Towards a reliable smart city through formal verification and network analysis

Walid Miloud Dahmane, Samir Ouchani, Hafida Bouarfa

Towards a Reliable Smart City through Formal Verification and Network Analysis

Walid Miloud Dahmane[a], Samir Ouchani[b], Hafida Bouarfa[a]

[a] *Computer Science Department, Saad Dahlab University, Blida, Algeria*
[b] *LINEACT, École d'Ingénieur CESI, 13545 Aix-en-Provence, France*

Abstract

With the immense increase of population density, many challenges facing organizations and governments. Thus, it has become mandatory to turn up our cities to be intelligent by introducing IoT and smart grids to build smart buildings, smart communication technologies, smart healthcare systems, smart transportation, etc. Smart cities guarantee the healthy living of indoor inhabitants by sensing, processing and controlling all possible indoor-outdoor measures. In this paper, we develop a framework that systematically builds a reliable and secure Smart City Model (**SCM**) to be integrated then exploited by the building information model (BIM). **SCM** encloses both physical and digital models which highlight smart buildings in particular. First, the proposed solution identifies and models **SCM** components including their appropriate architectures that are responsible for communication, extension, information flow, and protection. To ensure **SCM** functional and security requirements, we develop a sound hybrid approach that relies on formal methods and network analysis. Uppaal model checker is used to verify the satisfiability of the smart city requirements whereas Cooja is deployed to simulate the connectivity and the communication coverage of the developed **SCM**. The obtained results, in Uppaal, showed that the different implemented scenarios are satisfying the functional correctness and security policies. Moreover, the simulation through Cooja showed that how different obstacles and positions of nodes affect the communication coverage and the energy consumption regarding the deployed nodes. Experimentally, the effectiveness of the developed framework has been shown through practical scenarios that are

difficult to model and analyze.

Keywords: Smart City, Cooja, Uppaal Model Checker, TCTL, IoT Protocols, Timed Automata, Access Control Policies.

1. Introduction

UNESCO[1] stated that through innovative urban systems, smart cities play an important role in socio-economic development while improving people's lives [1]. Also, UNECE [2] asserted that a smart sustainable city is an innovative city based on ICTs (Information and Communication Technologies) and other technologies to optimize quality of life, the efficiency of urban operation and services, and competitiveness [2]. A smart city [3, 4, 5] is defined as a wide area occupied by citizens, and divided into many smart components such as smart buildings, smart ICTs, smart transportation, smart health, smart grids, and other services. It supports a hierarchical network model, where the data captured can be published, stored, and analyzed [6].

Internet of things (IoT) is a network that combines physical components as sensors, smartphones, servers, etc, with the ICTs to sense in real-time the environment's measures, process the collected data, remotely control and make decisions, etc. The IoT network is characterized by low cost, large coverage, high secure level, scalability, and low latency. However, IoT is used in diverse applications domains like modern cities, industrial, home appliances, healthcare, transportation, sensors development, emergency, and other cases. It adopts some communication protocols and information sensing equipment to achieve smart deployment, controlling, and monitoring resources in real-time [7] while respecting the security standards and measures [8]. For a reliable network, the data flow traffic is distinguished by the automated process, where the analysis level treats the received data from the sensors and makes the decisions through machine learning-based supports. However, the adopted technologies should be

[1] United Nations Educational, Scientific and Cultural Organization.
[2] United Nations Economic Commission for Europe.

"secure, flexible, extensible, and sustainable" [9]. Further, the used protocols in smart cities are different.while IoT devices are featured by the low memory and low processing of data.

Many challenges are facing smart cities such as safety, security, energy, coverage, etc. For example, the energy consumption is estimated to be increased by 32% [10]. Hence, the lifetime of a building network relies on the quantity of energy provided to the smart appliances, the characteristics of the object that may cause high consummation, the used communication protocols, and the number of operations applied in the network. Also, the increasing demands for internet services cause the high latency, which impose us to integrate technologies of higher band-width to achieve higher data transfer. In addition, cyber risks are a big problem in the IoT paradigm since the cyber security standards do not cover precisely sensors and objects, and therefore it is difficult to monitor the corporations that provide IoT services [11].

However with any system, before deploying a concrete smart city, it is necessary to design its components and their relations, as well as ensure their functional correctness. Farther, such design dedicated to a smart city should achieve its main requirements, especially: safety, low energy consumption, low latency, network interconnectivity, and scalability. This paper develops a framework to ensure the good development of a more secure and reliable smart city by:

1. Designing a secure and robust Smart City Model (**SCM**) that can be integrated within the building information model (BIM).

2. Developing a formalism dedicated to smart cities by enclosing their different digital and physical components. It includes also their connection supports and adopted communication protocols.

3. Proposing an hybrid approach that is based on formal methods and network analysis to analyze the correctness of the designed **SCM**.

4. Enhancing the security level of **SCM** by proposing a set of access control policies and a dedicated algorithm to protect objects from unauthorized

access.

5. Proposing the use of temporal logic formalism to express **SCM** requirements.

6. Using the Cooja simulator to check the connectivity and energy consumption in **SCM**, the Uppaal model checker to verify the correctness of **SCM** and how well the security access policies are respected.

In the next section, we review the related work to modeling and security analysis of smart cities. Then in Section 3, we will give an overview of smart city components and compare it with the traditional city. Section 4 represents our smart city model which combines the physical and the digital models and details our methodology that analyzes **SCM** by ensuring its correctness and security. In Section 5, we validate our developed framework by experimenting with a fire emergency, navigation services, control access scenarios, and the wireless coverage of nodes. Finally, Section 6 concludes this contribution and gives hints about our research perspectives.

2. Related Work

Several research initiatives have been proposed for the smart city with a focus on IoT modeling, smart city components and requirements, and others on indoor management. This section surveys the recent literature related to them.

The term smart city includes many aspects, this is what Saraju .P *et al.* [12] touched upon, where, they presented general definitions about the smart city. They covered them as generalities in terms of applications (smart infrastructure, smart transportation, smart energy, smart healthcare, and smart technology), requirements (sustainability, quality of life, urbanization and smartness), impacts (society, economy, environment, and governance), and infrastructures (physical objects, ICT, and the service). This contribution is rich in concepts but it needs more experiments to demonstrate how the mentioned applications function together.

Ouchani [13] suggested a framework that supports IoT modeling, probability and costs of actions, analyzes their correctness, and estimated their protection level through the probabilistic model checking PRISM. To check the functional correctness of an IoT-based system, the framework encloses five phases: defining the IoT nodes, modeling the IoT architecture through the algebra expression, specifying the IoT requirements in PCTL, transforming the IoT system into PRISM language to verify the IoT requirements on the IoT model. However, the framework was provided with many data and exchanged messages which make the probabilistic model checking affects the process and storage operations.

Centenaro *et al.* [14] focused on the wireless telecommunication LPWANs[3] in a smart city using $LoRa^{\text{TM}}$. The aim was to estimate the number of nodes to cover a smart city (inexpensive or not) and to show their advantages after the deployment. They experimented $LoRa^{\text{TM}}$ on 19 floors of a building to measure temperature and humidity through one gateway and 32 nodes. Then, they estimated the number of the needed gateways to cover Padova city. They deployed a gateway without antenna gain in a building of two floors to assess the 'worst case'. The obtained result showed that $LoRa^{\text{TM}}$ technology could cover a cell of a 2 km radius. They also concluded that 30 gateways were needed to cover Padova. However, $LoRa^{\text{TM}}$ had an acceptable range of coverage in worst cases, but the number of ports of the gateways was limited and did not support the evolution of IoT technology.

Concretely, the flexibility of a network depends on the smart city architecture. K. Zhang *et al.* [15] classified the applications of the smart city on energy, environment, industry, living, and services. Then, they proposed an architecture to control them by modeling: the physical world that contains sensing and operating components, the communication world that integrates the heterogeneous networks, the information world which includes the control, analysis, and stored modules. Finally, they discussed the challenges of security and privacy through some applications by showing the possible mitigation solutions. How-

[3]LowPower Wide Area Networks

ever, the defined IoT components need more details especially their properties (e.g., the latency, capacities, security, etc). Moreover, the security has been sketched without showing how to deploy protocols within the involved encryption methods. Unfortunately, the experiments have been excluded to validate the proposed approach.

Practically, the real-world application is the best way to study the behavior of the appliances. Luis Sanchez *et al.* [16] proposed an architecture to monitor the air quality, luminosity, noise, temperature, irrigation monitoring and environmental station in Santander city (Spain). The architecture was composed of three levels: IoT peripherals such as the sensors and APIs, the gateway level, and the IoT server located in the cloud computing service. They tested the architecture to monitor the temperature and the humidity of soil by giving the users access control to their resources through OTAP technology since the solution was not wired. Compared to our contribution, it needs to include the control of sensors and the used protocols to estimate the protection level, and the transmission cost and coverage.

A. Zanella *et al.* [17] proposed a solution for Padova city to collect environmental data. The architecture of this solution contains devices such as sensors, a database server using CoAP[4] and 6LoWPAN[5], and unconstrained devices using the traditional communication technologies like HTML protocol. The architecture has been introduced as an intermediary gateway and HTTP-CoAP proxy-grown between the users and the sensors. Weekly, the solution measures the changes in temperature, humidity, light and benzene. Then, the proxy makes compatibility between the constrained and unconstrained devices in only one network. This solution was based on a limited number of protocols without concerns about security and the correctness of the requirements.

Among the studies made by the deployment of the Wireless Sensors Network (WSNs) in a smart area of interest, K. Loizos *et al.* [18] proposed a methodology

[4]Constrained Application Protocol

[5]IPv6 Low power Wireless Personal Area Networks

to deploy WSNs and IoT nodes in complex urban environments. The aim was to create a preliminary system in network simulators to facilitate the management and deployment of the network in an area of interest. The methodology ran on two steps: the first was to integrate the deployment in TruNET wireless which is a realistic 3D polarimetric physical layer simulator and the second was to export the results obtained from TruNET to the Cooja simulator which is specially designed for WSNs or IoT networks. They concluded that the simulation results did not much the real results, so they were insufficient to build a real network. In addition, the obtained results regarding the physical layer data were less realistic. This problem can be overcome through simulation and verification as well as by covering latency of protocols, propagation signal method, and coverage.

Hemant . G *et al.* [19] proposed an approach for smart homes and buildings to monitor the life of inhabitants by detecting the inhabitant's events that were collected from IoT nodes (sensor, coordinator, and the gateway). Also, they discussed the mitigation that can be deployed for the connectivity of the IoT system by taking into account the physical separators. However, the proposed architecture did not deal with the integrity of the measured data, and it required an action level to execute the operations according to the collected data.

To improve the level of protection of the Constrained Application Protocol (CoAP) and the encryption in DTLS protocol, S. Arvind *et al.* [20] set a client/server architecture, which was composed of the constrained devices that communicate together through CoAP protocol. The establishment of the architecture has been done by the Cooja simulator installed in the Contiki OS. They intercepted the communication by installing a proxy system in the middle to simulate the sniffing attack. As a result, the data was transmitted in plain text which increased the possibility of attacks on CoAP. Since the DTLS protocol used strong encryption, it is difficult to evaluate its security level by simulation. In addition, this type of attack needs powerful resources to be broken.

Concerning the reviewed initiatives in solving problems related to the smart city and IoT applications. Our focus is to compare our contribution within

the literature in terms of **automation** (automatic analysis of **SCM**), **security** (respecting the security requirements), **architecture** (scalable and supporting different ranges of components), **access control** (manage the access authorization to **SCM** resources and components), and **analysis** (the used technique to check and validate the smart city requirements). We found that our contribution covers the identified issues compared to the reviewed ones.

