CHEDDAR

UNIVERSITY of York

3.2 Accessible Formal Verification and Debugging Framework for Secure Protocol Design and Deployment in O-RAN Systems

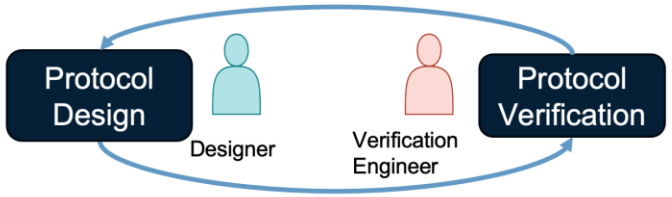
Communications Hub for Empowering Distributed clouD computing Applications and Research

3.2 Accessible Formal Verification and Debugging Framework for Secure Protocol Design

CHEDDAR

University of York

Problems and Motivation

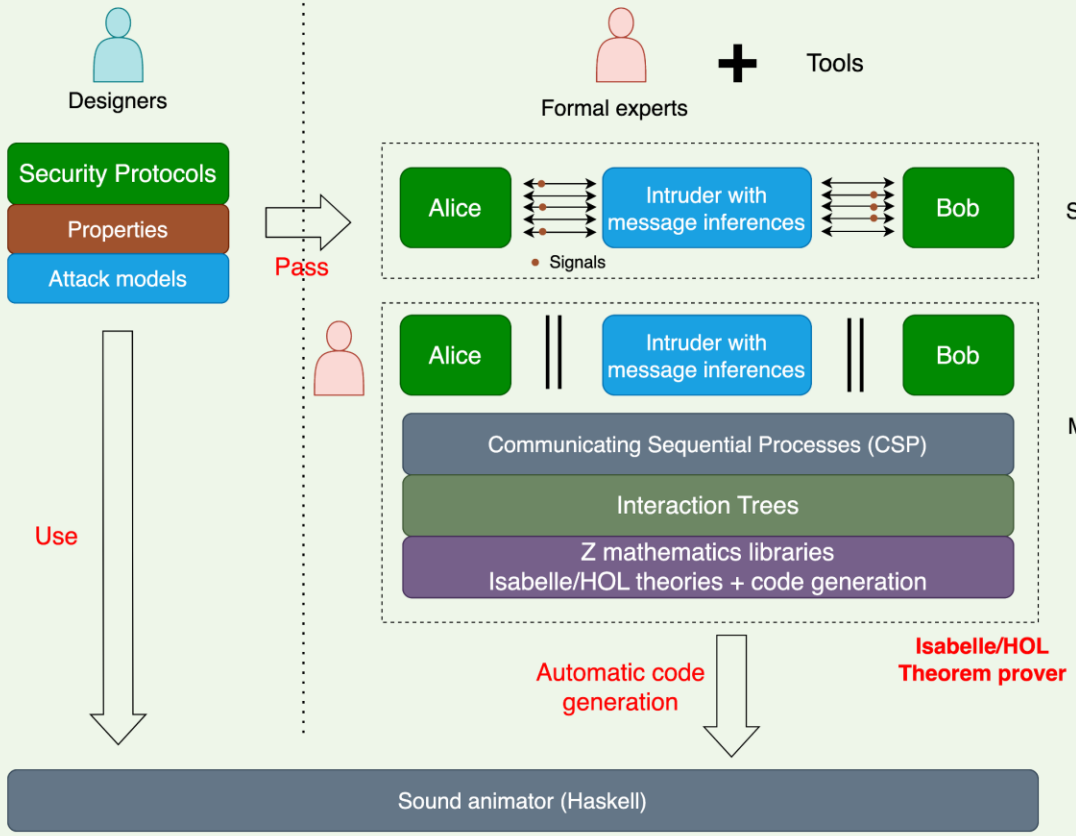


Verification Problems

- Without rigorous guarantee
- Inaccessible to designers
- Slow iteration

A real challenge is to address all problems together

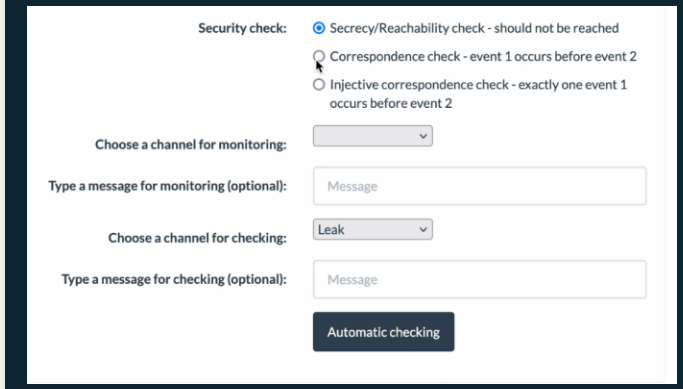
Approach: automatically generated model checker from theorem prover

