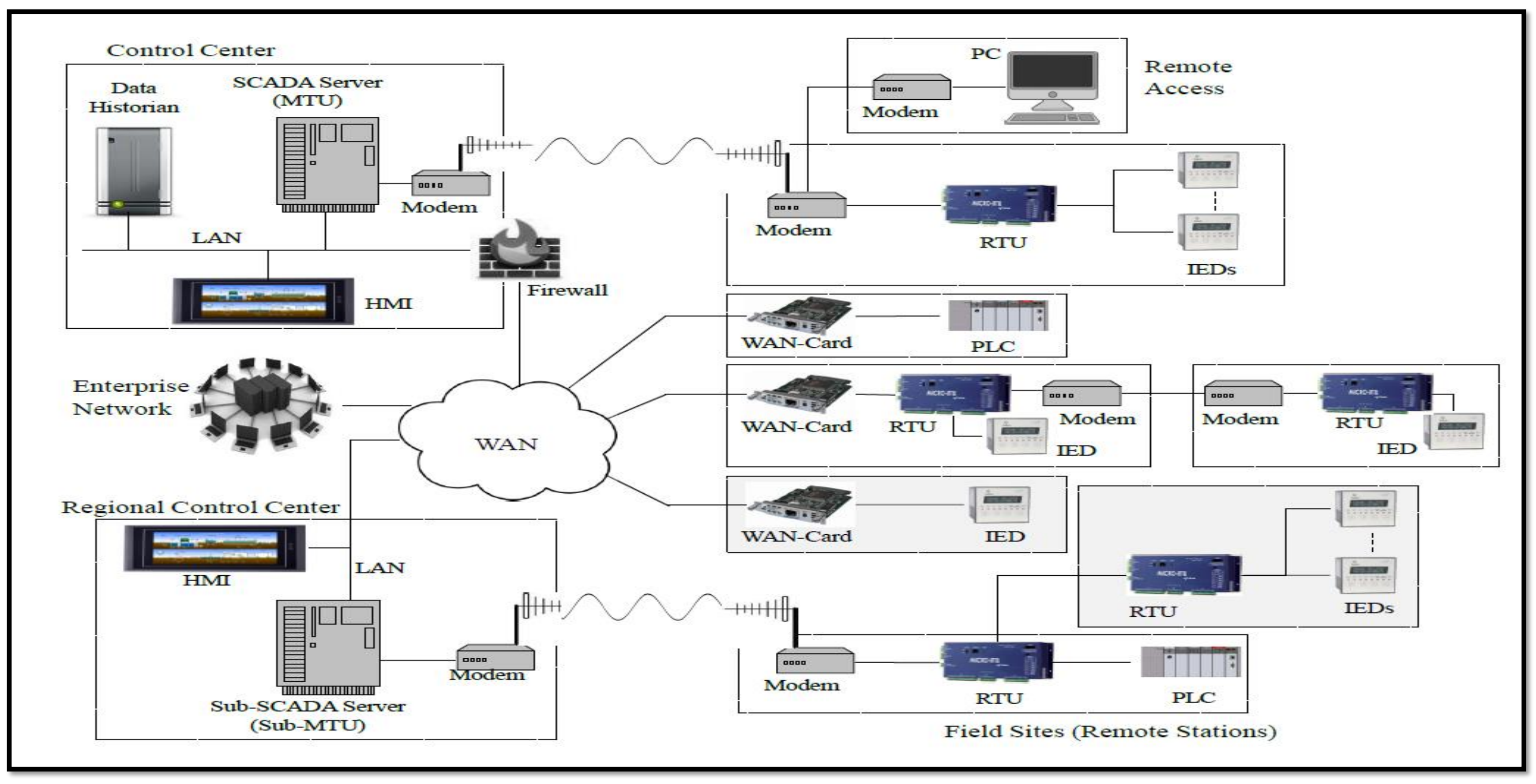
Resilient Architectures

Verification & Synthesis of K-resiliency for Dependable SCADA

Ashiqur Rahman
Abdullah Al Farooq
PI: Ehab Al-Shaer
UNC Charlotte

Motivation

Hierarchical Architecture	• Susceptible to coordinated attacks
Challenging Configuration	• Physical components with various communication and industrial protocol
Incorrect State Estimation	• Cause by data unavailability and false data injection
Control Decision	• Variety of control routines for smart grid
Resiliency Effectiveness	• Lack of scientific foundation for proactive resiliency analysis for SCADA



