Chapter 23
Blockchain-Based Incentive Announcement Network for Communications of Smart Vehicles

Shouryadhar Karamsetty
Asia University, Taiwan

ABSTRACT

The emergence of embedded and connected smart devices, systems, and technologies has given rise to the concept of smart cities in modern metropolises. They've made it possible to connect "anything" to the internet. As a result, the internet of vehicles (IoV) will play a critical role in newly constructed smart cities in the approaching internet of things age. The IoV has the ability to efficiently tackle a variety of traffic and road safety issues in order to prevent fatal crashes. Furthermore, ensuring quick, secure transmission and accurate recording of data is a particular problem in the IoV, particularly in vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) connections. Furthermore, the authors qualitatively examined the suggested overall system performance and resiliency against popular security assaults. The proposed method solves the primary issues of vehicle-to-x (V2X) communications, such as centralization, lack of privacy, and security, according to computational experiments.

INTRODUCTION

With the help of numerous sensing, networking, and data analysis techniques, automobiles have recently gained more autonomy. Internal and external information about a vehicle can be communicated to base stations or neighboring vehicles via wireless channels, due to onboard sensors. Security is frequently viewed as a critical concern in wireless communication systems due to the open surroundings, especially in automobile networks, which have far more complicated and fast-changing situations. As a result of the lack of appropriate ways, attackers may counterfeit or manipulate important messages, compromising the security and efficiency of vehicle networks. The Internet of Things (IoT) is a network of physical

DOI: 10.4018/978-1-7998-9640-1.ch023

devices, such as home appliances, automobiles, and other goods, that are embedded with network connectivity, actuators, sensors, software, and electronics (Atzei et.al,2017)

. Each device is identified and integrated into the Internet infrastructure using embedded computing systems. Such gadgets can be controlled remotely thanks to the network infrastructure. As a result, computer-based systems are becoming more integrated with the real environment, resulting in cost savings, increased accuracy, and efficiency, as well as less human intervention.

Traditional vehicular ad-hoc networks (VANETs) are being transformed into the Internet of Vehicles (IoV) by the Internet of Things. The Internet of Vehicles (IoV) represents real-time data interaction between vehicles and infrastructures via smart terminal devices, vehicle navigation systems, mobile communication technology, and information platforms that allow for information exchange, sharing of driving instructions, and network system control.

This notion has made information about automobiles and infrastructures easier to collect and share. It also enables data collecting, computation, and exchange in Internet-based systems and other information platforms.

This concept has recently gained traction in the real world. 25 billion things are expected to be connected to the Internet in the near future, with autos accounting for a substantial portion. Intelligent Transportation Systems (ITS) in Japan and Europe have already deployed certain versions of IoV technology, while New Delhi has equipped 55,000 licensed rickshaws with GPS sensors. This concept has sparked a lot of research and commercial interest due to the rapid growth of communication and processing technology. Identity identification, digital signatures, and data encryption are only a few ways that have been extensively researched to meet the first two goals. However, studies focusing on the third goal, data credibility, are significantly lacking. In addition, initiatives to verify identity and maintain data integrity may be futile once the content of a message is compromised.

Smart automobiles are also becoming more connected to the Internet, other adjacent vehicles, and traffic management systems (Bader et.al, 2018). Vehicles are being integrated into the Internet of Things in this fashion (IoT). Despite its undeniable benefits, however, this notion has several drawbacks. Importantly, because of their increased connectivity, smart vehicles are difficult to secure, making them vulnerable to malevolent actors. Furthermore, a sensitive data exchange raises new privacy concerns.

Challenges in IOT

1. **Lack of Privacy**: In most contemporary communication designs, user privacy is not secured. In all the other words, data about the vehicle is shared without the authorization of the owner.
2. **Scalability:** Due to the rapid rise in embedded technologies, the utilization of miniature devices such as actuators and sensors has increased. Meanwhile, the amount of data generated by these devices continues to rise endlessly. As a result, another key IoV difficulty is managing the amount of devices and the data they generate.
3. **Centralization:** Smart car architectures are currently based on centralised, mediated communication mechanisms. All of the vehicles are identified, authenticated, authorized, and connected by central cloud servers. It is unlikely, however, that this model will be scaled.
4. **Threats to Safety:** The number of self-driving features in smart cars is increasing. As a result, a security breach caused by a malfunction caused by malicious software installation can result in car accidents, putting road users at risk.