Two-step process for secure registration of nodes in IoT systems

Milan Stojkov*, Miloš Simić*, Goran Sladić*, Branko Milosavljević*
* Faculty of Technical Sciences, University of Novi Sad, Novi Sad, Serbia
{stojkovm, milos.simic, sladicg, mbranko}@uns.ac.rs

***Abstract*— Edge computing is recognized as an architecture which is well suited for the integration with the Internet of Things. A new layer of devices, also called nodes, between cloud services and end-users, can provide new services with fast response and great quality. On the other hand, new layer devices introduce more architectural and security challenges which were not yet considered. In this paper, the main focus is directed towards security issues, especially those concerning safe (re)authentication of the nodes in the already established IoT system. We defined a two-step process for a secure registration of the nodes in IoT system that includes a solution for protection against the physical replacement of the nodes with corrupted ones. Our approach uses public key cryptography based on ECCDH algorithm and communication between nodes, gateways and authentication services in the cloud.**

Keywords: Internet of Things, authentication, node capture attack, industrial IoT, smart grid

I. INTRODUCTION

Edge (or fog) computing is getting more popular nowadays since it is an architecture that is organized by networking edge devices which provide computing services for the customers in the space between cloud servers and end-users. Considering it is a distributed architecture where devices can collect, process and store data on their own this approach can be more beneficial for the end-users. These devices can provide services with faster response and greater quality in comparison with cloud computing [1]. Thus, edge computing is a suitable architecture to be integrated with the Internet of Things (IoT). IoT brings more architectural and security challenges into the picture. A big problem is that devices are not secure by default, which leaves the potential risk of a large number of unsecured devices connecting to the Internet. We currently do not have full control over IoT devices and Mirai and Mirai-like threats such as Persirai, IoTroop, etc. are just a few examples of how insecure these IoT systems are. Taking into consideration that IoT is multilayered architecture [1], the whole classes of security issues exist on each layer starting from the devices and ending with the applications these devices communicate with (Figure 1). Thus, the security mechanisms in existing communication protocols need to be modified or extended to harden the IoT systems. In this paper, the authors tackle problems that occur on the lowest layer that involves communication between the devices, particularly their secure authentication.

The rest of this paper is organized as follows: Section II presents related work for node authentication and authorization in IoT. Section III describes IoT architecture and introduces node classification. In Section IV, the problem to be solved is presented, along with the assumptions as prerequisites for the designed solution, while in Section V the two-step process for secure registration of the nodes is presented in detail. The discussion for the presented process is given in Section VI.

II. RELATED WORK

The design phase for the IoT solution includes significant effort invested in different security and privacy restrictions as this solution has to be integrated into the existing digital ecosystem. Therefore, the detailed analysis of these security and privacy issues has to be carried out to suppress threats for IoT solutions [7]. Certainly, the most discussed questions are about authentication and authorization. Different authentication schemes are presented in [5], [8] and [9]. All of them consider using public key infrastructure, especially Elliptic Curve Cryptography algorithms, for secure communication. In [10], authors have presented ECC based mutual authentication protocol for IoT using hash functions. These solutions discuss only the key establishment between the nodes and the key distribution platform that is centralized. The problem of secure communication and authentication based on the shared key is presented in [11] and is applicable to limited location and cannot be used for a wide area. All solutions for authentication and access control previously mentioned tackle the problems to the certain extent in order to fulfill all requirements for IoT, and the authors of this paper go further and propose the solutions that solve observed oversights.

III. IOT ARCHITECTURE

Lots of proposed IoT architecture solutions are strictly coupled with a certain use-case, and there is not enough accent put on the interoperability among different devices in different IoT systems. Different research has shown that the IoT can be considered as multi-layer architecture which is roughly divided into three layers: perception layer, network layer, and application layer [1]. The perception layer is the lowest abstraction layer which goal is to measure physical quantities through physical equipment. The devices in the perception layer are uniformly called nodes but their characteristics are often omitted. Since these nodes are different in terms of processing power, energy, and storage, they cannot be considered as equal. That is

why more sophisticated classification should be defined. The authors propose classification which consists at least of 3 types of nodes:

