A Solution for Industrial Device Commissioning along with the Initial Trust Establishment

Apala Ray*†, Johan Åkerberg*†, Mikael Gidlund* and Mats Björkman†
*ABB Corporate Research
†Mälardalen University; School of Innovation, Design, and Technology

***Abstract*—Industrial device commissioning along with the initial distribution of keying material is an important step for the security of industrial plants. An efficient key management system is required in cryptography for both symmetric key or public/ private key encryption. Most of the key management system use either pre-installed shared keys or install keys using out-of-band channels. In addition to that, the sensor devices both wired and wireless need to be verified whether it is connected to the correct physical entity since these devices are linked with the physical world. Therefore in industrial plants there is a requirement to automate the trust bootstrapping process, where the devices from upper level in communication network will be aware that the communication device from below level is trusted. In this work, we present a workflow that uses the existing trust mechanism on employees to enable the initial bootstrap of trust in the devices, and also optionally support the commissioning engineer to download the required configuration data in the device as well. Thus, this approach presents a unique solution to the initial trust distribution problem reusing the existing features and facilities in industrial plants.**

***Index Terms*—Key Distribution, Industrial Wireless Sensor Networks, Security, Device commissioning.**

I. Introduction

The automation industry is exploring to shift substantial parts of the traditionally wired industrial infrastructure to wireless technologies. This leads to a requirement of unified commissioning and engineering workflow for both the wired and wireless devices with adequate security. For wired protocols, the slave device is required to be configured with an address, so that it can respond upon master queries. The wireless protocols have been designed in a way which is different than typical automation protocols. In wireless protocols, once the device is authenticated to join in the network, the master device initiates all communication and downloads device configuration as well.

The automation security aims to protect the devices (sensors/actuators/controllers) from security attacks and the first level of security is achieved from access control and user authentication which can be addressed by physical security aspect of plant premises. The second level of defense is in the security of various communication protocols which is used between various devices (sensors and actuators) and controllers inside a plant network. The communication security uses different cryptographic algorithms and the security of cryptographic algorithms lies on underlying secret key. Therefore it requires key management which deals with key generation, key distribution, key update and key storage. Whether symmetric key or public/ private key are used for cryptography, both will require an efficient key management system. In addition to that, in any architecture of communication network security, there is either an explicit assumption or an explicit mechanism to establish the initial trust among the communication parties. The initial trust establishment in wireless network is a well-known problem as wireless is a broadcast medium. Therefore, to allow the wireless device in the network, the device needs to be authenticated as trusted. In addition to that, out-of-band initial trust bootstrapping with a handheld device is an additional burden as a typical paper mill has 30 to 50000 sensors and actuators. It is also a non-trivial task for a commissioning and maintenance engineer to find the physical devices that are spread over large areas and not always visible. If pre-shared key is used, the commissioning and maintenance engineer also needs to manually enter the keys specific to the device. This may introduce errors in commissioning also. On the other side, the wired devices also always need to be connected to the *real world* since the devices are linked with physical entities. Therefore, it would be interesting to not only establish initial trust, but also optionally allow the commissioning engineer to download the unique tag-name in the device as well. In today's scenario, every signal needs to be manually checked prior to cold commissioning such that the right data is received and transmitted to the correct physical entity. Later, commissioning engineer signs off the result in traditional commissioning reports. In practice, this is a critical and dangerous process since it is very likely that not all signals have been checked due to the large number of signals. In addition to that this work involves several persons over several days.

In this paper, we present a workflow that uses the trust which already exists inside a plant for employees and enables the initial bootstrap of trust during the device commissioning by using the same trust of the employee. This workflow also optionally supports the commissioning engineer to download the required configuration data in the device as well. Our workflow provides a generic and protocol independent addressing scheme since protocol dependent parameters can be discovered based on the initial trust and its embedded discovery and control parameters that were programmed. With this solution, we can scan the network to see which devices have been commissioned or not. Moreover, by using asymmetric crypto for initial trust establishment, it is even supporting non-repudiation. In this paper, section 2 discusses the related

work. Section 3 presents the overview of proposed initial trust establishment mechanism. In section 4, the assessment of our proposed workflow has been presented. Finally, the conclusions are presented in section 5.