3. Problem statement

Many contributions describe the components of the smart city [21, 22, 23] as collections of smart buildings, smart transportation, smart ICT, smart health, smart infrastructure, smart economy, and smart government. However, the increasing population in the cities during the last years has resulted in many problems like the great energy consumption, management difficulty of big data, covering more areas with high communication quality, dealing with the emergencies in the buildings, protecting digital data from the collapse of the information system or hackers, transportation management, waste management, etc. These challenges cost the government a substantial amount of losses. To mitigate these problems, many recent projects are funded as shown in Table A.5 [24].

To motivate the trend towards a smart city, Table A.6 shows the difference between the traditional and the smart cities. The comparison leads us to conclude that the smart city overcomes many of the problems faced by the current traditional cities. Based on this comparison and the previously reviewed contribution in Section 2, we realize that we must convert the actual cities to be smarter by deploying robust and secure components, respecting security policies and the smart city norms.

4. Smart City Modeling and Analysis

This section covers the proposed framework to create a realizable smart city model. As depicted by Figure 1, it starts by creating the smart city model that includes both **P**hysical **M**odels (**PM**) and **D**igital **M**odels (**DM**), where

both models contain ingredients that are detailed textually and formally. The analysis step checks, then it validates how well **SCM** models are functionally correct through verification and simulation techniques. This step considers the developed **SCM** models as a network of Timed Automata (TA) and expresses the **SCM** requirements as TCTL [6] formula [25]. Hence, the Uppaal model checker is used to check if the requirements are satisfied, or not. Consequently, the Cooja network simulator previews if WSNs achieve a low consummation of energy with high coverage of the area of interest. If the outputs obtained from this step declare errors, it is necessary to return to the previous step in order to rebuild the **SCM**, else the verified model has the ability to be deployed in the BIM and the area of interest.

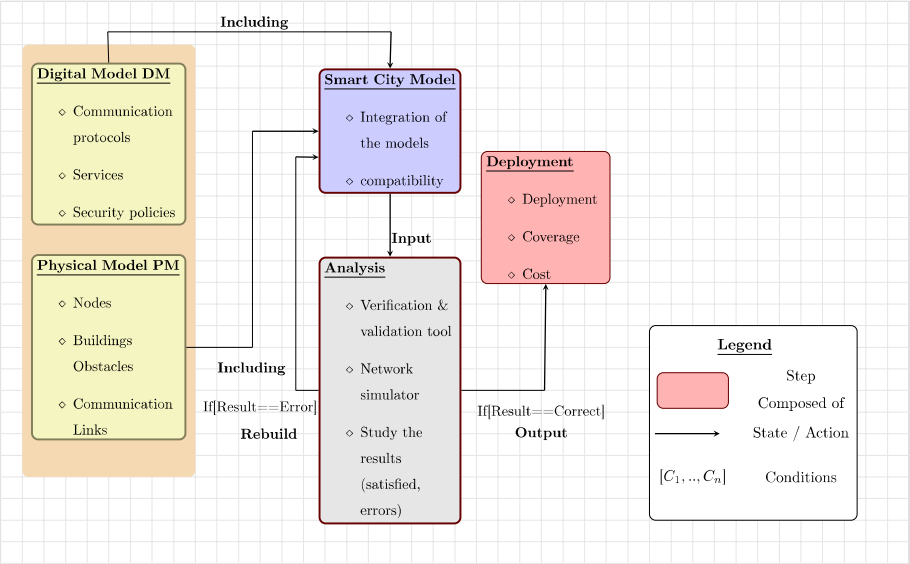


Figure 1: The methodology to construct SCM.

4.1. Smart City Model

Our proposed **SCM** architecture is divided into three levels (see Figure 2). The third level is dedicated to processing and storage services by including dif-

[6] Timed Computation Tree Logic

ferent resources such as the servers and calculators with software to receive, process, and share data (e.g., a server receives and processes the temperature measures that are captured by sensors, then gives the appropriate control commands). Since this level deals with sensitive data, we isolate it through three cloud services: *Saas* (Software as a service), *Paas* (Platform as a service), and *Iaas* (Infrastructure as a service) [26]. Physically, there is a long distance between the first and the third level components, e.g. when the request is forwarded from the *third* level devices to the cloud computing server. The transmission will have a high latency, which is one of the basic requirements in IoT systems. To resolve the latency issue, we add fog computing [27] to the third level that is located close to the lower levels. Thus, the "most used services" are installed in the fog whereas the "less-used services" are in the cloud. In addition, in order to serve the first level requests, a set of servers are equipped in this level e.g., Web servers, FTP, Mail, etc.

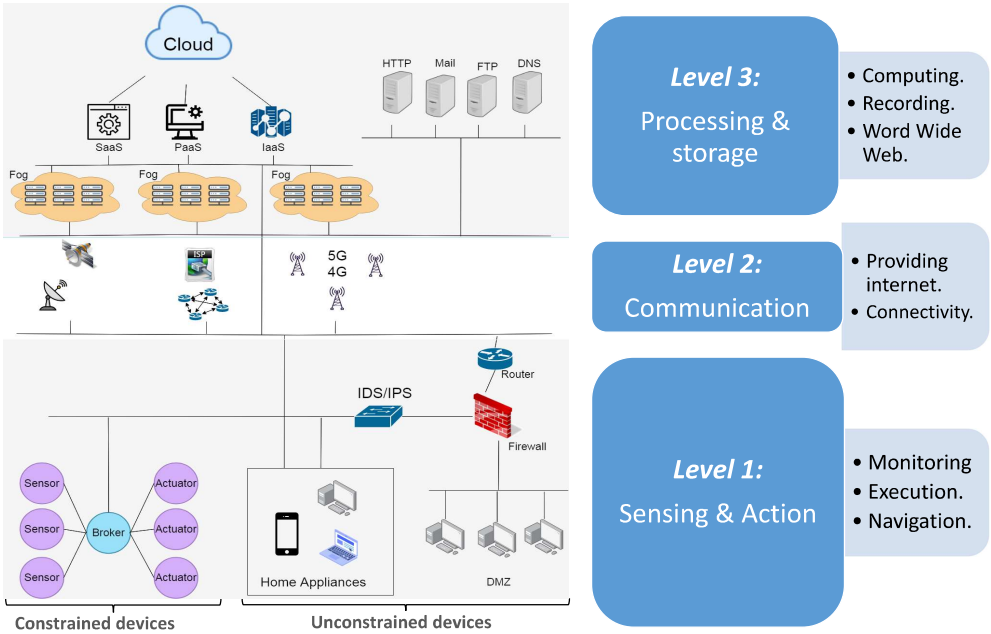


Figure 2: Smart City Architecture.

The second level (**Communication**) is a collection of internet stations and providers to link the other levels. It includes ISP (Internet service provider), 5G Mobile Broadband Providers, and Satellite Internet Providers. The quality of services is related to the type of internet providers, so, the differences among them are due to the differences in the variables: latency, coast, coverage, security, etc. For example, 5G technology is a fast-wireless communication, ADSL is more reliable, satellites provide coverage in the worst places.

The first level (*Sensing and Action*) is the indoor sub-architecture secured by hardware and software tools. The firewall is a necessary device to filter the input/output data and to construct sub-architecture as the Demilitarized Zone (DMZ)[28]. The Intrusion Detection System (IDS) [29] or Intrusion Prevention System (IPS) [30] are installed to detect and prevent BIM's intrusions. It contains unconstrained devices [7], that are responsible to monitor and request data (like computers and smartphones) through different protocols: HTTP, FTP, SMTP, POP,and others. Further, this level has constrained devices [8], especially sensors to monitor and share the conflicting changes in the environment (such as temperature, movements, noises, fire, etc.). We classify two types of sensors, wired sensors and Wireless Sensors Network (WSNs). The latter are the most important since they are mobile and support many IoT communications protocols like (Zig-bee, Bluetooth low energy, IEEE 802.15.4e, RPL, etc.). In addition, the actuators are objects that receive the commends and execute the appropriate actions (like turn on the air conditioner, open the door, etc.)

We consider an **SCM** as an association that brings together both the digital and physical models (Figure 3).

*4.1.1. The Physical Model (**PM**)*

PM is a set of hard components that visually construct the concrete building/city, and it includes:

[7] Devices that are characterized by large memory and processing capacities.
[8] Devices, that are characterized by low memory and processing capacities.

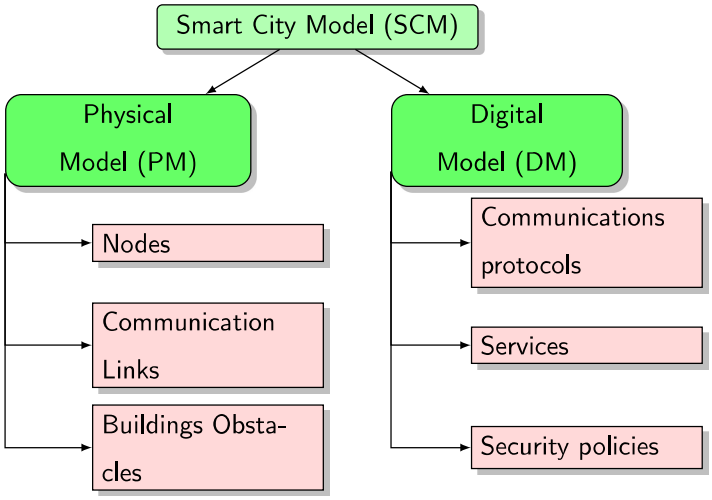


Figure 3: Smart City Model.

Nodes.

They are a set of sensing, application, processing, routing, and storing appliances such as sensors [31], actuators [32], servers [33], routers[34], and data center [35]. We define a $Node$ by the tuple $\langle attr, action, State, Behavior \rangle$, where: $attr$ is a set of *static* and *dynamic* attributes evaluated by the value val. The "*static*" attributes are fixed while a node is running, *e.g.* the size of an object, memory capacity, etc. The *dynamic* ones change when a node executes its proper *actions*, e.g, the battery degree, availability (On/Off), etc. The evaluation of $attr$ by val can be real or boolean. $action$ is the functions that take a set of parameters $IN \subseteq attr$ as input to evaluate the node attributes "$attr$". Its execution produces the changes in the output parameters: $OUT \subseteq attr$, $action : attr \rightarrow attr$ where $action(IN_i, ..., IN_n) = \{OUT_j, \ldots, OUT_m : i, n, j, m \in \mathbb{N}\}$. A given $Node$ can execute during during its life cycle (see Figure 4) the following actions: $Turn\_on()$, $Turn\_off()$, $Send()$, $Receive(msg)$, $Store(info_1, .., info_n)$, $Process(info_1, .., info_n)$, $Charge\_power()$, and $Consume\_energy()$.

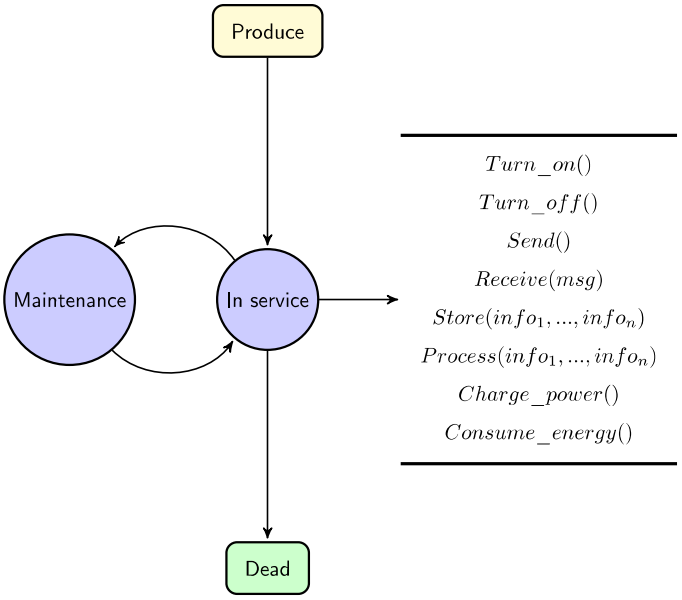


Figure 4: Cycle life of $Node$.

