scientific reports

OPEN

Vehicular ad hoc networks verification scheme based on bilinear pairings and networks reverse fuzzy extraction

Zaid Ameen Abduljabbar[1,2,3]✉, Vincent Omollo Nyangaresi[4,5], Ahmed Ali Ahmed[6], Junchao Ma[2]✉, Mustafa A. Al Sibahee[6,7], Mohammed Abdulridha Hussain[1], Zaid Alaa Hussien[8], Ali Hasan Ali[9,10,11], Abdulla J. Y. Aldarwish[1] & Husam A. Neamah[12,13]

Vehicular Ad-Hoc Networks (VANETs) have facilitated the massive exchange of real-time traffic and weather conditions, which have helped prevent collisions, reduce accidents, and road congestions. This can effectively enhance driving safety and efficiency in technology-driven transportation systems. However, the transmission of massive and sensitive information across public wireless communication channels exposes the transmitted data to a myriad of privacy as well as security threats. Although past researches has developed many vehicular ad-hoc networks security preservation schemes, several of them are inefficient or susceptible to attacks. This work, introduces an approach that leverages reverse fuzzy extraction, bilinear pairing, and Physically Unclonable Function (PUF) to design an efficient and anonymity-preserving authentication scheme. We conduct an elaborate formal security analysis to demonstrate that the derived session key is secure. The semantic security analyses also demonstrate its resilience against typical VANET attacks such as impersonations, denial of service, and de-synchronization, instilling confidence in its effectiveness. Moreover, our approach incurs the lowest computational overheads at relatively low communication costs. Specifically, our protocol attains a 66.696% reduction in computation costs, and a 70% increment in the supported security functionalities.

Keywords Attacks, Bilinear pairing, Fuzzy extraction, Privacy, PUF, Security, VANET

The continued developments in communication and networking technologies have influenced the massive deployments of VANETs. This has seen enhancements in both transportation efficiency and safety. In VANETs, each vehicle acts as a node whose capabilities include data sensing, communication with other network entities as well as processing. This communication is accomplished using the Dedicated Short-Range Communication (DSRC) protocol[1]. In this protocol, messages related to safety are sent out by the vehicles after every 100 to 300 milliseconds. The transmitted messages may be about bad weather or traffic congestions, which can help in traffic navigation, management services, and collision avoidance. By exchanging real-time traffic density information and prevailing weather conditions, VANETs can help prevent collisions and road congestions,

[1]Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah 61004, Iraq. [2]College of Big Data and Internet, Shenzhen Technology University, Shenzhen 518118, China. [3]Department of Business Management, Al-imam University College, Balad 34011, Iraq. [4]Department of Computer Science and Software Engineering, Jaramogi Oginga Odinga University of Science & Technology, Bondo 40601, Kenya. [5]Department of Applied Electronics, Saveetha School of Engineering, SIMATS, Chennai 602105, Tamil Nadu, India. [6]Department of Management and Marketing, College of Industrial Management for Oil and Gas, Basrah University for Oil and Gas, Basrah 61004, Iraq. [7]National Engineering Laboratory for Big Data System Computing Technology, Shenzhen University, Shenzhen 518060, China. [8]Information Technology Department, Management Technical College, Southern Technical University, Basrah 61005, Iraq. [9]Department of Mathematics, College of Education for Pure Sciences, University of Basrah, Basrah 61004, Iraq. [10]Technical Engineering College, Al-Ayen University, Thi-Qar 64001, Iraq. [11]Institute of Mathematics, University of Debrecen, Pf. 400, Debrecen 4002, Hungary. [12]Department of Electrical Engineering and Mechatronics, Faculty of Engineering, University of Debrecen, Otemeto u.4-5, Debrecen 4028, Hungary. [13]College of Engineering, National University of Science and Technology, Dhi Qar 64001, Iraq. ✉email: zaid.ameen@uobasrah.edu.iq; majunchao@sztu.edu.cn