Research Objectives

- Developing k-resiliency properties and metrics
- Verify and measure the resiliency of SCADA configuration against state corruption and flooding coordinated attacks to ensure e2e data integrity
- Identifying attack vector and weak configuration for mi

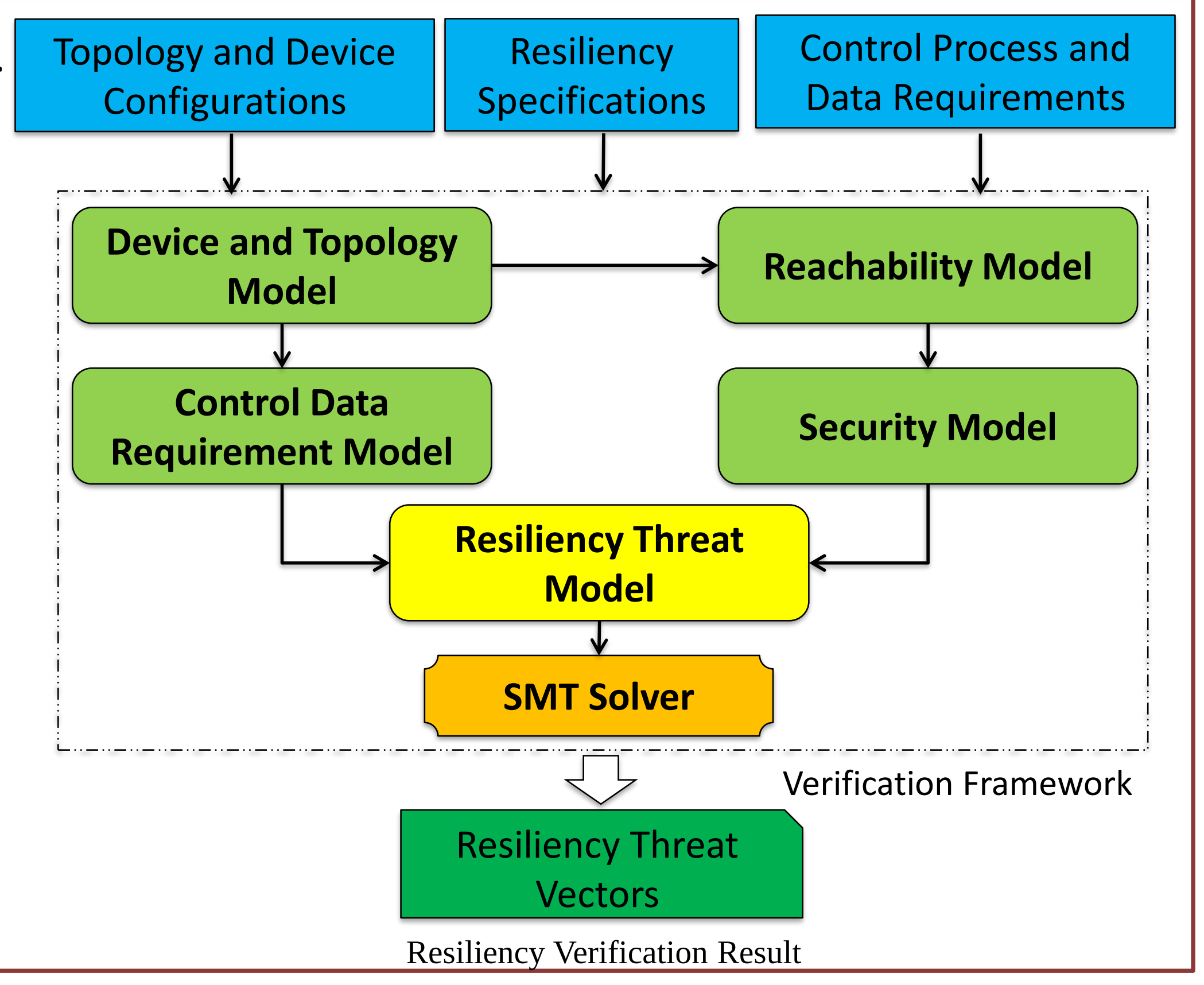
k- Resiliency

- ***k*- resilient observability** verifies whether observability is ensured if *k* field devices are attacked/unavailable (reachability).
- ***k*- resilient secured observability** verifies whether secured observability is ensured if *k* field devices are attacked (reachability & security integrity)
- **(*k*,*r*) – resilient bad data detectability** bad data is detectable even if *k* devices are attacked and *r* measurements are corrupted.

Framework

Modeling the following SMT logics

- ○ SCADA configuration,
- ○ Reachability & secured delivery among SCADA parties
- ○ SCADA Operational requirements
- ○ K-resiliency specification.



Topology and Device Configurations

Resiliency Specifications

Control Process and Data Requirements

Device and Topology Model

Reachability Model

Control Data Requirement Model

Security Model

Resiliency Threat Model

