National Institute of Technology Rourkela

Registration Seminar

Seminar Title	: Designing a Secure Software-Defined VANET Framework for Resilient DDoS Detection and Mitigation
Speaker	: Aishwarya (Rollno : 921cs5006)
Supervisor	: Arun Kumar
Venue	: Department Meeting Room
Date and Time	: 18 Aug 2025 (4:30PM)
Abstract	: The growing intricacy and ever-changing structure of Software-Defined Vehicular Networks (SDN-VANETs) have brought about notable progress in intelligent transportation systems. Nonetheless, this development has also widened the attack surface, rendering these networks particularly vulnerable to advanced Distributed Denial-of-Service (DDoS) attacks. Within SDN-enabled VANETs, the centralized SDN controller serves as the main decision-maker, making it a key target for attackers. A successful DDoS assault on the controller can severely impair network performance, disrupt real-time vehicular communication, and potentially jeopardize road safety. Traditional DDoS detection methods in VANETs often depend on static rules, known attack signatures, or threshold-based techniques, which fall short in addressing zero-day attacks and dynamic attack patterns. Additionally, centralized detection systems face challenges with latency, scalability, and robustness in non-IID and mobile vehicular settings. To address these challenges, there is an urgent need for a scalable, intelligent, and adaptive security framework that can ensure resilient DDoS detection and mitigation while meeting the low-latency demands of vehicular communication. In this study, we introduce an innovative, intelligent multi-agent deep learning framework for coordinated DDoS detection and mitigation in SDN-VANET environments. This framework incorporates a multi-layered security architecture, utilizing the centralized control of SDN and the distributed sensing capabilities of edge nodes and roadside units (RSUs). At its core, the system features an intelligent Intrusion Detection and Mitigation System (IDMS) that employs a hybrid approach, combining machine learning and deep learning models. These models are trained on a diverse array of statistical and temporal features, such as packet rate, flow entropy, inter-arrival times, and source diversity, enabling precise differentiation between normal and malicious traffic behaviors. The deep learning models, particularly Long Short-Term Memory (LSTM) networks, are designed to capture the sequential nature of traffic patterns, making them highly effective in identifying low-rate and stealthy DDoS attacks. The system demonstrates self-adaptive behavior, dynamically adjusting detection thresholds and mitigation strategies in response to network context and mobility patterns. This ensures high detection accuracy while maintaining false positive rates below 1%, which is crucial for uninterrupted vehicular services. To mitigate detected attacks in real-time, the system leverages the programmability of SDN to enforce dynamic traffic control rules, including rate limiting, traffic rerouting, flow isolation, and node quarantine.