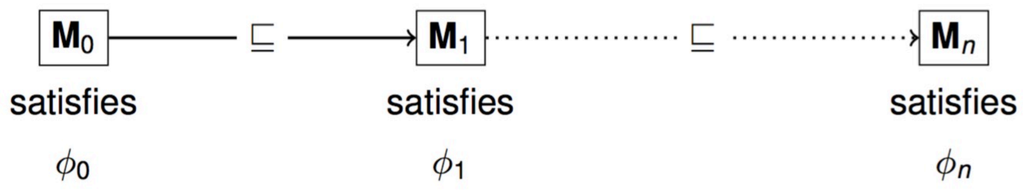
Safety and Security in IoT Systems

UNIVERSITY OF Southampton

Thai Son Hoang, Michael Butler, and Colin Snook

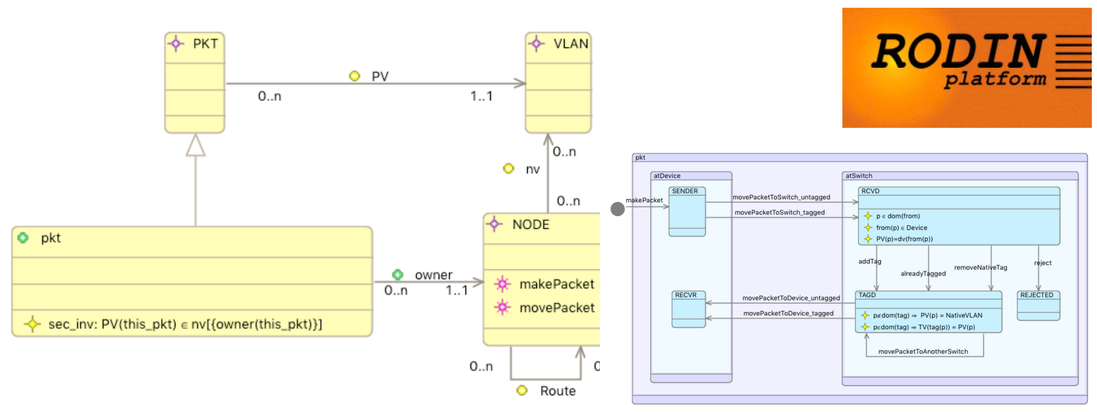
Formal System Modelling using Event-B

- First-order logic + Set theory
- Discrete transition systems
- **Refinement**: Gradually introduce model details
- **Formal proof**: Strong assurance that the system satisfies safety and security properties for all instantiations
- **Analysis**: Model checker to find counter-example
- **Validation**: Animation to ensure that the system meets its requirements



Formal System Modelling using iUML-B

- "UML-like" **diagrammatic** notation
- **Formal semantics** is given in Event-B.
- **Class diagrams** visually model data relationships
- **State-machines** visually model system dynamic behaviour



Ensuring Safety of a Multi-UAV System

Context

- Multiple UAVs "controlled" by a base station
- The routes are sent to UAVs
- **Collision-free**: No collision between any pair of UAVs
- **Restricted air space**: UAVs must avoid restricted air space

Objectives

- Develop **architecture pattern** and **verification method** for assurance of multi-UAV coordination system.

Challenges

- Complex path-planning algorithm
- Combination of human operator / automated algorithm

Approach

- **Architecture**: Separate movement generation from movement validation via **policing function**.
- **Verification**: focus formal modelling and verification on safety policing function

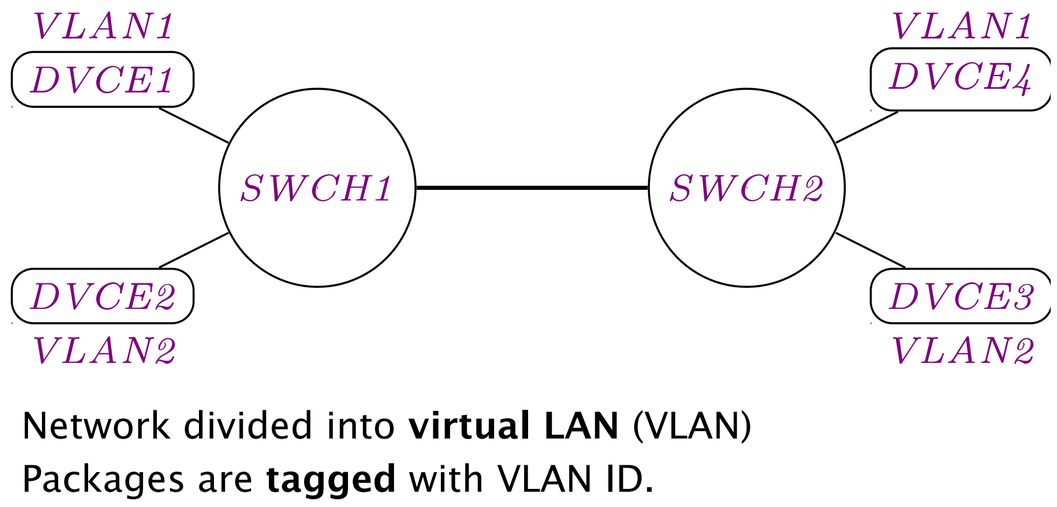
Rationale

- Movement **generation** can be **non-deterministic** and difficult to formalise
- **Safety** properties can be characterised and **formally verified**.
- **Algorithms** can be **improved** or swapped out without changing the validation approach.

(Joint work with Tekever Ltd., Southampton)

Analysing Security Protocols using Refinement

Context



- Network divided into **virtual LAN** (VLAN)
- Packages are **tagged** with VLAN ID.
- Packages for **native VLAN** do not required tagging
- A package must only be **seen by nodes in the same VLAN** as the device that made it.

Objectives

- Building approach for **develop**, **analyse**, and **verify** network protocols.

Challenges

- Properties must hold for **any network configuration**

Approach

- Build an **abstract model of the security property**
  - iUML-B class diagrams show entity relationship
  - Security properties model as invariants
- Refines to introduce **design that achieves security**
  - iUML-B state-machines show the behaviour of the design
  - V&V by animation, model checker, theorem provers

Rationale

- Identify **different points** leading to security breach
  - A **security attack** is initiated (e.g., double tagging)
  - **Design** assumptions are **violated** (e.g., tagging assumption)
  - **Security is breached** (e.g, packages to wrong VLAN)

(Case study provided by Airbus, part of Enable-S3 project)

CENTRE FOR INTERNET OF THINGS AND PERVASIVE SYSTEMS

Author contact details
Email: t.s.hoang@ecs.soton.ac.uk

C-IoT Launch Event, 26 June 2018, Southampton