sensors

MDPI

Article

Environmental Monitoring with Distributed Mesh Networks: An Overview and Practical Implementation Perspective for Urban Scenario †

Aleksandr Ometov [1], Sergey Bezzateev [2], Natalia Voloshina [3], Pavel Masek [4] and Mikhail Komarov [5,*]

1 Tampere University, 33720 Tampere, Finland; aleksandr.ometov@tuni.fi
2 Saint Petersburg State University of Aerospace Instrumentation, 190000 St. Petersburg, Russia; bsv@aanet.ru
3 ITMO University, 197101 St. Petersburg, Russia; nvvoloshina@itmo.ru
4 Brno University of Technology, 60190 Brno, Czech Republic; masekpavel@vutbr.cz
5 National Research University Higher School of Economics, 101000 Moscow, Russia
* Correspondence: mkomarov@hse.ru

† This paper is an expanded version of the conference paper: Bezzateev, S.; Voloshina, N.; Zhidanov, K.; Ometov, A. Secure Environmental Monitoring for Industrial Internet of Things: From Framework to Live Implementation. In Proceedings of the International Conference on Localization and GNSS (ICL-GNSS), Nuremberg, Germany, 4–6 July 2019.

Received: 23 October 2019; Accepted: 13 December 2019; Published: 16 December 2019

Abstract: Almost inevitable climate change and increasing pollution levels around the world are the most significant drivers for the environmental monitoring evolution. Recent activities in the field of wireless sensor networks have made tremendous progress concerning conventional centralized sensor networks known for decades. However, most systems developed today still face challenges while estimating the trade-off between their flexibility and security. In this work, we provide an overview of the environmental monitoring strategies and applications. We conclude that wireless sensor networks of tomorrow would mostly have a distributed nature. Furthermore, we present the results of the developed secure distributed monitoring framework from both hardware and software perspectives. The developed mechanisms provide an ability for sensors to communicate in both infrastructure and mesh modes. The system allows each sensor node to act as a relay, which increases the system failure resistance and improves the scalability. Moreover, we employ an authentication mechanism to ensure the transparent migration of the nodes between different network segments while maintaining a high level of system security. Finally, we report on the real-life deployment results.

Keywords: environmental monitoring; authentication mechanism; security; wireless sensor network; distributed systems

1. Introduction

To date, the development of various industries has brought a tremendous impact on our climate. According to the National Aeronautics and Space Administration (NASA), global climate change already has effects that can be observed in the environment. Glaciers have shrunk, ice on rivers and lakes is melting ahead of time, plant and animal habitats have changed, and trees bloom ahead of expected dates [1]. The previously predicted effects from global climate change are already happening: (i) loss of sea ice; (ii) accelerated sea-level rise; and (iii) more intense heat waves [2].

According to the European Commission, the main impact on climate change is due to the greenhouse effect, which is mainly caused by CO_2 emissions, in turn being mainly a result of human activities (64% of global warming is human-made [3]). Its concentration in the atmosphere is currently

40% higher than it was during the beginning of industrialization [4]. This impact is mainly due to: (i) burning coal; (ii) gas and oil; (iii) deforestation; (iv) increasing livestock farming; and (v) a rise in fluorinated gases amount.

One of the critical aspects in reducing the negative impact on the climate is efficient monitoring of the environmental data in addition to prompt actions aiming to reduce such impact in dedicated areas. Indeed, many researchers are actively improving and developing new solutions utilized for monitoring. After broad adoption of the Internet of Things (IoT), growing interest from industry, researchers, governments, and developers was given to IoT's particular niche — Industrial IoT (IIoT) [5]. This sector aims at covering the machine-to-machine communications (M2M) domain and topics related to modern Wireless Sensor Networks (WSNs) including ones operating in both licensed [6,7] and unlicensed bands [8,9].

IIoT provides a number of main machine-oriented development directions, including: (i) factory automation; (ii) mission-critical communications; and, generally, (iii) monitoring [10]. Historically, monitoring solutions are well-known from WSNs, and the world of today could not be imagined ignoring this section of IIoT [11].

In this context, environmental and agricultural monitoring fields are ideal candidates for trialing and deploying the IIoT solutions [12]. No doubt, the utilization of sensors may be vastly applicable for it, e.g., for monitoring of humidity, emissions, and temperature levels; for production chain control; for air pollution maps construction; for immediate alert triggers; and others.

The industrial trends of today aim at "connecting the unconnected". Presently developed systems sometimes fall behind the expectations due to their complexity and lack of proper community support. Thus, freely programmable and advanced Cyber-Physical Systems (CPS) should replace conventional programmable logic controllers in managing physical objects [13]. Simultaneously, blind development of said systems may be harmful from the information security perspective, and threats (primarily related to authentication) should be carefully taken into consideration [14–16].

Current research is also vital for the analysis of technological requirements and interconnections between different characteristics for distributed ledger technology (DLT) design. Developers need to conduct a comprehensive comparison between prospective DLT designs before starting the implementation suitability for a particular application [17]. Environmental monitoring system based on mesh network approach falls into the specific domain of distributed systems, which can be implemented on the DLT basis, where sensing devices could vary depending on different manufacturers or service-providers and where the level of trust to the sensing data will be higher due to the DLT implementation. An example of a distributed mobility platform was presented in [18] demonstrating its technical feasibility and showing that the introduction of distributed mobility concept will benefit both the supply and demand sides of public transportation at the same time.

In this paper, we propose and develop the CPS system titled "Galouis", which is a flexible environmental monitoring tool relying on the distributed network architecture. Dell-EMC carefully managed this work and supported the deployment in the metropolitan area. The main contributions of this work are:

1. Modern environmental monitoring applications and scenarios are reviewed.
2. The pairwise key-based authentication mechanism was applied for urban environmental monitoring, allowing to handle individual system operational phases, e.g., the addition of new nodes, (un-)authorized migration of the node from one network segment to another, etc.
3. An analytical framework based on Markov chain analysis that allows evaluating potential network topology changes is presented.
4. A prototype of the proposed secure distrusted sensor network (operating based on the discussed authentication mechanism) was deployed in a real-life scenario.

The paper is structured as follows. Section 2 provides an overview of the leading environmental applications and related security aspects. Section 3 provides the system description and highlights

the main problematics. Section 4 overviews the developed secure operation enablers of the system. Section 5 shows the developed analytical approach and selected numerical results. Section 6 provides technical details of the prototype and real-life deployment. The last section concludes the paper.

2. Overview on Environmental Monitoring Applications and Main Security Specifics

Focusing mainly on the Smart City paradigm from the IIoT perspective, the main activities of environmental monitoring could be listed as the following [19] (see selected ones in Figure 1). The first group of applications corresponds to the paradigm of urban environmental monitoring [20]. It consists of the following subgroups: (i) structural health [21]; (ii) light pollution monitoring [22]; (iii) waste management [23]; (iv) noise monitoring [24]; and (v) air pollution [25].

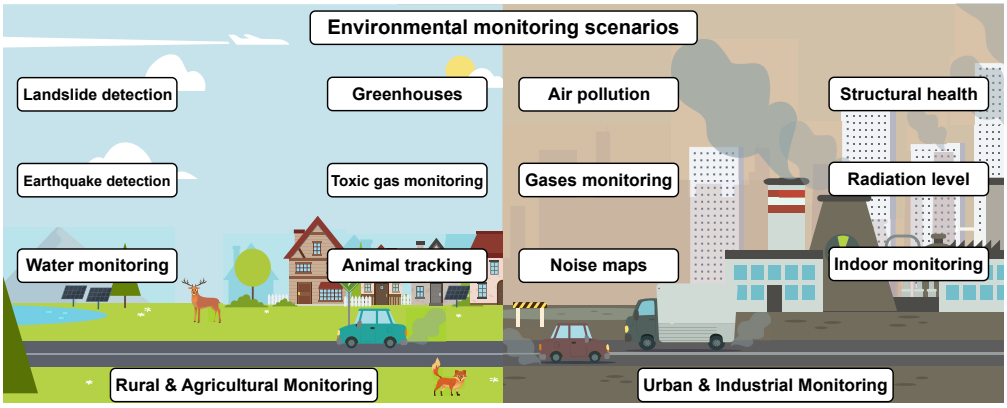


Figure 1. Selected monitoring scenarios and applications.

