Procedures for sensor nodes operation in the secured domain

Janusz Furtak | Zbigniew Zieliński | Jan Chudzikiewicz

Faculty of Cybernetics, Military University of Technology, Warsaw, Poland

Correspondence
Janusz Furtak, Faculty of Cybernetics, Military University of Technology, 00-908 Warsaw, Poland.
Email: janusz.furtak@wat.edu.pl

1 | INTRODUCTION

Shortly, the number of network nodes that will be the source of data will grow rapidly. The number of recipients of this data will also increase quickly. Some sources indicate that shortly, the Internet of Things will have about 50 billion devices. The skillful use of such large amounts of data, especially those that are the freshest and up-to-date, will be a big challenge for recipients. The possibility of a wide use of a large amount of very up-to-date data sounds very promising, but this process will undoubtedly be accompanied by the appearance of new threats related to trust in this data. Another big challenge will be building trust between the data source and their recipient, and building mechanisms that enable secure data transfer. In the risk analysis methodologies, it will be necessary to take into account the reliability of the data depending on the sources of origin for government applications, the freshness of data for crisis management systems or both for military applications.

The concept of building a secure domain of sensor nodes,* which is a very reliable source of data, has been presented in the work of Furtak et al.1 In this approach, it was assumed that the network of sensor nodes creates a domain in which data transfer is protected by cryptography. Cryptographic material stored in the resources of sensor nodes is also protected by cryptography, and data obtained from sensor nodes from the place of their acquisition to the sink node of the domain and outside the domain are secured. Each of the sensor nodes is equipped with a Trusted Platform Module† (TPM). TPM is used to support the process of securing the sensitive data stored in resources of the domain and also during the transmission of these data. TPM also makes it possible to build mechanisms to detect unauthorized interference in the hardware configuration of the node and its software and to respond to such interferences.

*Sensor node - the element of sensor network, which includes at least the measuring element (sensor), microcontroller and communication module that allows transfer of measured data through wireless connections. Sensor - measuring component of the sensor node.
†Trusted Platform Module (TPM) was developed by Trusted Computing Group (TCG), and was standardized by International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) in 2009 as ISO/IEC 11889. TPM is a secure crypto processor and can be used for device identification, authentication, encryption, and device integrity verification. Currently available are the TPM implementations designed according to the older specification (version 1.2) and newer specification (version 2.0). Differences between versions relate to the strength of implemented cryptographic algorithms. For example, in the older version, the RSA 2048 algorithm was implemented, and in the newer version RSA 3072 and ECC 256. It does not matter which version of TPM is used to verify the correctness of the solution proposed in this paper. Due to good knowledge and several years of use, the authors of the study in experiments used Cryptotronix CryptoShield containing the Atmel TPM v.1.2 module.

This is an open access article under the terms of the Creative Commons Attribution NonCommercial License, which permits use, distribution and reproduction in any medium, provided the original work is properly cited and is not used for commercial purposes.

© 2019 The Authors Concurrency and Computation: Practice and Experience Published by John Wiley & Sons Ltd

Concurrency Computat Pract Exper. 2020;32:e5183.
https://doi.org/10.1002/cpe.5183
In this approach, the sensor nodes that are planned to work in a secure domain are first prepared in a safe and controlled space outside their normal working area. Only later, when they are moved to unprotected space, they will be ready to start work there. This paper presents the procedures necessary to prepare sensor nodes for work in a secure domain.

The rest of this paper is organized as follows. Section 2 describes the overall security requirements for the secure domain of sensor nodes. In Section 3, the concept of a secured domain is explained. Section 4 describes the idea of protections for sensor nodes, but Section 5 presents the procedures for initiating a secure domain of sensors. Section 6 presents some concluding remarks.

2 MOTIVATION

An attempt to precisely define the concept of “secured network of sensors” is a quite big challenge, especially in the context of the Internet of Things. By adopting different assumptions, looking at the problem from different points of view, one can come to very different solutions to the problem. However, regardless of these different approaches, it seems that secured network certainly will include only the protected sensor nodes. A secure network of sensor nodes should ensure the following:

- protection of confidentiality of all data gathered, stored, processed, and transmitted between network nodes and to its sink. Particularly, all cryptographic material should be protected against disclosure (or tampering);
- protection of the integrity of network nodes data and software;
- protection of the integrity of data transmitted between network nodes;
- availability of data and services provided by the network.