II. Related Work

An authentication protocol is a sequence of message exchanges between entities to distribute secrets or to allow some secret to be recognized [1]. Till now a lot of authentication protocols have been specified and implemented. In In [2], an exhaustive survey on authentication protocols has been presented. There are also enormous number of works have been done and still going on key management issues. It is very difficult to compile all state-of-art for this topic. There are many surveys which cover this dynamic field of research. In [3], Camtepe and Yener cover deterministic, probabilistic and hybrid pre-distribution schemes for distributed networks and propose to establish pair-wise, group-wise and network-wise keys in hierarchical networks. Together with their historical evolution, this work analyzes many of the security and efficiency related characteristics. There are many survey papers on key management and they have classified the mechanisms in different categories [4]–[8]. Each of the key distribution protocols has its own benefits and disadvantages, and moreover they can be suitable for particular application requirements. However, it has been shown in [9] that the assumptions or pre-requisite of existing key distributions are not suitable for Industrial Automation environment, since industrial plant has specific requirements on availability and at the same time easier workflow for commissioning or maintenance engineer. In [10], a method for integrating WirelessHART networks in distributed control systems using PROFINET IO has been proposed which uses user-friendly tag names. In our paper, we will present a workflow, which complements the work done in [10]. This will enable efficient device commissioning along with distributing initial trust between industrial devices.

III. Device commissioning with the initial trust establishment - Overview

In this section, we present the concept and the design goals of the device commissioning with the initial trust establishment workflow. The role of the components are described along with the assumptions. The sequence of workflow phases and the involvement of the user are described.

A. Workflow objective

Our objective is to ensure that in the industrial plants the communication is happening between entities which are allowed to communicate with each other. This implies that the intelligent devices need to be authenticated before it is part of the network. To achieve this, the network can be configured in a way where messages can only be sent to the devices which are allowed to communicate each other or the receiver can authenticate the sender identity and throw away the messages which are from not from authorized sources. As discussed in [9], an initial element which is going to be used in a key management system requires a trusted, or trusted and secured channel. This leads to a solution requirement of investing further how initial trust to the device can be distributed considering the plant environment. This workflow is designed to meet the following goals, which we have identified as the major objectives to get fulfilled.

Device identification: The commissioning engineer or the maintenance engineer needs to identify the devices which are going to be commissioned are physically connected to the correct machinery at right place. While commissioning, the person will also check whether the devices are not tampered.

Device authentication: The device needs to be authenticated before it gets access inside the network. The other devices which are not authenticated will not be able to join the network.

User friendliness: The commissioning engineer or the maintenance engineer (skilled/ unskilled) should be able to replace devices in case of failure. When a new device is being introduced, minimal manual intervention and less reconfiguration time is expected.

B. System components and the assumptions

In this paper we explore the idea of distributing the initial trust [9] between the devices in a comparatively easier workflow for commissioning or maintenance engineer. Note that, for our workflow the plant size and the number of devices are not constraint. The number of device can range from 10 to 10000. We assume that in the current scenario of any industrial plant, some level of trust already exists. The plant has access control in place and the employees who are authorized to enter inside that plant will have an ID card and password which is monitored centrally. The commissioning engineer who is going to deploy the devices inside the plant should be authorized personnel. The employee is supposed to keep its password secret. We have also assumed that the devices inside the plant should have an interface through which the initial information can be downloaded to the device and the initial information for the device is written on write-only memory and the information cannot be read from outside. Generally in industrial plants, there is commissioning device like handheld which is capable of writing some initial information to the device. This device is also capable of reading certificates from chip enabled card. It should have strong security assumption as it has to be trusted and confidential. Because no attacker should be able to steal secret information or handheld device should not leak secret information. It may require high computation capability.

The components which participate in the workflow are presented below.