- nodes which are collecting the data from the source and forwarding that data further – these nodes have low computational power and thus are only relevant for data streaming
- nodes which are collecting data and executing simple tasks – these nodes are more powerful in terms of storage, computational power, and energy consumption, hence they can cache the data or do initial preprocessing
- gateways which are collecting the data from other nodes, monitoring them and doing further data processing – these nodes represent the most sophisticated devices in this hierarchical classification

When there is some sort of node classification, then different problems can be tackled more precisely, especially in terms of security. As the main purpose of the devices in the perception layer is to collect data, the main security issues which should be addressed are compromisation of the devices and forging the collected data. Different authors tackled these problems in Wireless Sensor Networks (WSN) which are one of the technologies for the perception layer. Other technologies include Radio-Frequency Identifier (RFID), the implantable medical devices (IMDs), Global Positioning System (GPS), etc. Many proposed security schemes either ignore some classes of attacks such as node capture attack and some of them are trying to make all the nodes tamper-resistant increasing the overall cost for the system implementation [2]. Strict process for (re)authentication of the devices in the system and detection of compromised nodes should be defined. In this paper, authors proposed a process for secure registration of the new/old device into the system.

The nodes are connected to the second layer, the transport layer, via a gateway which represents a subnet manager for these nodes. The transport layer represents robust and high-performance network infrastructure that is responsible for the transmission of information from perception layer, initial processing of information and classification.

The application layer provides a user interface for the IoT services. These services cover various sectors like healthcare, supply chains, government, transportation, retail, smart grid, etc.

IV. Problem Statement

For the design of the secure authentication process, authors made some assumptions. Different complex IoT solutions are already established and functional. From the architectural point of view, a lot of assumptions described in the further text are already a common practice and are considered the stable architectural approach in these solutions but additional constraints must be given. IoT system consists of a lot of interconnected nodes scattered on some area. The nodes are often strategically grouped in a specific area which means IoT network segmentation can be made. Having strictly defined areas, additional targeted processing and hardening can be made. Every segment can have different types of nodes. The assumption that all nodes have unlimited power and memory and that they are protected from physical access from the attacker by default

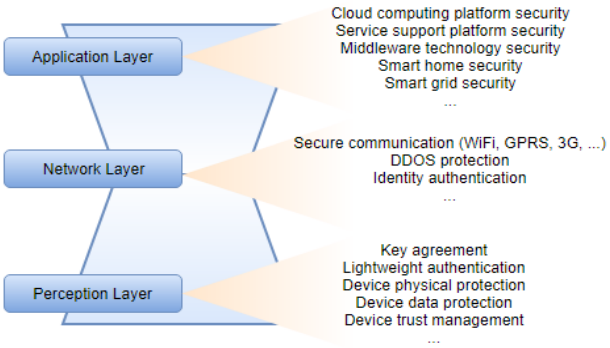

Figure 1. Security concerns in IoT multi-layer architecture

is not viable for the IoT system. That is why nodes in the IoT system must be classified according to their capability to collect, process, store and send data as previously mentioned. The nodes which are not capable to store secrets due to low memory are excluded from the process since their authentication can be done, for example, by using physically unclonable functions (PUFs) [3]. Further, every segment should have one or more gateways which have the greater processing power and power supply and can monitor all the nodes in that segment to compensate their limitations. The existence of the gateways can be one link in a process for preventing the distributed denial of service (DDOS) attacks [4]. Finally, gateways are the nodes which communicate with the services running in the cloud. Having set up the IoT system like this where a multi-layer IoT architectural form is fulfilled, we can address the problem of secure registration of the nodes and node capture attack. The node capture attack removes a node from the network and redeploys it to perform various attacks or tampers with the hardware on the existing node. In the authentication process nodes are authenticated against gateways and a random number of other nodes in a subnetwork or directly against authentication service in the cloud.

V. Solution

The whole communication takes place between three entities: a node, a gateway, and a cloud authentication service. The process for the secure authentication of the new node in the subnetwork consists of two steps:

1. the node, after key establishment, authenticates against a local gateway
2. if the first step fails, the node authenticates with the authentication service in the cloud

At the beginning of the IoT era, it has been a lot of debate which cryptography mechanism is the most suitable to use. Symmetric keys were the first option due to fast computation and energy efficiency, but scalability problems and memory requirement to store keys make this approach inefficient for heterogeneous devices in IoT [5]. A public key cryptography overcomes this challenges because of its high scalability, low memory requirements and no-requirement of key pre-distribution infrastructure. The Elliptical Curve Cryptography Diffie Hellman (ECCDH) algorithm is now widely used as the algorithm for the key generation as it is lightweight and suites well for the IoT purposes [6]. ECCDH is a symmetric key agreement protocol that allows two devices that have no prior knowledge about each other to establish a shared

secret key. The protocol itself uses one or more Key Distribution Centers (KDCs) which create domain parameters. This KDCs can be a part of a gateway or an authentication service located in a cloud. In this way, we gain redundancy for the component that is crucial for the keys distribution. The algorithm based on ECCDH is used in this proposed solution.

