INDIAN INSTITUTE OF TECHNOLOGY GUWAHATI
SHORT ABSTRACT OF THESIS

Name of the Student	:	DIPOJJWAL RAY
Roll Number	:	156201002
Programme of Study	:	Ph.D.

Thesis Title: Modeling and Verification of Lightweight Defense Strategies in IoT Security: A Discrete Event System Approach

Name of Thesis Supervisor(s)	:	DR. PINAKI MITRA, DR. SANTOSH BISWAS
Thesis Submitted to the Department/ Center	:	Computer Science & Engineering
Date of completion of Thesis Viva-Voce Exam	:	24-10-2024

Key words for description of Thesis Work : Internet of Things, Formal Verification, Cyber Physical Systems, Discrete Event Systems, Security

SHORT ABSTRACT

The Internet of Things (IoT) revolution has ushered huge technological benefits and has made future communication and human lives easier. However, the rapid proliferation of IoT introduces numerous security challenges. IoT systems have been shown vulnerable to device-level attacks. Also indubitably, there exists a multitude of network-level attacks that make IoT systems vulnerable due to lack of secure provisions in place. At the device-level, secure IoT devices can be heavily compromised to various side-channel attacks. There exists scan-based side-channel attacks for which the proposed countermeasures are either insufficient, or compromise on testability, or of high-overhead. At the network-level, IoT-specific protocols are prone to varied internal DDOS attacks at each layer. Given the resource-constrained environment, lightweight, accurate and malicious node identification schemes are highly demanding among attack mitigation techniques. For genuine reasons, Intrusion Detection Systems (IDS), a software or hardware component monitoring host or network threats, are widely used to secure IoT systems and deemed suitable for most of such detection or prevention scenarios. The two most popular IDS-based design techniques are Signature based IDS, which use known signatures, and Anomaly-based IDS that use statistical features. However, there exists no known signatures or features in attacks like RPL rank attack, RPL version number attack, 6LoWPAN based fragmentation attacks, CoAP request spoofing and CoAP response spoofing attacks, rendering Signature-based and Anomaly-based methods futile. Basically they generate lots of false positives since the IoT network traffic, operational under attack, cannot be differentiated from the normal traffic. This dissertation presents few novel attack mitigation and attack node location identification mechanisms for IoT security, utilizing controller and IDS implementations, while using various Discrete Event System (DES) based formalisms. DES models are designed for the IoT systems under normal and abnormal conditions. DES based formalisms ensure proofs of correctness and completeness which are preferable. DES security and Fault Detection and Diagnosis (FDD) theoretic properties in Finite State Automata are leveraged for the proofs.