Secure environmental monitoring for industrial internet of things

Secure Environmental Monitoring for Industrial Internet of Things: from Framework to Live Implementation

Sergey Bezzateev[1], Natalia Voloshina[2], Konstantin Zhidanov[1], Aleksandr Ometov[3]

[1]SUAI University, St. Petersburg, Russia
[2]ITMO University, St. Petersburg, Russia
[3]Tampere University, Tampere, Finland
Email: aleksandr.ometov@tuni.fi

***Abstract*—Worldwide changes in climate and increasing pollution level are tremendously affecting the need for environmental monitoring solutions. Recent activities in wireless sensor networks (WSNs) together with Cloud computing paradigm brought an entirely new perspective on monitoring as part of the Industrial Internet of Things (IIoT). However, most of the systems developed today are still facing lack of flexibility and security. This work presents the results of prototyping the IIoT wireless environmental monitoring system from both hardware and software sides. The developed mechanisms enable connectivity in infrastructure and mesh-like modes, where each sensor could act as relay allowing for improved node-failure resistance and scalability. Next, the authentication mechanism is proposed to enable transparent migration of any node between different network segments while keeping the overall operation secure. Finally, proof of the concept prototype deployment in real-life conditions shows the potential of metropolitan-scale utilization of the developed system.**

***Index Terms*—prototype, environmental monitoring, IIoT, authentication, security, sensor network**

I. Introduction

After broad adoption of the Internet of Things (IoT), growing interest from industry, researchers, governments and developers were given to IoT's particular niche – Industrial IoT (IIoT) [1], which aims at covering the machine-to-machine comms (M2M) domain as a significant part of the Smart City concept [2].

IIoT provides a number of main machine-oriented development directions, including factory automation, mission-critical communications, and, generally, monitoring [3]. Historically, monitoring solutions are well-known from wireless sensor networks (WSNs) and the world of today could not be imagined ignoring this section of IIoT [4]. In this context, environmental and agricultural monitoring fields are ideal candidates for trialing and deploying the IIoT solutions [5]. The use of sensors may be vastly applicable for it, e.g., for production chain control; monitoring of humidity, emissions and temperature levels; for air pollution maps construction; for immediate alert triggers; and others.

978-1-7281-2445-2/19/$31.00 ©2019 IEEE

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 [6]. At the same time, blind development of said systems may be still harmful from the information security perspective, and threats (especially related to authentication) should be carefully taken into consideration [7].

In this paper, we propose and develop the CPS system titled 'Galouis', which is a flexible tool for the environmental monitoring nodes management. The developed system is also supplemented with specifically designed authentication mechanisms allowing to handle individual cases of such network monitoring, e.g., the addition of new nodes, (un-)authorized migration of the node from one network segment to another, etc. Dell-EMC carefully managed this work and supported the deployment in the metropolitan area.

The paper is structured as follows. Section II provides an overview of the main environmental applications and related security aspects. Next, Section III outlines the main network specifics and solutions enabling secure operation of said system. Section IV details the developed framework and executed trial. The last section presents the conclusions and future work of this study.

II. Environmental monitoring security aspects and main applications

Focusing mainly on Smart City paradigm from the IIoT perspective, the main activities of the environmental monitoring could be listed as following [8]. The first group of applications is related to the paradigm of *urban environmental monitoring* [9]. It consists of the following subgroups: (i) structural health; (ii) smart lightning; (iii) waste management; and (iv) air pollution.

A massive section of this group is related to *Industrial control* [10] aiming at: (i) indoor air quality; (ii) temperature monitoring; (iii) ozone presence; and (iv) indoor positioning. Nonetheless, security and emergency scenarios are also to be considered [11] as, for example, (i) perimeter access control; (ii) liquid presence; (iii) radiation levels; and (iv) explosive and hazardous gases in mines.

The second big group is related to *Rural environmental monitoring* [12]: (i) landslide and avalanche prevention; (ii) earthquake early detection; and (iii) forest fire detection. A standalone section within rural monitoring is dedicated to *Agricultural monitoring* covering the following applications: (i) greenhouses; (ii) meteorological station network; (iii) animal tracking; (iv) wine quality enhancing; and (v) monitoring of toxic gas level.

Important to notice that the entire deployment predictivity of the IIoT sensor network is somewhat challenging due to 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. Evidently, 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 lack of centralized authority coordination. Such center should provide storage, generation and dissemination of the certificates to each sensor node operating within public key infrastructure (PKI) paradigm [13]. 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 to have just a single authentication center, a great 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.

III. Security and Scalability for Environmental Monitoring Sensor Networks

Today, many critical issues of security in the transmission and processing of data are present in managing dynamic sensor networks with variable topology. In particular, a critical problem here is to provide a secure device 'arrival' to the existing network since reconfiguration in a centralized manner may be challenging. In situations when trusted authority is unavailable (for example, due to connectivity issues), the operation of mutual network device authentication becomes much more complicated [14].