A massive section of this group is related to industrial control [26], aiming at: (i) indoor air quality monitoring [27], i.e., monitoring of toxic gas and oxygen levels inside chemical plants and office spaces to ensure safety; (ii) temperature monitoring [28], i.e., control of the temperature inside industrial and medical fridges with sensitive products; (iii) ozone level monitoring [29], i.e., monitoring of ozone levels inside food factories; and (iv) indoor positioning [30], i.e., indoor asset location utilizing active (ZigBee and Ultra-Wideband (UWB)) and passive (Radio Frequency Identification (RFID) and Near Field Communication (NFC)) tages. Nonetheless, security and emergency scenarios are also to be considered [31] as, for example: (i) perimeter access control [32], i.e., border surveillance and intrusion detection; (ii) dangerous liquid presence and leak detection [33,34], i.e., monitoring of the lower explosive limit of potentially dangerous gases and vapors; (iii) radiation level monitoring [35], i.e., real-time monitoring of radiation levels at nuclear facilities and surrounding areas; and (iv) explosive and hazardous gases in underground environments [36], i.e., continuous monitoring of the ambient characteristics of the mining environment.

The second big group is related to rural environmental monitoring [37]: (i) landslide and avalanche prevention [38], i.e., monitoring of soil moisture, vibrations, and earth density to detect dangerous patterns of inland conditions; (ii) earthquake early detection [39], i.e., distributed control in specific places of tremors; and (iii) forest fire detection [40], i.e., monitoring of combustion gases and preemptive fire conditions to define alert zones. A standalone section within rural monitoring is dedicated to agricultural monitoring [41] covering the following applications: (i) greenhouse parameter control [42], i.e., control of micro-climate conditions to maximize the production of fruits and vegetables and its quality; (ii) meteorological station network [43], i.e., monitoring of weather conditions in fields to forecast ice formation, rain drought, snow, or wind changes; (iii) animal tracking [44], i.e., location and identification of animals grazing in open pastures or location in big stables; (iv) wine production and quality enhancing [45], i.e., monitoring the productive cycle of high-quality wine; (v) monitoring of the toxic gas level of farm animals [46], i.e., a study of ventilation and air quality in farms and the

detection of harmful gases from excrements; and (vi) compost monitoring [47], i.e., control of humidity and temperature levels in alfalfa, hay, straw, etc. to prevent fungus and other microbial contaminants.

It is important to notice that the entire deployment predictivity of the IIoT sensor network is somewhat challenging due to a significant number of nodes involved. Moreover, devices could disconnect from the network, reconnect again, or move to another segment of the network without notifying the coordinator. The use of distributed sensor networks with flexible topology requires the utilization of secure yet straightforward authentication protocols.

One of the most significant challenges of dynamic WSNs is the lack of centralized authority coordination. Such a center should provide storage, generation, and dissemination of the certificates to each sensor node operating within the public key infrastructure (PKI) paradigm [48]. If the agreement of using a single authentication center could be reached, it is relatively straightforward to perform mutual node authentication and secret key generation for secure data transmission. If there is no possibility of having just a single authentication center, a high demand to create and use reliable authentication protocols appears together with the need for the application layer management platform operating in a straightforward and flexible way.

3. System Description and Problem Statement

The developed system is a distributed self-organizing sensor network designed to monitor the parameters of the urban environment. It allows for the data transmission only from the trusted sensors that confirm their association with a specific network. The monitoring of the data is carried out remotely using a trusted Internet portal with a graphical user interface (GUI). A trusted addition and removal of the sensor are carried out using a smartphone application given the assumption that the device supports IEEE 802.11 protocol operation.

The system was designed considering the requirements of urban environmental services, city administration, and emergency services. In addition, some information received and processed by the system can be provided to third parties for planning mass events, as well as to citizens to inform them about the environmental situation. In the case of providing information to citizens, data may be shown in quantitative form, e.g., in the form of geographical information systems (GIS).

The developed system aims at solving the problem of promptly informing relevant services regarding possible emergency situations, allowing for better prediction and fast reaction.

The system is designed to operate in three different modes:

1. Simplex mode: The operation of the system is executed according to the "star" topology, and the transmission of messages to the Access Pontes (APs) directly using a controlled sleep mode.
2. Duplex mode: The operation of the system is executed according the mesh network mode with relaying via the closest network nodes using a controlled sleep mode.
3. Half-duplex mode: The operation the system is executed via the star topology but using a predefined sleep mode, i.e., the preset of the optimal mode for a given scenario and operating conditions are applied.

Utilization of relaying strategy in duplex mode can significantly reduce the number of APs required for a deployable wireless network reducing the system's overall deployment cost.

The proposed system allows us to solve the task of environmental monitoring by constructing a self-organizing network of sensors using a secure protocol for direct data exchange between the nodes or through a third-party network. The obtained data can be aggregated and visualized at the dedicated server, indicating the geo-position of the device for collecting visualized data. Such online portal allows for quick response to critical changes in the selected parameters as well as in the data analysis for future prediction.

The main challenges of urban environmental monitoring are the deployment simplicity and flexibility in terms of the mesh network reconfiguration [49] as well as resistance to the "malicious" sensor connection [50]. The main problems include: (i) the difficulty of initializing a network with a

large number of devices; (ii) connecting a new sensor to an existing network; (iii) network scalability; (iv) the ability to use a trusted sensor in a network location other than the legal installation place; and (v) the ability to detect a malicious device (sensor) presence.

In this paper, we propose an advanced protocol for the initial authentication and addition of sensor nodes to an existing distributed network. During the operation of the system, a secure data transfer protocol is implemented based on pairwise authentication of the sensors in terms of their location, which protects the system from the unauthorized introduction of a malicious sensor or a critical change in the location of the legally installed sensor, and also prevents from false information updates. The system aims to enable flexible and efficient support for potential sensor network topology dynamics. The resulting general overview of the environmental situation will allow responding to critical changes in the monitored parameters quickly. Nonetheless, a flexible network configuration feature aims to cover the monitored territories in order to obtain the most accurate and useful data that can be further used for the analysis of the urban situation and planning measures to improve it.

4. Security and Scalability for Environmental Monitoring Sensor Networks

Today, there are many critical security issues in the data transmission and processing in the scope of dynamic sensor networks with variable topology [51]. In particular, the critical problem is to provide a secure device "arrival" to the existing network since reconfiguration in a centralized manner may be challenging. In situations when a trusted authority is unavailable (for example, due to the connectivity issues), the operation of mutual device authentication becomes much more complicated [52].

This section is mainly focused on possible solutions for the sensor networks creation and providing support for secure mutual authentication of their sensors (nodes) that could be utilized for urban environmental monitoring.

For our system, we assume that the network components are classified to only two groups, as shown in Figure 2:

- Gateway or Access Point (AP) is used for the end-node data aggregation. APs could also perform edge preprocessing of the incoming sensor data before the cloud delivery. Each data packet from each sensor node is encrypted using cloud public key to provide an additional level of the data integrity.
- Monitoring nodes are equipped with different sensing devices with the primary goal of collecting the specified environmental parameters, e.g., temperature, humidity, noise level, etc. The nodes could either connect directly to the AP or relay the data through the neighboring nodes to the AP in the ad hoc-like way.

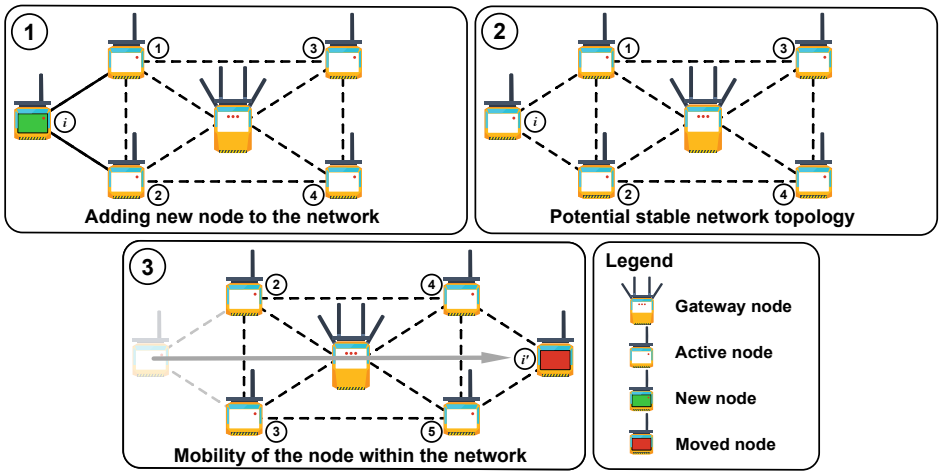


Figure 2. Monitoring systems operational states.

The main abbreviations used in this work are given in Table 1 and the system operation could be divided into the following operational phases.

Table 1. Main notations used in the paper.

