Rail Internet of Things: An Architectural Platform and Assured Requirements Model

Mahmoud Hashem Eiza, Martin Randles, Princy Johnson, Nathan Shone, Jennifer Pang and Amhmed Bhih
School of Engineering/Computing and Mathematics Sciences
Liverpool John Moores University
Liverpool L3 3AF, U.K.
{M.Hashemeiza, M.J.Randles, P.Johnson, N.Shone}@ljmu.ac.uk, J.P.Pang@2013.ljmu.ac.uk, A.A.Bhih@2011.ljmu.ac.uk

***Abstract*—Given the plethora of individual preferences and requirements of public transport passengers for travel, seating, catering, *etc*., it becomes very challenging to tailor generic services to individuals' requirements using the existing service platforms. As tens of thousands of sensors have been already deployed along roadsides and rail tracks, and on buses and trains in many countries, it is expected that the introduction of IP networking will revolutionise the functionality of public transport in general and rail services in particular. In this paper, we propose a new communication paradigm to improve rail services and address the requirement of rail service users: the Rail Internet of Things (RIoT). To the best of our knowledge, it is the first work to define the RIoT and design an architectural platform that includes its components and the data communication channels. Moreover, we develop an assured requirements model using the situation calculus modelling to represent the fundamental requirements for adjustable, decentralised feedback control mechanisms necessary for the RIoT-ready software systems. The developed formal model is applied to demonstrate the design of passenger assistance software that interacts with the RIoT ecosystem and provides passengers with real-time information that is tailored to their requirements with runtime adaptability.**

Keywords—Assistance; Assured model; Inclusive; IoT; Rail Internet of Things (RIoT); Situation Calculus

I. INTRODUCTION

Currently, the Internet of Things (IoT) is receiving much research attention and effort from academia and industry worldwide [1]. IoT is expected to provide the backbone of modern, smart societies and pave the way for the next generation of Internet technology. It envisages that every object, or 'thing', has a unique identifier and is able to transfer data through wired and wireless connections to the network to cooperate with other 'things' and create new services to satisfy the functional goal of the object. The number of connected devices is estimated to reach 33 billion by 2020 [2]. This revolutionary principle of connecting everything to the Internet, with the potential to bring many benefits and improve users' life styles, is advancing quickly, where many applications are seeking to take advantage of the emerging infrastructure.

Smart cities, smart energy, smart mobility and transport, *e.g.*, vehicular networks [3-5], and smart healthcare are a few examples of the IoT smart-X applications. The IoT will not be seen as an individual system, but as a critical, integrated infrastructure upon which many applications and services can run [6]. Fig. 1 shows examples of IoT applications and use case scenarios as measured using of what people search for on Google, what they talk about on Twitter, and what they write about on LinkedIn [7].

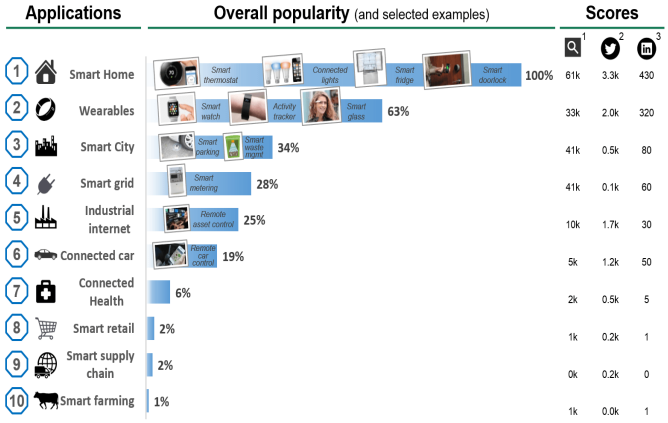

Figure 1. IoT in the context of Smart Environments and Applications

One of the main application areas currently under-investigated, that could be radically reshaped and leveraged by IoT, is the transportation sector. With the increasing demands of passengers on rail transportation, it becomes very challenging to keep public transport travel as a competitive alternative to travelling by car. As tens of thousands of sensors have already been deployed along roadsides and rail tracks, and on buses and trains in many countries, the introduction of IP networking will revolutionise the functionality of public transport in general and rail services in particular. For instance, Network Rail in the UK has signed a contract with Cisco to implement an IP Multiprotocol Label Switching (MPLS) trackside network to deliver and support a number of new services it hopes to deliver [8]. Consequently, across the rail environment, large quantities of data will be collected and utilised to provide interested parties with information relevant to their

requirements. There is, however, a significant problem with integration caused by the lack of interoperability between different systems and the need to acquire data from new assets [9]. The operational principles of IoT could be the practical solution for these issues where data sources share their output with data receivers that subscribe to receive the latest updates.