The KDC selects particular elliptic curve (e.g. secp256k1 used in Bitcoin) over finite field *GF (p)* where p is a prime and makes base point P with large order q (where q is also prime). KDC then picks random $x \in GF(p)$ as a private key and publishes corresponding public key $Q = x \times P$. KDC generates random number $K_d \in GF(p)$ as a private key for device d and generates corresponding public key $Q_d = K_d \times P$. The key pair $\{Q_d, K_d\}$ is given to device d [5]. This process is repeated for any number of nodes where the only agreement is on base point P. Generated key pairs are then used to share common secret key using ECCDH. Every node receives its pair of keys during the bootstrapping phase. The bootstrapping phase is the process by which devices join the IoT ecosystem at a given location and point in time and where they also gain credentials.

The process for the secure authentication of the new node in the subnetwork consists of two steps. In the first step, the first substep is key establishment process based on ECCDH where one-way authentication of the node towards the gateway is performed in a secure manner.

After successful key establishment, the gateway selects a configured number of nodes which have to check if the registered node is available at specific intervals. If the node is unavailable at check-times, the information will be sent to the gateway and node will be blacklisted. In this way, if the node malfunction is not announced earlier, it is possible that the node capture attack is taking place.

In the second step of this process, the node has to communicate directly with the authentication service which resides in the cloud. The node has to send the same data to the authentication service as it would to the unavailable gateway through the key establishment. After the configured number of unsuccessful authentication attempts, the node is blacklisted and blocked for further communication with gateway or cloud services. If the node is successfully authenticated, as soon as gateway becomes available and reauthenticates to the cloud authentication service, the gateway will receive information about all newly registered nodes during the offline period. The gateway will then pick a configured number of devices in a subnetwork to occasionally monitor new nodes. The second step is performed only if the first step is finished unsuccessfully. This step further hardens the process, and as it is only a backup step, it does not burden the whole process by default. The two-step process is presented in Figure 2.

