



ShieldBlackhole: A Blockchain and Cryptography-based Credible Scheme to Mitigate Blackhole Attacks in SDVN

T.M.N.G.S. Karunaratna¹, P.A.D.S.N. Wijesekara^{1}, G.H.N. Lankesha¹,
N.M.K.M. Bandara¹, B.K.K.N. Rodrigo¹*

¹ Department of Electrical and Information Engineering, Faculty of Engineering,
University of Ruhuna

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

Blackhole attacks are a major threat to Software-Defined Vehicular Networks (SDVNs) since they enable malicious nodes to drop packets rather than forward them, resulting in loss of information and decreased network efficiency. Existing research has concentrated very poorly on blackhole attacks in the SDVN domain, and existing methods depend mainly on a centralized authority, while current blackhole mitigation techniques in SDN and MANET domains suffer from limited reliability under high-mobility and poor resistance to coordinated attacks. Although blockchain has been proposed for security in SDN, its usage in high-mobility SDVN environments, tailored for blackhole attack mitigation, has not been fully analyzed in current studies. This study introduces a hybrid mitigation framework that combines log-based verification and blockchain-based overhearing for secure end-to-end packet forwarding. Within this framework, the controller collects and processes transmission and reception logs of vehicular nodes to detect instances of receiving-side forwarding failure, while neighboring vehicular nodes observe and report packet forwarding behavior by placing votes onto the blockchain. To improve security, the control plane communication is encrypted with integrity protection using HMAC, while authenticity is improved by signing. A smart contract aggregates votes to dynamically update each node's trust value by imposing penalties on nodes that exhibit blackhole behavior. As a reliability measure for the controller, a group of trusted nodes periodically validates the controller function and triggers an automatic failover if any malfunction is detected. The proposed ShieldBlackhole method was implemented using NS-3 for network simulation and Hyperledger Fabric for blockchain functionality. It has been compared with existing blackhole mitigation techniques using key performance evaluation metrics including packet delivery ratio, average latency, Matthews correlation coefficient, precision, and recall. This research shows that the proposed ShieldBlackhole method sustains over 80% packet delivery ratio with 40% attacks, maintains MCC above 0.7, and achieves approximately 0.9 precision and 0.75 recall, outperforming existing solutions.

Keywords: Blackhole attack mitigation, SDVN, Blockchain, NS-3 simulation, Hyperledger Fabric, Smart contracts