Current research is bringing forward new models, tools and techniques to support the design, deployment and management of a new generation of goal-oriented software systems. These software systems are required to exhibit agility and self-organisational capabilities, in optimising goals and operating conditions. Such models are envisaged to support emerging systems of systems and the IoT to bring forward new models of interaction and autonomous intelligent provision of data and services to rail service users; a Rail Internet of Things (RIoT) system. However, little is known on the foundation of IoT ready systems design and management; and in particular the fundamental requirements for adjustable, decentralised feedback control mechanisms necessary for software systems ready to take advantage of RIoT.

In this paper, we aim to understand and utilise the design principles of networked cognitive observers on complex heterogeneous systems such as RIoT. This will support new models of decentralised situated feedback control mechanisms, which cater for the scale, unpredictable dynamics, and heterogeneity anticipated in the RIoT system and exhibit these requirements in an assured requirements model using the situation calculus modelling. This will involve producing formal models suitable to represent requirements, design, implementation, and testing. Finally, we apply the developed requirements formal model to demonstrate the design of assistance software that interacts with RIoT and provides passengers with the required real-time information to meet the individual needs of the passengers.

The rest of this paper is organised as follows. Section II overviews the state-of-the-art of utilising IoT in transportation. Section III presents the architectural platform of the RIoT system including its components, structure, and simplified data flow model and discusses its security requirements and concerns. The optimised service platform for RIoT is developed in Section IV including an assured requirements model and a demonstration of the design of passenger assistance software using some examples from the rail environment. Finally, Section V concludes the paper.

II. State of the Art

To the best of our knowledge, there are no previous studies on utilising IoT to improve the public transport passengers' experience. The majority of the current research focuses on employing IoT for monitoring purposes only [10, 11].

In [12], Fu *et al*. proposed Wisdom subway information platform, an intelligent information platform for a subway system based on IoT. Wisdom platform depends on four layers namely IoT sensing layer, data transmission layer, data processing layer, and platform application layer. The IoT sensing layer is composed of communication signal sensors, locomotive equipment sensors, and wireless sensors to monitor the temperature, humidity, and smoke in the subway station. The IoT sensing layer transmits the collected information to the data processing layer through the data transmission layer. This multi-sensor data is then fused and utilised to monitor the rail transportation equipment and infrastructure and provide early warning messages of any predicted failure.

In [13], Kim *et al*. proposed three location-based services for assisting mobility for visually impaired (VI) people using an IoT infrastructure. These services are Swipe and Scan Your Surroundings (SaSYS) [14], TalkingTransit [15], and Smart Building Application. They can be used from a smartphone utilising its built-in sensors and customised gestures without requiring additional hardware like Braille keyboards [16], vibrotactile motors attached to a smartphone [17], vibrotactile bracelet [18], *etc*. The authors proposed an IoT environment where 'things' and places, *i.e.*, points of interest, are assigned with unique identifiers (*ucode*), which are 128-bit numbers that can be stored into any type of tag medium such as RFID, QR-code, NFC, *etc*. Sensors for location-awareness and environment sensing are deployed indoors and outdoors. The collected information is then stored in the cloud while the *ucodes* are utilised to manage, access, and control every 'thing' uniquely through web APIs [19, 20]. In this way, visually impaired users can easily access rich information about their surroundings and find their way to their destination that could be a general store, bus stop, or train platform.

III. Rail Internet of Things (RIoT): An Architectural Platform

In this section, we propose an architectural model for the RIoT system and provide examples to demonstrate how the RIoT can improve rail passengers' experience.

A. RIoT System Components

In the RIoT system, the following components are expected to coexist and interact among each other.

