specifically, a vehicle can recognize a peer's identity by determining the intersection between their lists of link values. It can recognize if a peer is trusted by determining if there is any common item between the peer's list of link values and its list of values linked to the trustworthy nodes. The vehicle can easily switch between allowing and disallowing a peer to recognize it by including or excluding the shared link value from its list. To protect the private lists of link values in intersection operations, we propose using Private Set Intersection (PSI) and Private Set Intersection Cardinality (PSI-CA) protocols.

We also design ATMS to support adaptive trust management under the privacy context set by ALRS. A vehicle *adapts* the approach to evaluate event data based on its distance to the data originator. Specifically, if the distance is near enough, it can verify the event by directly observing if the movement response of the data originator is consistent with the event. Otherwise, it can collect different event reports and aggregate them in consideration of its trusts towards the data originators, which may not be obtainable directly under the privacy context. Thus the vehicle needs to *adapt* the entity trust setting based on the linkability level granted by other nodes in ALRS. To achieve this, we design a decision tree for vehicles to derive the entity trust value from the available linkability information.

We simulate VANET scenarios to evaluate ATMS's performance under different settings of recognition enabled in ALRS. The simulation results show that our framework achieves high rate of accurate node's decision towards the reported event data and high detection rate of malicious nodes which deliberately report the wrong events. It also proves that trust recognition helps to improve the decision performance, thus allowing nodes to balance between privacy and trust management.

The rest of the paper is organized as follows. In Section 2, we define our security and privacy goals and present the basic idea of how to achieve them. Section 3 reviews the PSI/PSI-CA techniques used in ALRS. In Sections 4 and 5, we describe the details of ALRS and ATMS respectively. Section 6 evaluates our framework's performance and overhead. Section 7 summarizes the existing works on privacy and trust management in VANET. Section 8 concludes the paper.

2. Overview

2.1. Network model

We assume that VANET uses identity-based cryptography (IBC) system to provide authentication, encryption and privacy to the vehicles. In IBC, a trusted third party, called the Private Key Generator (PKG), is responsible for generating the private keys for nodes from their distinct identities. First, PKG publishes the master public key to the network but keeps the corresponding master private key. Any node can compute the public key corresponding to an identity based on the master public key and the identity value. However, only the node owning that identity can obtain the corresponding private key by requesting PKG, which uses the master private key to generate the private key for the identity.

Given a node A, denote its identity, the corresponding public key and private key as ID_A, P_A and S_A respectively. For the authentication service, node A signs the message with its private key S_A and attaches its identity ID_A with the message. Other nodes verify the signature with the public key P_A that can be computed from ID_A. For the encryption service, other nodes encrypt the message with A's public key P_A so that only node A can decrypt to read the message using its private key S_A.

When a node uses the same identity all the time, its privacy is leaked to the eavesdroppers that correlate the identities to the locations. To protect nodes' privacy, we adopt IBC pseudonym [26, 27] which is a pair of pseudo-identity and corresponding private key where pseudo-identity is a random value. Thus, different pseudonyms are uncorrelated to one another and uncorrelated to the real identity and nodes can avoid being traced when changing pseudonyms over time. PKG is in charge of issuing multiple pseudonyms to each node for use in the future. The node stores these pseudonyms and uses one of them at a time for authentication and encryption purposes. To further enhance privacy, nodes can incorporate existing strategies such as [31–34] which propose proper locations and times for nodes to change pseudonyms.

Each node maintains a local reputation list of nodes it has encountered and the corresponding trust values. The trust value is quantified as a number in the range of [0, 1]. 0 means no trust and 1 means total trust. Denote TR_{AB} as the trust value of A towards B recorded in A's local reputation system. When two nodes A and B first meet, they set the initial trust to each other with the value TR_{init}. If the trust value TR_{AB} drops below a threshold TH_{evil}, A considers B as malicious and isolates B by not sending or receiving any message from B.

2.2. Problem statement

When nodes use pseudonyms for privacy purposes, they cannot recognize each other, rendering it impossible to make use of entity trust. Our goal is balancing between trust and privacy by designing a secure linkability scheme to enable legitimate nodes