Notation	Description
k	Number of sensors
i, j, l, n	Indexes
MK	Master Key
ID_i	ith sensor node unique identifier
$H(*)$	One-way function
$K_{i,j}$	Auxiliary key for ith and jth nodes
T_{rm}	MK lifetime period after the initialization phase
S_i	Subset of nodes that have pairwise connection with ith node
$J(S_i)$	Number of nodes in S_i
p	Single node failure probability ($q = 1 - p$)
S	State space of the Markov chain
$P_{i,j}$	Transition probability from state i to state j

1. **Sensor initialization (addition)**: For example, a phase when a new node should be connected to any available node or AP in range (see Figure 2, Case 1). Assuming that both devices are operating in the same predefined way from the information security point of view, we consider two possible scenarios:
   - Simultaneous initialization of several sensors in one secure network. This situation is common for initial network deployment when a number of devices is more than two, $k > 2$.
   - Adding a single new sensor to an existing secure sensor network.
2. **Stable sensor network operation**: In this scenario, sensors are neither added nor excluded from existing topology, and their logical position is static with respect to their neighbor nodes (see Figure 2, Case 2).
3. **Sensor migration**: In this scenario, the network faces the topology change (see Figure 2, Case 3) that could be caused by different factors:
   - Legally moved sensor is within the network segment with established pairwise relation;
   - Illegally moved sensor.
4. **Sensor removal**: In this scenario, two possible scenarios may be present:
   - Removed sensor is excluded from a particular secure network and could be used in the future only through new node initialization procedure.
   - Removed sensor is migrated to another segment of an existing network without reinitialization.

After careful evaluation of each of the mentioned scenarios, we decided to use the master key of sensor network [53,54] for initial authentication. At the first step of the sensor network initialization, it is necessary to provide mutual authentication for the single network segment. The segment is specified by the radio link range of the desired technology. For the sensor mutual authentication, we utilize the Lightweight Extensible Authentication Protocol (LEAP) -like protocol [55]. The main difference between common mutual authentication protocols for sensor networks on the stage of initialization is the level of master key protection on the next steps of the network life cycle:

1. The master key used on the initialization step is not removed and is kept in the so-called tamper resistance memory of the node [56]. This approach allows us to change the configuration of the

network by simple displacement of the earlier installed node from one segment of the secure network to another (see Figure 2, Case 3). The displaced node can then authenticate with any other neighboring node in the same network if the nodes have the same master key. However, this feature becomes a disadvantage in the case it is necessary to prevent illegal movement (for example, if there is a need to be aware of the actual location of each node [57]). In this case, we should utilize an additional user authentication protocol for the system operator, which is required to make legal replacement of the active node, i.e., only the authenticated user should have an opportunity to move the sensor from one segment of the secure network to another. Any unauthorized movement should be prohibited.

2. The master key used at the step of initialization is destroyed after predefined time calculated from the moment when the initialization step was completed [55]. This scenario strongly limits the possibility of previously installed sensor movement from the initial sensor network segment to another part of the same network. This feature of the protocol allows obtaining a rather stable structure of the network. In this case, the probability of getting false information from the nodes is significantly reduced due to the location change.

Evidently, the second protocol is preferred in real-life dynamics of urban monitoring purposes. This protocol could be described as follows.

4.1. First Initialization of Several Sensors for New Secure Sensor Network

- Initially, the master key MK is defined for a new secure network. Each node i has its own unique identification number ID_i, $ID_i > ID_j$ for $i > j$. Next, we define one-way function—$H(*)$.
- During the initial initialization, nodes can only exchange data in wireless link range, as depicted in Figure 2 (Case 2). Here, sensors 1, 2 and 3 exchange their unique IDs ID_1, ID_2, and ID_3.
- Each of the nodes utilizes the information about unique IDs of other sensors and the master key MK to calculate pair-wise keys for mutual authentication. For example, sensor 1 calculates pair keys for sensors 2 and 3 as:

$$K_{1,2} = H(ID_1||ID_2||MK), \tag{1}$$
$$K_{1,3} = H(ID_1||ID_3||MK). \tag{2}$$

where $x||y$ stands for the concatenation.

Consequentially, sensors 2 and 3 also calculate the same pair-wise keys for the sensor 1:

$$K_{2,1} = H(ID_1||ID_2||MK) = K_{1,2}, \tag{3}$$
$$K_{3,1} = H(ID_1||ID_3||MK) = K_{1,3}. \tag{4}$$

- To provide the scalability, each sensor also calculates auxiliary key $K_{i,i} = H(ID_i||MK)$ for adding new sensors in the future.
- Each sensor removes its master key MK after predefined interval T_{rm} from the first initialization process. This way, sensor 1 in Figure 2 (Case 2) would have the same information $\{K_{1,1}, K_{1,2}, K_{1,3}\}$ after the end of the initialization phase.

Generally, after deleting the master key from the memory of the node, secure communications would only be available with ones that have already established the pairwise keys at the initialization step of the protocol. However, each node should have the possibility to connect with new nodes for better system scalability. Each new node at the initialization step has a stored predefined MK—the node has a possibility to calculate $K_{i,i}$ as a pairwise key with already known node with ID_i as $K_{i,i} = H(ID_i||MK)$.

4.2. Stable Sensor Network Operation

During the normal operation, nodes utilize pair keys that they have obtained during the first initialization for mutual authentication and generation of the session key. For example, sensors ID_1 and ID_2 use pair-wise keys $K_{1,2}$ and $K_{2,1}$ consequently.

4.3. Adding New Sensor to Existing Secure Sensor Network

According to Figure 2 (Case 2), a new ID_i sensor appears in the range of sensors 1 and 2 of the existing network.

The new ith sensor should generate pair-wise keys for neighbor sensors 1 and 2 using master key MK (preinstalled earlier), and calculate new pair keys $K_{i,1} = H(ID_1||MK) = K_{1,1}$ and $K_{i,2} = H(ID_2||MK) = K_{2,2}$ to establish a connection with sensors 1 and 2. In this case, new node is treated as one legally added to the network.

On the next step, ith sensor should delete its master key MK. A new node should create a new auxiliary key $K_{i,i}$ before the master key removal. As a result, the new added node will store the key sequence $\{K_{i,i}, K_{i,1}, K_{i,2}\}$ after the initialization process.

4.4. Legal Sensor Moving to Another Secure Sensor Network Segment of Existing Network

We also consider the case of the sensor node migration from one network segment to another. For this scenario, we define the network segment S_i as a subset of nodes $J(S_i)$ that have previously established pairwise keys with this ID_i node, i.e., $K_{i,j} = H(ID_i||ID_j||MK)$ or $K_{i,j} = H(ID_i||MK)$, $j \in J(S_i)$.

Indeed, segment S_k for a selected node ID_k could also have some nodes from S_i, which is defined by the network topology. In the case node ID_i is moved from S_i to S_k, it will remain connected to nodes that are a part of both subsets $S_k \cap S_i$ and, therefore, existing pairwise keys could be used. In the case S_k does not involve any nodes from S_i, the reinitialization of the node would be required. Fortunately, if the node ID_i is moved back next to any known ones from S_i, it can have an opportunity to reinitialize the connectivity automatically.

4.5. Illegal Sensor Moving to Another Secure Sensor Network Segment of Existing Network

In the case of illegal sensor movement from S_i, e.g., without the master key MK updates (see Figure 2, Case 3), the process of mutual authentication will fail. This authentication failure will occur because the pair-wise key generated on the initialization step could not be used for any (new) neighbor sensors of a new segment due to the unique properties of the pairwise keys (similar to the legal movement procedure). This property of the authentication protocol decreases the probability of receiving incorrect data when the location of the node changes illegally.

5. Selected Numerical Results

The usage of routing and secure pairwise authentication protocols for legal network sensors [58] allowed us to cover a large part of territory without additional APs and by using already existing infrastructure for data aggregation, which potentially decreases the operational cost of the system. On the other hand, if we consider a farm monitoring IoT scenario, there is an open task to evaluate the required density of relatively cheap (compared to the AP price) sensors with respect to both coverage area and reliability.

In the simplest scenario, we may analyze the system from the network node density perspective. In particular, we focus on the scenario when the goal is to minimize the number of nodes while maintaining a high level of mesh reliability. We assume that the network segment has around one public transport stop equipped with the city public network AP per 400 m, which corresponds to the suboptimal traffic stops distance in the urban scenario for Europe [59]. At the same time, the node placement was selected to be on the lighting poles, generally separated by approximately 10 m in

urban areas [60]. Therefore, the maximum number of potential placement locations is 39 between each pair of public transport stops, and thus a maximum number of potential hops in our mesh networks equals 40. In the worst scenario, some mesh network segments could be isolated if the connectivity to any AP is not available, which may be a result of inefficient nodes placement, e.g., when any node has only two links to its neighbors. By increasing the number of nodes, the overall reliability will grow along with the network cost.

In this work, we vary the availability of the sensor node for the lifetime of 10 years, which is suitable for environmental and urban monitoring [61,62]. As for the selected technology, the practical range is set to be 50 m [63].

We developed a Markov chain model (see Figure 3), describing the failure process of a series of sensor nodes with k overlapping connections shown in Figure 4. If a node has failed (with probability p), we make a transition to the right on the Markov chain, but if the node has not failed (with probability $q = 1 - p$), we make the transition to the left. To isolate a group of nodes in the presence of "k-extra" connections, k consecutive nodes must fail on both sides of a group. It can be represented as a stochastic counting process that moves to the next state if it encounters a failed node and returns to the initial state if it encounters a working node.