1) ***Trains.*** Each train is composed of many passenger cars, *i.e.*, coaches, where different types of technologies are installed such as heat sensors, capacity/seats sensors, beacons, Wi-Fi hotspots, *etc*.

2) ***Tracks.*** In the RIoT system, tracks only interact with trains and the central rail control system. Different technologies are installed along the tracks such as GSM-Railway (GSM-R), RFIDs, and balises.

3) ***Stations.*** Different objects and systems can be found in a rail station including the rail information system, ticketing system, Wi-Fi hotspots, beacons, vending machines, *etc*.

4) ***Passengers.*** This component of the RIoT system presents the smart devices and/or wearable devices that passengers may have and/or wear. These devices contain

many sensors that could provide specific information related to the journey requirements, *e.g.*, location, destination, journey preferences, *etc*.

5) ***Rail Control Centre (RCC)***. RCC coexists alongside RIoT components and interacts with them through the current rail communication network. Moreover, RCC can harness the available information in RIoT to help rail operators to plan for a better rail service.

Fig. 2 shows the architectural platform of the RIoT system.

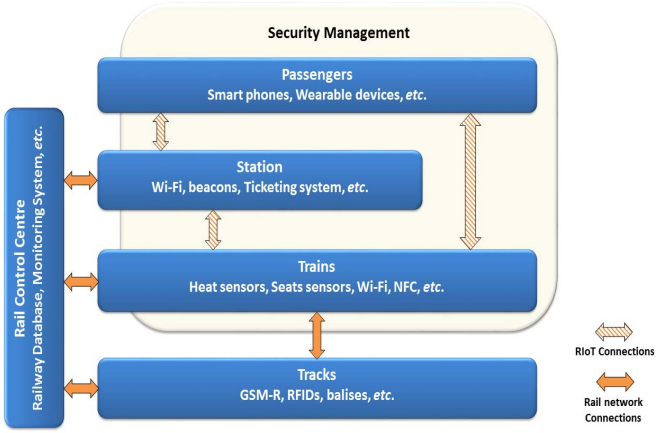

Figure 2. RIoT System: An architectural platform

B. *Simplified Data Flow Model in RIoT*

The RIoT system integrates effortlessly alongside the current rail communication network by utilising existing data resources leveraged with a digital eco-system to allow enhanced RIoT capabilities to optimise the rail passenger's experience. To model the data flow among RIoT system components, as shown in Fig. 2, we use the reduction semantics of π *Calculus*, a process algebra. The process in process algebra refers to the behaviour of a system that can be defined as all possible actions or events the system can perform. π *Calculus* can model concurrent computations, which allows data channels to work in parallel by sending and receiving messages. As we simply wish to express the communication channels between the data resources, π *Calculus* fits this purpose as it has clear and concise semantics.

1) ***Passenger-to-Station-to-Train.*** In the RIoT system, passenger and station behavioural events could range from passengers waiting at the station having access to variable real-time data available through their RIoT software such as (*a*) valuable data that includes real-time train data, indicating exactly how many more minutes their train is away from pulling into the station and which platform it is approaching, (*b*) assistance data that includes giving the location of all station facilities, with an assisting 'where am I?' feature providing the quickest or the shortest route navigation through the station, and (*c*) convenience data that includes listing the locations of lifts, toilets, and vending machines with the added feature of product availablility, prices, and stock level indicators.

Using π *Calculus* to model passenger P_n and station S_n processes, given if $\bar{x}(d_1)$ represents the sending of data d_1 along the channel x from process P_n to process S_n, where e_1 is a place holder to be substituted by the arriving data, then for processes P_n and S_n, we write:

$$\bar{x}(d_1) * P_n \,||\, x(e_1) * S_n = P_n \,||\, S_n\left\lfloor {}^{d_1}\!/_{e_1} \right\rfloor \tag{1}$$

2) ***Passenger-to-Train.*** For passenger and train behavioural events, we expect the RIoT system to be able to provide on-board passengers with (*a*) real-time valuable data such as the time left until arrivng at their destination and the current location of the train, with an optional pre-programmable feature to remind the passenger prior to arriving at their destination, (*b*) assistance data that could enable the passenger to change his/her seat location as well as locate warmer seats within coaches and other on-board facilities, such as nearest toilets and whether they are currently vacant or occupied, and (*c*) convenience data that includes the location of the on-board cafe or trolley with an added feature of the current price list of products and stock-levels.

