Contents lists available at ScienceDirect

Microprocessors and Microsystems

journal homepage: www.elsevier.com/locate/micpro

ELSEVIER

MICPRO

Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm

Ankit Kumar[a], Vijayakumar Varadarajan[b], Abhishek Kumar[c], Pankaj Dadheech[a], Surendra Singh Choudhary[d], V.D. Ambeth Kumar[e], B.K. Panigrahi[f], Kalyana C. Veluvolu[g,*]

[a] *Department of Computer Science and Engineering, Swami Keshvanand Institute of Technology, Management & Gramothan, Jaipur, India*
[b] *Department School of Computer Science and Engineering, The University of New South Wales, Australia*
[c] *Department of Computer Science, Institute of Science, Banaras Hindu University, Varanasi, India*
[d] *Department of Computer Science and Engineering, Sri Balaji College of Engineering and Technology, Jaipur, India*
[e] *Department of computer science and engineering, Panimalar Engineering College, Anna University, Chennai, India*
[f] *Department of Electrical Engineering, Indian Institute of Technology, New Delhi, India*
[g] *School of Electronics Engineering, Kyungpook National University, Daegu, South Korea*

ARTICLE INFO

Keywords:
Mobile ad-hoc networks (MANET)
Vehicular ad-hoc networks (VANET)
Routing protocol
Ad-hoc on-demand distance vector (AODV)
Performance parameters
Black hole attack

ABSTRACT

Vehicular ad hoc networks (VANETs) has received significant attention in the research domain of intelligent transportation system (ITS) as they provide safety and security to drivers and passengers. As compared to mobile ad hoc networks (MANETs), VANETs are mainly different in terms of characteristics, and system architecture. Security in VANET has been an important issue as it effects the communication between both (V-2-V) vehicles-to-vehicle and (V-2-I) vehicle to infrastructure. In VANET, malicious attacks affect the security of the networks, and it is necessary to identify and prevent such security attacks. In VANET network, any node can function as a router for the others nodes, and a malicious node connected to the network may inject spoofed routing tables to the other nodes thereby affecting the operation of the network. To overcome this issue, a secure AODV routing protocol is developed for detection of black hole attack in this paper. The proposed method is a modified version of the original AODV routing protocol with improvements in the RREQ packet and RREP packet protocols. For added security, a cryptography function-based encryption and decryption is included to verify the source and destination nodes. The proposed approach is demonstrated on a NS-2.33 simulator using different network parameters like drop packets, end-to-end delay, and packet delivery ratio (PDR) and routing request overhead. Results demonstrate that the proposed method outperforms existing AODV routing protocol under black hole attack and improves the network performance.

1. Introduction

VANET is defined as vehicular Ad-Hoc that works on the security of roadside vehicles and involves the management of road traffic and transportation through its intelligent transportation system (ITS) [1]. Within a network, because of having a distributed infrastructure, security and privacy becomes a critical issue for VANET, which makes the network more secure during the communication. VANET handles road security and controls the traffic jams through smart transportation within the network. It also allows communication between different vehicles. In VANET, the vehicles are considered as the nodes with mobility, and for this reason, security becomes an important issue in the wireless connection for the VANET.

VANET is a technology that allows creating a network dynamically to use and obliterate the network when it is not required. VANET is a subdivision of MANET (Mobile Ad-hoc Network). MANET is a technology that applies to Mobile networks, whereas VANET technology is employed on Vehicular networks. The primary difference between MANET and VANET is of their MAC address because MANET works on Wi-Fi IEEE 802.11m and VANET works on Wi-Fi IEEE 802.11p technology. In the speed of exchanging data, the rate of Vehicular networks are faster than of Mobile networks. Vehicular networks are dynamic and organized, the nodes know the path of their network, but mobile

* Corresponding author.
E-mail addresses: ankit.kumar@skit.ac.in (A. Kumar), v.varadarajan@unsw.edu.au (V. Varadarajan), abhishekryan@bhu.ac.in (A. Kumar), pankaj@skit.ac.in (P. Dadheech), surendra.choudhary@sbss.ac.in (S.S. Choudhary), vdambethkumar@panimalar.ac.in (V.D.A. Kumar), bkpanigrahi@ee.iitd.ac.in (B.K. Panigrahi), veluvolu@ee.knu.ac.kr (K.C. Veluvolu).

https://doi.org/10.1016/j.micpro.2020.103352
Received 2 October 2020; Received in revised form 14 October 2020; Accepted 19 October 2020
Available online 21 October 2020
0141-9331/© 2020 Elsevier B.V. All rights reserved.

Please cite this article as: Ankit Kumar, *Microprocessors and Microsystems*, https://doi.org/10.1016/j.micpro.2020.103352