

ABSTRACT

Mobile Ad-hoc Networks (MANETs) are integral to modern communication systems, yet their susceptibility to security threats demands innovative solutions. This thesis introduces an advanced machine learning-based trust computational model designed to strengthen the trustworthiness and security of MANETs. This research is conducted in two phases. The outcomes of Phase 1 of this research constitute a multifaceted approach to enhancing trust and security within MANETs. At its core, a Deep Q-learning-based Node Trust Computational Model was developed, serving as the foundational element for evaluating trustworthiness within MANETs. Complementing this model, an Ant Colony Optimization-based Trust Routing Protocol was implemented, leveraging trust values to optimize routing decisions, thereby improving network efficiency and reliability. Furthermore, a Support Vector Machine (SVM) Classifier was crafted for node classification, proficiently categorizing nodes as either trustworthy or malicious. This classification mechanism plays a pivotal role in fortifying network security by aiding in the identification and mitigation of potential threats. Phase 2 delved into enhancing the security measures of the network while refining trust value calculation. This phase innovatively integrated blockchain technology to authenticate MANET nodes based on their behavioral patterns and trustworthiness. The primary outcome of Phase 2 was a Blockchain-enabled Deep Q-learning-based Node Trust Computational Model. The predictions from this model were cyclically employed to retrain both the route optimizer and the node classifier, ensuring adaptability to evolving network conditions. In Phase 1, the Deep Q-learning-based Node Trust Computational Model achieved an accuracy of 80% in computing trust, while Phase 2 enhanced this performance, reaching an impressive accuracy of 90% through the integration of blockchain technology. By combining cutting-edge machine learning techniques, blockchain technology, and trust-based routing protocols, this research offers a novel approach to fortifying the trustworthiness and security of MANETs, addressing the critical challenges associated with trust and security in dynamic wireless communication environments.

Keywords: Mobile Ad-hoc Networks (MANETs), Deep Q-learning, trust, blockchain, security