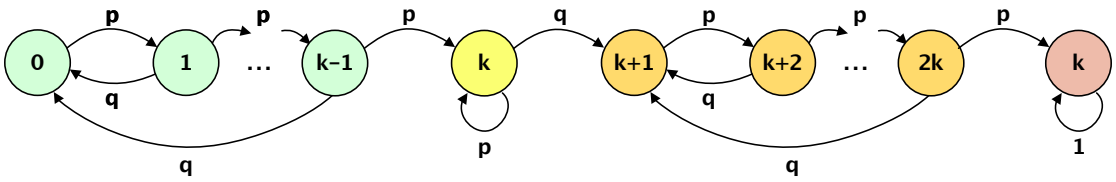


Figure 3. Markov chain utilized for the network segment analysis.

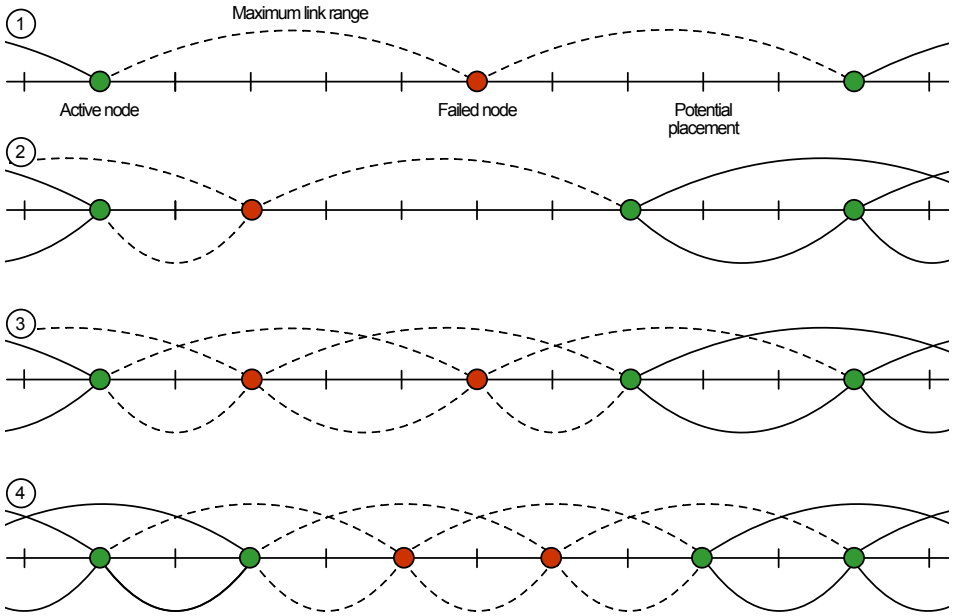


Figure 4. Potential node placement strategies: solid line, active link; dashed line, disrupted link.

The Markov chain with the state space $S = \{0, 1, \cdots, 2k+1\}$ has four communicating classes: $0, 1, \ldots, k-1, k, k+1, \ldots, 2k, 2k+1$. The first class represents the states in which we encountered less than k failed nodes in a row. Once we encountered $\geq k$ failed nodes, we make a transition to the second class and stay in this class if we encounter more consecutive failed nodes. Once we encounter at least one working node (after a breaking sequence), we move to the third class. The fourth class is a final absorbing state, which is reached if we encounter $\geq k$ failed nodes in a row for the second time. In summary, Class 1 represents the situation when we have a connection to both gateways.

Classes 2 and 3 correspond to situations when a connection is lost to one of the gateways. Class 4 is the absorbing state $2k+1$, which depicts the situations when we lose connection to both of the gateways. The transition probability matrix is given in Table 2, where p is the sensor failure probability and $q = 1 - p$. To find the probability of isolation of a group of nodes in a series of nodes of length n, we must find the n-step transition probability $P^{(n)}_{0,2k+1}$ from state 0 to state $2k+1$.

Table 2. Transition probability matrix.

State	0	1	⋯	$k-1$	k	$k+1$	⋯	$2k$	$2k+1$
0	q	p	0	⋯	⋯	⋯	⋯	⋯	0
1	q	0	p	0	⋯	⋯	⋯	⋯	0
⋮	⋮			⋱					⋮
$k-1$	q	0	⋯	0	p	0	⋯	⋯	0
k	0	⋯	⋯	0	p	q	0	⋯	0
$k+1$	0	⋯	⋯	⋯	0	q	p	0	0
⋮	⋮					⋮		⋱	⋮
$2k$	0	⋯	⋯	⋯	0	q	0	0	p
$2k+1$	0	⋯	⋯	⋯	⋯	0	⋯	0	1

In the first scenario, we focus on the mesh operation between two public transport stops, and the results are given in Figure 5. Here, both axes have a logarithmic scale. Here, the horizontal black line represents the overall system reliability equal to 99.999%, and we vary the probability of a single node to fail, thus, eliminating at least two links between the neighbors. By increasing k value, we introduce a higher number of additional links, as shown in Figure 4, which decreases the probability of the network segment separation. Following the overall reliability requirement, we can conclude that having $k = 3$ almost reaches the required threshold and thus could be used for the actual system deployment. Therefore, the sensors could be placed at three out of five lighting poles for the node reliability of 99% per 10 years operational time.

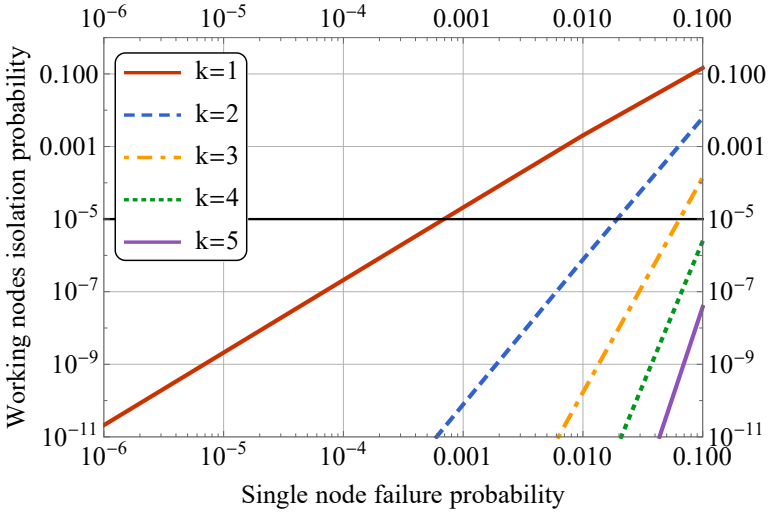


Figure 5. Effect of node placement density: between traffic stops.

For edge operation, i.e., when there is just one public transport stop available, we reduce the Markov chain by accumulating Classes 2–4 into a single absorbing state k, similar to state $2k+1$ in a

nonreduced case. The corresponding results are given in Figure 6. Evidently, the system reliability is much lower than compared to the first case, mainly due to a lower number of backup links available and a higher probability of the network separation in case of the close-to-AP node failure.

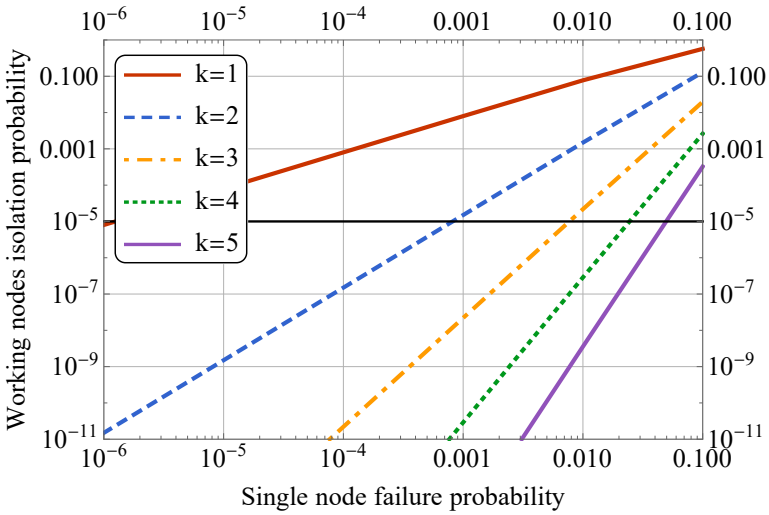


Figure 6. Effect of node placement density: edge operation.