These sensor nodes will have their identifiers and will be authenticated before they start any operation in such a network, and the communication links used by these nodes will be secured. Considerable attention in such a network should be focused on the problem of the resistance of such a network to damage understood as stopping the proper operation of individual sensor nodes, loss of connectivity due to the nodes leaving the wireless network operation area, or battery discharge.

The protected sensor node should be resistant to an unauthorized interference with its hardware configuration, software, and data stored in its resources. Each such sensor node should be equipped with mechanisms for detecting attempts of such events and reacting to such events. Such a reaction may consist, eg, in sending a message about such an event to other network nodes, blocking the operation of the node, resetting the node's resources. Each such sensor node should be equipped with mechanisms for detecting attempts of such events and reacting to such events.

The domain of the sensors can be said to be secure if all activities performed at each stage of the life cycle of individual sensor nodes and each stage of life cycle of the sensors' domain, will be safe. We distinguish the three phases in the secured domain lifecycle.

1. The preparation phase - activities related to the preparation\footnote{The procedure of preparing the sensor node for work in a secure domain of sensors will be referred to as the preparation procedure.} of the sensor nodes for work in the sensors' domain, in particular with the protection of the sensor nodes software, protection of the equipment of the sensor nodes, and data there stored. This phase includes the following procedures:

2. Master node (M node) - at a given moment, such a node is only one in the security domain of the sensor nodes. M node is a security authority in the domain and stores in its resources a description of all nodes of the secure domain and in particular the cryptographic material necessary to authenticate all other nodes of the secure domain. This sensor node is also equipped with measuring elements and is a regular source of sensor data.

3. Replica node (R node) - there can be many such nodes in the domain. R node in its resources stores a copy of the domain description obtained from M node. In case of failure of the node performing the Master role, one node is elected from R nodes to take over the role of Master in the domain. R node is also equipped with measuring elements and is a regular source of sensor data.

4. Gateway node (G node) - at a given moment, such a node is only one in the sensor nodes domain. This sensor node is the sink node for measurement data acquired by domain nodes and is responsible for the secure transfer of this data from a secure domain to the recipient. The Gateway role can be played both by M node and R node.

The domain of the sensors can be said to be secure if all activities performed at each stage of the life cycle of individual sensor nodes and each stage of life cycle of the sensors' domain, will be safe. We distinguish the three phases in the secured domain lifecycle.

1. The preparation phase - activities related to the preparation\footnote{The procedure of preparing the sensor node for work in a secure domain of sensors will be referred to as the preparation procedure.} of the sensor nodes for work in the sensors' domain, in particular with the protection of the sensor nodes software, protection of the equipment of the sensor nodes, and data there stored. This phase includes the following procedures:
1. The procedure for initiating Base node (B node).
2. The procedure for preparing a sensor node for registration it in the security domain.

II. The deployment phase of solutions - activities related to the creation of the secure domain of sensor nodes and registration new sensor nodes in the domain.

3. The procedure for initiating M node - creation of data structures in the node resources, which is to act as a Master in the domain.
4. The procedure of restoring M node and the entire description of the security domain - recovery and verification of data after power on M node.
5. The procedure for registering a sensor node in the security domain.
6. The procedure for node status confirmation - the procedure starts when the node is powered up.

III. The phase of normal domain operation with secure due diligence (security policy) - activities related to secured exchanging of the data between of the sensor nodes in the domain and between domains of sensor nodes.

7. The procedure for sending data from the R node to the G node.
8. The procedure for sending data from G node outside the domain.
9. The diagnostic procedure for the domain.
10. The procedure for electing of a new M node.
11. The procedure for deleting nodes of the domain on M node.
12. The procedure for electing of a new G node.

In this paper, the attention will be focused on the security mechanisms for preparing the sensor nodes for work in the sensors' domain.

3 | THE CONCEPT OF SECURED DOMAIN

When developing the concept of a secured domain, the following assumptions were taken into account: sensor nodes are mobile, the communication medium used has a low bandwidth and low range, and sensor nodes have limited resources (a small memory resources, low computing power, and limited power capabilities). For this reason, protection of sensor nodes network should be designed in small sensor clusters.4 From the security point of view, each cluster of sensor nodes should be autonomous. The structure of such a cluster may be similar to that shown in Figure 1.

**FIGURE 1** Structure of a sensor nodes network cluster
Cluster objects (sensor nodes) cooperate. An example of such an object can be a soldier who is equipped with measuring sensors. The receiver of the data from these measuring sensors is the soldier’s device,§ which will represent all of the soldier measuring sensors in the cluster of sensors.