- *Employee management system*: Inside the plant there is a first level of access control and the employee management system securely stores the employee access data. The employee collects their employee ID card from the employee management system and the employee management system has its private-public key pair $K_{pr(EMS)}$ and $K_{pub(EMS)}$. Employee management system may be

physically protected and is responsible for issuing the certificates for the employee. This component is considered to be trusted component inside the plant.

- *Commissioning engineer/ maintenance engineer*: The engineer who has access to configure or commission devices prior to the operational phases. He will have an ID card which is registered with the *Employee management system* and has a unique passcode for the ID card.
- *ID card of commissioning engineer*: The certificate for the commissioning engineer provided by the *Employee management system* is stored inside chip. This is the public key of the commissioning engineer $K_{pub(EMP)}$, signed by the private key of *Employee management system* $K_{pr(EMS)}$. This ID card also has the certificate for the card which contains the public key of chip enabled card, $K_{pub(CARD)}$ and authentication parameter (APARAM) signed by the private key of the commissioning engineer $K_{pr(EMP)}$. This APARAM is used to provide authenticity during the device commissioning and consisted of a static component for employee along with a random generated number and nonce.
- *Commissioning device*: The commissioning device is primarily used for injecting the employee related authentication information to the device. The commissioning device should have the public key of *Employee management system* $K_{pub(EMS)}$ for employee verification. Optionally, the certificate for the commissioning device provided by central device management system can also be stored inside chip. This is the public key of the *Commissioning device* $K_{pub(HH)}$, signed by the private key of central device management system. This is not mandatory; instead the unique ID number of commissioning device can be stored centrally for verification.
- *Slave device*: This component is the device which needs access for the network. During commissioning phase the trust from the commissioning engineer is transferred to this slave device. If the commissioning engineer verifies that this device can be part of the network, then the certificate of commissioning engineer is provided to the slave device. By presenting the certificate along with time stamp, the slave devices can send the network access request for the master network. If the slave device is configured with the correct tag-name, this information can be uploaded to the master device. After verification step, the master device will know that the slave device is connected to the correct physical entity, which will help to map the tags automatically to the corresponding control applications.
- *Master device*: This component resides at the upper communication level than the slave device. This component can query the slave devices which are configured with the correct tag-name. On the other hand, this component can have the security features to verify the authentication of the slave device. It will give network access to the slave devices once the device is authenticated as trusted.

C. Proposed Workflow - Device commissioning with the initial trust establishment

In Figure 1, our proposed workflow for initial trust distribution for the devices is presented. During commissioning phase or maintenance phase, when the device is required to be commissioned for network access, the commissioning engineer or maintenance engineer brings the commissioning device. The commissioning engineer swipes his ID card, in the commissioning device. Then the commissioning device checks the authentication of the card and then verifies the authenticity of the commissioning engineers. Once this verification is done, the commissioning device retrieves the security parameters from the employee card to sign the configuration data for the device to be commissioned.

Generally, the automation protocols which are designed for wired devices require prior configuration of parameters, so that the devices can respond to their master's queries. On the other hand, the wireless protocols enable network and device configuration once the device is authenticated to access the network. Therefore, in our proposed workflow we have flexibility to support both the features. If the plant infrastructure supports for a central database with the required tag-names for the devices to be commissioned, the commissioning device can download the information from there. This option will provide higher consistency of the tag-names and less manual errors. However, this feature reduces the scalability as every time a new device comes in the plant, the database has to be updated and the commissioning device always need to have access to this central database. For this reason, our workflow supports another feature, where the commissioning engineer enters manually the tag data according to the plant documentation as currently available. After creating the configuration data for the slave device, the commissioning device creates a packet encrypting the APARAM (authentication parameter) with private key of employee. Then the commissioning device transfers the configuration data along with encrypted APARAM to the slave device. If the configuration is not required to be uploaded to the slave device, the commissioning device creates loads the network access data along with encrypted APARAM. The commissioning device also supplies its own identity and the public key of employee management system to the device. There is two possibilities of supplying commissioning device's identity to the device. In first approach, if the commissioning device itself is registered with any central device management unit, then the commissioning device will have its own certificate. This certificate can be passed to the device, which will provide the non-repudiation features for the commissioning device. However, in the second approach, if there is no central device management unit which keeps track of the commissioning device, then the commissioning device can send its serial number or device identity to the device to be commissioned. This will help to keep track of the commissioning device which is used for downloading parameters to the device, though it does not support the non-repudiation feature.