6. Prototyping Aspects

In this section, we describe our custom platform, which was developed aiming to improve the process of secure monitoring IoT system development ease and is based on the REpresentational State Transfer (REST) principle. Additionally, this platform improves the initialization process by the automated *MK* distribution and visualization of the node location on the map. The developed platform is a set of components allowing to build IoT solutions based on Atmel ATmega328P controller [64] equipped with wireless ESP8266 module [65]. The primary platform segments are: (i) firmware (binary image for ESP8266 chip); (ii) Android software (Java libraries and sample applications); (iii) web software (JavaScript library and sample pages); (iv) server-side services (user interface, data processing scripts, and database access scripts); and (v) database (MySQL). Their relations are highlighted with the same colors in Figure 7.

The primary goal of the platform was to handle issues related to security, connectivity, and access management, while the developer only needs to design the device and customize the data processing. In particular, the platform is prepared to be transparent for developers to perform the following:

1. Initialization "duckling" of the devices [66] by using any available wireless technology of the user smartphone, i.e., Bluetooth, WiFi, or NFC [67];
2. Access sharing;
3. Routing between devices;
4. Remote access; and
5. Setting up the network credentials, and other tasks.

The platform allows rapid development of the user application using Java library based on the following list of actions:

- To register in the cloud and generate its encryption key. In this case, the generated encryption key is stored only on the user smartphone but could be sent to the cloud.
- To perform node initialization.
- To interact with already initialized devices directly when they are in the communication range of the selected wireless technology.
- To specify access credentials of known APs and distribute those to all related devices.

- To interact with the devices via the infrastructure network. In this case, all transferred data are protected with end-to-end encryption between the smartphone and the node.

When initialized, ESP8266 can be accessed by Universal Asynchronous Receiver/ Transmitter (UART) protocol, e.g., it could be used to securely send/receive arbitrary JSON-packed data to/from server or smartphone.

According to the proposed platform and the above described protocols, we developed an urban monitoring system prototype based on ESP8266. Our nodes are currently equipped with the following sensors: CO_2, radiation, and noise level. The deployment took place in Novosibirsk's satellite city Koltsovo, Russia, and currently consists of seven monitoring devices. A photo of the deployed system is given in Figure 8. The complete device fulfills the requirements of IP 65. More technical details on the developed system are given in Table 3. In this project, we equipped our sensor nodes with three potential energy sources: (i) battery; (ii) solar panel; and (iii) wired power supply. The selection was made according to the need for autonomous operation and resistance to potential blackouts. Overall, the placement of the nodes on the lighting poles provides access not only to the powerline but allows for the utilization of energy harvesting technologies [68,69] that may be added to our project in the future.

Table 3. Main components of the node.

Component	Type	Description
Atmel ATmega328P	Data processing and control	Micro-controller is dedicated to the system operation, which holds the functionality of the data processing unit (DPU) and control unit (CU) [64].
Data Processing Unit	Data processing and control	DPU is implemented in ATmega328P and performs the functions of preprocessing information received from sensors for secure and reliable transmission to the server unit. Data pre-processing is carried out in accordance with the previously developed and used Galouis platform.
Control Unit	Data processing and control	CU is implemented in ATmega328P and ensures the operation of the radio module and the DPU, determining their operation in various modes in accordance with the Galois platform used. Besides, CU regulates the mode of operation of the sensors, ensuring efficient energy consumption in the respective modes of the system (simplex, half-duplex, and full-duplex), and also allows the interaction through the radio module with the mobile device during the initialization of the sensor and the end of its operation.
ESP8266 radio module	Communications	Provides data transfer via IEEE 802.11n protocol [65]. The radio module receives data from DPU according to the control commands from the CU and transfers it to the networking part of the system or the nearest sensor located in its communications range. Note, in the duplex mode of operation, the radio module relays the data received from the sensors located in its coverage area according to the commands received from the control unit.
Power Control Unit (PCU)	Power supply	Provides safe switching between available power sources in order to realize the uninterrupted power supply of the sensor, regardless of weather conditions and the state of available power sources. As a baseline element, the system utilizes the SII-8205A board [70].
Battery	Power supply	Li-ion, 6800 mAh, 3.7 V.
Solar panel	Power supply	45 W, 12 V (optional).
Power source	Power supply	12 V, 2 A (optional).

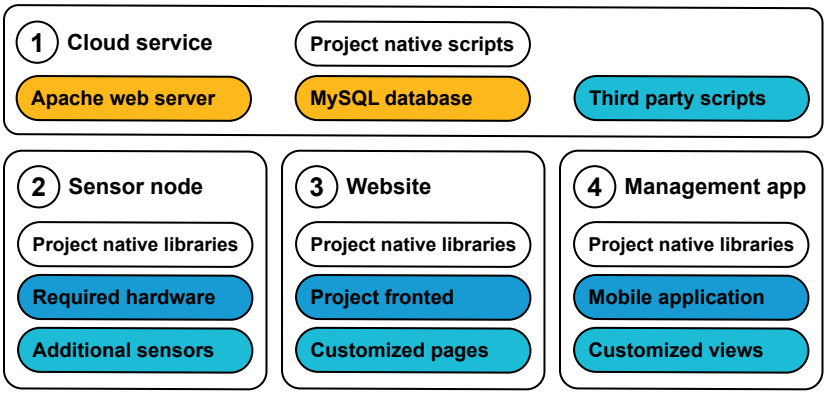
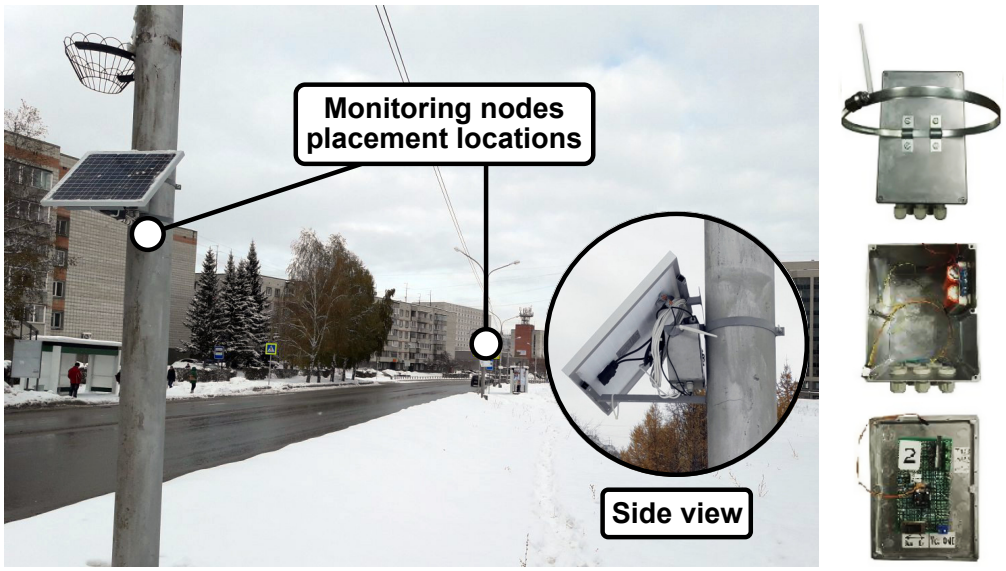


Figure 7. Main system components.



(a) Photo of the deployed prototype.

(b) Completed sensor box.

Figure 8. Trial-related photos.

For ease of use, we developed a custom monitoring data representation. The visualization side is a software module written in Hypertext Preprocessor (PHP) that generates a Hypertext Markup Language (HTML) views. Each view provides the user with an intuitive representation of the monitoring data received from the database after required Cloud processing. The information on the HTML page is updated via asynchronous requests. Measurements visualization, represented by the corresponding graphs, is carried out using the FlotJS library [71]. A sensor location map is generated using Yandex Maps API 2.0 [72], and the information about the location of each sensor is determined based on its initial placement.

The system is composed of two modules responsible for: (i) data analysis; and (ii) CU. The CU allows to modify the operating mode of each node (simplex, half-duplex, and duplex) remotely and provides the legal user with a mobile application for initializing sensors.

The overview of the user Dashboard view is given in Figure 9. The dashboard is a web page visually divided into three parts. At the top is a map with markers indicating the location of available sensors. A list of sensors is located on the left side, and on the right is the data area of the selected sensor. The selection of the sensor could be made either with the map or the list.

After the selection, the panel shows each sensor's location along with the monitored environmental data visualized in the plot. The axes are scaled automatically according to the data

received. The representation could be changed based on the control buttons located below the plot. For example, there is a possibility for scrolling the graph to overview previous results, selection of the displayed data range, and control of the measuring interval of the sensor in half-duplex mode. From the developed authentication methodology perspective, we tested all the cases listed in Section 4 during the deployment successfully.

