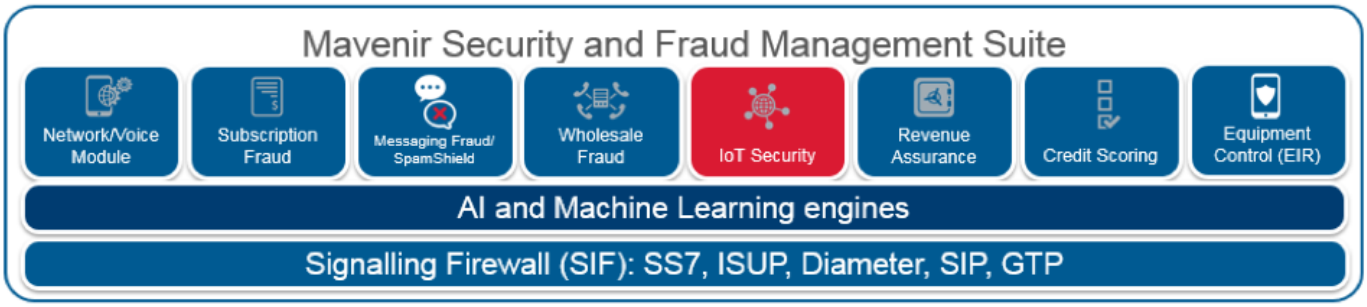
IoT Security



Evolution of mobile networks to 5G is putting a lot of focus on various IoT and M2M use cases and today, mobile IoT use-cases are already actively supported by various networks and being actively pushed by MNOs. Current IoT scenarios are clearly relying on traditional network communications primarily using SMS messaging and data channels.

However, operators may be missing an opportunity with IoT communications. It is quite common for small and medium scale business to use standard subscription or pre-paid connections for IoT communication today. Uncontrollable IoT communication is a risk for a mobile operator ranging from incidental network overload that could result in a Denial of Service attack on specific network elements or even cause revenue loss when IoT devices are compromised and communication services are misused.

Today's typical strategy for IoT device control is to limit communication services to the specific use-case demand. Often that is either forgotten or impossible due to technical limitations so mobile operators need a system embedded into their networks that can:

- Identify IoT communication type
- Automatically differentiate between different IoT types
- Prevent service misuse
- Block fraud attempts caused by compromised IoT devices in real time

Given the nature of IoT communication today, it is virtually impossible to pre-provision various IoT behavior types and control various devices without dedicated architectures in place, though many operators are exploring 3GPP IoT architectures.

Mavenir's IoT Security module is relying on special machine learning techniques that automatically group various types of IoT devices together based on their communication patterns and track any potential violations of these patterns over time. This enables detection of a potential intruder break-in into a specific IoT use-case or prevent service mis-use, e.g. generating voice minutes or SMS Spam from a typical IoT device like electricity meter, parking meter or traffic camera.

Integration with the EIR module also enables automatic locking of the SIM card to a specific device preventing a fraudster taking SIM card and mis-using it.