Apr 12th, 10:00 AM - 10:00 AM

Radio Identity Verification-based IoT Security Using RF-DNA Fingerprints and SVM

Donald Reising
University of Tennessee at Chattanooga

Joseph C. Cancelleri
NASA MSFC

T. Daniel Loveless
University of Tennessee at Chattanooga

Farah Kandah
University of Tennessee at Chattanooga

Tony Skjellum
University of Tennessee at Chattanooga

Radio Identity Verification-based IoT Security Using RF-DNA Fingerprints and SVM [1]

Donald Reising*, Joseph Cancelleri*, T. Daniel Loveless*,
Farah Kandah^, and Anthony Skjellum^
Electrical Engineering Dept.* and Dept. of Computer Science & Engineering^
THE UNIVERSITY OF TENNESSEE CHATTANOOGA

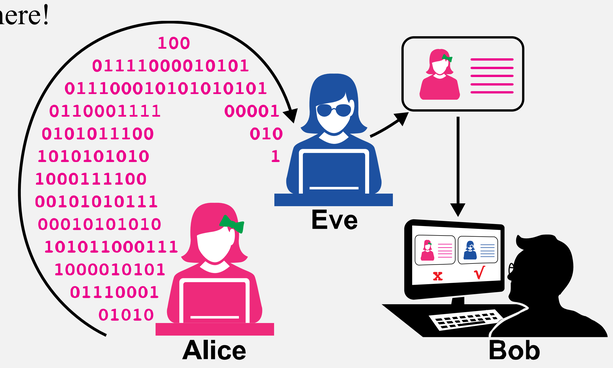
RESEARCH DIALOGUES 2021

Research Question

What is the lowest signal-to-noise ratio (SNR) that Radio Frequency-Distinct Native Attributes (RF-DNA) fingerprints can verify authorized IoT devices while rejecting rogue IoT devices?

Introduction

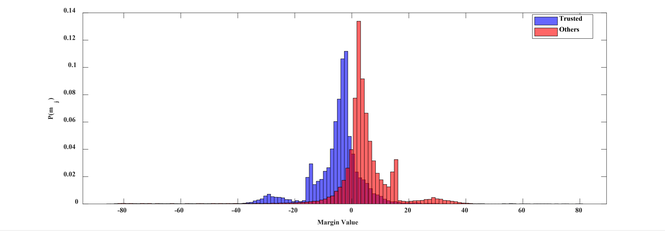
- Internet of Things (IoT) devices are everywhere!
  - 46 billion ... in 2021 [2-4]
  - 75 billion … by 2025 [2-4]
- IoT security is weak or non-existent
  - 70% lack encryption [5]
  - Exploited by nefarious actors [6-8]
- Specific Emitter Identification (SEI)
  - Physical IoT security solution
  - Exploits unique & inherent waveform features
  - Achieves serial # discrimination
    - Most challenging!
  - Verify authorized IoT devices
  - Reject illegitimate IoT devices … Rogues!
  - Steals authorized IoT devices' digital identity
  - Uses stolen identity to pose as authorized



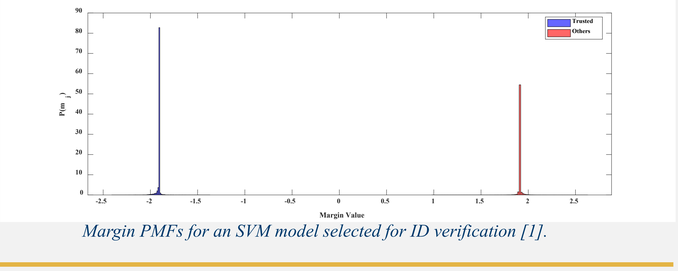
Threat Model: Lacking encryption, the rogue device Eve is able to trick Bob, another authorized IoT device or IoT infrastructure monitor, into thinking that Eve is the authorized IoT device Alice by presenting Alice's digital identity credentials [1].