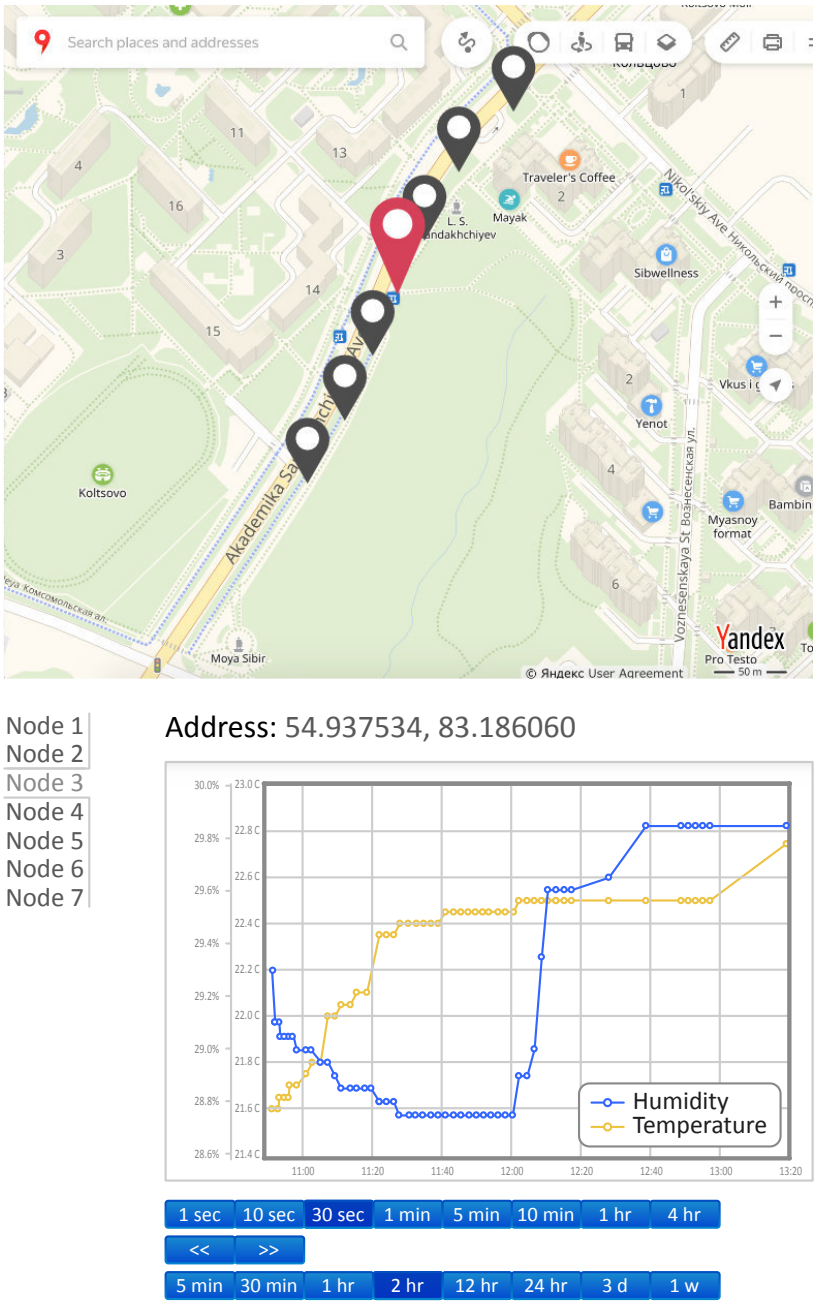


Figure 9. Application interface: Collected humidity and temperature view.

7. Conclusions

Climate change brings the problem of environmental monitoring to an entirely new level, especially for urban scenarios. In particular, the leading cause of indoor air pollution is inefficient fuel combustion from rudimentary technologies used for cooking, heating, and lighting in addition to complex traffic conditions in metropolitans. All of the above require practical and flexible enablers for monitoring the emission levels, temperature, and other factors affecting citizens' lives.

In this work, we first discussed a pairwise key-based authentication methodology followed by the prototype of the secure urban environmental monitoring system and the executed field trial. Despite conventional sensor network goals, the system allows protecting a sensor network from unauthorized topology changes, keeping the properties of scalability and security from a communications perspective. The platform was developed to enable efficient and fast network initialization, received information processing, and handling potential topology changes. The use of mutual authentication protocol, together with our platform, allowed us to build an efficient, safe, and easily scalable sensor network to collect and process environmental information. The expertise collected during this system prototyping would be further used for the DLT design principles formulation.

Concluding, the developed system received positive feedback from the customer (DELL) and the research community during the IoT Summit Siberia, where the solution was presented to the broad public. The mayor of the city also provided his vision on how to further utilize the system for environmental and Smart City purposes. The developed system could also be efficiently utilized in farm and suburban scenarios where the connectivity to the gateway access point is relatively close to any segment of the mesh network.

Author Contributions: Conceptualization, S.B., N.V., and P.M.; methodology, S.B. and A.O.; software, A.O.; validation, A.O., N.V., P.M., and M.K.; formal analysis, A.O. and M.K; investigation, P.M.; resources, S.B.; writing—original draft preparation, A.O., and S.B.; writing—review and editing, A.O. and P.M.; visualization, A.O.; supervision, S.B. and A.O.; project administration, A.O.; and funding acquisition, S.B., P.M., and M.K.

Funding: The described research was supported by the National Sustainability Program under grant LO1401. For the research, the infrastructure of the SIX Center was used. Research was supported by the Russian Science Foundation (Project No. 19-41-06301). It was also supported by the Academy of Finland (project #313039—PRISMA). The prototype of the developed secure environmental monitoring IoT system was successfully approved as part of active Smart City programs in Saint-Petersburg and Koltsovo. This article was prepared with the financial support of the Ministry of Science and Higher Education of the Russian Federation under the agreement No. 075-15-2019-1707 from 22 November 2019 (identifier RFMEFI60519X0189, internal number 05.605.21.0189).

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AP	Access Point
API	Application Programming Interface
CPS	Cyber-Physical System
CU	Control Unit
DPU	Data Processing Unit
GIS	Geographical Information Systems
GUI	Graphical User Interface
HTML	Hypertext Markup Language
ID	Identifier
IEEE	Institute of Electrical and Electronics Engineers
IIoT	Industrial Internet of Things
IoT	Internet of Things
IP (Code)	International Protection Marking
JSON	JavaScript Object Notation
LEAP	Lightweight Extensible Authentication Protocol
M2M	Machine-to-Machine Communications
MK	Master Key
NASA	The National Aeronautics and Space Administration
NFC	Near Field Communications
PCU	Power Control Unit
PHP	Hypertext Preprocessor
PKI	Public Key Infrastructure
REST	Representational State Transfer
RFID	Radio-frequency Identification
SQL	Structured Query Language
UART	Universal Asynchronous Receiver/Transmitter

UWB	Ultra-wideband Radio Technology
WiFi	Wireless Fidelity
WSN	Wireless Sensor Network