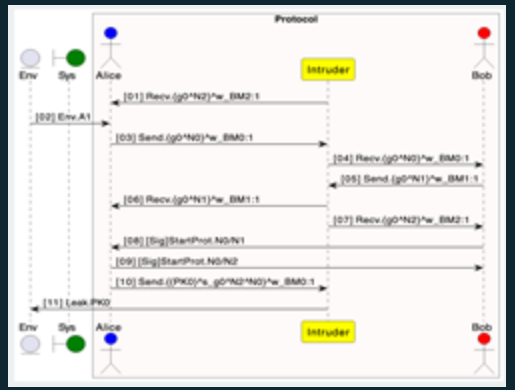


Terminal and web interfaces

```
/private/tmp/isabelle-ky582/process15874344610300865240/itree-simulate61782612> ./simulate/Simulation
/private/tmp/isabelle-ky582/process15874344610300865240/itree-simulate61782612>
Starting ITree Animation...
Events:
 (1) Env [Agent (Snatmake (Nat 0))] Agent (Snatmake (Nat 1));
 (2) Env [Agent (Snatmake (Nat 0))] Intruder;
 (3) Recv [Agent (Snatmake (Nat 1))<=Intruder] {<Nnatmake (Nat 2), Agent (Snatmake (Nat 0))>}^a_Kp (Knatmake (Nat 1));
 (4) Recv [Agent (Snatmake (Nat 1))<=Intruder] {<Nnatmake (Nat 2), Intruder>}^a_Kp (Knatmake (Nat 1));

[Choose: 1-4]:
```