SMT Solver

Verification Framework

Resiliency Threat Vectors

Resiliency Verification Result

Model of *k*- Resilient Observability

Formalization of *k*- Resilient Observability

$$((N - \sum_{1 \le i \le N} Node_i) \le k) \wedge \neg Observability \rightarrow \neg ResilientObservability$$

$$((N_1 - \sum_{1 \le i \le N_1} (Node_i \times Ied_i)) \le k_1) \wedge$$
$$((N_2 - \sum_{1 \le i \le N_2} (Node_i \times Rtu_i)) \le k_1) \wedge$$
$$\neg Observability \rightarrow \neg ResilientObservability$$

- *Assured data delivery constraint* was formalized
- *State estimation observability constraint* was formalized

Model of *k*- Resilient Secured Observability

Formalization of *k*- Resilient Secured Observability

$$((N - \sum_{1 \le i \le N} Node_i) \le k) \wedge \neg Observability \rightarrow \neg ResilientSecuredObservability$$

$$((N_1 - \sum_{1 \le i \le N_1} (Node_i \times Ied_i)) \le k_1) \wedge$$
$$((N_2 - \sum_{1 \le i \le N_2} (Node_i \times Rtu_i)) \le k_2) \wedge$$
$$\neg Observability \rightarrow \neg ResilientObservability$$

- *Secured data delivery constraint* was formalized
- *State estimation secured observability constraint* was formalized.