Similarly, for passenger P_n and train T_n processes given if $\bar{y}(d_2)$ represents the sending of data d_2 along the channel y from process P_n to process T_n, where e_2 is a place holder to be substituted by the arriving data, then for processes P_n and T_n, we write:

$$\bar{y}(d_2) * P_n \,||\, y(e_2) * T_n = P_n \,||\, T_n\left\lfloor {}^{d_2}\!/_{e_2} \right\rfloor \tag{2}$$

C. *RIoT System Security Management - Requirements & Analysis*

As shown in Fig. 2, the RIoT system is a large-scale, distributed, and decentralised network, which possesses many characteristics that make it difficult to manage and secure. Its ad-hoc, dynamic, and open nature means that traditional boundary-based security is extremely difficult to define or enforce. Therefore, there are numerous security concerns that need to be taken into consideration whilst operating the RIoT system.

Currently, the preeminent security obstacle facing the (R)IoT is the limited computing capabilities of its constituent 'things', *e.g.*, sensors, actuators, and controllers [6]. These limited capabilities are rendering some devices unable to adequately secure their communications. For instance, some devices have insufficient processing power to run cryptographic algorithms, *e.g.*, asymmetric encryption, or security protocols such as Transport Layer

Security (TLS) [21]. This leaves leaving devices susceptible to a wide range of basic and remediable security attacks, such as cross-site scripting (XSS) and brute force password cracking [22]. Unfortunately, the majority of IoT devices are still in an early stage of development and the standard of security is poor, as manufacturer focus is on time-to-market. This point is emphasised by a recent study by HP labs, which found that 70% of the devices surveyed were using unencrypted communications [22].

Currently, there are several potential attack vectors that may face RIoT devices, the most significant of which are as follows:

- *Exploitation of Lax Device Security*. Many RIoT devices lack adequate security, whether this refers to their communication channels, interfaces, update mechanisms or authentication strategies. Presently, IoT devices have an inherent trust of local networks, *i.e.*, not requiring local authentication, but with the number of remote access technologies this is a dangerous strategy that must be mitigated. The lack of confidentiality, *i.e.*, no encryption or integrity checking mechanisms in IoT makes devices and their data highly vulnerable to a multitude of attacks, including eavesdropping, credential theft, payload manipulation, and other man-in-the-middle strategies.
- *Privacy Abuse*. One of the largest growing problems within the whole IoT concept is the issue of privacy. As services become increasingly tailored to user needs, data collection is becoming a highly intrusive, ubiquitous, and opaque process. Users are increasingly unaware of why, how or when their data is collected, or how it is used. Currently, there is no enforcement of private data collection to ensure that only data required for the provision of functionality is collected. Additionally, the heterogeneous nature of RIoT means that it is composed of devices from a multitude of geographical locations and manufacturers. Each operates their own privacy policies and there is no standardisation amongst the RIoT devices. In a recent investigation by HP labs [22], 80% of the IoT devices surveyed raised privacy issues and 90% were observed to be collecting personal information.
- *Physical Tampering*. As RIoT devices are embedded in a public environment, they are highly susceptible to physical interference. This can refer to malicious or accidental damage, alteration of the device's surroundings to falsify readings, *e.g.*, putting heat source next to a heat sensor, or the misuse of physical ports.
- *Signal Injection*. This involves impersonation of genuine devices in order to inject falsified sensor data values into the system [23], *e.g.*, masquerading as a smoke detection sensor to send fabricated data to the fire system thus simulating the presence of fire.
- *Side-channel Attacks*. These are sophisticated attacks that rely on information gained from the physical implementation of cryptographic techniques, rather than using brute force or vulnerability exploitation. For instance, information such as timing, power consumption or acoustic output can be utilised to break the system [24].
- *Denial of Service*. The computational limitations of many devices in RIoT also limits their ability to deal with mass-driven attacks, such as Denial of Service (DoS) or Distributed DoS (DDoS) attacks. These kinds of attacks can cause malfunctions or render devices unusable, which could have potentially catastrophic consequences.
- *Denial of Sleep*. Some devices in RIoT, especially sensors, rely on battery packs as their only source of power. To preserve power, these devices reside in a state of sleep when they are not in use. However, knowledge of a device's power configuration can facilitate the orchestration of attacks designed to prevent sleep. This ultimately leads to the deterioration of the device's lifespan, *e.g.*, reducing it from years to days, which can have a devastating impact on the network.
- *Wireless Signal Jamming*. The majority of RIoT devices utilise wireless communication methods, *e.g.*, GSM-R, Wi-Fi, Bluetooth, NFC, ZigBee, *etc*. Unfortunately, this means they are also susceptible to attacks that can degrade or disrupt these radio signals [25]. Thus leading to reduced network functionality or accessibility.
- *Rogue/Malicious Devices*. RIoT systems are inherently vast and form complex networks, comprised of thousands of individual devices. Therefore, there is a risk that rogue devices or access points could be deployed, in an attempt to steal information from unsuspecting users [26].