A $State_i \in State$ defines the status of the $Node$ when an $action$ is applied and characterized by the evaluation of its proper attributes given by $State_i = (attr_1 = val_1) \wedge \ldots \wedge (attr_n = val_n)$. Furthermore, $Behavior$ of a $Node$ is a timed automata showing the changes of its "$state$", where : $Behavior = State \times action \times State$.

Example 5 shows the timed automata of the fire sensor $node$. In the on state, it measures the conflicting changes (degree of the smoke) in the air. If this measurement exceeds a predefined threshold parameter, the sensor sends an alert message to the receiver $Node$. The sensor will be out of order if it is turned off. This $action$ includes the process of turning off or running out of power in the battery.

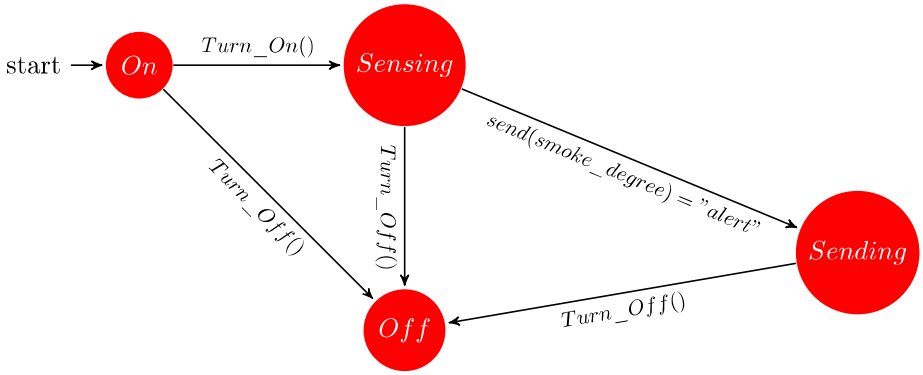


Figure 5: TA of Sensing/Action fire system.

Connection links

They are the wire or wireless *links* that relate nodes through their ports. $connection = \langle N, L \rangle$ is a direct graph (see. Figure 6), where: N is a set of $Nodes$, and L is the set of $Links$ relating $Nodes$, given by $L \subseteq \{(x,y)|(x,y) \in N \times (N)\, and\, x \neq y\}$, the pair (x,y) indicates that the $Node$ x has the ability to send a message to the $Node$ y.

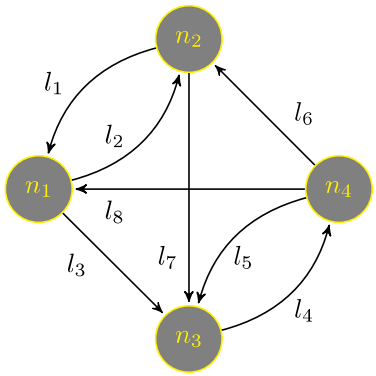


Figure 6: The connection links of the fire sensors node as a directed graph.

Building obstacles

They are a set of barriers, called "*Obstacles*", which construct the smart city form such as the buildings, roads, markets, homes, etc. The *Obstacles* have a negative *impact* on the propagation of the signal in the air, taking into

account its *type* "γ" (wall, wood, glass, etc.), *thickness* "τ", *number* ω, and the *distance* "α" between the two points (transmitter and receiver). The following path-loss models PL [36] shows how to calculate the value of the signal through the previously mentioned variables

$$\text{PL}=\text{PL}_0 + 10n\,log(\alpha) + \sum_{i=1}^{\omega} PL(\gamma,\tau)_i \tag{1}$$

Where, PL_0 is the path loss over a distance of one meter, and n is the path-loss exponent that indicates how fast the path loss increases with distance.

*4.1.2. The Digital Model (**DM**)*

DM is a collection of digital components and rules to guarantee the functional correctness of **ICTs**. The proposed **DM** covers the adopted protocols, services, and security protocols.

Communications protocols

The IoT communication requirements like the low consummation energy, the reliable connectivity, and the security level are related to the selected communications protocols. For each layer, we adopt the appropriate protocol regarding IoT networks requirement as follows.

Data link layer

- IEEE 802.15.4e is suitable for low power communication. It uses time synchronization and channel hopping to enable high reliability, low cost, and meet IoT communications requirements.

- IEEE 802.11 known as WiFi, where, the original version is the IEEE 802.11 wireless medium access standard. Generally, WiFi does not support IoT devices due to it needs to large power consumption. Its version sister IEEE 802.11 AH treats power consummation problem by increasing the sleep time period. It is suitable for constrained devices having a small memory and low processing by defining a short MAC frame of 12 bytes.

- WirelessHART runs on the top of IEEE 802.15.4 PHY and chooses Time Division Multiple Access (TDMA) in its MAC. It is reliable and secure for small devices supporting security mechanisms for end-to-end, per-hop, or peer-to-peer networks, and, it encrypts messages with advanced encryption.

- Z-Wave is a low-energy protocol and suitable for smart structures with communication of about 30 meters. It is used to communicate short messages like controlling temperature, humidity, light, etc.

- Bluetooth Low Energy consumes less power than the classic Bluetooth protocol, while its latency can reach 15 times more than the initial one.

- Zigbee Smart Energy is suitable for a large range of IoT devices like remote controls and healthcare systems. ZigBee supports the constrained devices and symmetric-key exchange, and it is more scalable by using stochastic address assignment.

- LoRaWAN is to reduce the consummation of IoT device energy. It is characterized by the low cost, secure, mobile, and bi-directional communication for IoT applications.

Network Layer

- Routing Protocol for Low-Power and Lossy Networks (RPL) supports different data link protocols such as IEEE 802.15.4, Bluetooth, Low Power WiFi, etc. It creates Destination Oriented Directed Acyclic Graph (DODAG).

- IPv6 over Low power Wireless Personal Area Network (6LoWPAN) encapsulates IPv6 long headers in IEEE802.15.4 small packets, which cannot exceed 128 bytes. It supports different length addresses, low bandwidth, low cost, different topologies, mobility, scalable networks, unreliability and long sleep time.

- IPv6 over Bluetooth Low Energy supports a short-range wireless communication technology that aims at ultra-low power. It is suitable for

sensors transmitting data infrequently or peripherals using asynchronous communication.

Table A.7 compares the mentioned protocols in terms of architecture, message size, security and IP address used.

Session layer

- Message Queue Telemetry Transport (MQTT) is based on a Publish/Subscribe architecture that is composed from three devices: publisher, broker, and the subscriber. The broker is implemented by the set of topics which have an hierarchical form that is divided into multi-level (e.g: Building/room_1/temperature), the subscribers relate these topics, the publisher as the sensors puts its collected information at one topic in the broker. Then, the broker forwards messages to the nodes subscribed in the same topic (Figure 7).

  The sequence diagram in Figure 7 illustrates the *connection link* of, the example of a fire case, three main *Nodes* communication through the MQTT protocol: Sensor (senses a measurement as a smoke degree), Broker (subscribe the *Nodes*, receive the messages from the *Nodes* published and send the commands to the *Nodes* subscribed) and Actuator that executes an action (spray the water).

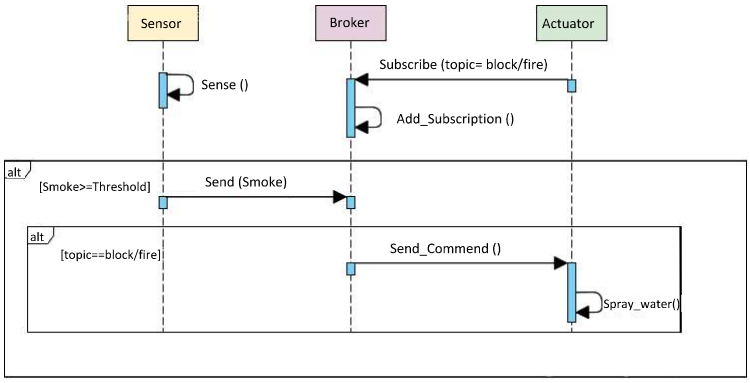
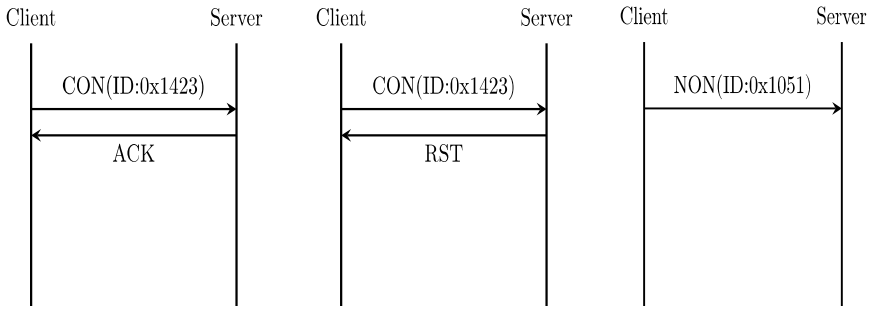


Figure 7: The sequence diagram of the MQTT protocol.

- The Constrained Application Protocol (CoAP) runs in REST architecture (client/server). The sent message from the client to the server is one of the four RESFful methods (GET, PUT, PUSH and DELETE). It is featured by the low energy consummation, secure by the DTLS protocols [37] that encrypts the data flow, and high latency based on UDP protocol. This protocol has low bandwidth with a loss of information. The end-to-end communication used by this protocol consists of two kind of messages: Confirmable and Non-Confirmable messages. The first is a request sent from the client to the server and requires an acknowledgement from the server, when the server receives this message, it responses by the message ACK, else, it sends rest message (RST) 8(a). The Non-Confirmable message does not need an acknowledge by the server 8(b).



(a) Confirmable Messages (Reception/Loss). (b) Non-Confirmable Message.

Figure 8: CoAP processes.

- The Advanced Message Queuing Protocol (AMQP) runs over TCP and based on the publish/ subscribe architecture. The broker is divided into two components: exchange and queues. The exchange receives published messages from the producers and transmits them to queues which send them to the consumers. Four methods are used to transform the message from the exchanges to the queues. Direct, where, the exchange routes the message to the queues that have the binding key equals the routing key of

the message (Fig.9). Fan-out, where ,the exchange transmits the message to all the queues related with it without constraints. Header, where the message transmitted from the exchange has the pair Key-Value to identify which queue can receive this message. Topic is when the exchange sends the massage to the queues if the queues patterns are identical with the routing key of the message.

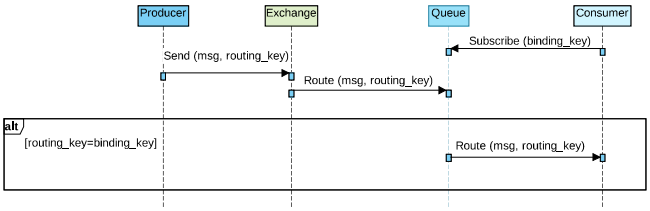


Figure 9: The operation of AMQP with Direct exchange method.

These messaging protocols differ on message size, power consummation, latency, QoS, security level and the number of M2M usage [38]. CoAP has the lowest message size and overhead compared to MQTT and AMQP. CoAP protocol requires lower power and resources than the MQTT and AMQP protocol. CoAP protocol offers lowest bandwidth and latency than the MQTT and AMQP protocol. MQTT has the highest level of quality of services with the least interoperability between them. AMQP provides the highest level security and additional services, while MQTT supports the lowest level of security and additional services. MQTT is used by many organisations but it does not remain a global standard.

Table A.8 compares the discussed protocols in terms of architecture, abstraction, header size, message size, communication methods, quality of service, security and communication port.

As example, the sequence diagram in Figure 10 illustrates the behavior of the IoT appliances that communicate with the session layer protocols, MQTT in particular. We propose a fire scenario in a smart building equipped by a fire sensor and the actuators to extinguish the fire by spray water. The MQTT broker processes the received message from the fire sensor, then, it sends a

command to the actuator to put the fire out, as well as, it sends an alert message to the fire service.