Model of (*k*,*r*) – Resilent Bad Data Detection

r- Bad Data Detectability Constraint

$$\forall_Z \forall_{X \in StateSet_Z} \; S_Z \rightarrow SE_{X,Z}$$

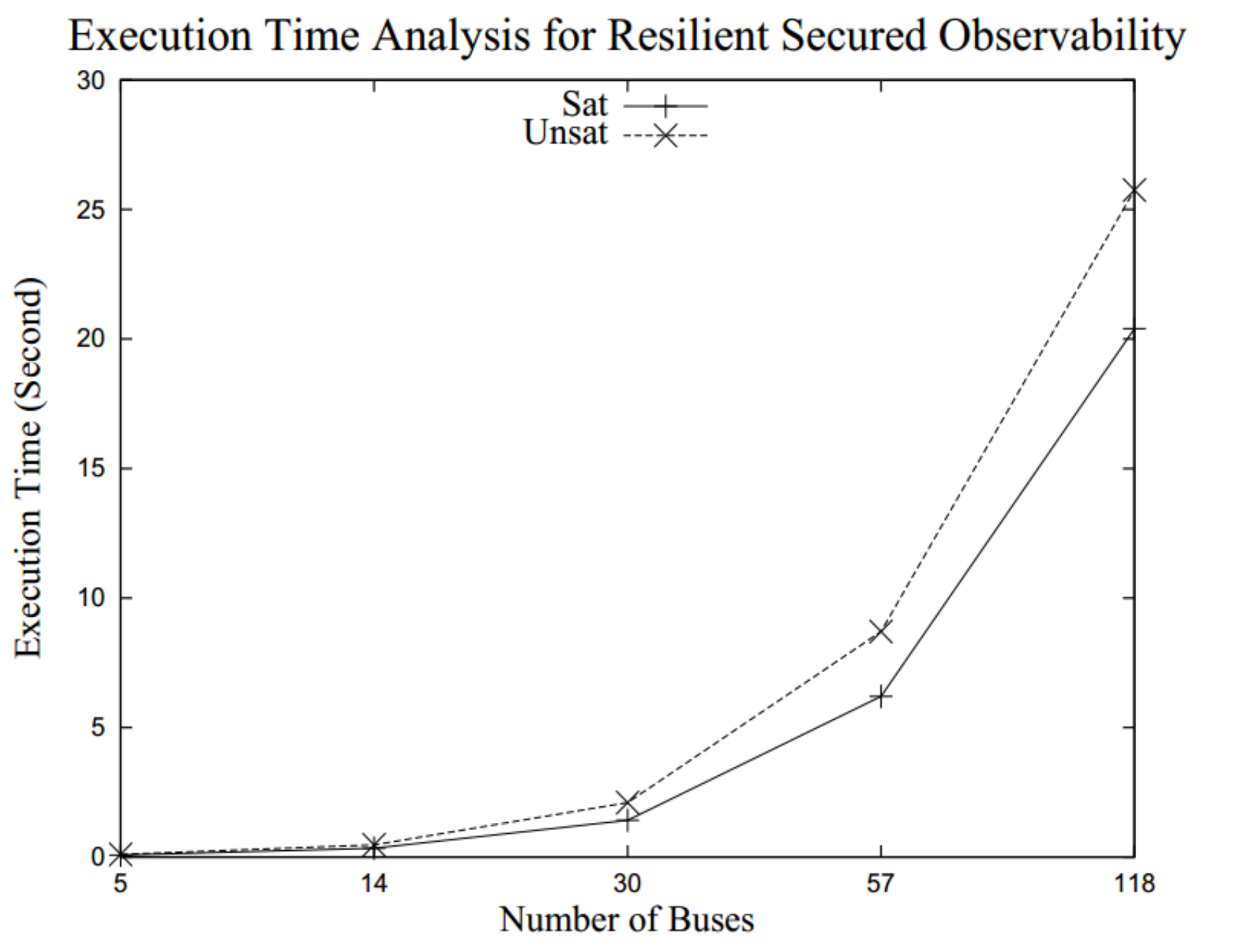
$$\forall_Z \forall_{X \in StateSet_Z} \; \neg S_Z \rightarrow \neg SE_{X,Z}$$

