Chapter 11
Mechanism for Privacy Preservation in VANETs

Brijesh K. Chaurasia  
Indian Institute of Information Technology, India

Shekhar Verma  
Indian Institute of Information Technology, India

G. S. Tomar  
Malwa Institute of Technology and Management, India

ABSTRACT
This paper proposes a mechanism for sustaining privacy of a vehicle in a vehicular ad hoc network (VANET) through pseudonym update. In a VANET, vehicles on the road are involved in dissemination of information as they move. An association can be formed between the physical location of the source vehicle and the transmitted messages. This relationship between the physical vehicle and its identity can breach its privacy. In this work, a strategy for optimal pseudonym update for maximizing privacy has been formulated when a vehicle is being observed by adversaries with different capabilities. Results indicate that updating pseudonyms in accordance to the strategy maximizes the privacy of a vehicle in the given situation.

INTRODUCTION
A vehicular ad-hoc network (VANET) is a network of vehicles supported by fixed infrastructure. The vehicular networks are characterized by a highly dynamic topology with vehicles moving in restricted geographical strait jackets (roads). The vehicles exchange information via vehicle to vehicle and vehicle to road side infrastructure in both manners. The road side infrastructure acts as access points in vehicular communication are known as road side unit (RSU). A vehicle is equipped with on board unit (OBU). RSU are located along the roads at certain points. A bandwidth of 75 MHz has been allocated in the 5.850-5.925 GHz band for communication in such networks (Raya & Hubaux, 2005). In a VANET, an adversary can find the identity of the vehicle from message contents and to some extent its position through localization based on signal...
Mechanism for Privacy Preservation in VANETs

strength etc. (Raya & Hubaux, 2007; Dotzer, 2005). Over a time period, the physical vehicle and its communication identity can be related (Raya & Hubaux, 2005; Papadimitratos et al., 2007) to breach the location privacy of the user. This link can be used to disclose personal data of a user and would potentially dissuade a user from joining a VANET (Raya & Hubaux, 2007).

To obtain and sustain anonymity, a temporal identity, pseudonym, is used for communication. Pseudonyms allow a vehicle to interact with other vehicles anonymously. Pseudonyms are ephemeral and distinct pseudonyms hide their relation from each other and to the user’s identity (Pfitzmann & Hansen, 2004). To preserve privacy, a pseudonym system must prevent credential forgeability and disallow usage of false pseudonym by a user. Moreover, the transaction of obtaining and the process of switching pseudonyms should not reveal the identity of the user or link pseudonyms to each other. Continually changing pseudonyms conceal the real identity of a vehicle by de-linking the source of signals to its original identity (Gerlach & Guttler, 2007). But, the relation between a communicating vehicle and its estimated location can reveal the identity of a vehicle. This vehicle can, then, be physically traced and switching pseudonyms would be meaningless (Sha et al., 2006). A vehicle can be under sustained observation and transmissions at different intervals of time with the same pseudonym can reveal the relation between physical vehicle and its current pseudonym if the vehicle is relatively isolated in a crowd. This relation can be established even when pseudonyms are updated when the time interval between transmission prior to and after the update is short (Sampigethaya et al., 2007). There is, moreover, one more challenge that needs to be addressed. When a vehicle under observation moves from one cluster and enters another cluster and changes its pseudonym, it can be spotted with high probability as soon as it transmits. This can happen if the number of vehicles from the previous cluster to the current cluster is small and the pseudonyms of vehicles belonging to current cluster are known a priori. The anonymity of the vehicle under observation is limited by the number of vehicles that join the current cluster from the previous cluster Sun (Zhang & Fang, 2007; Fonseca, 2007).

PROBLEM DESCRIPTION

A link between the personal interests of a user with physical locations of a vehicle can breach the location privacy and reveal the identity. In this mobile broadcast environment, a vehicle’s privacy can be sustained through unobservability (Claub & Schiffner, 2006). A vehicle would be unobservable if its communication can be distinguished from others in the group. The effective crowd that hides the vehicle is a function of the capabilities of the attacker, the actual size of the crowd and the unlinkability of the messages emanating from the crowd (Gerlach & Guttler, 2007). The size of the crowd is the number of vehicles in the anonymity zone $Z$. The position of a vehicle cannot be predicted accurately from its transmission (Sampigethaya et al., 2007). To avoid breach of privacy, a vehicle using pseudonyms and continuously updates it. The problem is that even a large pseudonym pool would be depleted quickly if every transmission uses a separate pseudonym. This requires a strategy for update for conservation of this pseudonym pool.

Anonymity Metrics

The level of anonymity of a vehicle is the inability of the adversary to pinpoint a vehicle as the source of the communication in the set of vehicles $V$ (anonymity set) in the region estimated from the communication. This anonymity set $V \subseteq V_{\text{total}}$ with $V_{\text{total}}$ being the total number of vehicles in $Z$. The cardinality of the anonymity set is the measure of the anonymity of a vehicle in the set.