In order to mitigate these threats, we propose the implementation of the following mitigation strategies within the RIoT system.

- Ensure all communication channels are encrypted; this will either involve developing lightweight cryptographic techniques or utilising sensors with enhanced computing capabilities.
- Develop a lightweight and scalable form of authentication and access control for use throughout the RIoT. These crucial techniques need to be adaptable, contextually-aware, and identity-aware to be suitable for such a highly dynamic environment.
- Increase security standardisation by implementing a RIoT-wide security and privacy policy, which all deployed devices must adhere to. As there are many basic measures that can be put in place on RIoT devices to mitigate the majority of security threats.
- Perform risk analysis of all devices before their deployment, to identify and mitigate existing

security risks, *e.g.*, open ports and lack of authentication.
- Increase the transparency of the personal data collection process and implement privacy-management techniques to ensure only necessary data is gathered.
- Ensure the adequate redundancy provision of devices to protect against failure, corruption, and signal jamming.
- Implement device load-distribution mechanisms to protect against signal jamming and to ensure availability at peak periods.
- Implement physical measures to reduce the risk of device tampering, *e.g.*, mounting out of reach or using disguised casing.

IV. Optimised Service Platform for RIoT

It is clear that the nature and scope of the RIoT system necessitates the formulation of a novel approach to setting the system requirements. In essence, the full requirements of the system cannot be fully specified or known at design time and so it must be possible for the system to adapt to requirements at runtime. The operative function through these processes is observation. This observation and the methods of achieving reliable observation are crucial to this work.

Therefore, we propose an observer system that allows the RIoT system to be seen as component parts, of a single parent level, with interactions that cause the whole system behaviour not to follow in a linear manner, but rather emerge from the interactions of the components. The RIoT system ought to use its own computational resources to perceive, through sensors and instrumentation, and perform operations, through procedures and effectors, to ground its symbol set to interpret system signals. This will then permit the implementation of known emergent behaviour, through the observer system, as a Markov Decision Process using in this case the Situation Calculus [27].

The proposed observer system is built around the deployment of appropriate monitoring and sensing modules, with guards to bound component autonomy and ensure legitimate operation, for the system components. These components may be further reduced to component level with appropriate monitoring and guard facilities. Through this representation, the formal account can be expressed from any reasonable perspective.

The flexibility of this observer model lies in its self-similar structure at each hierarchical level of the RIoT system. Each, separated out, observer monitors a set of components, which may themselves consist of components with separate observer systems. Thus, the system is open-ended in either direction through the hierarchy and may be followed upwards, where more high-level goals may be set, or downwards to ever-smaller components, where more low level functional goals will be satisfied.

A. RIoT-ready Software Fundamental Requirements Model

In order to accommodate runtime composition of user requirements into customised software based on RIoT device, monitoring, reasoning, deduction, and induction need to be performed on the data to supply receptors for perceived signals. In this way, new interactions that cause no harm, and may be beneficial, are allowed. In line with situation calculus, action histories are considered where if s is a sequence of actions, *i.e.*, a history, then do (a, s) represents the new action history of adding the action a to the sequence s. Sensing results for the system can then be evaluated. For instance, the action history can be represented as follows.

$$do(a_1, do(a, s)) \text{ with } SR(a, s) \neq SR(a_1, do(a, s)) \quad (3)$$

Here, $SR(a, s)$ is the sensing result based on the sensing action a, $a = sense_f$ for attribute f, and a_1 is a deterministic action that can be used to provide a new prediction for the results of action a where the values of other attributes in situation s form the action precondition axioms for a_1 as a context. In this way, action a_1, executing in the context of situation s, grounds the signal for f.

