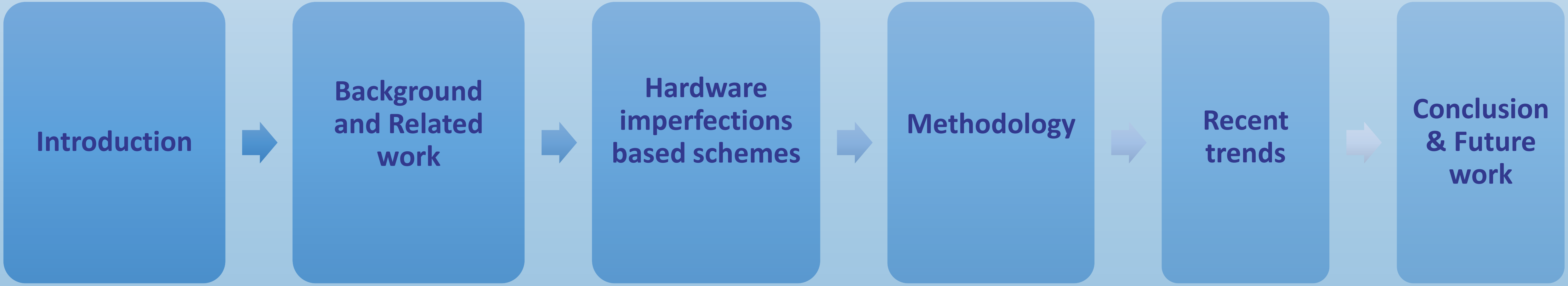
Survey on Hardware-based Physical Layer Authentication in Next Generation Networks

**Sachinkumar B. Mallikarjun, *Mihiraj Dixit, and **Hans D. Schotten

*Department of Computer Science, Saarland University, Saarbrücken
**WICON Chair, Department of Electrical and Computer Engineering,
University Of Kaiserslautern (RPTU), Kaiserslautern, Germany

Agenda



Introduction

Background and Related work

Hardware imperfections based schemes

Methodology

Recent trends

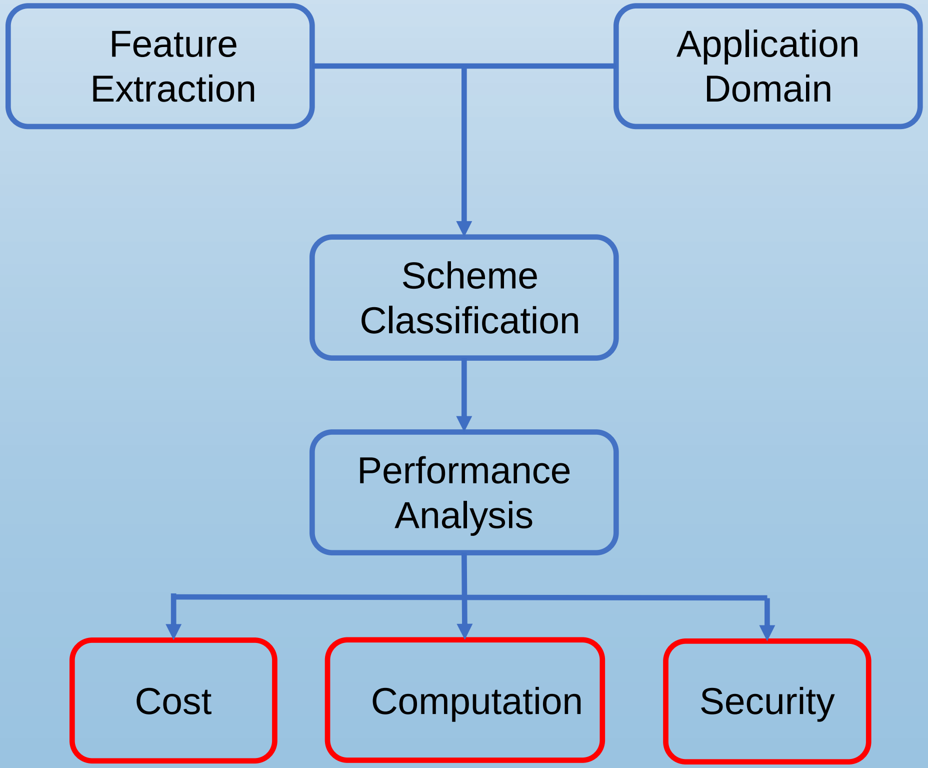
Conclusion & Future work

Introduction

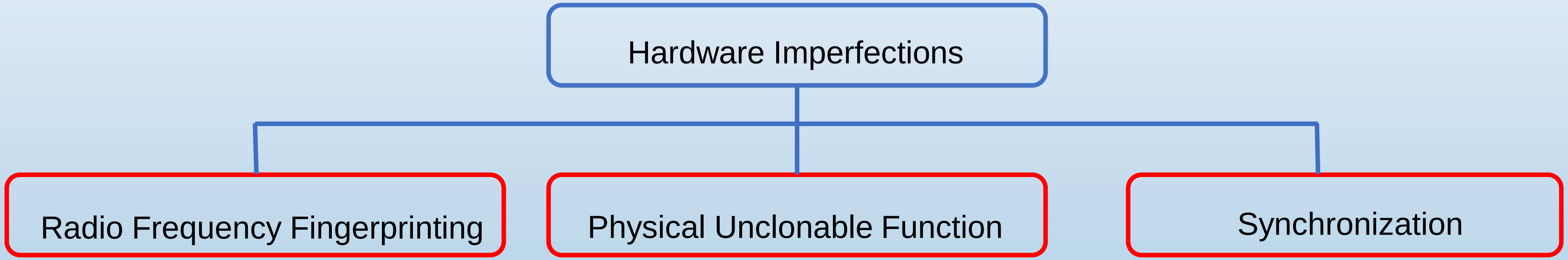
- Motivation
  - Authentication of an entity is vital to safeguard integrity and legitimacy against threats like man-in-the-middle attacks, data leakage, data injections, and jamming pose risks
  - PLA leverages inherent wireless channel characteristics or intrinsic hardware attributes, making it resilient to attacks targeting higher protocol stack layers
  - PLA strengthens cellular networks, particularly in scenarios where cryptographic methods face vulnerabilities with attacks like replay and man in the middle
  - Lower computational complexity suits resource-constrained devices, facilitating efficient authentication in high-density deployments
  - PLA schemes to bolster wireless security, the literature needs a comprehensive overview of hardware-based PLA schemes.

