WP5: Application and Validation

Maurice ter Beek

FMT, ISTI–CNR, Pisa

IT MaTTerS kick-off meeting, University of Pisa

14-10-2019
Maurice ter Beek

- Member of Formal Methods and Tools lab at ISTI–CNR since ’03, coordinator since August ’19
- M.Sc. (’96) and Ph.D. (’03) degrees from Leiden University (NL)
- Positions in HU (’95–’96,’02), BE (’05), IT (’00–’01), NL (’12–’13,’15)
Maurice ter Beek
- Member of Formal Methods and Tools lab at ISTI–CNR since ’03, coordinator since August ’19
- M.Sc. (’96) and Ph.D. (’03) degrees from Leiden University (NL)
- Positions in HU (’95–’96,’02), BE (’05), IT (’00–’01), NL (’12–’13,’15)
Responsible: Maurice ter Beek

The work on WP5 will be carried out by all partners

- Demonstrate feasibility and impact of techniques, methodologies and tools developed in IT MaTTerS

- By applying them to three challenging smart-system scenarios of different scales:
  - Smart Cities
  - Smart Housing
  - Smart Transportation
Scenarios also serve to validate the methodologies, technologies and tools developed in IT MaTTerS:

- Runtime monitoring can control the interactions and sensors of the involved IoT/cyber-physical ‘smart’ systems
- Integrating runtime-monitoring techniques and control activities (such as lighting and heating services) with analyses performed at design time allow one to enforce non-functional properties (e.g. energy efficiency and security of smart-housing systems)
- Smart transportation systems cause a shift from the analysis of safety requirements of software systems that control their functioning to the development of applications to improve the user experience through efficient scheduling and management (e.g. by optimising the exploitation of railway lines or by improving the operational efficiency of a bus network via advanced bus arrival prediction systems)
Scenarios also serve to validate the methodologies, technologies and tools developed in IT MaTTerS:

- Runtime monitoring can control the interactions and sensors of the involved IoT/cyber-physical ‘smart’ systems
- Integrating runtime-monitoring techniques and control activities (such as lighting and heating services) with analyses performed at design time allow one to enforce non-functional properties (e.g. energy efficiency and security of smart-housing systems)
- Smart transportation systems cause a shift from the analysis of safety requirements of software systems that control their functioning to the development of applications to improve the user experience through efficient scheduling and management (e.g. by optimising the exploitation of railway lines or by improving the operational efficiency of a bus network via advanced bus arrival prediction systems)
WP5: Application and Validation

Scenarios also serve to validate the methodologies, technologies and tools developed in IT MaTTerS:

- Runtime monitoring can control the interactions and sensors of the involved IoT/cyber-physical ‘smart’ systems

- Integrating runtime-monitoring techniques and control activities (such as lighting and heating services) with analyses performed at design time allow one to enforce non-functional properties (e.g. energy efficiency and security of smart-housing systems)

- Smart transportation systems cause a shift from the analysis of safety requirements of software systems that control their functioning to the development of applications to improve the user experience through efficient scheduling and management (e.g. by optimising the exploitation of railway lines or by improving the operational efficiency of a bus network via advanced bus arrival prediction systems)
Scenarios also serve to validate the methodologies, technologies and tools developed in IT MaTTerS:

- Runtime monitoring can control the interactions and sensors of the involved IoT/cyber-physical ‘smart’ systems

- Integrating runtime-monitoring techniques and control activities (such as lighting and heating services) with analyses performed at design time allow one to enforce non-functional properties (e.g. energy efficiency and security of smart-housing systems)

- Smart transportation systems cause a shift from the analysis of safety requirements of software systems that control their functioning to the development of applications to improve the user experience through efficient scheduling and management (e.g. by optimising the exploitation of railway lines or by improving the operational efficiency of a bus network via advanced bus arrival prediction systems)
Smart Cities

Responsible site: GSSI Centre for Urban Informatics and Modeling

- Make L’Aquila a “smart city”
- “Environmental Monitoring”:
  - Collect and analyze data for informed decisions that improve the quality of life
  - Manage large number of sensors, with behaviour to be modelled, verified during pre-deployment and monitored at runtime
- Runtime monitoring for IoT systems is challenging:
  - Complex interaction among sensors, APIs and systems
  - Huge amount of collected data
Mining Flickr to better understand tourist behaviour

- Why analyse tourist behaviour and movement patterns?
  - To implement better destination marketing strategies
  - To develop appropriate infrastructure and transport systems
  - To improve managing social, environmental and cultural impact

- Flickr: popular photo-sharing and hosting service
  - Extract spatial distribution (coordinates) and seasonality (time)
  - Improve tourism services in most crowded areas

- GSSI: developed user-friendly instrument to easily understand spatial and temporal distribution of tourist behaviour towards tourist attractions in a specific area
Proposed architecture

Map-based View for Urban Planner

Detailed View for Urban Planner

Data Visualization

Data Analysis

Data Storage

Data Aggregator

Data Retrieval

Proposed Platform

flickr

Flickr API
Integrate new Campus with a framework for “smart housing”:
- A building with a system of devices to monitor and control activities and services

Use the techniques developed in IT MaTTerS:
- Integrate runtime monitoring techniques driven by the analyses performed at design time
- Enforce non-functional properties such as security and efficiency (e.g. reduction of energy consumption)
Concrete proposal

The new campus at Camerino consists of 20 blocks each with 4 flats.