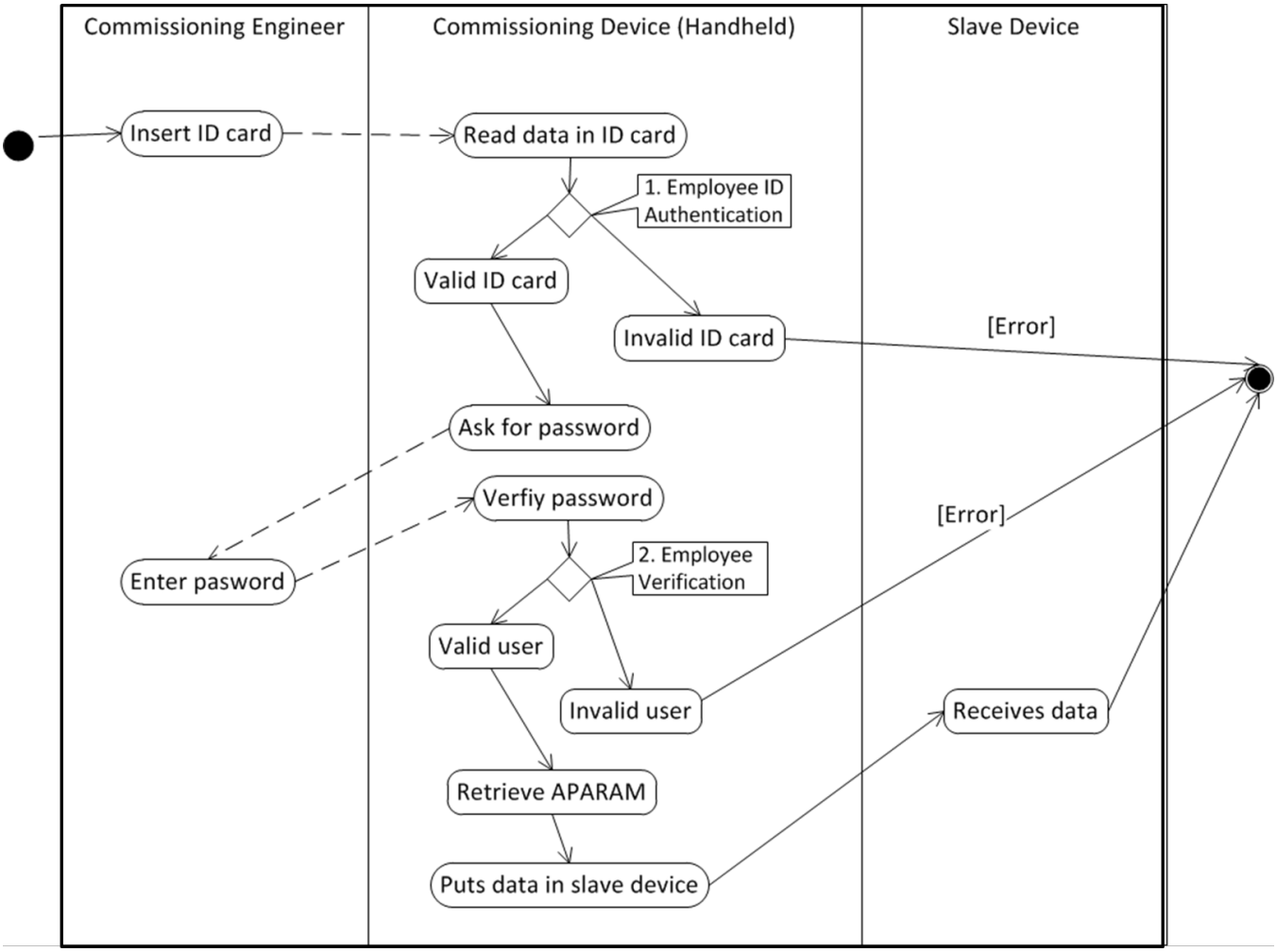

Fig. 1. Proposed Workflow

Once the slave device is configured with its unique tagname, the slave device can upload this encrypted APARAM along with the identity of the slave device. Then the master device can verify that the device is properly commissioned by an authentic commissioning engineer and as well as the device is connected to the correct physical entity. Thus, it will be easier to map the tags automatically to the corresponding control applications. On the other hand, if the slave device is not commissioned with configuration data, the slave device can send encrypted network access data along with the certificate of employee. Once the master device verifies whether the device is commissioned by the trusted engineer and using trusted commissioning device, it can download the network configuration to the slave device. The master device can provide the necessary keys for further communication in the network also.

The following section presents the authentication mechanism employed in our proposed workflow.

ID card authentication: When the commissioning engineer swipes his ID card in the terminal of commissioning device, the commissioning device reads the certificate of the employee ($Cert_{EMP}$) and the certificates of the card ($Cert_{CARD}$).

$$\%Cert_{EMP}$$
$$IDCard \rightarrow HH : \{K_{pub(EMP)}\}_{K_{pr(EMS)}} \quad (1)$$
$$\%Cert_{CARD}$$
$$IDCard \rightarrow HH : \{K_{pub(CARD)}\}_{K_{pr(EMP)}} \quad (2)$$
$$IDCard \rightarrow HH : \{APARAM\}_{K_{pr(CARD)}} \quad (3)$$

$Cert_{EMP}$ contains the public key of the commissioning engineer $K_{pub(EMP)}$, signed by the private key of *Employee management system* $K_{pr(EMS)}$. Using the public key of *Employee management system* $K_{pub(EMS)}$ the commissioning device verifies that the card is issued by *Employee management system*.

$Cert_{CARD}$ contains the public key of the ID card $K_{pub(CARD)}$, signed by the private key of *EMP* $K_{pr(EMP)}$. Using the public key of *Employee* $K_{pub(EMP)}$ the commissioning device retrieves public key of the ID card.

Using the public key of the ID card $K_{pub(CARD)}$, the commissioning device also retrieves the authentication parameter (APARAM). This APARAM will be encrypted with the private