- Our contribution
  - A detailed survey of different PLA Schemes based on hardware imperfections over past 5 years
  - Unified taxonomy for surveyed PLA schemes
  - Key trends and findings

Assessment framework for existing PLA schemes



Hardware Imperfection based PLA schemes



- sample the received radio signal, preprocess it to eliminate noise, and extract features that distinguish one device from others.
- Received Signal Strength (RSS), Carrier Frequency Offset, Phase, Amplitude, Frequency, and more

- PUFs emphasize the hardware imperfections within integrated Circuits, utilizing their unique signal responses primarily for authentication and key generation.
- Categorised based on source on electric signal variation, randomness from source internally or externally

- Clock Skew
  - clock skews are intrinsically tied to the device's clock
  - clock skew-based schemes impact factors - aging and temperature
- Frequency Deviation
  - Frequency Shift Keying (FSK), which involves the signal deviating from its reference frequency
  - clock frequency offset and carrier frequency offset.

Methodology

Deterministic

- Hardware determinism due to imperfections – a rare phenomenon
- The distinctive and non-reproducible characteristic
- Inherent to hardware
- Can be Directly used in Cryptographic schemes

Non-Deterministic

- Observed over extended period to collect patterns
- Pattern depends on the time or external factors like temperature variations
- ML models can be trained with patterns to authenticate the hardware.
- Or Statistical methods based on threshold values

Type	Subtype	Author	Methodolgy	Approach	Application
RFF	Radio circuitry/ IQ Imbalance	Sankhe et.al	Non-Deterministic	CNN	Wireless Radio
RFF	IQ Imbalance	Oligeri et.al	Non-Deterministic	CNN	LEO Satellites
RFF	Signal Strength - Location Estimation	Ayaz et.al	Deterministic	Threshold	V2X Communication
RFF	OFDM Pilot Signals	Li et.al	Non-deterministic	2D-CNN	Passive Optical Network
RFF	Polarization	Xu et.al	Non-deterministic	CNN	LoRAWAN
RFF	Device Authentication Code - Mobility	Bassey et.al	Non-deterministic	Statistical Analysis	Zigbee / USRP / IoT
RFF + Sync-FD	CFO/Waveform	Zhang et.al	Non-deterministic	CNN	IoT
RFF + Sync-FD	CFO/Amplifier Non-linearity	Fu et.al	Non-deterministic	CNN	5G Mobile devices
RFF	SNR	Huang et.al	Non-deterministic	Ensemble Learning	Wireless Devices
RFF	Signal Strength	Nouichi et.al & Weinand et.al	Deterministic	Statistical Threshold	IoT
PUF	Generic	Mitev et.al	Deterministic	Static Algorithm	IoT
PUF	Generic	Smet et.al	Deterministic	Static Algorithm	FoG computing
RFF	Beam Pattern	Balakrishnan et.al	Deterministic	Classification	Millimeter-Waves
PUF	Memory-based	Urien et.al	Deterministic	Threshold	IoT
Sync - FD	FSK \CFO	Oh et.al	Non-deterministic	ML Classifier	Iot – WiSun Device
Sync - CS	Clock Deviation	Pestourie et.al	Deterministic	Threshold	IoT - UWB

Recent Trends and Key Findings

- Hardware imperfections are often non-deterministic, influenced by physical obstacles, signal interference, temperature, aging variation, etc. However, they may demonstrate deterministic traits within a short interval or controlled environment.
- Radio Frequency Fingerprinting PLA schemes outnumber other categories, and many prioritize a single unique hardware feature, rendering them vulnerable to exploitation by attackers.
- Non-deterministic authentication techniques have utilized the deep learning-based Convolutional Neural Network (CNN) approach
- PUF-based PLA schemes exhibit a higher level of determinism than RF-based schemes. Moreover, PUF schemes typically offer faster computational speeds than RF-based approaches.
- RF-based approaches necessitate model training over a duration, contrasting with the static algorithmic nature of PUF-based schemes.
- Research on utilizing unique synchronization-based features for authentication is a rare and emerging field. Typically, these features are integrated with other methods to bolster security guarantees further.

Conclusion

- PLA is a security measure that strengthens data privacy and integrity in wireless networks, especially in IoT and ultra-dense networks

- 33 research and survey papers from the last five years were studied
  - First, existing surveys were studied to establish an assessment framework.
  - Analyzed common hardware flaws and how they can be exploited
  - explore the methods used to differentiate between patterns that can be identified through fixed thresholds and those that require adaptive learning due to variations
  - Lastly, we summarize our findings and key insights.

Thank you for your attention