Soundness

- Formal Verification
- Mathematics Proofs
- Model checker from theorem prover

Efficiency

- Automatic code generation
- Manual exploration
- Automated model checking

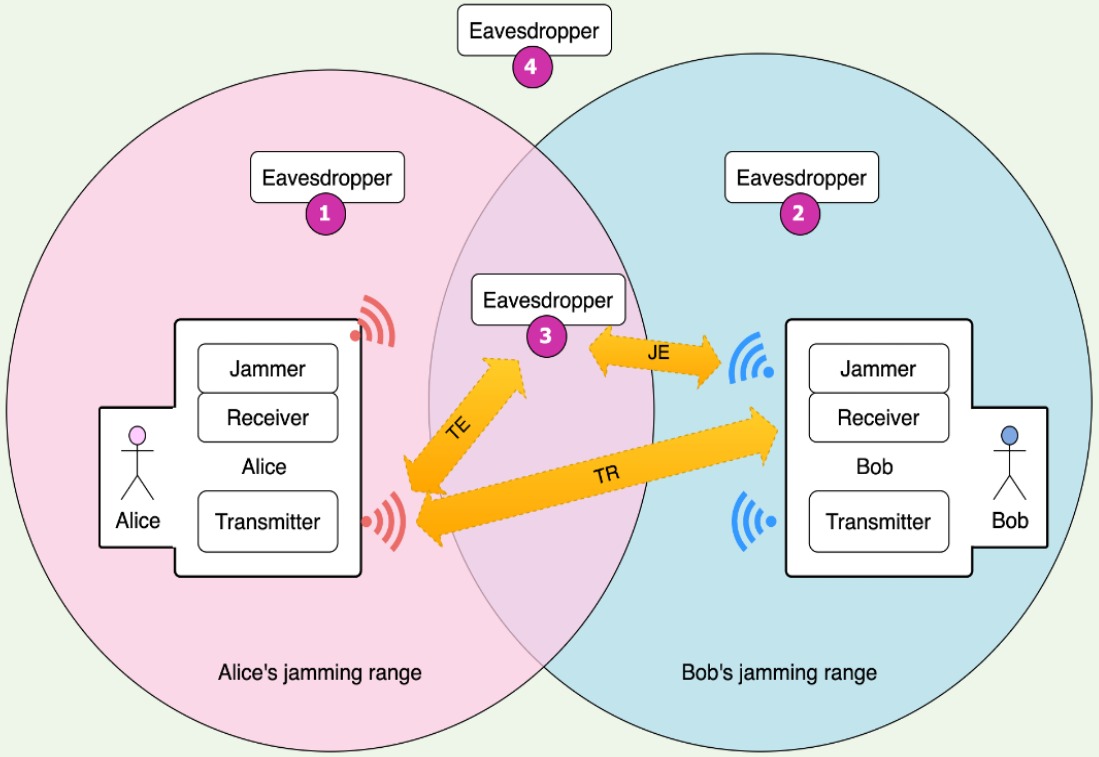
Accessibility

- Zero-Knowledge Requirement
- User-Friendly Interfaces: Terminal + Web
- User-guided verification

3.2 Accessible Formal Verification and Debugging Framework for Secure Protocol Design

Applications: PLS-based protocols

Verification of Physical Layer Security protocols using **watermarking** and **jamming** with two legitimate agents (Alice and Bob) and an eavesdropper in different spatial locations in terms of the agents' jamming ranges. There are four combinations of locations, denoted as Eve1, Eve2, Eve3, and Eve4.



Findings

Properties	NSPK	NSWJ				NSWJ Passive†				DH	DHWJ			
		E1	E2	E3	E4	E1	E2	E3	E4		E1	E2	E3	E4
Secrecy	○	○	○	●	○	○	○	●	○	○	○	○	●	○
Authenticity for Alice	●	●	●	●	●	●	●	●	●	○	●	●	●	●
Authenticity for Bob	○	●	●	●	●	●	●	●	●	○	●	●	●	●

- Needham-Schroeder public key protocol (NSPK) and Diffie-Hellman key exchange protocol (DH). Original versions are cryptographic and not secure.
- Their PLS versions (NSWJ and DHWJ): the secrecy relies on the Eve location, and authenticity always hold
- DHWJ now supports authentication though DH itself doesn't
- No difference between active and passive attackers

Visible Light Communication (VLC) with Reflective Intelligent Surface (RIS)-aided is a possible technology to implement the PLS to ensure Eve within the secure region.

Future interests

Model and verify security protocols used in IoT devices in 6G

- DTLS + Zero Knowledge Proof in Thread MeshCoP
- Ephemeral Diffie-Hellman Over COSE (EDHOC) - RFC 9528
- Privacy

Fully automated approach for Designers

3.2 Achieving Energy Efficiency and Service Availability in 6G O-RAN via Formal Verification

Problems and Motivation

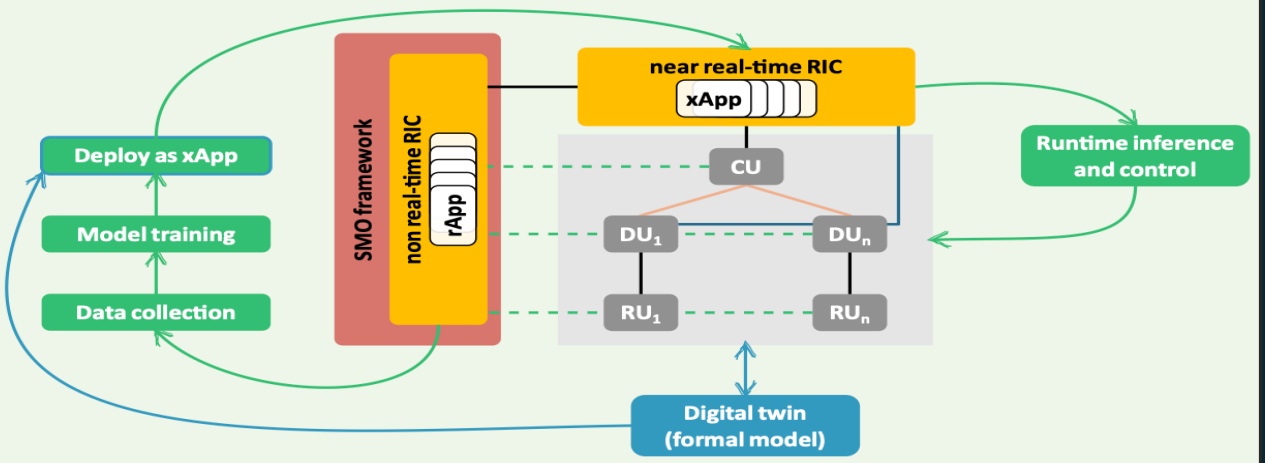
O-RAN: Open interfaces and **AI-driven applications** for real-time network optimization and energy efficiency