References

1. NASA's Jet Propulsion Laboratory. Facts | The Effects of Climate Change. 2019. Available online: https://climate.nasa.gov/effects/ (accessed on 14 December 2019).
2. Pritchard, H.; Ligtenberg, S.; Fricker, H.; Vaughan, D.; Van den Broeke, M.; Padman, L. Antarctic ice-sheet loss driven by basal melting of ice shelves. *Nature* **2012**, *484*, 502. [CrossRef] [PubMed]
3. Kim, H.Y.; Park, S.Y.; Yoo, S.H. Public acceptability of introducing a biogas mandate in Korea: A contingent valuation study. *Sustainability* **2016**, *8*, 1087. [CrossRef]
4. European Commission. Causes of Climate Change. 2019. Available online: https://ec.europa.eu/clima/change/causes_en (accessed on 14 December 2019).
5. Zhu, C.; Rodrigues, J.J.; Leung, V.C.; Shu, L.; Yang, L.T. Trust-based Communication for the Industrial Internet of Things. *IEEE Commun. Mag.* **2018**, *56*, 16–22. [CrossRef]
6. Mozny, R.; Masek, P.; Stusek, M.; Zeman, K.; Ometov, A.; Hosek, J. On the Performance of Narrow-band Internet of Things (NB-IoT) for Delay-tolerant Services. In Proceedings of the 42nd International Conference on Telecommunications and Signal Processing (TSP), Budapest, Hungary, 1–3 July 2019; pp. 637–642.
7. Hosek, J.; Masek, P.; Andreev, S.; Galinina, O.; Ometov, A.; Kropfl, F.; Wiedermann, W.; Koucheryavy, Y. A SyMPHOnY of integrated IoT businesses: Closing the gap between availability and adoption. *IEEE Commun. Mag.* **2017**, *55*, 156–164. [CrossRef]
8. Lee, H.C.; Ke, K.H. Monitoring of large-area IoT sensors using a LoRa wireless mesh network system: Design and evaluation. *IEEE Trans. Instrum. Meas.* **2018**, *67*, 2177–2187. [CrossRef]
9. Ometov, A.; Daneshfar, N.; Hazmi, A.; Andreev, S.; Carpio, L.F.D.; Amin, P.; Torsner, J.; Koucheryavy, Y.; Valkama, M. System-level Analysis of IEEE 802.11ah Technology for Unsaturated MTC Traffic. *Int. J. Sens. Netw.* **2018**, *26*, 269–282. [CrossRef]
10. Sisinni, E.; Saifullah, A.; Han, S.; Jennehag, U.; Gidlund, M. Industrial Internet of Things: Challenges, Opportunities, and Directions. *IEEE Trans. Ind. Inform.* **2018**, *14*, 4724–4734. [CrossRef]
11. Masek, P.; Hudec, D.; Krejci, J.; Ometov, A.; Hosek, J.; Samouylov, K. Communication Capabilities of Wireless M-BUS: Remote Metering Within SmartGrid Infrastructure. In *International Conference on Distributed Computer and Communication Networks*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 31–42.
12. Talavera, J.M.; Tobón, L.E.; Gómez, J.A.; Culman, M.A.; Aranda, J.M.; Parra, D.T.; Quiroz, L.A.; Hoyos, A.; Garreta, L.E. Review of IoT Applications in Agro-industrial and Environmental Fields. *Comput. Electron. Agric.* **2017**, *142*, 283–297. [CrossRef]
13. Sadeghi, A.R.; Wachsmann, C.; Waidner, M. Security and Privacy Challenges in Industrial Internet of Things. In Proceedings of the 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), San Francisco, CA, USA, 8–12 June 2015; pp. 1–6.
14. Frustaci, M.; Pace, P.; Aloi, G.; Fortino, G. Evaluating Critical Security Issues of the IoT World: Present and Future Challenges. *IEEE Internet Things J.* **2018**, *5*, 2483–2495. [CrossRef]
15. Ullah, I.; Ul Amin, N.; Zareei, M.; Zeb, A.; Khattak, H.; Khan, A.; Goudarzi, S. A Lightweight and Provable Secured Certificateless Signcryption Approach for Crowdsourced IIoT Applications. *Symmetry* **2019**, *11*, 1386. [CrossRef]
16. Nesteruk, S.; Bezzateev, S. Location-Based Protocol for the Pairwise Authentication in the Networks without Infrastructure. In Proceedings of the 22nd Conference of Open Innovations Association (FRUCT), Jyvaskyla, Finland, 15–18 May 2018; pp. 190–197.
17. Kannengießer, N.; Lins, S.; Dehling, T.; Sunyaev, A. What Does Not Fit Can be Made to Fit! Trade-Offs in Distributed Ledger Technology Designs. *Trade-Offs Distrib. Ledger Technol. Des.* **2019**. [CrossRef]
18. Lamberti, R.; Fries, C.; Lücking, M.; Manke, R.; Kannengießer, N.; Sturm, B.; Komarov, M.M.; Stork, W.; Sunyaev, A. An Open Multimodal Mobility Platform Based on Distributed Ledger Technology. In *Internet of Things, Smart Spaces, and Next Generation Networks and Systems*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 41–52.
19. Vermesan, O.; Friess, P. *Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems*; River Publishers: Aalborg, Denmark, 2013.

20. Masek, P.; Masek, J.; Frantik, P.; Fujdiak, R.; Ometov, A.; Hosek, J.; Andreev, S.; Mlynek, P.; Misurec, J. A Harmonized Perspective on Transportation Management in Smart Cities: The Novel IoT-drive Eenvironment for Road Traffic Modeling. *Sensors* **2016**, *16*, 1872. [CrossRef] [PubMed]
21. Balageas, D.; Fritzen, C.P.; Güemes, A. *Structural Health Monitoring*; John Wiley & Sons: Hoboken, NJ, USA, 2010; Volume 90.
22. Pun, C.S.J.; So, C.W.; Leung, W.Y.; Wong, C.F. Contributions of artificial lighting sources on light pollution in Hong Kong measured through a night sky brightness monitoring network. *J. Quant. Spectrosc. Radiat. Transf.* **2014**, *139*, 90–108. [CrossRef]
23. Hannan, M.; Arebey, M.; Begum, R.A.; Basri, H. Radio Frequency Identification (RFID) and communication technologies for solid waste bin and truck monitoring system. *Waste Manag.* **2011**, *31*, 2406–2413. [CrossRef] [PubMed]
24. Segura-Garcia, J.; Felici-Castell, S.; Perez-Solano, J.J.; Cobos, M.; Navarro, J.M. Low-cost alternatives for urban noise nuisance monitoring using wireless sensor networks. *IEEE Sens. J.* **2014**, *15*, 836–844. [CrossRef]
25. Shaban, K.B.; Kadri, A.; Rezk, E. Urban air pollution monitoring system with forecasting models. *IEEE Sens. J.* **2016**, *16*, 2598–2606. [CrossRef]
26. Wang, S.; Wan, J.; Li, D.; Zhang, C. Implementing Smart Factory of Industrie 4.0: An Outlook. *Int. J. Distrib. Sens. Netw.* **2016**, *12*, 3159805. [CrossRef]
27. Karami, M.; McMorrow, G.V.; Wang, L. Continuous monitoring of indoor environmental quality using an Arduino-based data acquisition system. *J. Build. Eng.* **2018**, *19*, 412–419. [CrossRef]
28. Risteska Stojkoska, B.; Popovska Avramova, A.; Chatzimisios, P. Application of wireless sensor networks for indoor temperature regulation. *Int. J. Distrib. Sens. Netw.* **2014**, *10*, 502419. [CrossRef]
29. Cao, T.; Thompson, J.E. Personal monitoring of ozone exposure: A fully portable device for under $150 USD cost. *Sens. Actuators B Chem.* **2016**, *224*, 936–943. [CrossRef]
30. Lohan, E.; Torres-Sospedra, J.; Leppäkoski, H.; Richter, P.; Peng, Z.; Huerta, J. Wi-Fi crowdsourced fingerprinting dataset for indoor positioning. *Data* **2017**, *2*, 32. [CrossRef]
31. Krivtsova, I.; Lebedev, I.; Sukhoparov, M.; Bazhayev, N.; Zikratov, I.; Ometov, A.; Andreev, S.; Masek, P.; Fujdiak, R.; Hosek, J. Implementing a Broadcast Storm Attack on a Mission-critical Wireless Sensor Network. In *Wired/Wireless Internet Communications*; Springer: Berlin/Heidelberg, Germany, 2016; pp. 297–308.
32. Felemban, E. Advanced border intrusion detection and surveillance using wireless sensor network technology. *Int. J. Commun. Netw. Syst. Sci.* **2013**, *6*, 251. [CrossRef]
33. Santos, A.; Younis, M. A sensor network for non-intrusive and efficient leak detection in long pipelines. In Proceedings of the IFIP Wireless Days (WD), Niagara Falls, ON, Canada, 10–12 October 2011; pp. 1–6.
34. Makeenkov, A.; Lapitskiy, I.; Somov, A.; Baranov, A. Flammable gases and vapors of flammable liquids: Monitoring with infrared sensor node. *Sens. Actuators B Chem.* **2015**, *209*, 1102–1107. [CrossRef]
35. Gomaa, R.; Adly, I.; Sharshar, K.; Safwat, A.; Ragai, H. ZigBee wireless sensor network for radiation monitoring at nuclear facilities. In Proceedings of the 6th Joint IFIP Wireless and Mobile Networking Conference (WMNC), Dubai, United Arab Emirates, 23–25 April 2013; pp. 1–4.
36. Henriques, V.; Malekian, R. Mine safety system using wireless sensor network. *IEEE Access* **2016**, *4*, 3511–3521. [CrossRef]
37. Dlodlo, N.; Kalezhi, J. The Internet of Things in Agriculture for Sustainable Rural Development. In Proceedings of the International Conference on Emerging Trends in Networks and Computer Communications (ETNCC), Windhoek, Namibia, 17–20 May 2015; pp. 13–18.
38. Aziz, N.A.A.; Aziz, K.A. Managing disaster with wireless sensor networks. In Proceedings of the 13th International Conference on Advanced Communication Technology (ICACT2011), Seoul, Korea, 13–16 February 2011; pp. 202–207.
39. Faulkner, M.; Olson, M.; Chandy, R.; Krause, J.; Chandy, K.M.; Krause, A. The next big one: Detecting earthquakes and other rare events from community-based sensors. In Proceedings of the 10th ACM/IEEE International Conference on Information Processing in Sensor Networks, Chicago, IL, USA, 12–14 April 2011; pp. 13–24.
40. Aslan, Y.E.; Korpeoglu, I.; Ulusoy, Ö. A framework for use of wireless sensor networks in forest fire detection and monitoring. *Comput. Environ. Urban Syst.* **2012**, *36*, 614–625. [CrossRef]
41. Aqeel-ur-Rehma; Abbasi, A.Z.; Islam, N.; Shaikh, Z.A. A review of wireless sensors and networks' applications in agriculture. *Comput. Stand. Interfaces* **2014**, *36*, 263–270. [CrossRef]