This section is mainly focused on possible solutions for such 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 the network components classified to only two groups, as shown in Fig. 1:

- Gateway or access point (AP) is used for the end-node data aggregation. Here, APs could also perform edge preprocessing of the incoming sensor data before the cloud delivery.
- Monitoring nodes are equipped with different sensing devices with the primary goal of collecting specified environmental parameters, e.g., temperature, humidity, noise level, etc. It could either directly connect to the AP or relay the data through the neighboring nodes to the AP in the ad hoc-like way.

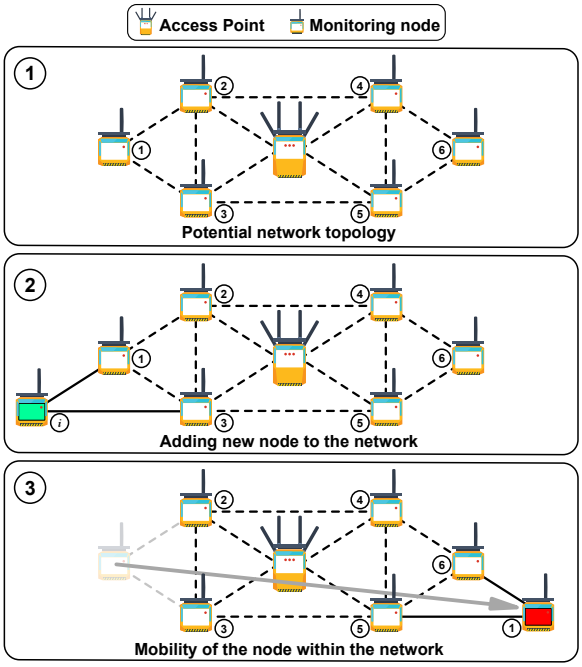


Fig. 1. Monitoring systems operational states

The system operation could be divided into the following operational phases.

1) **Sensor initialization**, e.g., a phase when a new node should be connected to any available node or AP in range, see Fig. 1 case (2). 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 case, sensors are neither added nor excluded from existing topology, and their logical position is static with respect to their neighbor nodes, see Fig. 1 case (1).
3) **Sensor removal.** In this case, two possible scenarios may be present, see Fig. 1 case (3):

- Removed sensor is excluded from a particular secure network and could be used in the future only through new node initialization procedure;
- Removed sensor will be migrated to another segment of an existing network without reinitialization.

Looking more precisely at each of the mentioned scenarios, we decide to use the master key of sensor network [15], [16] 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 sensor mutual authentication, we use LEAP-like protocol [17]. 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) Master key that was used on the initialization step is not removed and is kept in so-called tamper resistance memory of the node [18]. This approach allows 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 Fig. 1 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 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 [19]). In this case, we should utilize 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) Master key that was used on the step of initialization is destroyed after predefined time calculated from the moment when initialization step was completed [17]. 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 to obtain 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 more preferred in real-life dynamics of urban monitoring purposes. This protocol could be described as following.

A. 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 Fig. 1 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 master key MK to calculate pair-wise keys for mutual authentication. For example, sensor 1 calculates pair keys for sensors 2 and 3:

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

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

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

- In order to provide the scalability, each sensor also calculates auxiliary key $K_{i,i} = H(ID_1||MK)$ 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 the Fig. 1 case (2) would have same information $\{K_{1,1}, K_{1,2}, K_{1,3}\}$ after the end of the initialization phase.

B. Stable sensor network operation

During 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.

C. Adding new sensor to existing secure sensor network

According to Fig. 1 case (2), new sensor with ID_i appears in the range of sensors 1 and 2 of the existing network.

New i^{th} 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 $K_{i,2} = H(ID_2||MK) = K_{2,2}$ in order 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, i^{th} 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, new added node will store the key sequence $\{K_{i,i}, K_{i,1}, K_{i,2}\}$ after the initialization process, as shown in Fig. 1 case (3).

D. Illegal sensor moving to another secure sensor network segment of existing network

In case of illegal sensor movement, e.g., without rewriting of its master key MK, see Fig. 1 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 new segment due to unique properties of the pairwise keys. This property of the authentication protocol decreases the probability of receiving incorrect data when the location of the node changes illegally.

IV. Testing in real scenario

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 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[1] equipped with wireless ESP8266 module[2] (we planned to utilize IEEE 802.11ah [20] for connectivity, but faced no luck finding any market-available radio modules). The main 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, DB access scripts); (v) Database (MySQL).