It is now possible to begin specifying the requirements for the RIoT system that are captured by RIoT itself. Assume an attribute $Alert(s)$ that brings attention to a RIoT component, *e.g.*, a sensor or a coach, when it is working at over 60% capacity. The load sensing action is $a = sense_{LOAD}$ and $Load(s)$ indicates if there is a load in the situation s. Using (3), we can write:

$$Load(do(a, s)) \Leftrightarrow [Load(s) \wedge a \neq sense_{LOAD}] \vee [a = sense_{LOAD} \wedge SR(sense_{LOAD}, s)]$$

$$Alert(do(a, s)) \Leftrightarrow [Alert(s) \wedge ((a \neq sense_{LOAD}) \vee \neg (a = sense_{LOAD} \wedge SR(sense_{LOAD}, s) < 60))] \vee [a = sense_{LOAD} \wedge SR(sense_{LOAD}, s) > 60]$$

Thus, an action a_1 may be assigned a predicted outcome via the construct in (3) to deduce

$$Knows(Alert, s) \wedge Knows(\neg Alert, do(a_1, s)) \quad (4)$$

Here, $Knows(Alert, s)$ indicates that the system is now aware of the alert situation and $Knows(\neg Alert, do(a_1, s))$ indicates that when a_1 is performed, the alert situation ends.

B. The Passenger Assistance Software

The previous subsection shows how the application may ground signals to be used for future scenarios, allowing the system to adapt to new circumstances. In order to show how the specification is directly executable, a use case may be considered. Examples includes: Instant updates to traveller information with Notifications/Announcements; 'Take me to the warmest coach' request; Guidance to the coach with specific facilities, *e.g.*, toilets, wheelchair space, bike space, *etc*.; 'Change my seat during the journey' requests, *etc*. All of these rely on an alert raised from a RIoT device that

belongs to the passenger. There are, thus, a number of primitive actions:

- *Forward*(*n*). Move forward to coach *n*
- *Back*(*n*). Move back to coach *n*
- *Cancel*(*n*). Turn off the alert for coach *n*

where *n* is the coach *ID* number. There are also attributes:

- *CurrentUnit*(*s*) = *n*. In situation *s*, the passenger is in coach *n*.
- *On*(*n*, *s*). In situation *s*, there is an active alert in coach *n*.

Additionally the actions will have preconditions:

- *Poss*(*Forward*(*n*), *s*) → *CurrentUnit*(*s*) > *n*. It is possible to move forward to coach *n* if the passenger is in coach *n*-1.
- *Poss*(*Back*(*n*), *s*) → *CurrentUnit*(*s*) < *n*. It is possible to move back to coach *n* if the passenger is in coach *n*+1.
- *Poss*(*Cancel*(*n*), *s*) → *On*(*n*, *s*). It is possible to turn off the alert if the passenger is in coach *n*.

With successor state axioms:

$$CurrentUnit(do(a, s)) = n \Leftrightarrow a = [Forward(n) \vee a = Back(n) \vee (CurrentUnit(s) = n \wedge (\neg(\exists n)\, a = Forward(n) \wedge \neg(\exists n)\, a = Back(n))]$$

$$On(n, do(a, s)) \Leftrightarrow On(n, s) \wedge a \neq Cancel(n)$$

Fig. 3 shows a pseudo code implementation indicating a direct execution in *Prolog*.

```
%Basic control actions

action(cancel(N)).       %Cancel alert in coach N
action(forward(N)).      %Move forward to coach N
action(backward(N)).     %Move backward to coach N

%Complex control actions

CCA(goUnit(N), ?(currentUnit(N)) #forward(N) #back(N)).
CCA(attend(N), goUnit(N): cancel(N)).
CCA(attendAunit, (?(nextUnit(N)): attend(N))).

/* Main control loop. While there is an active alert, a coach is attended */

CCA(control, while(some(N, on(N)), AttendAUnit): idle).

%Preconditions

Poss(forward(N), S):- currentUnit(M, S), M > N.
Poss(back(N), S):- currentUnit(M, S), M < N.
Poss(cancel(N), S):- on(N, S).

%Successor states

currentUnit(M, do(A,S)):- A=forward(M); A=back(M); not
A=forward(M), not A=back(M), currentUnit(M,S).
on(M, do(A, S)):- on(M, S), not A = cancel(M).
```