We have developed a low-cost sensor board that allows to collect environmental data.

In IT MaTTTerS we could:

1. Develop a *predictive model*
2. Study the impact of possible control policies
3. Generate a *control system* to deploy
4. Instrument a *runtime monitor* that is able to learn environmental conditions from the acquired data.
Concrete proposal

The new campus at Camerino consists of 20 blocks each with 4 flats.

We have developed a low-cost sensor board that allows to collect environmental data.

In IT MaTTerS we could:

1. Develop a predictive model
2. Study the impact of possible control policies
3. Generate a control system to deploy
4. Instrument a runtime monitor that is able to learn environmental conditions from the acquired data
Smart Transportation (1/2)

Responsible site: Formal Methods and Tools lab, ISTI–CNR

Lab with longstanding experience in modelling and analysis of smart transportation systems, from bike-sharing to train-signalling systems

- **FP7 QUANTICOL – A Quantitative Approach to Management and Design of Collective and Adaptive Behaviours:**
  - Systematic evaluation of options for improvement (cost/benefit) of a bike-sharing system *before* actually implementing them (e.g. mean field and statistical spatio-temporal model checking)

- **H2020 ASTRail – SAtellite-based Signalling and Automation SysTems on Railways along with Formal Method and Moving Block Validation:**
  - Modelling and analysis of a moving block railway signalling scenario (e.g. statistical model checking)
Reachability properties in graphs (discretised physical space)

\[ \Phi ::= p \quad \text{[ATOMIC PROPOSITION]} \\
    \quad T \quad \text{[TRUE]} \\
    \quad \neg \Phi \quad \text{[NOT]} \\
    \quad \Phi \land \Phi \quad \text{[AND]} \\
    \quad \mathcal{N} \Phi \quad \text{[NEAR]} \\
    \quad \Phi \mathcal{S} \Phi \quad \text{[SURROUNDED]} \]

Derived operators, like interior: \( I \Phi = \neg \mathcal{N} \neg \Phi \)

Spot congestion in bike-sharing system:
- full = \([\text{vacantPlaces} == 0]\)
- cluster = \( I \) full
- eventuallyCluster = \( EF \) cluster
Probability that train enters safe state Stop upon timeout:

\[ P_M(\diamond_{\leq \text{timeout}} \text{Controlling.Stop}) \]

Uppaal SMC [Larsen et al.] reports that this probability is in the interval \([0,9.99994\times10^{-5}]\), with confidence 0.995, obtained from 59912 runs in ±5 minutes (\(M\) is the model).
Responsible site: Formal Methods and Tools lab, ISTI–CNR

- **POR–FESR STINGRAY – SmarT station INtelliGent RAilwaY:**
  - Renew the role of railway stations in the future’s smart cities (e.g. energy management and infomobility)

- **H2020 4SECURail – Formal methods and CSIRT (Computer Security Incident Response Team) for the railway sector:**
  - Develop demonstrator of state-of-the-art formal methods to evaluate the learning curve and to perform a cost/benefit analysis of adopting formal methods in railway industry

The railway sector’s robust safety requirements call for state-of-the-art formal methods and tools for modelling and analysing technological advances during development and for monitoring them at runtime.
Ideas for future work

Extensions of spatio-temporal model-checking applications developed during QUANTICOL and ASTRail

- Operational correctness of a bus network
  - Robustness of spatio-temporal requirements of train schedules to railway interruptions
  - Ciancia, Gilmore, Grilletti, Latella, Loreti & Massink @ STTT’18

- Moving block railway signalling scenario
  - Spatio-temporal requirements of moving block railway signalling protocols and verification
  - Basile, ter Beek & Ciancia @ ISoLA’18
  - Basile, ter Beek, Ferrari & Legay @ FMICS’19
31st CONCUR – 25th FMICS – 18th FORMATS – 17th QEST:
Theory, formal modelling, verification, performance evaluation and engineering of concurrent, timed and other systems

PC chair FMICS: Formal Methods for Industrial Critical Systems

http://qonfest2020.conf.tuwien.ac.at/