Vehicular Communications ••• (••••) ••••••

Contents lists available at ScienceDirect

Vehicular Communications

www.elsevier.com/locate/vehcom

B-IoMV: Blockchain-based onion routing protocol for D2D communication in an IoMV environment beyond 5G

Rajesh Gupta [a], Sudeep Tanwar [a,*], Neeraj Kumar [b,c]

[a] Department of Computer Science and Engineering, Institute of Technology, Nirma University, Ahmedabad, Gujarat, India
[b] Department of Computer Science Engineering, Thapar Institute of Engineering and Technology, Deemed to be University, Patiala, Punjab, India
[c] School of Computer Science, University of Petroleum and Energy Studies, Dehradun, Uttarakhand, India

ARTICLE INFO

Article history:
Received 31 March 2021
Received in revised form 15 July 2021
Accepted 18 August 2021
Available online xxxx

Keywords:
Internet of military vehicles
Beyond 5G
Blockchain
Onion routing
Smart contract
Security
Privacy

ABSTRACT

Blockchain technology's popularity in terms of security, privacy, traceability, and trust is being applied in various major applications concerning connected autonomous vehicles. One of the most sensitive applications is military operations. We do not compromise with either security, privacy, trust, or communication latency of connected military vehicles, i.e., Internet of military vehicles (IoMVs). Achieving anonymity along with the security and privacy of sender, receiver, and data path for IoMVS is still an open question. Efforts we have made to address the aforementioned issue by proposing a blockchain-based onion routing protocol for IoMVs, i.e., B-IoMV, to achieve secure, trusted, and anonymous D2D communication. We studied the working of onion routing and presented a blockchain and token-based solution to strengthen the security and anonymity of IoMVs. A blockchain-based solution is quite costly and we use InterPlanetary File System (IPFS) to make the proposed B-IoMV system cost-effective. Finally, results show that the proposed B-IoMV system achieved better communication latency, data storage cost, and network bandwidth utilization.

1. Introduction

In recent years, road fatalities have been increased a lot due to traffic crashes. As per the world health organization (WHO), the approximate number of humans who lose their lives each year due to road crashes is 1.35 million [1]. Fig. 1 shows the number of road fatalities from 2015 to 2020 of countries India, US, and UK. These fatalities were either due to human error or vehicle impairment. One of the possible solutions to mitigate the aforementioned issue (i.e., minimizing road fatalities) is the introduction of an intelligent transportation system (ITS), i.e., Internet of things (IoT)-based smart and connected vehicles (SCV) [2,3]. SCV's are driverless vehicles having various applications in public as well as private sectors such as traffic management, military operations, carriage holders, message passing, and many more. The most focused application of SCV is military operations, which can be used for patrolling in the most sensitive border areas and exchange information with the military base station. For such purposes, multiple SCVs (also called the Internet of military vehicles (IoMV)) are required for cooperative data exchange as in device to device (D2D) communication [4].

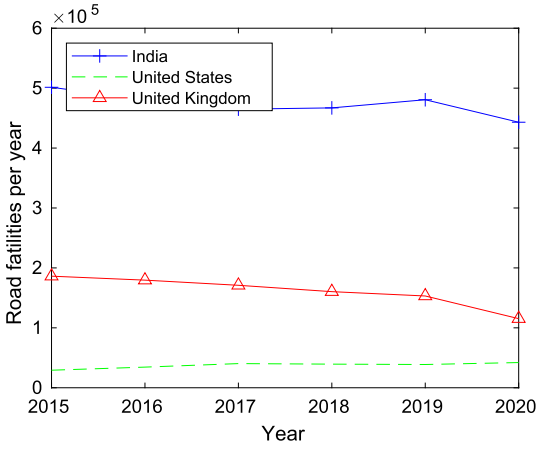

Fig. 1. Number of road fatalities from 2015 to 2020 of countries India, US, and UK [5–7].

IoMVs help save soldiers' lives as it can be controlled remotely by the base station over the wireless communication channel, which is open in nature and vulnerable to various security threats such as data sniffing, data modification, and denial of service.

* Corresponding author.
E-mail addresses: 18ftvphde31@nirmauni.ac.in (R. Gupta), sudeep.tanwar@nirmauni.ac.in (S. Tanwar), neeraj.kumar@thapar.edu (N. Kumar).

https://doi.org/10.1016/j.vehcom.2021.100401
2214-2096/