BNIS- Bot Node Isolation Strategy to Prevent DoS Attacks: An Improved Overhearing Solution

Satyam Mishra ¹, Nguyen Van Tanh ², and Vu Minh Phuc ²

¹International School - Vietnam National University
²Affiliation not available

December 7, 2023

Abstract
This research addresses the issue of information security in the RPL routing protocol against denial of service (DoS) attacks in wireless sensor networks. Our study proposes solutions to detect and prevent DoS attacks using the Contiki operating system to simulate illustrated scenarios and conduct tests on real sensor environments with a network model basis. This helps to demonstrate the impact of DoS attacks on IoT networks and the effectiveness of the proposed security mechanism. The solution proposed involves improving the overhearing mechanism based on a proposed algorithm of listening around to detect which node is performing the attack. The attacking node is then blacklisted and isolated to prevent it from affecting data exchange throughout the network, thereby limiting heavy damage from denial-of-service attacks on low-resource IoT environments. Simulation experiments and real device models demonstrate that implementing the improved overhearing solution can detect the attacking node in a short time with a relatively simple algorithm. Isolating the attacking node has a positive effect, reducing damage in DoS attacks. The proposed solution has the advantage of minimizing energy consumption when compared to previous proposals of the same nature, making it suitable for wireless sensor networks of small and medium scale with limited resources. Additionally, this solution incorporates a Bot node isolation plan to maintain the normal operation of the WSN network while ensuring that Bot infection is avoided, thereby limiting the harm of DoS attacks.

Hosted file