The properties of each sensor node are as follows:

- is mobile and uses a wireless connection to exchange data between the sensor nodes;
- collects and preprocesses data from sensors placed in each of the objects;
- can ensure secure transfer of data collected by objects of one cluster to other clusters;
- can carry out diagnostics and reconfiguration inside the cluster;
- ensures transmission security in the cluster and authentication of objects in the cluster.

There are two domains in each cluster1 (each cluster object belongs to each domain):

- **Security domain.** In the domain exists exactly one sensor node (M node), which plays the Master role for the domain and is the authority in the domain. Other sensor nodes (R nodes) of domain exchange with M node the data used to authenticate the nodes in the domain. A symmetric key (Node Secure Key (NSK)), which is used to secure transmission between a given node and the M node, is known only to these two nodes. For this reason, despite using the XBee link, the logical network topology is the topology of the star (Figure 2A). In this domain are also implemented the diagnostic procedures. Then another symmetric key (Node Diagnostic Key (NDK)) is used, which is common to all members of the domain.

- **The domain of protected transmission.** The data obtained from all sensor nodes of the cluster are transferred to one node (G node), which plays the Gateway role in the domain. That operation uses a symmetric key (Node Transfer Key (NTK)) common to all members of the domain. The G node is also responsible for the protected transfer of the data to other clusters. Logical topology of the network in the domain is shown in Figure 2B.

The diagnostic procedures are designed to check if the domain sensor nodes are working correctly, ie, they are fault free. If a failure or a malfunction of the Master node or the Gateway node will be detected, the election procedure of domain node will start. The promoted node will be playing a role previously performed by the damaged node.

### 4 THE CONCEPT OF PROTECTIONS FOR SENSOR NODES

It assumes that each domain node would be using its local trust structure. This structure will protect cryptographic keys and other sensitive node data. For this reason, each domain node will be equipped with a TPM module that will support the creation and use of the trust structure.

The trust structure is based on the hierarchy of asymmetric keys (RSA 2048). On the top of the hierarchy is the Endorsement Key (EK), which can be generated only once for a given TPM module. It is not possible to modify or delete this key. Additionally, its private part is not accessible to the module surroundings.

The next key in the hierarchy is Storage Root Key (SRK) followed by the Domain Key (DK). The SRK is created during the TPM ownership takeover procedure. During this procedure, a string of characters (the secret) is defined, which will later enable the sensor node to perform

---

§The soldier device will be called the sensor node.
authorized actions. It is possible to renew the SRK, but then all cryptographic material stored on the node (which was protected by the old SRK) will be lost. The DK key is common to all nodes of the secure domain. This key is transferred between nodes of the domain only once. For this purpose, a special method has been developed for the secure transfer of this key.

From the point of view of the security procedures described, the EK key can be treated as the sensor node identifier in the domain and the DK key as the domain identifier.

The node that supports the functioning of the security domain is a node named Base (B node). The creation of a security domain will begin with the generation of asymmetric Domain Key (DK) and other domain parameters in the resources of this node. These parameters include the following:

- DN - sensors' domain name;
- time periods (ie, Period of Replication (PR), Period of Nonsuccess Replication (PNR), and Time of data validity (TDV)) associated with the operation of R nodes;
- PAN_ID (ID of Personal Area Network) - the identity of the wireless network (XBee) used in sensors' domain;
- CH - operating channel in a wireless network (XBee) used in sensors' domain;
- PIK - (PAN Interface Key) - symmetric key used by the XBee module, common to all nodes in the PAN.

Additionally, N_ID identifiers will be generated for sensor nodes which in future will be registered in the security domain. The block diagram of the B node is shown in Figure 3, and the structure of data stored in the resources of the B node is shown in Figure 4.

---

Footnote: In all figures depicting the structure of data stored in the sensor node resources, asymmetric keys are presented in the form of a rectangle containing a picture of two keys (private and public), i.e., the name of the key is given next to the rectangle. Symmetrical keys are also shown in the form of a rectangle containing the key name on the left, and on the right a string "IV," which means the Initiating Vector. This vector is used in symmetric cryptography in CBC (Cipher Block Chaining) mode.
4.1 The architecture of the sensor node

The sensor node (Figure 5) is a mobile device and includes the following components: Arduino microcontroller, TPM module connected via the I²C bus, LoRa interface connected via SPI, XBee interface connected via the Serial link, and one or more measuring sensors. The LoRa interface is intended for exchanging data with other domains if the node will act as a Gateway in the domain. The XBee interface is designed to exchange data between sensor nodes inside the security domain. The Serial2 port is used to exchange data during the sensor node preparation procedure to work in the security domain.