$$\neg BadDataDetectability \rightarrow \exists_X (\sum_Z SE_{X,Z} < r + 1)$$

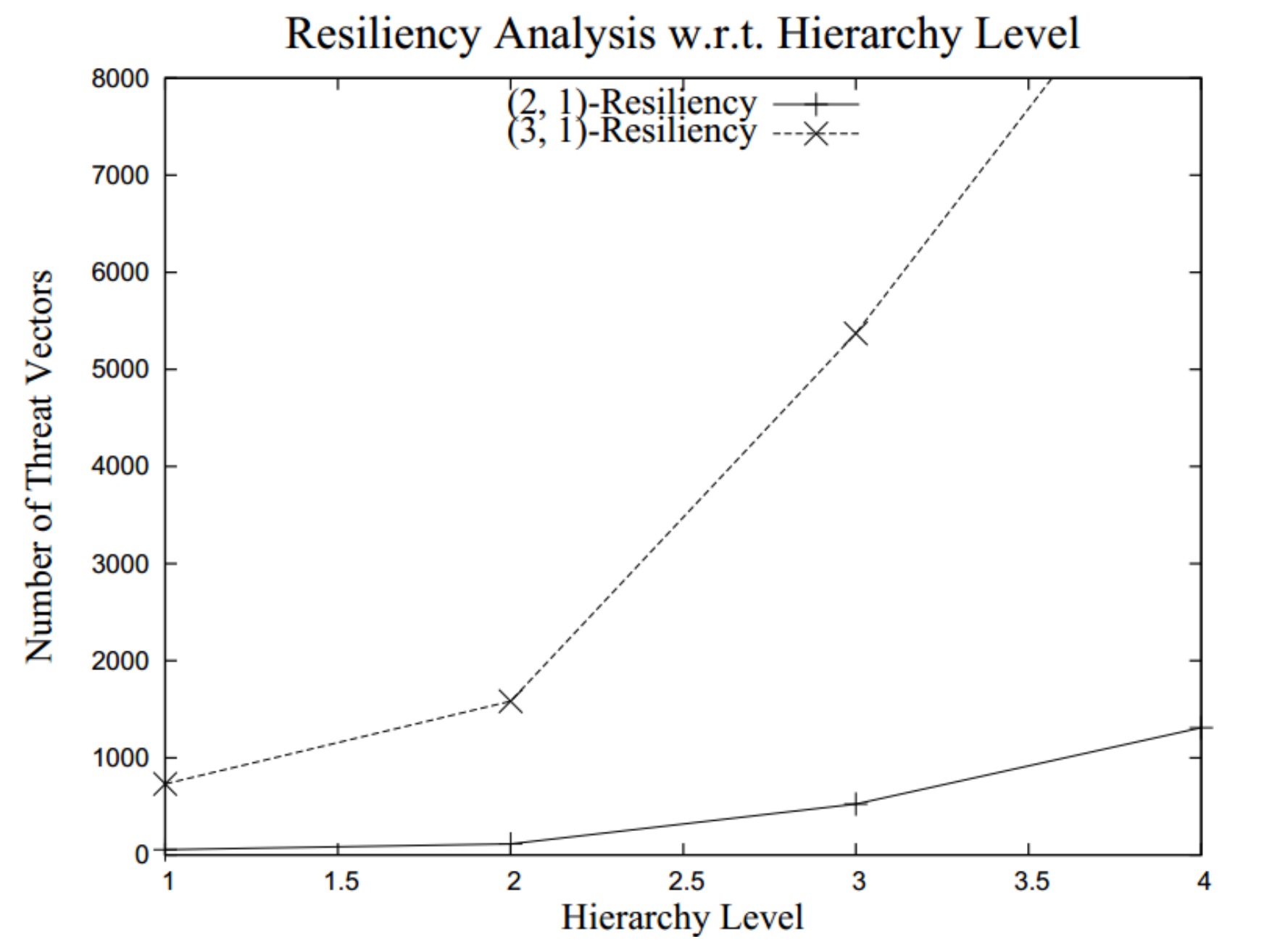
(*k*, *r*)- Resilient Bad Data Detectability Constraint

$$((N - \sum_{1 \le i \le N} Node_i) \le k) \wedge \neg BadDataDetectability \rightarrow \neg ResilientBadDataDetectability$$

Evaluation



The increase in execution time with respect to bus size lies between linear and quadratic orders.



The higher the hierarchy level, the larger the threat space

"Formal Analysis For Dependable Supervisory Control and Data Acquisition in Smart Grids", the 46th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Toulouse, France, June 2016

Science of Security Lablet

SOS Lablet Meeting
July 27-28, 2016