Methods

- Focused on ID of *Authorized* Radios
  - Features selected & SVM development
- Eight (8) feature selection methods
  - Dimensional Reduction Analysis
  - Linear Discriminant Analysis
  - Principle Component Analysis
  - Neighborhood Component Analysis
  - Probability Of Error + Average Correlation Coefficient
  - T-test
  - Bhattacharyya Coefficient
  - Relief-F… ***Proved superior!***
- AI … Support Vector Machines (SVM)
  - Novel selection of "best" model
  - Separability via increasing dimensionality

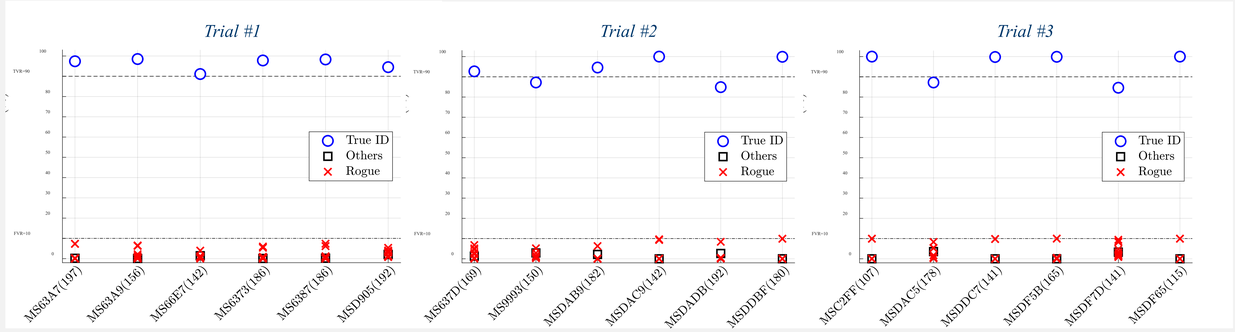


*Margin PMFs for a SVM model **not** selected for ID verification [1].*



Margin PMFs for an SVM model selected for ID verification [1].

Results



ID verification and rogue rejection performance for the six authorized radios of all three trials using Relief-F feature selection at a signal-to-noise ratio of three (3) decibels. The x-axis labels indicate the claimed digital identity with the number of retained features in parentheses and "Others" indicates the five authorized radios whose identities are not being verified and each red cross represents a rogue radio [1].

Relief-F method proved superior in authorized radio identity verification and rogue radio rejection when compared to the other seven (7) feature selection approaches. Using Relief-F selected RF-DNA fingerprint features resulted in:

- 90% or better rejection of all rogue radio spoofing attacks (72 per trial & 216 overall).
- Verification of all (six per trial) authorized radios' identities at a rate of 85% (4 of the 18 radios) or better.

Conclusions

- Achieves authorized identity verification of 90% or better for:
  - 18-of-18 devices at SNR = 6 decibels
  - 14-of-18 devices at SNR = 3 decibels
- Successfully rejects 100% of rogue radio spoofing attacks!
  - SNR = 3 decibels
  - 72 attacks per trial & 216 overall
- Level of success absent in literature
- Questions:
  - Scalability of the approach
  - Hardware integration & assessment
  - Homogeneous versus heterogeneous device deployments

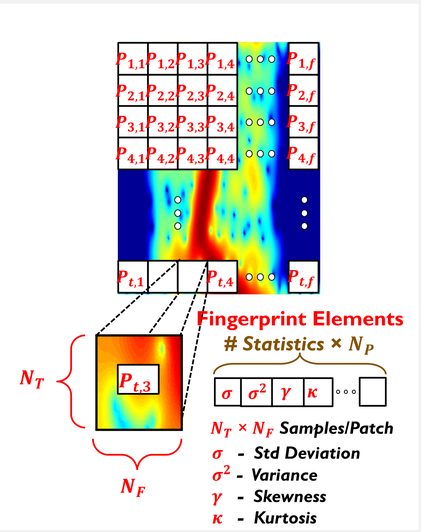


Illustration of Gabor-based RF-DNA fingerprint generation using two-dimensional time-frequency patches extracted from the centered, normalized, magnitude-squared Gabor coefficients.

References

1. Reising, Cancelleri, Loveless, Kandah, and Skjellum. "Radio identity verification-based IoT security using RF-DNA fingerprints and SVM." IEEE Internet of Things Journal, 2020.
2. Gartner Research, "Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015," Nov. 2015.
3. Juniper Research, "'Internet of Things' Connected Devices to Triple by 2021, Reaching Over 46 Billion Units," Dec. 2016.
4. Statista, "Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions),", 2019.
5. Rawlinson, K., "HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack," Jul. 2014.
6. Larsen, S., "A smart fish tank left a casino vulnerable to hackers,", Jul 2017.
7. Wright, J., and J. Cache,, Hacking Wireless Exposed: Wireless Security Secrets & Solutions, 3rd ed. McGraw-Hill, 2015.
8. Wright, J., "KillerBee: Practical ZigBee Exploitation Framework for 'Wireless Hacking and the Kinetic World'."