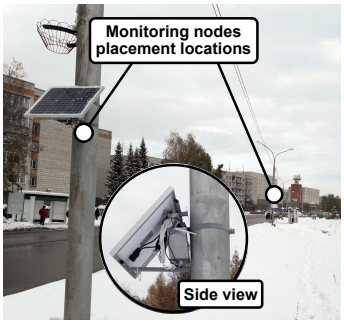
The primary goal of the platform was to handle issues related to security, connectivity, and access management while the developer only needs to design the device and customize the data processing. In particular, the platform is designed to be transparent for developers to perform the following actions: (i) initialization ('duckling') of the devices[3] by using any available wireless technology of the user smartphone, i.e., Bluetooth, WiFi, or NFC [21]; (ii) access sharing; (iii) routing between devices; (iv) remote access; (v) 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:

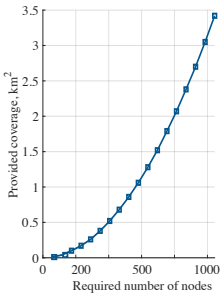
- Register in the cloud and generate its encryption key. In this case, the generated encryption key is stored only on the user smartphone but could be sent to the cloud;
- Perform node initialization;
- Interact with already initialized devices directly when they are in the communication range of the selected wireless technology;
- Specify access credentials of known APs and distribute those to all related devices;
- Interact with the devices via the infrastructure network. In this case, all transferred data is protected with end-to-end encryption between the smartphone and the node.

When initialized, ESP8266 can be accessed by UART, 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 described above protocols, we have 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 and currently consists of 7 monitoring devices, a photo of the deployed system is given in Fig. 2. The complete device fulfills the requirements of IP65.



(a) Photo of the deployed prototype.



(b) Estimate on the network coverage.

Fig. 2. Trial-related photos and planning estimate.

The usage of routing- and secure pairwise authentication protocols for legal network sensors 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 situation of IIoT of, for example, farm monitoring, there is a task to evaluate the required density of relatively cheap (compared to AP price) sensors concerning covered area. The tentative results are given in Fig. 2(b). Interestingly, that only the gateway node, highlighted in Fig. 3, together with two neighboring nodes were reachable by the infrastructure gateway. The rest of the nodes were communication with them in an ad hoc way in order to deliver their measurements to the cloud. In case the gateway becomes unreachable, the nodes initialize the procedure of looking for another known one obtained during the initialization.

Generally, the developed system received positive feedback from the customer (DELL) and the research community during the IoT Summit Siberia, where the solution was presented live. Mayor of the city also provided his vision on how to further utilize the system for environmental and Smart City purposes. Currently, we also plan to deploy the nodes indoor covering for factory automation scenario.

[1]See "ATmega328P – 8-bit AVR Microcontroller with 32K Bytes In-System Programmable Flash", by Atmel [Accessed 01.04.2019]: http://ww1.microchip.com/downloads/en/DeviceDoc/Atmel-7810-Automotive-Microcontrollers-ATmega328P_Datasheet.pdf

[2]See "ESP8266 – Low-power, highly-integrated Wi-Fi solution" by ESPRESSIF [Accessed 01.04.2019]: https://www.espressif.com/en/products/hardware/esp8266ex/overview

[3]See "Resurrecting Duckling: A Model for Securing IoT Devices" by Citrix [Accessed 01.04.2019]: https://www.citrix.com/blogs/2015/04/20/resurrecting-duckling-a-model-for-securing-iot-devices/

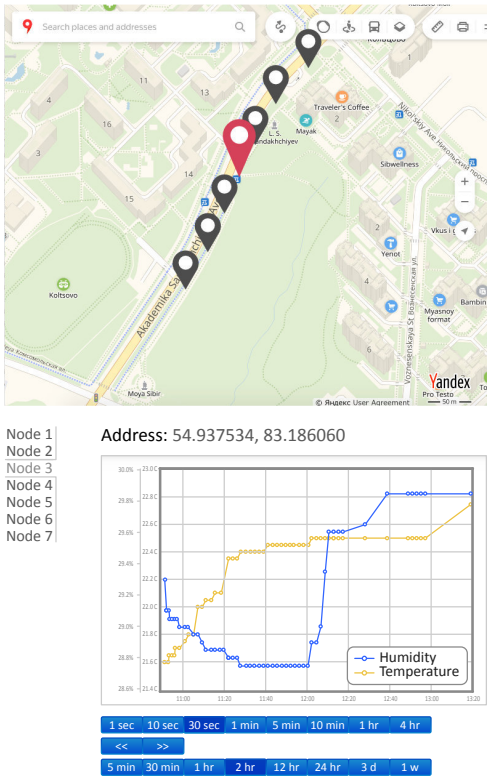


Fig. 3. Application interface example.

