ID: Type: **Poster**

Analysis of VSAT Jamming Attacks on the Recognition of Events

This study analyzes the potential impact of cyber attacks on the verification regime prior to the execution of an illegal nuclear test activity. In this matter, attacks on the availability of measurement stations by jamming their satellite up-links, namely the Very Small Aperture Terminals (VSATs), are relevant. The rationale is that any entity that wants to perform an illegal test activity will strive to cover its actions to evade liability. If the service of verification regime can be degraded to a point where the recognition of events is unreliable or disputable, the attacking entity can repudiate liability towards the States Parties. Devices to jam the VSATs' signals are cheap and available. Disrupting a station's communication capabilities might hamper the analysis procedures and in consequence the Quality-of-Service of the International Measurement System (IMS)-based data products. For instance, the temporal correlation of data items might be disturbed by disrupting their GPS-based timestamping. Therefore, we simulate a scenario in which an attacker maliciously launches a jamming attack to degrade the verification regime. We model the impact of single measurement signals on recognizing an Event and evaluate, if a jamming attack could force a configuration of signals such that the Event remains undetected.

Primary author: WASICEK, Armin (Vienna University of Technology)

Presenter: WASICEK, Armin (Vienna University of Technology)

Track Classification: Theme 3: Advances in Sensors, Networks and Processing