4.2 Protections used in sensor nodes

Mechanisms and security solutions for all types of sensor nodes (ie, B node, M node, and R node) used in the sensor’s secure domain are very similar. These include the following.

- The TPM module is an obligatory element of the hardware configuration of each node;
- The TPM module supports the procedures of creating and using a local trust structure, generating symmetric keys and determining SHA-1 and HMAC hashes;
- Cryptographic keys used by the sensor node and other sensitive node data (among others N_ID, PAN_ID, CH, and PIK) are stored in the nonvolatile memory of the TPM;
- Sensitive data regarding the secure domain stored in the EEPROM of the sensor node are protected by cryptography with the use of keys stored in the TPM;
- Platform Configuration Registers (PCR) of the TPM enable the protection of the software and hardware resources of the sensor node against unauthorized modification.

4.3 Data stored in the resources of the sensor node

For this reason, that each network node should be able to act as a Master a Gateway or both in the domain, resources of each node should be very similar. In nonvolatile memory of TPM are stored the necessary data to authenticate the node in the security domain and to cryptographically protect the data transmitted from the node. The EEPROM memory of the M node contains the description of the security domain and the description of registered nodes in the security domain. In EEPROM memory of the R nodes, which act as replicas of the M node, are stored the copy of the security domain description and the copy of the description of registered nodes in the security domain. Figure 6 shows the structure of the data stored in the M node and the R node.

Credentials stored by M node and by R node consist of three resources, ie, own data of the sensor node stored in NVRAM of the TPM, security domain description, and description of the security domain nodes stored in EEPROM of the sensor node. Additionally, in the RAM of sensor node are stored the status data of sensor nodes registered in the domain.

Own data of the sensor node include the following:

- asymmetric keys EK, SRK, and DK, which creates local trust structure;
- NTA: a special tag generated for the node in the node preparation procedure, which is intended for one time authentication of the node in the registration procedure of this node in the domain;
- N_ID sensor node identifier in the domain;
symmetric keys: NK for encrypting the data stored in EEPROM of the node, NSK for encrypting data in authenticating procedures of the node in the domain, NTK for encrypting transferred measurement data from sensor node to G node, and NDK for encrypting data in diagnostic procedures in the domain;
- addresses in the used wireless network: NAD - own address, MAD - address of M node, aand GAD - address of G node;
- parameters of the wireless network used in the domain (PAN_ ID, CH, and PIK).

5 | PROCEDURES FOR INITIATING A SECURE DOMAIN OF SENSORS

Activities to initiate a secure domain of sensors include the procedure for initiating Base node (B node) and the procedure for preparing sensor node for registration it in the security domain.

5.1 | The procedure for initiating B node

In the first step in creating a secure domain of sensors is generated an asymmetric DK key for the domain. This key will later be used to authenticate the sensor nodes in the nodes registration procedure in the domain. In this step, values for other domain parameters are also set. These parameters include the following:
- sensors' domain name (DN) and time domain parameters (ie, PR, PNR, and TDV);
- N_ID identifiers for sensor nodes which in future will be registered in the security domain;
- parameters of the wireless network used in the domain (PAN_ ID, CH, and PIK).

The B node initiation procedure involves generating the data mentioned above, the NK key to encrypt the data stored in the EEPROM of the B node, and the NSK key to encrypt data in the sensor nodes preparation procedure. The sequence diagram for the B node initialization procedure is shown in Figure 7, and the data stored on the B node after the procedure in Figure 8.

5.2 | Sensor nodes preparing procedure

This procedure is intended to prepare the node for registration it in the security domain (in this section, the sensor node being prepared will be referred to as a P node). The own data of the P node are generated, and the public key of the security domain is being obtained. It is assumed that during this procedure the node is connected to the B node via the USB interface. The sequence diagram for the sensor node preparing procedure
is shown in Figure 9. Obligatory activities of this procedure are performed for all prepared nodes, and the optional part is performed additionally only for the first node being prepared. This first node will be the initiating node of the domain, and this node will play a Master role in this domain.

Description of the most important steps of the procedure (the numbers in round brackets (e.g., (3)) in the following descriptions indicate the numbers of the individual steps that are given in Figure 9).