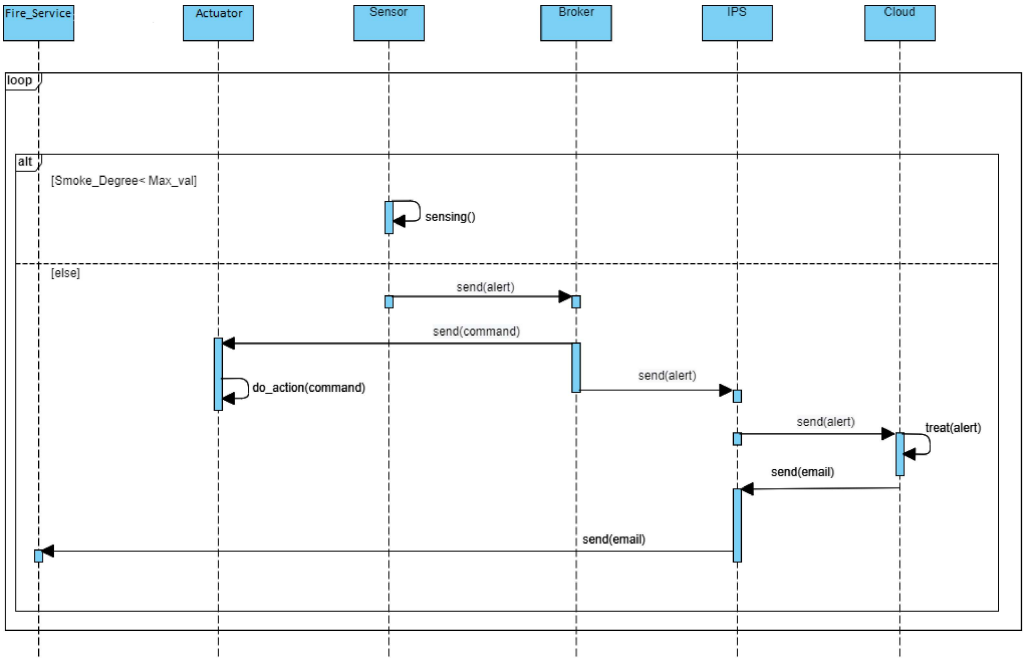


Figure 10: Fire example in the smart city.

4.1.3. Services

The management of a smart city platform needs several decisions to be taken in real-time to improve its QoS. The proposed framework develops the following services.

Security

- Secure sub-architecture: The internal sub-architecture is installed inside the building like the DMZ, the Virtual Local Area Network (VLAN) [39]; while the external sub-architecture is an outdoor network where the routing is based on IP addresses. It links the varieties of internal sub-architecture in one root like the cloud and the fog computing to analyze, store the received data, and manage the IoT networks.

- Secure components: Due to the threats that affect the communication network and operating systems with a direct influence on the information integrity and the availability of services, it has become necessary to distribute a set of protection tools, in all levels of the network. The security components encrypt the transmitted data, make an Access Control Lists (ACL), detect and prevent an intrusion. Among them we deploy firewall [40], VPN [41], IDS [29], IPS [30], Proxy [42], Kerberos Servers [43], and anti-virus [44], etc.

Communication supports

It is an adoption of facilities and materials designed by a low latency, a large coverage area, protection, low-cost (energy consummation, deployment, maintenance cost, etc.). These requirements are granted by considering the following technologies.

- 5G: It is widely used with portable devices, especially mobile phones, and this is due to its high frequencies, which need small pickups to match it. This service solves two IoT requirements: mobility and latency. This service is provided at the *communication level* of the proposed architecture.

- Optical fiber: This technology is deployed to connect remote points with high flow. It guarantees reliability and speed at the *communication level* of the architecture.

- Computing and storage layer: At the *processing and storage level*, it is configured to receive and process high flows, as the quality of service is related to their capabilities (processing, storage, protection, service presence, etc.).

Maintenance

The availability of services is one of the most important requirements in a smart city. In this paper, we consider the life-time of IoT nodes and the good functioning of the system. To Avoiding breakdown of the service, we monitor

the availability of the IoT devices and analyze the periodic reports in each sub-architecture. These actions allow the network to view the system functioning and predict the IoT problems, e.g., SQL log files records the applied operations and the states of the IoT devices. The file are analyzed by cloud applications as Apache^{TM} Hadoop and Apache Spark^{TM} [46].

Security Policies

To reinforce security in **SCM**, we propose Access Control Models **ACM** as a set of rules and decisions that categorize the responsibilities of the system components and attributes the authorization or prevention access to the components or resources.

ACM is defined by the tuple $\mathbb{M} = \langle\, Subjets, Nodes, Actions, Permissions, Security, Grant\rangle$, where:

- *Subjets* is a finite set of subjects that can execute actions in **SMC**.
- *Nodes* are all physical and digital objects and resources defined by **SMC**.
- *Actions* are all actions that can be executed by *Subjets* and *Nodes*.
- $Permissions = \{Read\_down, Write\_up, Access\}$ is a set of restrictions to be granted to the set of *subjects* and *nodes*.
- $Security: Subjects \cup Nodes \rightarrow Values$ is an assignment function that attributes a bounded value representing the security level of a subject or an object.
- $Grant: (Subjects \cup Nodes) \times Actions \times (Subjects \cup Nodes) \rightarrow 2^{Permissions}$ is a function that manages the execution of actions between nodes and subjects in **SMC**.

Algorithm 1 implements **ACM** in **SCM** where the set of permissions is defined as follows.

- ***read down*** allows the owner to access to the second node without updating its state. The action can be applied if the subject has a security level smaller than the the security level of the node.

- ***Write up*** allows the first node to update the state of the second node (e.g: add, update or delete information). The action can be applied if the subject has a security level greater than the the security level of the node.

- ***access*** is provided only to the *Admin* of the network. This property sets the degree of the security level of another $Non - Admin$ or $Node$.

4.2. Smart City Analysis

To ensure the correctness and security of the proposed architecture, we rely on UPPAAL model checker for the formal verification and Cooja networking analyzer for simulation.

4.2.1. Formal Verification

It is a modeling and verification tool, Uppaal allows to model the behavior of the IoT network nodes using timed automata formalism. The automata of a node is modeled to exchange the commands with another. To check the security and the correctness of the proposed network, we express the requirements on TCTL input language. It is based on two formulae types, path and state, the state formulae presents one state whereas the path formulae describes the execution of the constructed network. Path formulae has three types reachability, safety and liveness as presented in Figure 11 and described as follows.

- **Reachability**: There is a possibility to reach the state satisfying the state property p (E<> p).

- **Safety**: p is correct in all states (A[] p), or there is a path where p is true (E[] p).

- **Liveness**: p is correct in some states (A<> p), or if p is true, q is also true in all the paths (p –> q).

Algorithm 1 Access Control Management

```
//Case -1-: Read Action
if Action == Read then
    // o: object, s: subject, ω is the security level of the admin.
    if (s.security < o.security)Or(s.security == ω) then
        return (true)
    else
        return (false)
    end
else
    //Case -2-: Write Action
    if Action == Write then
        if (s.security > o.security)Or(s.security == ω) then
            return (true)
        else
            return (false)
        end
    else
        //Case -3-: Access Action
        // n: is an object or subject, ι: new level inserted if s.security == ω
        then
            n.security = ι return (true)
        else
            return (false)
        end
    end
end
```

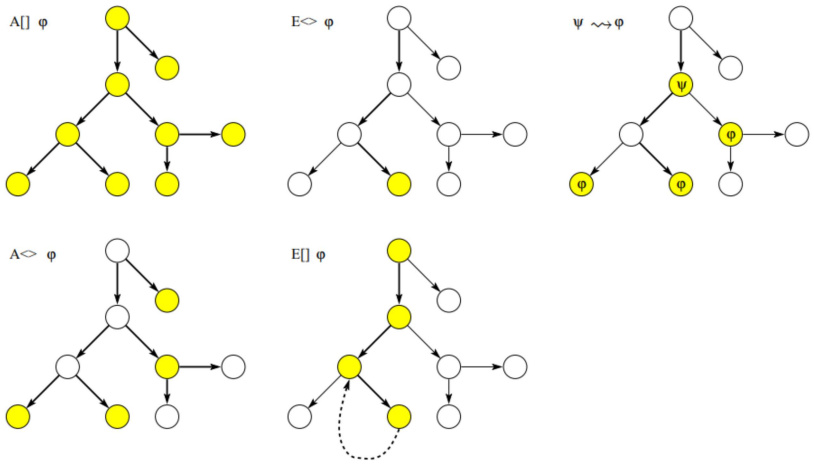


Figure 11: TCTL Path formulae semantics.

4.2.2. Network Analysis

Contiki is an open source OS, which is developed to study the behaviors of the WSNs nodes in the IoT networks through Cooja simulator [48] that provides — besides a GUI— the simulation of the radio medium. Its visualisation presents the propagation of the signal produced by the WSNs placed on the area of interest respecting the diffraction, refraction and reflection phenomena. Cooja simulator offers many radio medium types such as Unit Disk Graph Medium (UDGM), Directed Graph Radio Medium (DGRM), Multi-path Ray-tracer Medium (MRM), and others.

The simulation creates a wide environment to simulate the wireless networks through the integration of many types of predefined motes for example Sky motes, ESB mote, micaZ mote, etc. Also, it supports 6LoWPAN, CoAP and RPL protocols, and it gives to the network developers the access to update these packages and to optimize the security, mobility, latency, cost, and all the other IoT requirements. Based on the comparison presented in Table A.9, many features have been identified to chose Cooja as a network simulator. Indeed, it supports the concepts that are included in our proposition especially: the multi-path ray-tracing, the obstacles attenuation, constructs direct graph, TCP/UDP

protocols, and energy consummation model. Table A.9 shows the reason for choosing the Cooja simulator among the other network simulators.

5. Experimental Results

This section shows the effectiveness of our developed framework, in which validity and robustness of the proposed **SCM** are verified through experiments by applying verification and simulation techniques. First, we prepare our **SCM** model. Then, we use Cooja simulator to show the effect of IoT protocols on the consummation of energy for the constrained devices as well as the impact of the obstacles on the communication among the nodes to increase the network lifetime. Finally, we check the correctness of the **SCM** on Uppaal with respect on the functional, the behavior of the devices subject to the security policies is also studied.

*5.1. **SCM** description*

The area presented in Figure 12 has eight heterogeneous buildings that are divided into homes of $(10 \times 10m^2)$. Each building has a *sink* node to collect the temperature measures sent by *sensors*. The deployment of sensors are arbitrary distributed.

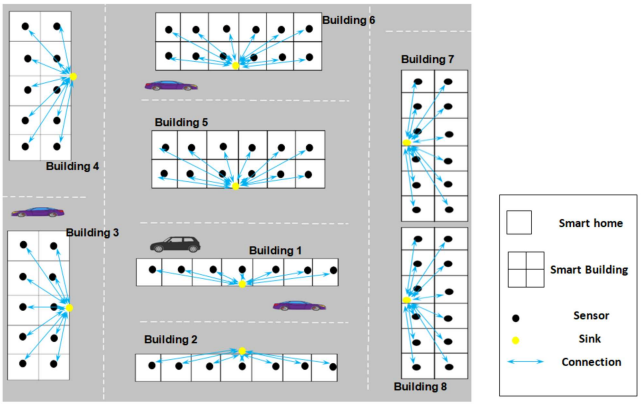


Figure 12: Area of interest: Set of a Smart Building

Figure 13 shows the architecture of our concrete **SCM** that we want to analyze. It is a client/server architecture based on RPL, CoAP, and MQTT protocols. The third level represented by the processing unit (as in Figure 2) is equipped by the cloud computing server that records less-used information (e.g, buildings status report per week) and the fog computing service which stores frequently the most used information (e.g, the measured data). Further, it has the ISP that supports the wire and wireless communication. In this architecture, we consider unconstrained and constrained devices; the unconstrained devices are the communication, filtering, routing and protecting appliances (computers, firewall, routers and the IDSs respectively). The constrained devices play the role of the fire detection system (fire sensor, broker, and an actuator that spray the water into the emergency case). The fire system nodes communicate through MQTT protocol.