Figure 3. A *Prolog* type requirement implementation

V. CONCLUSION

In this paper, we investigated the utilisation of IoT to address the requirements of rail service users and leverage the services provided by the rail transport. More specifically, we proposed the Rail Internet of Things (RIoT) system that is composed of passengers, trains, stations, tracks, and rail control centre. We discussed the security concerns of the RIoT system and suggested specific mitigation strategies. To address the scale, unpredictable dynamics, and heterogeneity of the RIoT system, we developed an assured requirements model using the situation calculus modelling. This model is then utilised to show how passenger assistance software can be specified. It has been shown that utilising IoT is a very promising opportunity to improve public transport services and travelling passengers' experience. Our future work consists of simulating the propose RIoT system and perform lab experiments to verify its usability.

ACKNOWLEDGMENT

The authors would like to thank Professor Qi Shi for his support and encouragement in writing this paper.

REFERENCES

[1] IERC-European Research Cluster on Internet of Things, "Internet of Things Pan European Research and Innovation Vision," European Communities, 2011. [Online]. Available: http://www.internet-of-things-research.eu/pdf/IERC_IoT-Pan European Research and Innovation Vision_2011_web.pdf. [Accessed 18 05 2015]

[2] D. Mercer, "Connected World the Internet of Things and Connected Devices in 2020," Strategy Analytics, Oct 2014.

[3] M.H. Eiza and Q. Ni, "A Reliability-Based Routing Scheme for Vehicular Ad Hoc Networks (VANETs) on Highways," in Proc. Of the IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), June 2012, Liverpool, pp. 1578-1585.

[4] M.H. Eiza and Q. Ni "An Evolving Graph-Based Reliable Routing Scheme for VANETs," IEEE Transactions on Vehicular Technology, vol. 62, no. 4, pp. 1493-1504, May 2013.

[5] M.H. Eiza, T. Owens and Q. Ni, "Secure and Robust Multi-Constrained QoS aware Routing Algorithm for VANETs," IEEE Transactions on Dependable and Secure Computing, vol. PP, no.99, pp.1-1, Jan 2015. DOI: 10.1109/TDSC.2014.2382602

[6] J. A. Stankovic, "Research Directions for the Internet of Things," IEEE Internet of Things Journal, vol. 1, no. 1, pp. 3-9, 2014.

[7] K. L. Lueth, "The 10 most popular Internet of Things applications right now," [Online]. Available: http://iot-analytics.com/10-internet-of-things-applications/ [Accessed 24 08 2015]

[8] A. Scroxton, "How the internet of things could transform Britain's railways," August 2014. [Online]. Available: http://www.computerweekly.com/feature/How-the-Internet-of-Things-could-transform-Britains-railways. [Accessed 18 05 2015].

[9] T. Taberner, "How the Internet of Things will change the way we monitor the Railways," Eurotech UK, 2013. [Online]. Available: http://www.eurotech.com/dla/Library/WP/Eurotech-White-Paper-Rail-Solutions-FINAL.pdf

[10] Wind River Systems, "Internet of Things: Transportation Use Case," Wind River Systems, Inc., Alameda, US, 2014. [Online]. Available: http://iot.windriver.com/resources/use-cases/WR-IoTUseCase-Transportation.pdf [Accessed 05 06 2015]

[11] M. Berg and M. Nordlindh, “Implementing Internet of Things in the Swedish Railroad Sector: Evaluating Design Principles and Guidelines for E-Infrastructures,” Department of Informatics and Media, Uppsala University, Sweden, 2012. [Online]. Available: http://www.diva-portal.org/smash/get/diva2:556647/FULLTEXT01.pdf

[12] J. Fu, Z. Zhang, X. Jin and Z. Hao, “Smart Subway Information Platform based on Internet of Things,” International Journal of Hybrid Information Technology, vol. 6, no. 6, pp. 177-186, 2013.