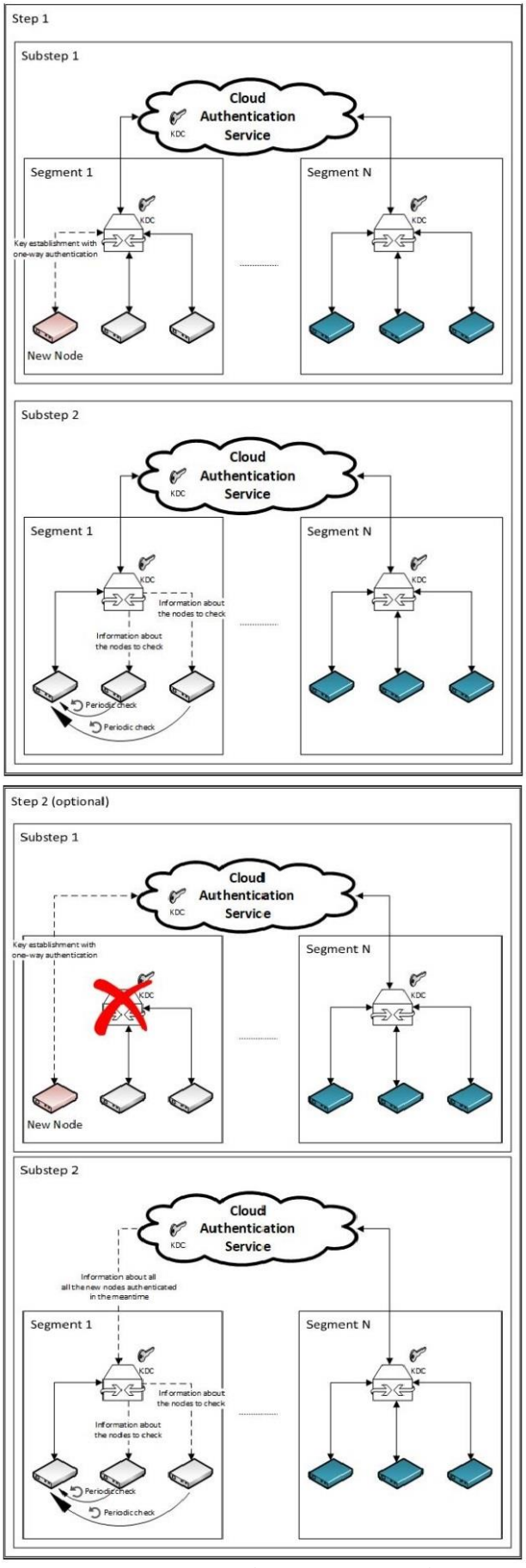

Figure 2. Two-step process for secure registration of nodes

VI. DISCUSSION

The authentication process is only one approach to address security issues. In fact, the authentication process is only the first step towards building a highly secure IoT protection framework which will include fine-grained access control model for these nodes, anomaly detection in

node-to-node communication, etc. Different authentication solutions consist of only one step, thus the second step in the proposed process only hardens the whole process and make it overall more complete solution. The Key Distribution Centers are distributed from one centralized cloud service to gateways too. In this way, the whole communication with cloud authentication service is more relaxed and cloud authentication service is no more candidate for a single point of failure. Since KDC has to be secure, trusted, and to do complex calculations, gateways that include KDCs must be powerful devices and physically secured as well. The node capture attack can take place on gateway too, in order to corrupt KDC, but if node capture attack is detected cloud authentication service has its own KDC to generate keys. This two-step process gives the opportunity to establish appropriate access control model that can make gateways centers for permission generation. If we consider different authentication and authorization solutions, we can make common multi-layer IoT architecture more secure starting from the design phase. The future work will be oriented towards secure-by-design IoT architectures that include the proposed solution. For the two-step process itself, it has broad use such as in industrial IoT manufacturing processes, smart healthcare, smart grid, etc.

REFERENCES

[1] J. Lin at al. A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. IEEE Internet of Things Journal, Volume: 4, Issue: 5, October 2017

[2] S. H. Jokhio, I. A. Jokhio, A. H. Kemp. Node capture attack detection and defence in wireless sensor networks. IET Wireless Sensor Systems, Volume: 2, Issue: 3, September 2012

[3] M. N. Aman, K. C. Chua, B. Sikdar. Mutual Authentication in IoT Systems using Physical Unclonable Functions. IEEE Internet of Things Journal, Volume: 4, Issue: 5, October 2017

[4] C. Zhang, R. Green. Communication security in Internet of Thing: Preventive measure and avoid DDoS attack over IoT network. Proceeding CNS '15 Proceedings of the 18th Symposium on Communications & Networking, April 12 - 15, 2015

[5] P. N. Mahalle at al. Identity Authentication and Capability Based Access Control (IACAC) for the Internet of Things. Journal of Cyber Security and Mobility, Vol. 1, 309–348, 2013.

[6] N. Koblitz. Elliptic curve cryptosystems. Mathematics of Computation, 48: 203–209, 1987.

[7] T. Heer, O. Garcia-Morchon, R. Hummen, S.L. Keoh, S.S. Kumar, K. Wehrle. Security challenges in the IP-based Internet of Things. Wireless Personal Communications 61(3), 527-542, 2011

[8] J. Liu, Y. Xiao, C. L. P. Chen. Authentication and Access Control in the Internet of Things. 2012 32nd International Conference on Distributed Computing Systems Workshops ICDCSW., June 2012

[9] Y.E. Ning at al. An Efficient Authentication and Access Control Scheme for perception layer of Internet of Things. Applied Mathematics & Information Sciences, Vol. 8, July 2014

[10] G. Zhao, X. Si, J. Wang, X. Long and T. Hu. A novel mutual authentication scheme for Internet of Things. Proceedings of 2011 IEEE International Conference on Modelling, Identification and Control (ICMIC), vol., no., pp.563-566, 26-29 June 2011

[11] D. Balfanz, D. K. Smetters, P. Stewart and H. C. Wong. Talking to strangers: Authentication in ad-hoc wireless networks. Network and Distributed Systems Security Symposium (NDSS), February 2002.