ID 111

Adaptive Security Protocols for Wireless Mobile Ad-hoc networks: A Review of Challenges and Innovations

Achini Gurusinghe[1#] and Malaka Pathirana[2]

[1]School of Computing, Achievers International Campus, Sri Lanka
[2]Department of Computer Science, Faculty of Science, University of Ruhuna, Sri Lanka

[#]achini@iaicampus.com

Mobile Ad hoc Networks (MANETs) are considered an innovative wireless technology that allows mobile nodes to network with each other without bounds of fixed infrastructure or centralized administration. MANETS are used in numerous industries, such as emergency services, the army, and increasingly, healthcare, and intelligent cities. On the other hand, these traits of open medium, diverse topology, and distributed nature are what make them susceptible to novel security threats. This paper gives a detailed description of MANET's security issues with conventional attacks such as blackholes, wormholes, and denial-of-service, as well as advanced ones arising from AI and IoT integration and the emergence of 5G networks. The questionnaire involves the weaknesses at different layers of the MANET protocol model and the latest methods in security, such as blockchain technology, intrusion detection systems using machine learning, and software-defined networking. Through studying these changing threats and measures developed to counter them, this study intended to enhance MANET security awareness and the design of more robust and reliable networking components for the time to come.

Keywords: *MANET security, emerging threats , AI-powered attacks, IoT security, 5G networks*