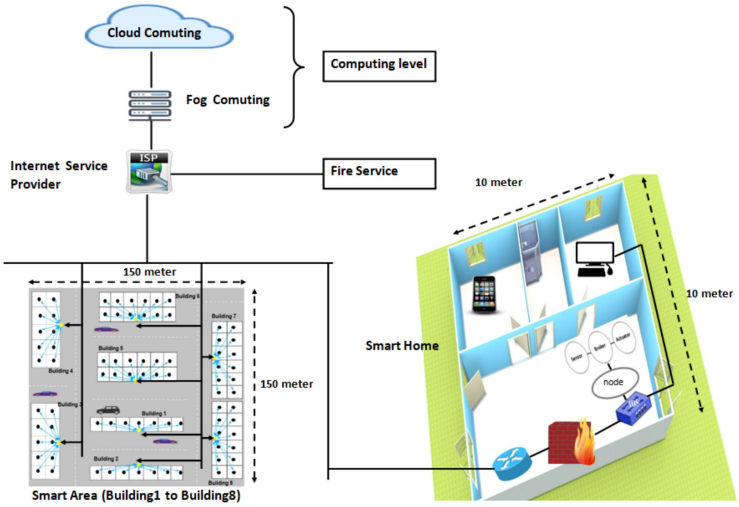


Figure 13: Area of interest: Smart City.

5.2. Cooja simulation

With this test, all the BIM sensors use RPL protocols to transmit the temperature measured in the buildings. The Multi-path Ray-tracer Medium (MRM) model is an extension chosen to simulate the presence of obstacles.

Table 1 shows the used parameters in MRM simulation that takes into account the refraction, reflection, and diffraction phenomena which affect the trend of the transmitted signals. By following the proposed architecture guidelines that avoid constructing the global network which helps to reduce the resources use of Contiki OS computer container. We divide the global network into multi sub-networks related by sinks. Then, the RPL protocol constructs a graph of routes (DODAG) using MRHOF algorithm, we chose this algorithm instead OF0 algorithm due to MRHOF is more reliable, because, in busy simulations, where, many nodes contain a high rate of data, MRHOF would reduce "Packet Drop Ratio" by 25.1% [50].

Figure 14 illustrates the probability of receiving the signal of one sensor in the area of interest (sensor 3, building 1, Figure 12), where the type of color (green, blue and red) determines the percentage of reception (strong, medium and week respectively). It is clear that the obstacles stop or decrease the signal propagation among nodes.

From the simulation results, we found that any WSN recognizes its neighbours to construct the DODAG. During 5 minutes of simulation, the nodes in each building constructs its DODAG, where the sink is the meeting point of all orientations. We observe that all WSNs are presented and connected to transmit the collected data to the sink. DODAG edges are weighted to represent the connectivity quality between nodes affected by the distance and obstacles.

Parameter	**Value**
Default transmitter output power	1.5 dBm
Receiver sensitivity	-100 dBm
Refraction coefficient	-3 db
Reflection coefficient	-5 db
Diffraction coefficient	-10 db
Obstacle attenuation	-3 db/m

Table 1: MRM Simulation Parameters.

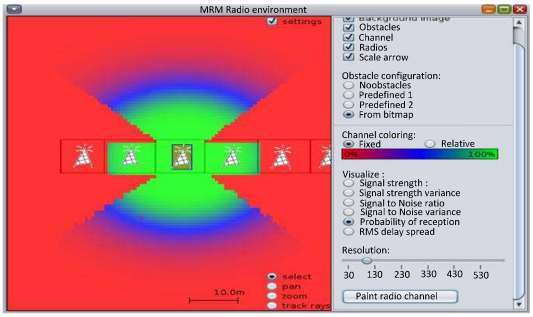
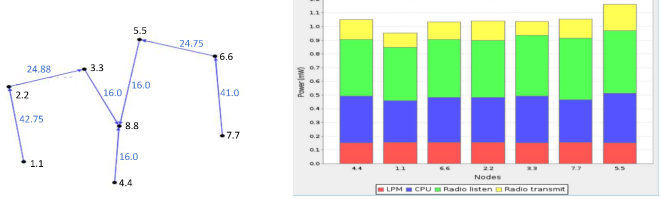


Figure 14: Probability of receiving signals.

Figures 15(a), 16(a), 17(a), 18(a), 19(a), 20(a), 21(a) and 22(a) are DODAGs for the buildings 1,$\cdots$, 8. If the value of a DODAG edge is high, it means that the possibility of receiving data between nodes connected by such edge is low. For example, $node_1$ represented in the DODAG of Figure 15(a), located in the first home of the Building 1, is far from the *sink* (*node* 8) and its wireless communication passes through many obstacles. Thus, it has the greatest value (42) compared to others.

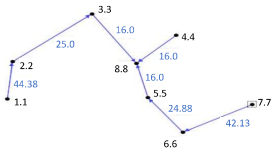


(a) DODAG. (b) Consummation of energy.

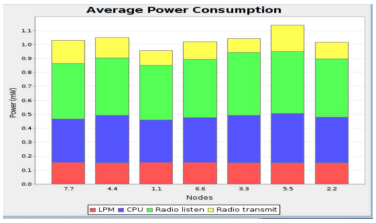
Figure 15: Results in building 1.

After the connectivity insurance, we analyze the energy consumption of nodes in each building. Figures 15(b), 16(b), 17(b), 18(b), 19(b), 20(b), 21(b), and 22(b) illustrate the energy consumed in all buildings nodes concerning the number of executed operations: sensing by using LPM (red color), processing by using a CPU (blue color), receiving using a radio listener (green color), and sending by using a radio transmitter (yellow color).

For example, Figure 15(b) represents the consummation of energy of the sub-

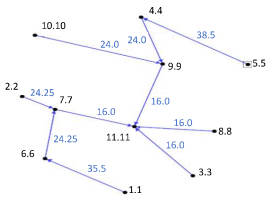


(a) DODAG.

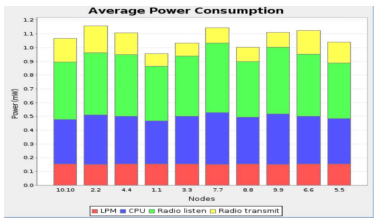


(b) Energy Consumption.

Figure 16: Results in building 2.



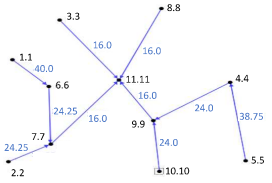
(a) DODAG.



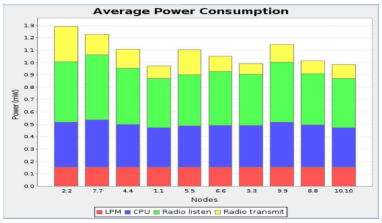
(b) Consumption of energy.

Figure 17: Results in building 3.

network which its DODAG is represented in the Figure 15(a). We observe that the node five has a huge consummation of energy compared to the other nodes due to its position, where, it plays the mediation role between the sink (node eight) and other distant nodes (six and seven). Thus, the node five executes many operations (receive, send, forward, process) to assure the transmission among the sink, itself and the distant nodes.



(a) DODAG.

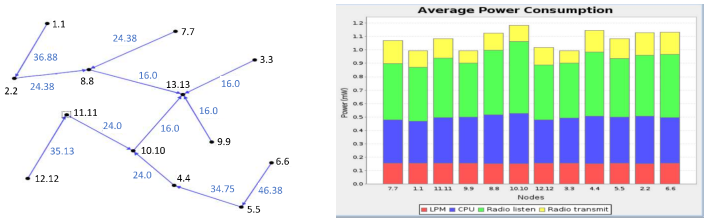


(b) Consumption of energy.

Figure 18: Results in building 4.

We observe that the most of nodes consume the same level of energy regard-

ing sensing operation while their energy consumption differs when processing, sending and receiving data.

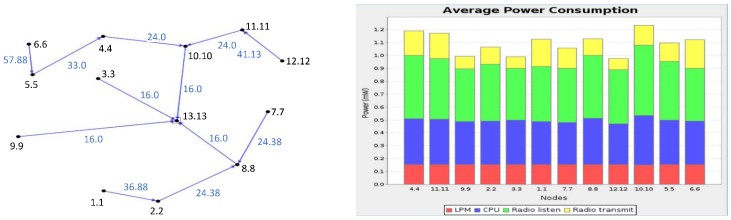


(a) DODAG. (b) Consummation of energy.

Figure 19: Results in building 5.

Finally, Table 2 compares the energy consumption of the deployed IoT nodes to some homes appliances [51]. The comparison shows that the IoT networks have more lifetime than other type of networks. At Cooja simulation, we assure that:

- Constrained devices are characterized by a low consummation of energy and, the use of RPL protocol can reduce the cost of the IoT network, and increase its lifetime.



(a) DODAG. (b) Consummation of energy.

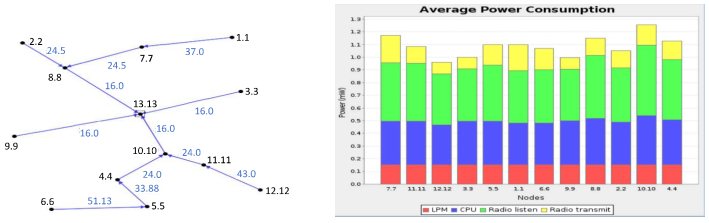
Figure 20: Results in building 6.

- Dividing the first level of the architecture (Figure 2) into multi sub-network decreases the load of operations applied to the sink node due to its low processing capacity and memory storage.
- The obstacles heavily impact the transmission of the signal that causes

Device	Wattage
IoT simulation node	0.00114
Desktop computer	6.25
Ceiling fan	2.92
Video game system	3
LED TV	6.58

Table 2: The parameters used in the MRM simulation.

low QoS. This issue motivates the integration of a new mechanism that finds the optimal positions for WSNs.



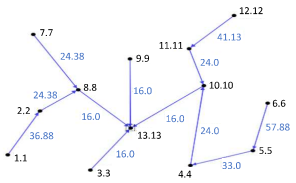
(a) DODAG. (b) Consummation of energy.

Figure 21: Results in building 7.

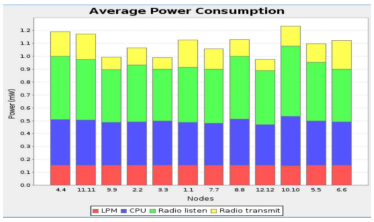
5.3. Uppaal Verification

As a second step, by using Uppaal we check the correctness and the security of the modeled **SCM** (Figure 13). First, we construct the automata of all **SCM** components which are: sensor, actuator, navigator, IDS, firewall, router, ISP, Fog and cloud service. Figure A.26 depicts each component semantics by representing their behaviors, including: actions, states, and attributes. Then, we run and verify four possible scenarios.

Scenario 1. The first scenario checks the RESTful Web services used by the CoAP based on the client-server architecture, and consists on the methods: GET, PUT, PUSH and DELETE. The building computer sends a GET request to the cloud service to access the data stored in cloud. The request traverses



(a) DODAG.



(b) Consummation of energy.

Figure 22: Results in building 8.

the three levels of architecture, and any node receiving the request will forward it to the following node. The progress of the behaviour nodes is represented in the sequence diagram showed in Figure 23.

