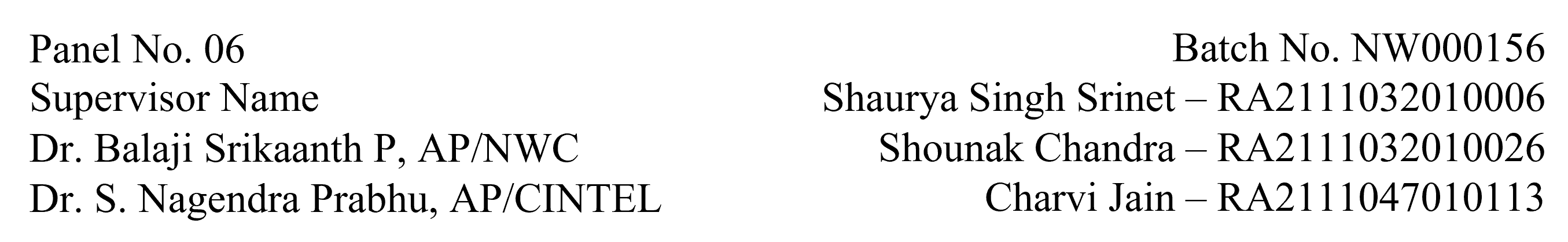
**AI-Driven Dynamic Fuzz Testing for IoT Security**

****

**Functional Document User Story 4: Implement Real-Time DDoS Mitigation in NS3**

**1. Introduction:**

This user story focuses on integrating a Graph Neural Network (GNN) model with the NS-3 simulation environment to enable real-time detection and mitigation of DDoS attacks. The objective is to ensure network security and operational efficiency while mitigating malicious traffic through dynamic packet filtering.

**2. Product Goal:**

The aim is to enhance the NS-3 environment by integrating AI-powered DDoS detection, utilizing the GNN model to analyze traffic patterns and implement a real-time mitigation strategy that drops malicious traffic while maintaining legitimate network flow.

**3. Demography (Target Audience):**

* **Security Engineers:** Focused on real-time threat detection and mitigation.
* **Network Administrators:** Responsible for securing IoT networks.
* **Researchers:** Investigating dynamic security solutions in IoT environments.

**4. Business Processes:**

* **GNN Model Integration with NS-3:**
  + Modify the existing NS-3 environment to interface with the GNN model.
  + Train the GNN model using IoT traffic data to detect anomalies such as DDoS attacks.
  + Implement real-time traffic analysis through the model to monitor for malicious activity.
* **DDoS Mitigation Strategy:**
  + Employ dynamic packet filtering to block malicious IP addresses.
  + Ensure minimal impact on legitimate traffic by optimizing the filtering mechanism.
  + Monitor network metrics (latency, throughput) during mitigation.

**5. Features:**

* **Integration of GNN with NS-3:**
  + Establish communication between NS-3 and the trained GNN model.
  + Facilitate real-time traffic analysis during simulation runs.
* **Dynamic Packet Filtering:**
  + Real-time detection and packet drop for malicious IP addresses.
  + Monitor and optimize the performance of the packet-filtering mechanism.
* **Monitoring Network Performance:**
  + Measure throughput, latency, and other performance indicators to ensure network stability.

**6. Roles & Authorization Matrix:**

|  |  |
| --- | --- |
| **Role** | **Access Level** |
| **Security Engineer** | Full access to configure real-time detection and mitigation. |
| **Network Administrator** | Monitoring access to ensure network security is maintained. |
| **Researcher** | Access to performance data and logs for testing purposes. |

**7. Assumptions:**

* The NS-3 simulation environment is stable and configured for IoT simulations.
* The GNN model has been trained with relevant datasets (including benign and DDoS traffic).
* Packet filtering libraries and dependencies are compatible with NS-3.

**8. Effort Estimation:**

* **GNN Model Integration with NS-3:** 4 days
* **Packet Filtering Mechanism Implementation:** 4 days
* **Testing & Validation:** 7 days
* **Documentation:** 1 day
* **Total:** 16 days

**9. Acceptance Criteria:**

* Successful integration of the GNN model with NS-3.
* Real-time detection of DDoS attacks and mitigation through packet filtering.
* The network performance remains stable with legitimate traffic unaffected.
* Full documentation of the real-time mitigation strategy and test results.

**10. Checklist:**

* GNN model integrated with NS-3.
* Real-time DDoS detection implemented.
* Packet filtering for malicious traffic configured and operational.
* Network performance metrics logged and analyzed.
* Documentation of results and findings completed.