(3) **Generate the data for P node:**
- generate the following symmetric keys (size 32 bytes):
  - NK - the key to encrypt the data stored in the EEPROM of the P node;
  - NSK - the key to encrypt data in the sensor nodes preparation procedure;
  - OTP (One Time Password) - it is used only to protect the transfer by Serial link the data during node preparing procedure and is stored in NTK field (the target NTK key content will be determined later during the node registration procedure in the domain);
- set NAD address – MAC address of XBee interface;

(6) **Acquire DK of domain** – acquire the migrate blob containing cryptographically protected DK of security domain from B node:
- acquire the public part of the SRK key from TPM of P node; send a `dom_key_req` packet from P node to B node through the serial line and get a `dom_key_ans` packet from B node (Figure 10);
- unpack migration blob and put the DK into the root of trust stored in TPM of P node.

(9) **Acquire node parameters** - acquire N_ID, RN, NTAG, and MAD. The P node should be connected to the node B via the USB interface. If the prepared node is the first one, the node will play a MASTER role in the security domain. Then, parameter RN is set to MASTER, MAD to NAD.
of the first node, and MAD is stored in nonvolatile memory of B node TPM. The content of the NTAG field is the result of the hash function SHA-1 for the sequence of fields DN, N_ID of the node, and twobytes field, which includes the number of the node description in the security domain. Do the following:

- send a \textit{par\_node\_req} packet from P node to B node; the packet is bound using public part of DK key (the blob includes the length of bound data (4 bytes) and bound data) - as an OTP is to be used the key stored in NTK field (see Figure 11);
- get from B node a \textit{par\_node\_ans} packet; the packet is protected using symmetric key OTP sent in the \textit{par\_node\_req} packet(see Figure 12);
- put obtained data into TPM nonvolatile memory of P node.

(12) \textbf{Acquire parameters of the wireless interface}: PIK, PAN_ID, and CH. The P node should be connected to the node B via the USB interface. Do the following:

- send a \textit{par\_interface\_req} packet from P node to B node; the packet is encrypted using the OTP key of P node (see Figure 13);
- get from B node a \textit{par\_interface\_ans} packet; the packet is protected using the OTP key (see Figure 14);
- put obtained data into TPM nonvolatile memory of P node.
(15) Acquire domain description (optional activity only for the first prepared node). Do the following:

- send a request of domain description (domain_descr_req packet) from P node to B node. The sequence number (SQ) of P node is initiated and used. The packet is encrypted using the OTP key of P node (see Figure 15);
- prepare domain description (domain_descr_ans packet) and send it to P node. The packet is encrypted using the OTP key of P node (see Figure 16);
- put obtained data into EEPROM of P node.

(18) Acquire initial data for nodes of domain (optional activity only for the first prepared node). The initial data of nodes, which are the potential members of the security domain, are transferred to the node. The number N of transferred descriptions is limited by the size area of the prepared node EEPROM or by the number of generated data on B node. Do the following:

- send a request of ith (i < 1; N >) node description (node_desc_req packet) from P node to B node. The sequence number (SQ) of the P node is initiated and used. The packet is encrypted using the OTP key of P node (see Figure 17);
- prepare domain description (node_desc_ans packet) and send it to P node. The packet is encrypted using the OTP key of P node (see Figure 18);
- put obtained data (NIDs) into EEPROM of P node;
- repeat the above steps as long as there is a place in the EEPROM memory of the P node.
FIGURE 16  The frame consisting of the sensor node domain

FIGURE 17  The frames used by P node to acquire the descriptions of domain nodes

FIGURE 18  The frame consisting of the descriptions of domain nodes

FIGURE 19  The data stored on M node (A) and R node (B) after preparing procedure

The content of the P node resource at the end of the preparing procedure depends on the role which the node will play in the security domain. The content of the M node resource is shown in Figure 19A, but the content of the R node resource is shown in Figure 19B. The fields of TPM nonvolatile memory, which so far has not been assigned values (they are reset), are indicated in gray.
The correctness of the described procedures was verified experimentally. For the needs of the experiment, a demonstrator of one type B node and several R type nodes was prepared.

Each sensor node (Figure 20A) used in the experiments was built with the following components: microcontroller Arduino Mega 2560 R3, Cryptotronix CryptoShield containing TPM\textsuperscript{v.1.2}, Dragino LoRa Shield - 868MHz v1.3, wireless communication module XBee, and ultrasonic distance sensor. In the procedure of preparing sensor nodes to work in the domain, the BASE node Figure 20B) is necessary. It was built with the following components: microcontroller Arduino Mega 2560 R3 and Cryptotronix CryptoShield with TPM v.1.2. Figure 20C shows the configuration of the demonstrator during the procedure of preparing the sensor node for work in the domain.

