RESEARCH ARTICLE

TriChain: Kangaroo-Based Intrusion Detection for Secure Multipath Route Discovery and Route Maintenance in MANET Using Advanced Routing Protocol

Jayantkumar A Rathod
Department of Computer Science and Engineering, Alva's Institute of Engineering (Affiliated to Visvesvaraya Technological University, Belagavi), Moodubidire, India.
jayant1977rathod@gmail.com

Manjunath Kotari
Department of Computer Science and Engineering, Alva's Institute of Engineering (Affiliated to Visvesvaraya Technological University, Belagavi), Moodubidire, India.
mkotari@gmail.com

Received: 21 November 2023 / Revised: 01 February 2024 / Accepted: 07 February 2024 / Published: 26 February 2024

Abstract – Several practical applications are combined in a new paradigm known as 5G-based mobile ad hoc networks (MANET) with cloud. Numerous existing works perform trust assessment, intrusion detection, and route discovery to improve secure data transmission in MANET. Route maintenance was not carried out in several of the existing works, and the absence of enumerating link status and node reliability during route maintenance results in link failure and increases packet loss. By considering the existing issues, a novel Kangaroo-based intrusion detection system was proposed to eliminate malicious nodes from the network using Bidirectional- Long Short-Term Memory (Bi-LSTM). This increases data transmission security. For graphical user authentication, encryption based on ASCII values of the Reflection tree (E-ART algorithm) is employed. In this paper, a divide well merge algorithm was implemented, which is a better approach for hierarchical clustering. This method consists of two phases: a Division and Merging phase. The effective route identification and route maintenance in MANET are implemented by using an Advanced Ad-hoc On-demand Distance Vector Protocol (Advanced AODV), which discovers the route using the Fire Hawk Optimization Algorithm (FHO) to obtain optimal multipath by contemplating trust, node connectivity, throughput, node degree, bandwidth, energy and distance where this protocol offers loop-free operation and enhance its scalability to numerous numbers of terminals. In this way, route discovery and route maintenance are established to enhance secure data transmission, thereby reducing packet loss. The modified blockchain called TriChain is proposed for enhancing data transmission security. For the Proof of Work based on Reputation (PoWR) consensus algorithm is used to reduce transaction confirmation latency and block creation time thereby increasing security. In this way, route discovery and route maintenance are established to enhance secure data transmission thereby reducing packet loss. The proposed work is evaluated using detection rate, energy consumption, packet delivery rate, throughput, authentication rate and delay.

Index Terms – 5G MANET, Kangaroo Intrusion System, Bi-LSTM, Encrypts Based on ASCII Values of Reflection Tree, Advanced AODV, Fire Hawk Optimization Algorithm.

1. INTRODUCTION

The distributed wireless connection is acknowledged as a Mobile Ad Hoc Network (MANET), which is without any infrastructure and auto-configured devices (mobile phones, laptops) that are connected wirelessly. The MANET benefits with effortless communication of mobile nodes due to their communication range. A radio transmitter and the recipient are installed in each node of a MANET, enabling wireless communication between the nodes and the system [1-3] The following are the primary explanations for why MANETs may send data with comparable properties while yet using an active strategy: It is unexpected that the transmission scope of this transmission is more limited than that of the previous transmission, which prevents any number of nodes from exchanging data across the system [4-6]. The fact that portable nodes in Wi-Fi Ad-Hoc networks rely on battery packs, which are typically underpowered in most environments and take an extended period to recharge or replace, is a major problem. Route discovery and data transfer are the two phases of MANET communication, both of which are subject to different types of attacks. Adversaries can obstruct route finding during the initial phase by feigning to be destination, responding with outdated routing information,