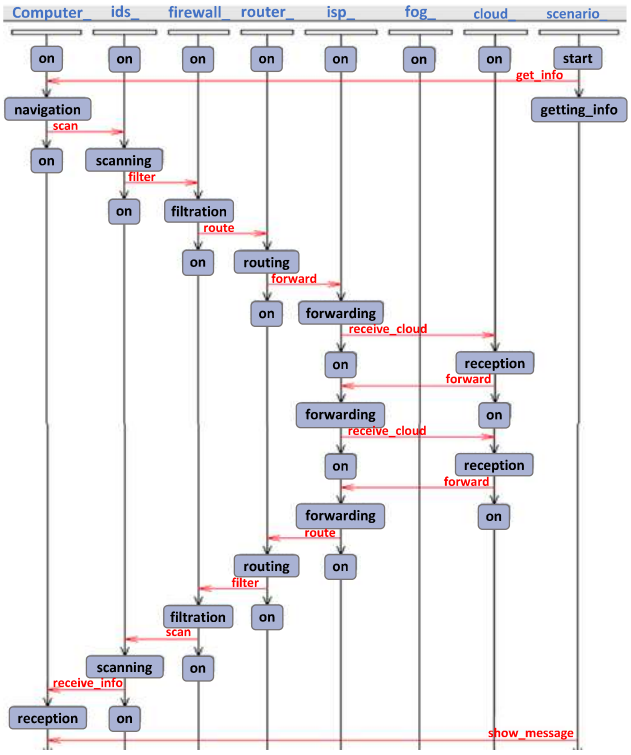


Figure 23: Sequence diagram of scenario 1.

Scenario 2. This scenario is similar to the first one, while, it uses the wireless

communication protocol to access to the fog service. The sequence diagram in Figure 24 shows the progress steps in this wireless navigation.

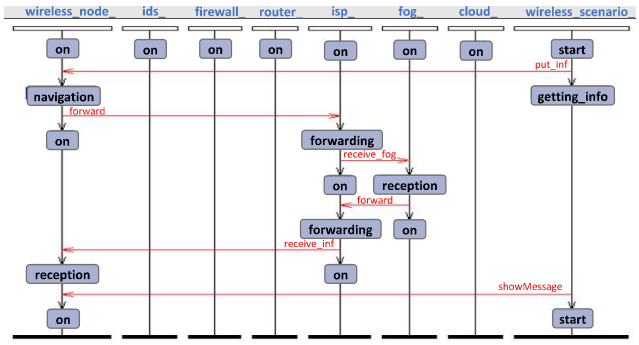


Figure 24: Sequence diagram of scenario 2.

Scenario 3. The third scenario aims to monitor the fire alarm system and to analyze the fire case resulting in smart buildings and also to check the reaction of the IoT nodes in the network. The proposed fire alarm system contains three main components: the sensor which monitors and sends an alarm to the broker in the fire case, the broker sends the command (stop the fire) to the actuator that is subscribed on it, and the subscribed actuator in the broker receives the command from it. We relate the broker by another node to inform the fire service (e.g., message describing the location of the building and the time of the incident). The sequence diagram presented in Figure A.27 illustrates the steps of this scenario.

Scenario 4. In this scenario, we test our proposed access control model, where, we model three automata: *Admin*, *Subject* and *Node*. The role of *Admin* is to set the security level in *Subject* and *Object*, the *Subject* randomly can be *Admin* or $Non-Admin$. The *Subject* applies actions to *Object* according to the security level of the *Subject* and *Object*. All security properties (**read, write and access**) are respected according to the alternative security level of the components presented in Figure 25.

Verification. By expressing the security and functional requirements in TCTL, Table 3 describes the list of the requirements to be valid without access

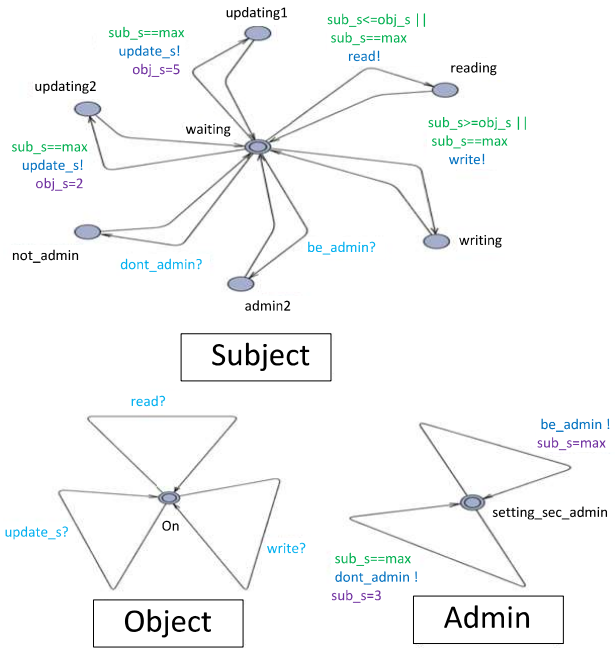


Figure 25: TA of ACM scenario.

control, whereas, Table 4 lists the set of properties proper to the access control. The verification results show that all the properties are satisfied which means that the architecture is correct and secure concerning the specified requirements.

6. Conclusion

For a more healthy daily life, this work developed a systematic method to transform the traditional city into a smart one. This contribution enriches the Building Information Model (BIM) by providing more Information and Communication Technologies (ICT) models. The proposed framework develops two main parts: designing a correct Smart City Model by looking into physical as well as digital parts. Each component has been well defined by including the technologies that it supports, while respects the smart city requirements. Further, the framework develops the access control policies that help to manage **SCM** assets and components more securely. The second part, it is automatic

TCTL proprieties	Description
A[] not deadlock	All nodes run without deadlock.
A[] not(ids_.scanning) and not(firewall_.filtration) and not(router_.routing) imply wire_connection==false	We cannot use the wire devices if the type of connection is wireless.
A[] sub2 == false imply not(fog_.reception)	If a node send the alert message that is not subscribed in the broker, then the fog service cannot receive the alert.
A[] sensor_.publishing imply (fire==true)	The sensor can publish in the broker only when it senses a fire case.
A[] node_.reception imply fire == true	The distant node like the fire service can receive alert message in the fire case.
A[] actuator_.action imply (fire==true and sub_actuator==true)	The actuator applies an action (e.g, spray water) when it subscribes in the broker and in the fire case.
A[] fog_.reception imply info==1 and pass_out==true and ware_connection==true	The fog service receives the appropriate information in the wire connection if the firewall gives access.

Table 3: TCTL properties for the functional correctness.

TCTL proprieties	Description
A[] sub.writing imply (sub_sec >= obj_sec) || sub_sec==Max	**Write** property management.
A[] sub.reading imply (sub_sec <= obj_sec) || sub_sec==Max	**Read** property management.
A[] sub.updating1 || sub.updating2 imply (sub_sec==Max)	**Access** property management.

Table 4: TCTL properties proper to the proposed ACM.

analysis of the security, the correctness, and the energy consumption of a deployed **SCM** using Cooja simulator and UPPAAL model checker. Finally, we conclude that the developed framework and the obtained results are a mainstay for a concrete deployment of a **SCM** free from errors, robust, and more secure.

In the future, we intend to extend this work with the following directions.

- Applying the framework on more real systems.
- Optimising the sensors deployment to minimize the cost and maximize the coverage of the network.
- Enhancing the security of **SCM** by introducing the *Blockchain* technology.

References

[1] https://en.unesco.org/courier/2019-2/towards-smart-cities. Accessed: 2021-08-25.

[2] https://unece.org/housing/sustainable-smart-cities. Accessed: 2021-07-26.

[3] Anthopoulos, Leonidas,et al. "A Unified Smart City Model (USCM) for Smart City Conceptualization and Benchmarking." Smart Cities and Smart Spaces: Concepts, Methodologies, Tools, and Applications, edited by Information Resources Management Association, IGI Global, 2019, pp. 247-264. http://doi:10.4018/978-1-5225-7030-1.ch011

[4] Bhagya Nathali Silva, Murad Khan, and Kijun Han. Towards sustainablesmart cities: A review of trends, architectures, components, and open challenges in smart cities.Sustainable Cities and Society, 38:697–713, 2018.

[5] Sally P. Caird and Stephen H. Hallett. Towards evaluation design for smartcity development.Journal of Urban Design, 24(2):188â€“209, 2019.

[6] Nguyen, T.A.; Min, D.; Choi, E. A Hierarchical Modeling and Analysis Framework for Availability and Security Quantification of IoT Infrastructures. Electronics 2020, 9, 155. https://doi.org/10.3390/electronics9010155

[7] Patel, Keyur & Patel, Sunil & Scholar, P & Salazar, Carlos. (2016). Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges.

[8] David Basin, Cas Cremers, and Catherine Meadows.Model Checking Se-curity Protocols, pages 727–762. Springer International Publishing, Cham,2018.

[9] Allam, Z.; Newman, P. Redefining the Smart City: Culture, Metabolism and Governance. Smart Cities 2018, 1, 4-25.

[10] Balaji, Bharathan & Bhattacharya, Arka & Fierro, Gabriel & Gao, Jingkun & Gluck, Joshua & Hong, Dezhi & Johansen, Aslak & Koh, Jason & Ploennigs, Joern & Agarwal, Yuvraj & BergÃ©s, Mario & Culler, David & Gupta, Rajesh & KjÃ¦rgaard, Mikkel & Srivastava, Mani & Whitehouse, Kamin. (2018). Brick : Metadata schema for portable smart building applications. Applied Energy. 226. 10.1016/j.apenergy.2018.02.091.

[11] Petar Radanliev, David Charles De Roure, Jason R. C. Nurse, Pete Burnap, Eirini Anthi, Uchenna Ani, La Treall Maddox, Omar Santos, andRafael Mantilla Montalvo. Definition of internet of things (iot) cyber riskdiscussion on a transformation roadmap for standardisation of regulationsrisk maturity strategy design and impact assessment, 2019.

[12] S. P. Mohanty, U. Choppali and E. Kougianos, "Everything you wanted to know about smart cities: The Internet of things is the backbone," in IEEE Consumer Electronics Magazine, vol. 5, no. 3, pp. 60-70, July 2016, doi: 10.1109/MCE.2016.2556879.

[13] Samir Ouchani. Ensuring the functional correctness of iot through formal modeling and verification. In Model and Data Engineering - 8th International Conference,MEDI 2018, Lecture Notes in Computer Science, pages 401â€“417. Springer International Publishing, 2018.

[14] M. Centenaro, L. Vangelista, A. Zanella, and M. Zorzi. Long-Range Communications in Unlicensed Bands: the Rising Stars in the IoT and Smart City Scenarios.IEEE Wireless Communications, 23, October 2016.

[15] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren and X. S. Shen, "Security and Privacy in Smart City Applications: Challenges and Solutions," in IEEE Communications Magazine, vol. 55, no. 1, pp. 122-129, January 2017, doi: 10.1109/MCOM.2017.1600267CM.

[16] Luis Sanchez, Luis MuÃ±oz, Jose Antonio Galache, Pablo Sotres, Juan R. San-tana, Veronica Gutierrez, Rajiv Ramdhany, Alex Gluhak, Srdjan Krco, Evange-los Theodoridis, and Dennis Pfisterer. Smartsantander: Iot experimentation over a smart city testbed.Computer Networks, 61:217 â€“ 238, 2014. Special issue on Future Internet Testbeds â€“ Part I.

[17] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi. Internet of things for smart cities.IEEE Internet of Things Journal, 1(1):22â€“32, Feb 2014.

[18] Kanaris, L.; Sergiou, C.; Kokkinis, A.; Pafitis, A.; Antoniou, N.; Stavrou, S. On the Realistic Radio and Network Planning of IoT Sensor Networks. Sensors 2019, 19, 3264.

[19] Ghayvat H, Mukhopadhyay S, Gui X, Suryadevara N. WSN- and IOT-Based Smart Homes and Their Extension to Smart Buildings. Sensors (Basel). 2015;15(5):10350-10379. Published 2015 May 4. doi:10.3390/s150510350

[20] S. Arvind and V. A. Narayanan, "An Overview of Security in CoAP: Attack and Analysis," 2019 5th International Conference on Advanced Com-

puting & Communication Systems (ICACCS), Coimbatore, India, 2019, pp. 655-660, doi: 10.1109/ICACCS.2019.8728533.

