Chapter 7
Misbehavior Detection in VANET: A Survey

Shefali Jain
Dhirubhai Ambani Institute of Information and Communication Technology, India

Anish Mathuria
Dhirubhai Ambani Institute of Information and Communication Technology, India

Manik Lal Das
Dhirubhai Ambani Institute of Information and Communication Technology, India

ABSTRACT

Vehicular Networks (VANETs) have received increased attention from researchers in recent years. VANETs facilitate various safety measures that help in controlling traffic and saving human lives. As VANETs consist of multiple entities, effective measures for VANET safety are to be addressed as per requirement. In this chapter, the authors review some existing schemes proposed for misbehavior detection. They categorize the schemes into two parts: data centric and non-data centric misbehaving detection. In data-centric misbehaving detection, the receiver believes the information rather than the source of the information. The authors compare schemes in each category with respect to their security strengths and weaknesses. The comparative results show that most of the schemes fail to address required security attributes that are essential for VANET safety.

INTRODUCTION

Vehicular ad-hoc networks (VANETs) allow vehicles to exchange information for human safety and convenience. VANETs consist of multiple entities such as vehicles (e.g. cars, trucks, and buses), on-board units (OBUs), road side units (RSUs) and a Trusted Authority (TA). The TA acts as the root of the VANET safety architecture. On-board units (OBUs) installed on vehicles which allow vehicles to communicate with other entities (e.g., vehicles, RSUs). OBU also has capability of storing information and verifying incoming messages. Road side units (RSUs) are typically

DOI: 10.4018/978-1-4666-4691-9.ch007

fixed infrastructure, installed in some designated places of roads. OBUs regularly broadcast safety related messages useful in gaining information of current traffic situation, which enables receiving vehicle to take early action for any abnormal situation like road blocks or accidents. Typically, whenever a potential warning message for road condition is detected by the OBU, it generates an appropriate message and disseminates the same to its neighbours. For example, consider a scenario where the attacker (misbehaving vehicle) attempts to either prevent other vehicles from taking some road segment or indirectly suggest an alternative one. In such a situation, the attacker can create a false traffic-jam warning message for the identified route and disseminate the message in bulk. As a result, vehicles who have received that message from the attacker will be misguided and chose a longer path than the actual ones.

VANETs and MANETs (mobile ad-hoc networks) share many common characteristics, but they also have some differences. The main differences between VANETs and MANETs are:

- In VANETs, there is no limitation of power consumption, as vehicle is assumed to have sufficient amount of power and computing resources. In case of MANETs, due consideration needs to be given for power consumption.
- VANETs are highly dynamic networks compared to MANETs, as vehicles are always moving at high speed.
- In VANETs, all vehicles are registered with a trusted authority so that they have a unique identity. In MANETs, this is not enforced.

Vehicles in VANET can communicate directly with other vehicles using vehicle-to-vehicle (V2V) mode through their respective OBUs and/or using vehicle-to-infrastructure (V2I) mode through RSUs. The Figure 1 depicts the architecture of VANET (Wasef, Lu, Lin, & Shen, 2010).

There are various applications of VANETs, some of which are important for safety reasons and others for user convenience. Safety by providing prior information of road situation helps driver to change the route and avoids accidents.

Figure 1. Architecture of VANET (Wasef, Lu, Lin, & Shen, 2010)