ISSN 2362–0412

ABS-076

LinkShield: Integrating Blockchain, Cryptography, and Reinforcement Learning to Prevent Link Discovery Attacks in SDVN

P.A.D.S.N.Wijesekara[1], K. L. K. Sudheera[1], G. P. Wijesiri[1]*

[1] Department of Electrical and Information Engineering, Faculty of Engineering, University of Ruhuna, Galle, Sri Lanka

**Corresponding author:* nilmantha@eie.ruh.ac.lk

A global network view-driven controller optimization can enhance the performance of vehicular networks in a Software-Defined Vehicular Network (SDVN). However, if Link Discovery (LD) Attacks (LDAs) contaminate the network architecture, such performance may be significantly impacted. Dynamic SDVN LD is less suitable for recent LDA mitigation techniques in the SDN realm. To address this research gap, we first show that five LDAs may be implemented in a typical SDVN architecture by taking advantage of flaws in the LD service and position tracking. Our main contribution, however, is to propose a novel framework to detect LDA by using a location-driven adaptive LD technique with Q-learning to derive link states. To mitigate the attacks, we use Diffie-Hellman (DH) symmetric key issuing, time-limited session-based Hash Message Authentication Codes (HMACs), Zero-Knowledge Proofs (ZKPs) of HMACs stored in the blockchain, packet limiting with signature matching, location verification, and cycle- and non-cycle-based digital signatures with a combination of post-quantum and classical cryptography. Additionally, a permissioned blockchain is used by employing a challenge-response mechanism for node registration with DH, global, and public key exchange and subsequent node authentication through established encrypted communication using signatures, ZKPs, attributes, and HMACs. A second smart contract is used to maintain non-tamperable node reputation and location scores by tracking node behavior and maintaining endorser trust scores for weighted reputation updates for consensus-based node blacklisting. We evaluate all five attack scenarios through simulations, and the findings indicate that the proposed technique is exceptionally effective in countering the five link discovery attacks outlined in this study, outperforming existing methodologies for SDN and Vehicular Ad hoc Networks. It achieved the second-best channel utilization during location-triggered flooding attack, the best link discovery latency during traditional flooding attack, and optimal packet delivery ratio and Matthews correlation coefficient, and zero packet interception ratios during fabrication, replay, and link vanishing attacks, in spite of its increased computational complexity.

Keywords: Blockchain, Link discovery attack, Reinforcement learning, SDVN, Vehicular networks