[21] Chiehyeon Lim, Paul P. Maglio Data-Driven Understanding of Smart Service Systems Through Text Mining. Service Science 10 (2) 154-180 https://doi.org/10.1287/serv.2018.0208

[22] S. P. Mohanty, U. Choppali and E. Kougianos, "Everything you wanted to know about smart cities: The Internet of things is the backbone," in IEEE Consumer Electronics Magazine, vol. 5, no. 3, pp. 60-70, July 2016, doi: 10.1109/MCE.2016.2556879.

[23] Weihua Duan, Rouhollah Nasiri, and Sasan Karamizadeh. 2019. Smart City Concepts and Dimensions. In Proceedings of the 2019 7th International Conference on Information Technology: IoT and Smart City (ICIT 2019). Association for Computing Machinery, New York, NY, USA, 488â€“492. DOI:https://doi.org/10.1145/3377170.3377189

[24] Mehmood, Yasir and Ahmad, Farhan and Yaqoob, Ibrar and Adnane, Asma and Imran, Muhammad and Guizani, Sghaier. (2017). Internet-of-Things Based Smart Cities: Recent Advances and Challenges. IEEE Communications Magazine.

[25] Etienne André, Didier Lime, and Mathias Ramparison. Tctl model checking lower/upper-bound parametric timed automata without invariants. InDavid N. Jansen and Pavithra Prabhakar, editors,Formal Modeling andAnalysis of Timed Systems, pages 37–52, Cham, 2018. Springer International Publishing.

[26] Mohamed Abdel-Basset, Mai Mohamed, and Victor Chang. Nmcda: Aframework for evaluating cloud computing services.Future GenerationComputer Systems, 86:12 â€“ 29, 2018.

[27] Dizdarevic, Jasenka and Carpio, Francisco and Jukan, Admela and Masip, Xavi. (2018). A Survey of Communication Protocols for Internet of Things

and Related Challenges of Fog and Cloud Computing Integration. ACM Computing Surveys. 51. 10.1145/3292674.

[28] Akbar Iskandar, Elisabet Virma, and Ansari Saleh Ahmar. ImplementingDMZ in Improving Network Security of Web Testing in STMIK AKBA.arXiv e-prints, page arXiv:1901.04081, January 2019.

[29] Ngoc, Nguyen and Nguyen, Van-Quyet and Choi, Jintae and Kim, Kyungbaek. (2018). Design and implementation of intrusion detection system using convolutional neural network for DoS detection. ICMLSC '18: Proceedings of the 2nd International Conference on Machine Learning and Soft Computing. 34-38. 10.1145/3184066.3184089.

[30] Das, Rishabh and Menon, Vineetha and Morris, Thomas. (2018). On the Edge Realtime Intrusion Prevention System for DoS Attack. 81-88. 10.14236/ewic/ICS2018.10.

[31] Khalaf, Osamah Ibrahim and B. Sabbar. â€œAn overview on wireless sensor networks and finding optimal location of nodes.â€ (2019).

[32] Monowar Hasan and Sibin Mohan. Protecting actuators in safety-critical iotsystems from control spoofing attacks, 2019.

[33] Bae, W., Kwak, J. Smart card-based secure authentication protocol in multi-server IoT environment. Multimed Tools Appl 79, 15793â€“15811 (2020). https://doi.org/10.1007/s11042-017-5548-2

[34] Alabady, S.A., Al-Turjman, F. & Din, S. A Novel Security Model for Cooperative Virtual Networks in the IoT Era. Int J Parallel Prog 48, 280â€“295 (2020). https://doi.org/10.1007/s10766-018-0580-z

[35] Chang, Ming, & Min Zhang. "Architecture Design of Datacenter for Cloud English Education Platform." International Journal of Emerging Technologies in Learning (iJET) [Online], 14.01 (2019): pp. 24-33. Web. 3 Sep. 2020

[36] T. Kang and J. Seo, "Practical Simplified Indoor Multiwall Path-Loss Model," 2020 20th International Conference on Control, Automation and Systems (ICCAS), 2020, pp. 774-777, doi: 10.23919/ICCAS50221.2020.9268260.

[37] Paul Fiterau-Brostean, Bengt Jonsson, Robert Merget, Joeri de Ruiter,Konstantinos Sagonas, and Juraj Somorovsky. Analysis of DTLS imple-mentations using protocol state fuzzing. In29th USENIX Security Sympo-sium (USENIX Security 20), pages 2523–2540. USENIX Association, August2020.

[38] N. Naik, "Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP," 2017 IEEE International Systems Engineering Symposium (ISSE), Vienna, 2017, pp. 1-7, doi: 10.1109/SysEng.2017.8088251.

[39] Al-Khraishi, Tareq, Performance Evaluation and Enhancement of VLAN via Wireless Networks using OPNET Modeler (2020). International Journal of Wireless Mobile Networks (IJWMN) Vol. 12, No. 3, June 2020, Available at SSRN: https://ssrn.com/abstract=3651911

[40] Yunzhe Li, Xingfu Zhang, and Bowen Jia. The design of hardware firewall-based on acorn RISC machine.IOP Conference Series: Earth and Environmental Science, 692(2):022038, mar 2021.

[41] S. Jahan, M. S. Rahman and S. Saha, "Application specific tunneling protocol selection for Virtual Private Networks," 2017 International Conference on Networking, Systems and Security (NSysS), Dhaka, 2017, pp. 39-44, doi: 10.1109/NSysS.2017.7885799.

[42] Islam Faisal and Sherif El-Kassas. Limited proxying for content filtering-based on x.509 proxy certificate profile. In Jean-Louis Lanet and CristianToma, editors,Innovative Security Solutions for Information Technology andCommunications, pages 218–233, Cham, 2019. Springer International Pub-lishing.

[43] Tbatou, Zakariae and Ahmed, Asimi and Younes, Asimi and Sadqi, Yassine and Guezzaz, Azidine. (2017). A New Mutuel Kerberos Authentication Protocol for Distributed Systems. International Journal of Network Security. 19. 10.6633/IJNS.201711.19(6).04).

[44] Shevchenko, S., Skladannyi, P., & Martseniuk, M. (2019). ANALYSIS AND RESEARCH OF THE CHARACTERISTICS OF STANDARDIZED IN UKRAINE ANTIVIRUS SOFTWARE. Electronic Professional Scientific Edition "Cybersecurity: Education, Science, Techniquequot;, 4(4), 62-71. https://doi.org/10.28925/2663-4023.2019.4.6271

[45] Biswas, Dwaipayan. (2017). Mordern Optical Fiber â€“ Communication Splitter IJSRP. International Journal of Scientific Research. 7. 317-320.

[46] Ilias Mavridis and Helen Karatza. Performance evaluation of cloud-basedlog file analysis with apache hadoop and apache spark.Journal of Systemsand Software, 125:133 â€“ 151, 2017.

[47] Bell, David Elliott and Leonard J. La Padula. â€œSecure Computer System: Unified Exposition and Multics Interpretation.â€ (1976).

[48] K. Roussel, Y.Q. Song, O. Zendra, â€œUsing Cooja for WSN Simulations: Some New Uses and Limitsâ€, Kay Roemer. EWSN 2016 - NextMote workshop, Feb 2016, Graz, Austria. Junction Publishing, Proceedings of the 2016 International Conference on Embedded Wireless Systems and Network - EWSN â€™16 - NextMote workshop, pp.319-324, 2016.

[49] Leila Ben Saad, Cedric Chauvenet, Bernard Tourancheau. Simulation of the RPL Routing Protocol for IPv6 Sensor Networks: two cases studies. International Conference on Sensor Technologies and Applications SENSORCOMM 2011, Sep 2011, Nice, France. ffhal-00647869f

[50] B. Safaei, A. M. H. Monazzah, T. Shahroodi and A. Ejlali, "Objective function: A key contributor in Internet of Things primitive properties,"

2018 Real-Time and Embedded Systems and Technologies (RTEST), 2018, pp. 39-46, doi: 10.1109/RTEST.2018.8397077.

[51] Electricity consumption comparisons for home appliances and electron-ics. https://www.reliant.com/en/residential/electricity/save-energy/tips-to-lower-your-electricity-bill/electricity-consumption-comparison.jsp, 2020.

[52] Bibri, S.E. The eco-city and its core environmental dimension of sustainability: green energy technologies and their integration with data-driven smart solutions . Energy Inform 3, 4 (2020). https://doi.org/10.1186/s42162-020-00107-7

[53] R. M. Elavarasan et al., "A Comprehensive Review on Renewable Energy Development, Challenges, and Policies of Leading Indian States With an International Perspective," in IEEE Access, vol. 8, pp. 74432-74457, 2020, doi: 10.1109/ACCESS.2020.2988011.

[54] rif Mahmud, Faria Hossain, Tasnim Ara Choity, and Faija Juhin. Simulation and comparison of rpl, 6lowpan, and coap protocols using cooja simu-lator. In Mohammad Shorif Uddin and Jagdish Chand Bansal, editors,Pro-ceedings of International Joint Conference on Computational Intelligence,pages 317–326, Singapore, 2020. Springer Singapore.

[55] Mehmet Akif Destek and Avik Sinha. Renewable, non-renewable energy-consumption, economic growth, trade openness and ecological footprint: Ev-idence from organisation for economic co-operation and development coun-tries.Journal of Cleaner Production, 242:118537, 2020.

[56] Anser, M.K. Impact of energy consumption and human activities on carbon emissions in Pakistan: application of STIRPAT model. Environ Sci Pollut Res 26, 13453–13463 (2019). https://doi.org/10.1007/s11356-019-04859-y

[57] S. Haider et al., "A Deep CNN Ensemble Framework for Efficient DDoS

Attack Detection in Software Defined Networks," in IEEE Access, vol. 8, pp. 53972-53983, 2020, doi: 10.1109/ACCESS.2020.2976908.

[58] Garcia-Font, V.; Garrigues, C.; Rifà-Pous, H. Attack Classification Schema for Smart City WSNs. Sensors 2017, 17, 771. https://doi.org/10.3390/s17040771

[59] Mesbahi, M.R., Rahmani, A.M. & Hosseinzadeh, M. Reliability and high availability in cloud computing environments: a reference roadmap. Hum. Cent. Comput. Inf. Sci. 8, 20 (2018). https://doi.org/10.1186/s13673-018-0143-8

[60] Toh, Chai. (2020). Security for Smart Cities. IET Smart Cities. 2. 10.1049/iet-smc.2020.0001.

[61] Yang Yu, Liping Zheng, Jianjie Zhu, Yingxiu Cao, and Bei Hu. Technology of short-distance wireless communication and its application based onequipment support.AIP Conference Proceedings, 1955(1):040135, 2018.

[62] Krittin INTHARAWIJITR, Katsuyoshi IIDA, and Hiroyuki KOGA. Simula-tion study of low latency network architecture using mobile edge computing.IEICE Transactions on Information and Systems, E100.D(5):963–972, 2017.

[63] Rani, S.; Chauhdary, S.H. A Novel Framework and Enhanced QoS Big Data Protocol for Smart City Applications. Sensors 2018, 18, 3980. https://doi.org/10.3390/s18113980

[64] Rao, S.K., Prasad, R. Impact of 5G Technologies on Smart City Implementation. Wireless Pers Commun 100, 161–176 (2018). https://doi.org/10.1007/s11277-018-5618-4

[65] Vijayan, D.S., Rose, A.L., Arvindan, S. et al. Automation systems in smart buildings: a review. J Ambient Intell Human Comput (2020). https://doi.org/10.1007/s12652-020-02666-9

[66] G. Arfaoui et al., "A Security Architecture for 5G Networks," in IEEE Access, vol. 6, pp. 22466-22479, 2018, doi: 10.1109/ACCESS.2018.2827419.

