Contextual Security
Secure Systems Group

CENTRE FOR DOCTORAL TRAINING *in* CYBER SECURITY

Relay Resilient Zero-Effort Authentication using Sensor Measurements

- Recognize walk path through on-board smart device sensors
- Energy-efficient relay-attack resistance with accelerometer & gyroscope data

Mika Juuti, Christian Vaas, Ivo Sluganovic, N. Asokan, Ivan Martinovic

Transparent Authentication

- Relies on wireless cryptographic authentication to a “Terminal” (verifier) over short range
- Examples: BlueProximity, Keyless Entry, etc.
- Inherently assumes spatial proximity of user with his “smart device” (prover)

Relay Attacks

- Attacker can emulate proximity with high-speed link between prover and verifier
- We prevent this by moving proximity verification to prover itself and thus making it a smart wallet for credentials

Path Recognition for Proximity Assertion

- Expected trajectory of prover towards verifier described as a reference path (e.g. history)
- Seamless authentication by comparing sensed trajectory (candidate path) to reference path
- Low confidence about path similarity triggers fall-back to manual authentication
- Information asymmetry: verifier can be Internet-of-Things device

Security Validation with Geospatial Maps

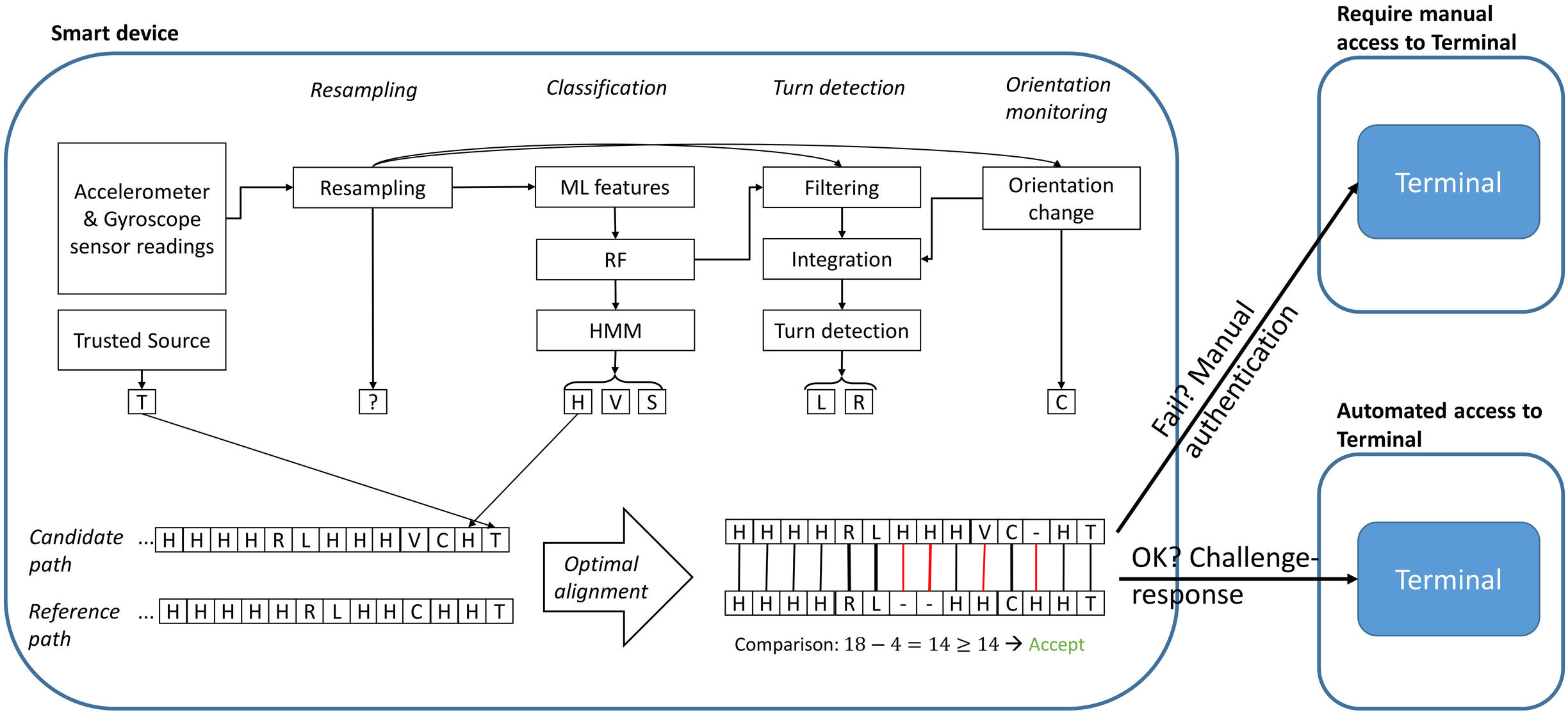
- Uniqueness assertion for a reference path prevents
  - Accidental authentication responses
  - Attacks launched by a stalker
- Measure of quality for reference paths

Usability through Machine Learning

- Path recognition gradually becomes confident
- Sequence alignment to verify similarity
- Design goal: resilience to sensor noise
- Modular design allows future improvement

Future Development

- Suggest improvements to low quality trajectory: how to make trajectories more unique
- Recognize more distinguishable events along trajectory: stairs, elevators, etc.
- Terminal-specific transition model



Aalto University
UNIVERSITY OF OXFORD
ACADEMY OF FINLAND
EPSRC Engineering and Physical Sciences Research Council