V. Conclusion

In this work, we have developed a prototype of the urban environmental monitoring system and executed field trial for the evaluation. The system allows to protect a sensor network from unauthorized topology changes keeping the property of scalability and security. 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 to build an efficient, safe and easily scalable sensor network to collect and process environmental information.

As a future work, our plan is to add at least one low-power wide-area network (LPWAN) radio module to our nodes in order to increase the applicability of the developed framework to a broader range of system and following the goal of reducing power consumption.

Acknowledgments

This work was 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.

References

[1] C. Zhu, et al., "Trust-based Communication for the Industrial Internet of Things," *IEEE Communications Magazine*, vol. 56, no. 2, pp. 16–22, 2018.

[2] I. Brusakova, et al., "Prospects for the development of IIoT technology in Russia," in *Proc. of Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*, pp. 1315–1317, IEEE, 2017.

[3] E. Sisinni, et al., "Industrial Internet of Things: Challenges, Opportunities, and Directions," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 11, pp. 4724–4734, 2018.

[4] P. Masek, et al., "Communication Capabilities of Wireless M-BUS: Remote Metering Within SmartGrid Infrastructure," in *Proc. of International Conference on Distributed Computer and Communication Networks*, pp. 31–42, Springer, 2018.

[5] J. M. Talavera, et al., "Review of IoT Applications in Agro-industrial and Environmental Fields," *Computers and Electronics in Agriculture*, vol. 142, pp. 283–297, 2017.

[6] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and Privacy Challenges in Industrial Internet of Things," in *Proc. of 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, pp. 1–6, IEEE, 2015.

[7] M. Frustaci, et al., "Evaluating Critical Security Issues of the IoT World: Present and Future Challenges," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2483–2495, 2018.

[8] O. Vermesan and P. Friess, *Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems*. River Publishers, 2013.

[9] P. Masek, et. al., "A Harmonized Perspective on Transportation Management in Smart Cities: The Novel IoT-drive Eenvironment for Road Traffic Modeling," *Sensors*, vol. 16, no. 11, p. 1872, 2016.

[10] S. Wang, et al., "Implementing Smart Factory of Industrie 4.0: an Outlook," *International Journal of Distributed Sensor Networks*, vol. 12, no. 1, p. 3159805, 2016.

[11] I. Krivtsova, et. al., "Implementing a Broadcast Storm Attack on a Mission-critical Wireless Sensor Network," in *Proc. of International Conference on Wired/Wireless Internet Communication*, pp. 297–308, Springer, 2016.

[12] N. Dlodlo and J. Kalezhi, "The Internet of Things in Agriculture for Sustainable Rural Development," in *Proc. of International Conference on Emerging Trends in Networks and Computer Communications (ETNCC)*, pp. 13–18, IEEE, 2015.

[13] M. Singh, et al., "Secure MQTT for Internet of Things (IoT)," in *Proc. of Fifth International Conference on Communication Systems and Network Technologies*, pp. 746–751, IEEE, 2015.

[14] A. Ometov, et al., "Securing Network-Assisted Direct Communication: The Case of Unreliable Cellular Connectivity," in *Proc. of IEEE 14th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, IEEE, 2015.

[15] J. Lee and D. R. Stinson, "Deterministic Key Predistribution Schemes for Distributed Sensor Networks," in *Proc. of International Workshop on Selected Areas in Cryptography*, pp. 294–307, Springer, 2004.

[16] S. Zhu, S. Setia, and S. Jajodia, "LEAP+: Efficient Security Mechanisms for Large-scale Distributed Sensor Networks," *ACM Transactions on Sensor Networks (TOSN)*, vol. 2, no. 4, pp. 500–528, 2006.

[17] J. Jang, T. Kwon, and J. Song, "A Time-based Key Management Protocol for Wireless Sensor Networks," in *Proc. of International Conference on Information Security Practice and Experience*, pp. 314–328, Springer, 2007.

[18] W. Zhang, et al., "A Random Perturbation-based Scheme for Pairwise Key Establishment in Sensor Networks," in *Proc. of the 8th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, pp. 90–99, ACM, 2007.

[19] E.S. Lohan, et al., "Benefits of Positioning-Aided Communication Technology in High-Frequency Industrial IoT," *IEEE Communications Magazine*, vol. 56, no. 12, pp. 142–148, 2018.

[20] A. Ometov, et al., "System-level Analysis of IEEE 802.11ah Technology for Unsaturated MTC Traffic," *International Journal of Sensor Networks*, vol. 26, no. 4, pp. 269–282, 2018.

[21] K.-F. Krentz and G. Wunder, "6DOKU: Towards Secure Over-the-Air Preloading of 6LOWPAN Nodes Using PHY Key Generation," in *Proc. of European Conference on Smart Objects, Systems and Technologies Smart SysTech*, pp. 1–11, VDE, 2015.