Appendix A. appendix

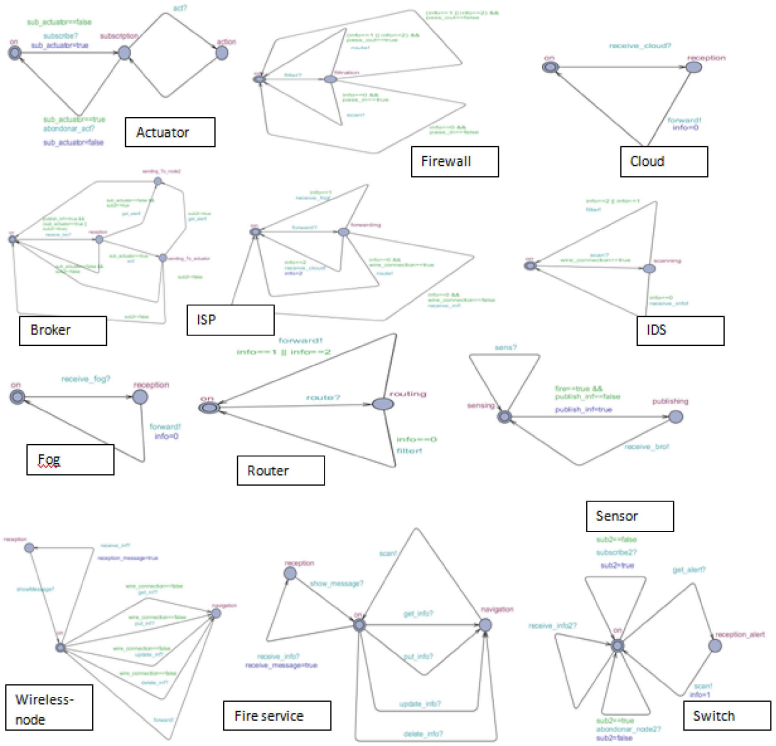


Figure A.26: Timed automata of smart city devices.

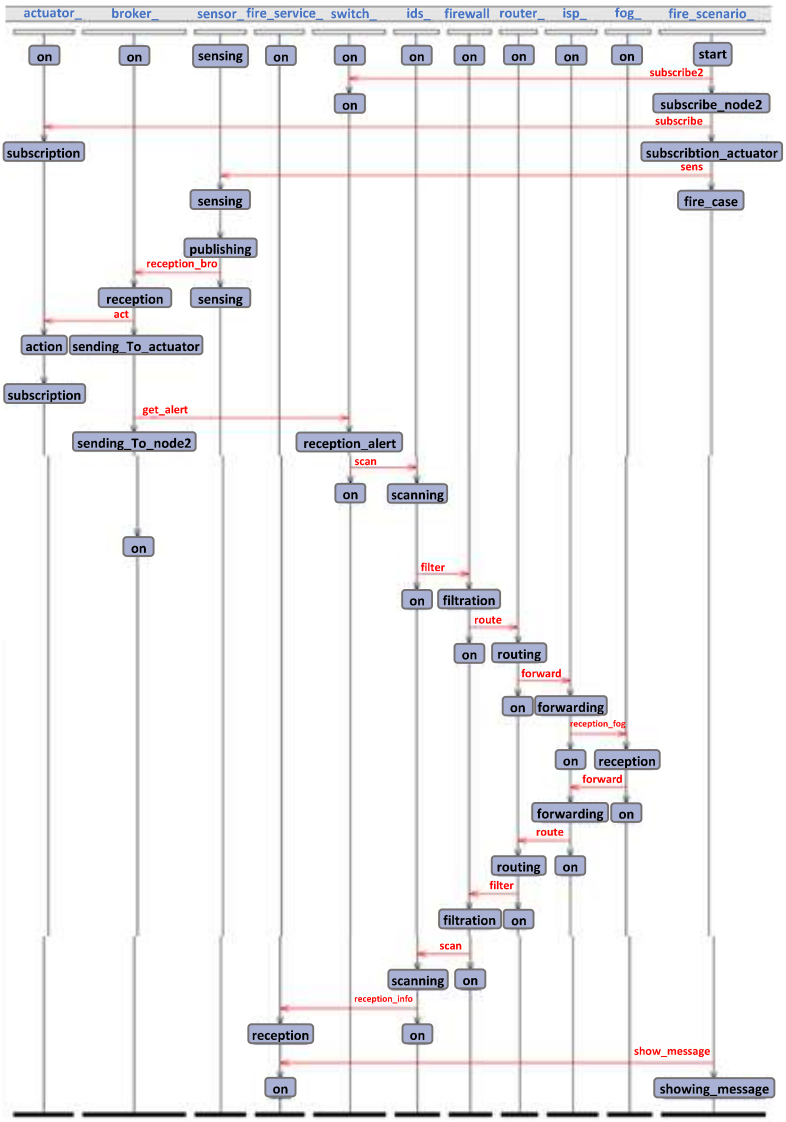


Figure A.27: Sequence diagram of scenario 3.

City and Country	Population	Solutions	Major partners	Challenges
Busan - South Korea	3.4 million	Safety service for children/elderly, drone-based smart marine, smart parking, crosswalk, and energy usage	Busan government, Cisco, ETRI, KETI, SK telecom, KT	- Approximate investment of US $452 million. - Deliver an improved transportation system. - Achievement an e-healthcare services. - Increased jobs and business opportunities. - Improved information accessibility.
Santander - Spain	0.1 million	Smart metering of temperature, traffic intensity, humidity, transportation plans, water needs, etc.	Ericsson, Telefonica, Telefonica I+D	- Managing 15 big participants companies. - Recording the transmit ed data collected by 20000 smart IoT devices. - Compiling the sensor data into a big picture.
Chicago United States	2.7 million	Smart grid, smart living, emergency alert, reduced crime	Cisco, IBM, Chicago government	- It Controls 300000 smart IoT devices. - It aims to reduce energy waste to save customers US$170 million. - Model has 31 variables to prevent rodent infestations.
Milton Keynes - United Kingdom	0.2 million	Smart transportation, reduced carbon emission, smart energy, water management	Milton Keynes Council, Samsung, Huawei, CATAPULT, Cambridge University	- Controlling carbon emissions and supporting sustainable growth without deploying additional infrastructure. - Resolving more issues like business, education, and community engagement activities.

Table A.5: Smart city projects.

Comparison Criteria	Traditional city	Smart city
Energy consummation	• Non-renewable energy [55]. • Energy is polluted [56]. • Large number of non-optimized devices. • The characteristics of theirs protocols do not serve the IoT network.	• Renewable energy [53]. • Green energy [52]. • Small number of IoT devices. • The IoT nodes use communication protocols suitable to low power as CoAP, RPL, 6LoWPAN, etc [54].
Large data	• Collapse of the information system [57]. • Low-security level [58]. • Bad service provided.	• Continued operation of the system and smart processing of information [59]. • High-security level [60]. • Availability and QoS[63].
Coverage and latency	• Small range and low speed of transmitted data due to it uses traditional communication technologies [61]. • Architecture bases to distant servers cause high latency [62].	• Large communication range and low latency due to it uses the high technologies as such as 5G [64]. • Architecture bases on fog computing that causes low latency.
Buildings	• Difficult to mitigate the building threats like fire, temperature, humidity, etc.	• It has IoT nodes Like sensors that can control the requirements building [65].
Security	• Information loss due to saturation of the server provider by the data flooding. • More vulnerable system.	• Smart architecture manage the data flow [66]. • Modern components with high security .

Table A.6: Comparison between smart and traditional cities.

Criteria	RPL	6LoWPAN	IPv6 over Bluetooth Low Energy
Architecture and network	DODAG	Wireless personal area network (WPAN)	Master / Slave architecture
Message size	5 bytes of compressed IPv6. 4 bytes for ICMP Type. 24 bytes for DIO Base Object. 16 bytes for DODAG Configuration Option	128-byte maximum frame length in IEEE802.15.4	The Logical Link Control and Adaptation Protocol (L2CAP) sublayer in Bluetooth already provides segmentation and reassembly of larger payloads into 27 byte L2CAP packets
Security	RPL network admits three possible security modes: unsecured, preinstalled, and authenticated. Recent implementations aim to securely connect constrained nodes (as IPsec, DTLS, and IEEE 802.15.4 link-layer security)	Depends on the 802.15.4 security sub-layer (by adding both a Message Integrity Code (MIC) and a frame counter to each frame).	Using the Cipher Block Chaining-Message Authentication Code (CCM) algorithm and a 128-bit AES block cipher. 4-byte Message Integrity Check (MIC) is included in the Bluetooth LE packets. Encryption is applied to the PDU payload and MIC fields.
IP address	IPv6	IPv6	IPv6

Table A.7: Comparison between the network layer protocols.

Criteria	MQTT	CoAP	AMQP
Architecture	Client/Broker	Client/Server or Client/Broker	Client/Broker or Client/Server
Abstraction	Publish/Subscribe	Request/Response or Publish/Subscribe	Publish/Subscribe or Request/Response
Header Size	2 Byte	4 Byte	8 Byte
Message Size	Small and Undefined (up to 256 MB maximum size)	Small and Undefined (normally small to fit in single IP datagram)	Negotiable and Undefined
Semantics/ Methods	Connect, Disconnect, Publish, Subscribe, Unsubscribe, Close	Get, Post, Put, Delete	Consume, Deliver, Publish, Get, Select, Ack, Delete, Nack, Recover, Reject, Open, Close
Quality of Service (QoS)/ Reliability	QoS 0 - At most once (Fire-and-Forget), QoS 1 - At least once, QoS 2 - Exactly once	Confirmable Message (similar to At most once) or Non-confirmable Message (similar to At least once)	Settle Format (similar to At most once) or Unsettle Format (similar to At least once)
Security	TLS/SSL	DTLS, IPSec	TLS/SSL, IPSec, SASL
Default Port	1883/ 8883 (TLS/SSL)	5683 (UDP Port)/ 5684 (DLTS)	5671 (TLS/SSL), 5672

Table A.8: Comparison between the session layer protocols.

Simulator	ns2	Castalia OMNet++	TOSSIM	Cooja/MPSim	WSim/WSNet
Level of details	generic	generic	code level	all levels	all levels
Timing	discrete event	discrete event	discrete event	discrete even	discrete event
Simulator platforms	FreeBSD, Linux, SunOS, Solaris, Windows (Cygwin)	Linux, Unix, Windows (Cygwin)	Linux, Windows (Cygwin)	Linux	Linux, Windows (Cygwin)
WSN platforms	n/a	n/a	MicaZ	Tmote Sky, ESB, MicaZ	MicaZ, Mica2, TelosB, CSEM Wisenode, ICL BSN nodes, eZ430
GUI support	Monitoring of simulation flow	Monitoring of simulation flow, c++ development, topology definition, result analysis, and visualization	None	Yes	None
Wireless channel	Free space, two-ray ground refection, shadowing	lognormal shadowing, experimentally measured, path loss map, packet reception rates map, temporal variation, unit disk	lognormal shadowing	multipath raytracing with support for attenuating for obstacles, unit disk, directed graph	file static, disk model, free space, tworay ground, lognormal shadowing, rayleigh fading, ITU indoor model, nakagami fading
PHY	Lucent WaveLan DSSS	CC1100, CC2420	CC2420	CC2420, TR1001	CC1100, CC1101,CC2500, CC2420
MAC	802.11, preambule based TDMA (preliminary stage)	TMAC, SMAC, Tunable MAC (can approximate BMAC, LPL, etc.)	Standard TinyOS 2.0 CC2420 stack	CSMA/CA, TDMA, XMAC, LPP, NullMAC, contikiMAC, SicslowMAC	DCF, BMAC, ideal MAC
Network	DSDV, DSR, TORA, AODV	Simple Tree, Multipath Rings	No data	RPL, AODV	Greedy Geographic, file static
Transport	UDP, TCP	None	No data	UDP, TCP	None
Sensing	Random process with Mannasim add-on	Generic moving time-varying physical process	No data	Moving nodes	Generic moving time-varying physical process
Energy consumption model	Yes	Yes	With Power TOSSIM add-on	Yes	Yes

Table A.9: Open-Source Simulators Comparison [49].