Challenges in balancing energy efficiency vs service availability: Continuous, highly dynamic, and adaptive management of network resources

Wrong data
- ➢ **Wrong adaptation** to real-time changes: **less efficient**
- ➢ **Misconfigurations**

Wrong algorithms in xApps
- ➢ **Logic inconsistencies**

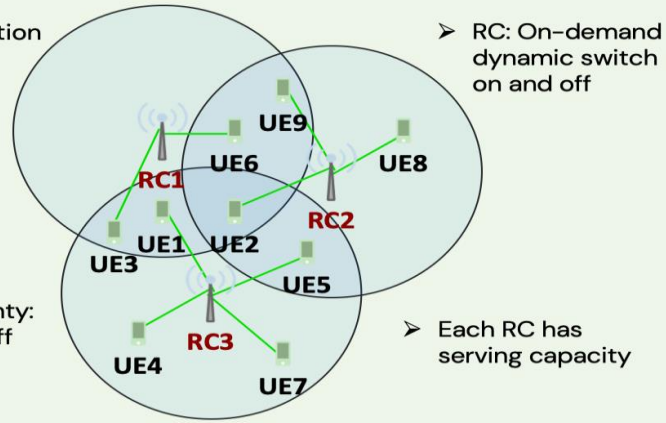
Approach: formal verification using probabilistic model checking



Create a small-scale **digital formal models** to verify properties before xApp deployment.

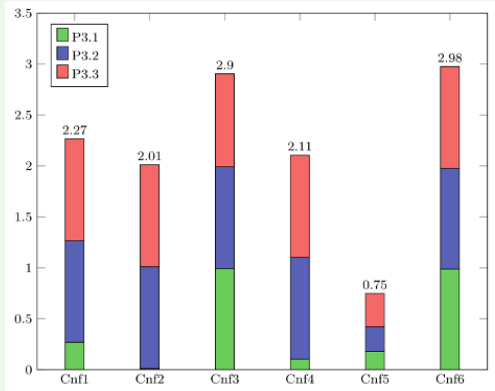
Scenario

- ➢ Fixed location
- ➢ RC: On-demand dynamic switch on and off
- ➢ Uncertainty: UE on and off
- ➢ Each RC has serving capacity

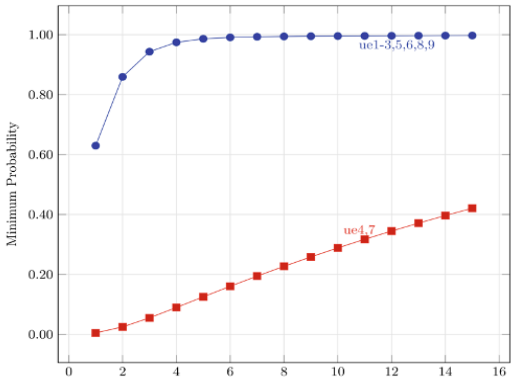


Goal: minimise the total power consumption by RCs while maintaining the QoS for each UE

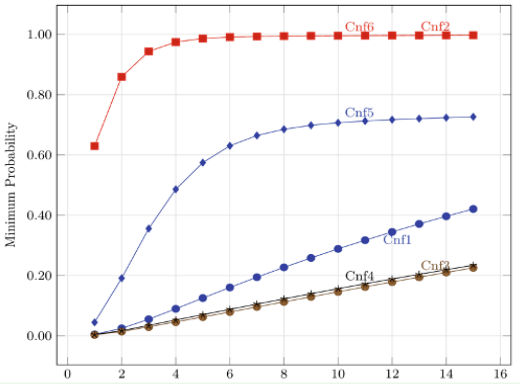
Results



Energy consumption for each RC in six configurations: capacity, uncertainty, and location differ.



The probability of a successful service connection in terms of time for each UE in a configuration



The probability of a successful service connection in terms of time for UE4 in different configurations