42. Chaudhary, D.; Nayse, S.; Waghmare, L. Application of wireless sensor networks for greenhouse parameter control in precision agriculture. *Int. J. Wirel. Mob. Netw.* **2011**, *3*, 140–149. [CrossRef]
43. Muller, C.L.; Chapman, L.; Grimmond, C.; Young, D.T.; Cai, X.M. Toward a standardized metadata protocol for urban meteorological networks. *Bull. Am. Meteorol. Soc.* **2013**, *94*, 1161–1185. [CrossRef]
44. Kim, S.H.; Kim, D.H.; Park, H.D. Animal situation tracking service using RFID, GPS, and sensors. In Proceedings of the Second International Conference on Computer and Network Technology, Bangkok, Thailand, 23–25 April 2010; pp. 153–156.
45. Medela, A.; Cendón, B.; González, L.; Crespo, R.; Nevares, I. IoT multiplatform networking to monitor and control wineries and vineyards. In Proceedings of the Future Network & Mobile Summit, Lisboa, Portugal, 3–5 July 2013; pp. 1–10.
46. Hwang, J.; Yoe, H. Study of the ubiquitous hog farm system using wireless sensor networks for environmental monitoring and facilities control. *Sensors* **2010**, *10*, 10752–10777. [CrossRef]
47. Casas, O.; López, M.; Quílez, M.; Martinez-Farre, X.; Hornero, G.; Rovira, C.; Pinilla, M.R.; Ramos, P.M.; Borges, B.; Marques, H.; et al. Wireless sensor network for smart composting monitoring and control. *Measurement* **2014**, *47*, 483–495. [CrossRef]
48. Singh, M.; Rajan, M.; Shivraj, V.; Balamuralidhar, P. Secure MQTT for Internet of Things (IoT). In Proceedings of the Fifth International Conference on Communication Systems and Network Technologies, Gwalior, India, 4–6 April 2015; pp. 746–751.
49. Zakaria, O.M.; Hashim, A.H.A.; Hassan, W.H.; Khalifa, O.O.; Azram, M.; Goudarzi, S.; Jivanadham, L.B.; Zareei, M. State-Aware Re-configuration Model for Multi-Radio Wireless Mesh Networks. *KSII Trans. Internet Inf. Syst.* **2017**, *11*. [CrossRef]
50. Ahmed, A.; Bakar, K.A.; Channa, M.I.; Haseeb, K.; Khan, A.W. A survey on trust based detection and isolation of malicious nodes in ad-hoc and sensor networks. *Front. Comput. Sci.* **2015**, *9*, 280–296. [CrossRef]
51. Pathan, A.S.K. *Security of Self-Organizing Networks: MANET, WSN, WMN, VANET*; CRC Press: Boca Raton, FL, USA, 2016.
52. Ometov, A.; Zhidanov, K.; Bezzateev, S.; Florea, R.; Andreev, S.; Koucheryavy, Y. Securing Network-Assisted Direct Communication: The Case of Unreliable Cellular Connectivity. In Proceedings of the IEEE 14th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Helsinki, Finland, 20–22 August 2015.
53. Lee, J.; Stinson, D.R. Deterministic Key Predistribution Schemes for Distributed Sensor Networks. In *International Workshop on Selected Areas in Cryptography*; Springer: Berlin/Heidelberg, Germany, 2004; pp. 294–307.
54. Zhu, S.; Setia, S.; Jajodia, S. LEAP+: Efficient Security Mechanisms for Large-scale Distributed Sensor Networks. *ACM Trans. Sens. Netw. (TOSN)* **2006**, *2*, 500–528. [CrossRef]
55. Jang, J.; Kwon, T.; Song, J. A Time-based Key Management Protocol for Wireless Sensor Networks. In *International Conference on Information Security Practice and Experience*; Springer: Berlin/Heidelberg, Germany, 2007; pp. 314–328.
56. Zhang, W.; Tran, M.; Zhu, S.; Cao, G. A Random Perturbation-based Scheme for Pairwise Key Establishment in Sensor Networks. In Proceedings of the 8th ACM International Symposium on Mobile Ad Hoc Networking and Computing, Montreal, QC, Canada, 9–14 September 2007; pp. 90–99.
57. Lohan, E.S.; Koivisto, M.; Galinina, O.; Andreev, S.; Tolli, A.; Destino, G.; Costa, M.; Leppanen, K.; Koucheryavy, Y.; Valkama, M. Benefits of Positioning-Aided Communication Technology in High-Frequency Industrial IoT. *IEEE Commun. Mag.* **2018**, *56*, 142–148. [CrossRef]
58. Nesteruk, S.; Kovalenko, V.; Bezzateev, S. A Survey on Localized Authentication Protocols for Wireless Sensor Networks. In Proceedings of the Wave Electronics and its Application in Information and Telecommunication Systems (WECONF), St. Petersburg, Russia, 26–30 November 2018; pp. 1–7.
59. Furth, P.G.; Rahbee, A.B. Optimal bus stop spacing through dynamic programming and geographic modeling. *Transp. Res. Rec.* **2000**, *1731*, 15–22. [CrossRef]
60. Traverso, M.; Donatello, S.; Moons, H.; Rodriguez, R.; Quintero, M.G.C.; JRC, Wolf, O.; Van Tichelen, P.; Van, V.; Hoof, T.G.V. *Revision of the EU Green Public Procurement Criteria for Street Lighting and Traffic Signals*; Publications Office of the European Union: Luxembourg, 2017.
61. Jelicic, V.; Magno, M.; Brunelli, D.; Paci, G.; Benini, L. Context-adaptive multimodal wireless sensor network for energy-efficient gas monitoring. *IEEE Sens. J.* **2012**, *13*, 328–338. [CrossRef]

62. Coleri, S.; Cheung, S.Y.; Varaiya, P. Sensor networks for monitoring traffic. In Proceedings of the Allerton Conference on Communication, Control and Computing, Monticello, IL, USA, 29 September–1 October 2004; pp. 32–40.
63. Devos, M.; Ometov, A.; Mäkitalo, N.; Aaltonen, T.; Andreev, S.; Koucheryavy, Y. D2D communications for mobile devices: Technology overview and prototype implementation. In Proceedings of the 8th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), Lisbon, Portugal, 18–20 October 2016; pp. 124–129.
64. Atmel. ATmega328P–8-bit AVR Microcontroller with 32K Bytes In-System Programmable Flash. 2019. Available online: http://ww1.microchip.com/downloads/en/DeviceDoc/Atmel-7810-Automotive-Microcontrollers-ATmega328P_Datasheet.pdf (accessed on 14 December 2019).
65. ESPRESSIF. ESP8266—Low-Power, Highly-Integrated Wi-Fi Solution. 2019. Available online: https://www.espressif.com/en/products/hardware/esp8266ex/overview (accessed on 14 December 2019).
66. Citrix. Resurrecting Duckling: A Model for Securing IoT Devices. 2019. Available online: https://www.citrix.com/blogs/2015/04/20/resurrecting-duckling-a-model-for-securing-iot-devices/ (accessed on 14 December 2019).
67. Krentz, K.F.; Wunder, G. 6DOKU: Towards Secure Over-the-Air Preloading of 6LOWPAN Nodes Using PHY Key Generation. In Proceedings of the European Conference on Smart Objects, Systems and Technologies, Aachen, Germany, 16–17 July 2015; pp. 1–11.
68. Zareei, M.; Vargas-Rosales, C.; Anisi, M.H.; Musavian, L.; Villalpando-Hernandez, R.; Goudarzi, S.; Mohamed, E.M. Enhancing the Performance of Energy Harvesting Sensor Networks for Environmental Monitoring Applications. *Energies* **2019**, *12*, 2794. [CrossRef]
69. Galinina, O.; Turlikov, A.; Hosek, J.; Andreev, S. Energy efficient power allocation in a multi-radio mobile device with wireless energy harvesting. In Proceedings of the 6th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), St. Petersburg, Russia, 6–8 October 2014; pp. 380–385.
70. Albic. S-8205A/B Series: Battery Protection IC for 4-Series or 5-Series Cell Pack. 2019. Available online: https://www.ablic.com/en/doc/datasheet/battery_protection/S8205A_B_E.pdf (accessed on 14 December 2019).
71. IOLA and Ole Laursen. Attractive JavaScript Plotting for jQuery. 2014. Available online: https://www.flotcharts.org (accessed on 14 December 2019).
72. Yandex. Maps API–JavaScript API. 2019. Available online: https://tech.yandex.com/maps/jsapi/ (accessed on 14 December 2019).