[13] J. Kim, M. Bessho, N. Koshizuka, and K. Sakamura, “Mobile Applications for Assisting Mobility for the Visually Impaired Using IoT Infrastructure,” in Proc. of the IEEE TRON Symposium (TRONSHOW), 2014, Tokyo, pp. 1-6.

[14] J. E. Kim, M. Bessho, N. Koshizuka and K. Sakamura, “SaSYS: A Swipe Gesture-Based System for Exploring Urban Environments for the Visually Impaired,” in Mobile Computing, Applications, and Services, Springer, pp. 54–71, 2014

[15] J. E. Kim, M. Bessho, N. Koshizuka and K. Sakamura, “Enhancing public transit accessibility for the visually impaired using IoT and Open Data infrastructures,” in Proc. of the 1st International Conference on IoT in Urban Space (Urb-IoT), 2014, pp. 80-86.

[16] N. Harrington, L. Antuna and Y. Coady, “ABLE Transit: A Mobile Application for Visually Impaired Users to Navigate Public Transit,” in Proc. of the 7th International Conference on Broadband, Wireless Computing, Communication and Applications (BWCCA), 2012, IEEE, pp. 402-407.

[17] K. Yatani, N. Banovic, and K. Truong, “SpaceSense: Representing geographical information to visually impaired people using spatial tactile feedback,” in Proc. of the SIGCHI Conference on Human Factors in Computing Systems (CHI ’12), ACM, pp. 415-424.

[18] L. Brunet, C. Megard, S. Panëels, G. Changeon, J. Lozada, M.P. Daniel and F. Darses, ““Invitation to the voyage”: The design of tactile metaphors to fulfil occasional travellers’ needs in transportation networks,” in Proc. of the World Haptics Conference (WHC), 2013, IEEE, pp. 259-264.

[19] Kokosil Ginza – Ubiquitous Spatial Information System. [Online]. Available: http://home.ginza.kokosil.net/en. [Accessed 04 06 2015]

[20] N. Koshizuka, “IoT, Ubiquitous Computing, and Open Data for Smart Environments” in ITU-T Workshop on “Internet of Things – Trend and Challenges in Standardization”, 2014, Geneva, Switzerland. [Online]. Available: http://www.itu.int/en/ITU-T/Workshops-and-Seminars/iot/201402/Documents/S4P3_Noburu_Koshizuka.pdf

[21] K. Masanobu and S. Moriai, "Lightweight cryptography for the Internet of Things", Sony Corporation, 2008. [Online]. Available: http://www.iab.org/wp-content/IAB-uploads/2011/03/Kaftan.pdf

[22] Hewlett-Packard, “Internet of Things Research Study,” Palo Alto, CA, 2014. [Online]. Available: http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-4759ENW&cc=us&lc=en. [Accessed 30 05 2015]

[23] I. Kamrul, S. Weiming and W. Xianbin, “Security and privacy considerations for Wireless Sensor Networks in smart home environments,” in Proc. of the 16th IEEE International Conference on Computer Supported Cooperative Work in Design (CSCWD), 2013, pp. 626-633.

[24] A. Atamli and A. Martin, “Threat-Based Security Analysis for the Internet of Things,” in Proc. of the 2014 International Workshop on Secure Internet of Things, pp.35-43.

[25] G.Matharu, P. Upadhyay and L. Chaudhary, “The Internet of Things: Challenges & security issues,” in Proc. of the International Conference on Emerging Technologies (ICET), 2014, pp.54-59.

[26] Y. Liu, S. Hu and T.Ho, “Vulnerability assessment and defence technology for smart home cybersecurity considering pricing cyberattacks,” in IEEE/ACM International Conference on Computer-Aided Design (ICCAD), 2014, pp.183-190.

[27] M. Randles, A. Taleb-Bendiab and P. Miseldine, “Addressing the signal grounding problem for autonomic systems,” in Proc. of the IEEE International Conference on Autonomic and Autonomous Systems, (ICAS '06), 2006.