6 | CONCLUSION

The procedures presented in this paper include the first steps to deploy a secure domain of sensor nodes. The procedures include the process of generating initial parameters and data for the secure domain and the process of preparing sensor nodes that are expected to work in the secure domain. Other activities necessary to run a fully functioning domain are out of the scope of this paper.

In the presented procedures, particular attention was paid to the security of data exchanged between nodes in all performed steps. It was assumed that the implementation of preparation procedures would take place in a safe and controlled environment. The steps start with the preparation of B node and create in its resources first the trust structure, and then generate initialization data for the domain. All these procedures are supported by TPM. During the preparation procedure, a direct serial connection between the B node and the node being prepared will be used. Only in the first step of the node preparation procedure the data is passed in plain text. This data includes only the public key of the node being prepared. This key is necessary for the special procedure of preparing the DK blob, which is performed by the TPM module of the B node. Such a blob can be transmitted to the node being prepared without any protection. Then, the public part of the DK key will be used to exchange the OTP symmetric key between the prepared node and B node. All other data transmissions are cryptographically protected using the OTP symmetric key. The resources of each sensor node are protected by an NK key, which is known and used only locally by the sensor node and is stored in the TPM resources of a given sensor node. During the node preparation procedure, a special node tag (NTAG) is assigned to each node, which is verified during the subsequent registration procedure of the node in the domain. The use of the NTAG eliminates the possibility of potential interference in the data of the prepared node before this node is registered in the domain. After completing the procedure of preparing the node, from the configuration of the sensor node, the serial interface can be removed, which will not be necessary for the further operation of the sensor node. Removing this interface will additionally reduce the chance of breaking the sensor node security.

The procedures necessary for the functioning of the domain have been implemented. For this purpose, a demonstrator of a secure domain, which includes four working mobile sensor nodes, has been developed. In this domain, one node acts as a Master (M node), another node acts as the Gateway (G node), and the others act as a Replicas (R nodes). In an experiment showing the functioning of the domain, the data generated by the domain sensors are collected by the node G and then are transferred to the recipient via the MQTT broker. The secure domain is naturally accompanied by the B node, which is necessary to create a domain and to prepare nodes to work in the domain. The concept of the secure domain, the presentation of the domain's operation, and the selected results of the experiments were described in the work of Furtak et al.\textsuperscript{1}

Our future work will focus on implementing procedures diagnostic procedures to detect misbehaved (faulty) sensor nodes, procedures for the election of new nodes M and G, in the case of detection of disability of sensor nodes that had performed this role until now and procedures for protecting a node against unauthorized interference.
REFERENCES

1. Furtak J, Zieleński Z, Chudzikiewicz J. Secured domain of sensor nodes - a new concept. In: Hodnoň M, Eichler G, Erfurth C, Fahrnberger G eds. Innovations for Community Services. I4CS 2018. Communications in Computer and Information Science. vol. 863. Springer, Cham; 2018. https://doi.org/10.1007/978-3-319-93408-2_15/cpe.5183

2. Al-Hajja QA, Tarayrah MA, Al-Qadeeb H, Al-Lwaimi A. Tiny RSA cryptosystem based on Arduino microcontroller useful for small scale networks. Procedia Comput Sci. 2014;34:639-646.

3. Koteshwara S, Das A. Comparative study of authenticated encryption targeting lightweight IoT applications. IEEE Des Tests. 2017;34(4):26-33. https://doi.org/10.1109/MDAT.2017.2682234/cpe.5183

4. Puschmann D, Barnaghi P, Tafazolli R. Adaptive clustering for dynamic IoT data streams. IEEE Internet of Things Journal. 2017;4(1):64-74.

5. Trusted Computing Group. TPM Main Part 1 Design Principles: Specification Version 1.2 Revision 116. Beaverton, OR: Trusted Computing Group, Incorporated; 2011.

6. NIST. Security requirements for cryptographic modules. Federal Information Processing Standard (FIPS 140-2). 2002.

How to cite this article: Furtak J, Zieleński Z, Chudzikiewicz J. Procedures for sensor nodes operation in the secured domain. Concurrency Computat Pract Exper. 2020;32:e5183. https://doi.org/10.1002/cpe.5183