key of *Employee* $K_{pr(EMP)}$ to provide authenticity of the device commissioned by right employee.

Employee verification: For password verification, the commissioning device asks commissioning engineer to enter his password and the entered password is sent to the ID card encrypted under the public key of the card, $K_{pub(CARD)}$. The card reports success or failure based on the input received from the commissioning device. The card keeps a counter for each password try. It decrements the retry counter after every wrong retry. Once the allowed try is over, the card gets blocked and an alarm is sent to the *Employee management system*.

Network access verification: The master device verify the authenticity of the data $APARAM_{K_{pr(EMP)}}$ along with the identity of commissioning device. If those data are okay, the device is allowed to access the network. However, we can have two scenarios based on the network architecture.

In first scenario, the network architecture demands that the slave device will have to provide the basic identity (unique tag name) for control application mapping. This is common in traditional automation wired protocols, where the unique tag name is used for the device and every parameter needs to be manually checked prior to cold commissioning such that the right data is received and transmitted to the correct physical entity. The commissioning device provides the configuration data for the slave along with the encrypted APARAM with its own private key. The master device can verify the authenticity of the packet using the employee certificate and employee management system. Then the master device will know that the slave device is commissioned by an authentic personal and the device is connected to the correct physical entity.

In second scenario, the network architecture demands that the slave device will need to show the authenticity, and then the network parameters can be downloaded from the master. This is common in wireless protocols where the device with proper join key gets network access and the further communication happens based on the data downloaded from the master device. In this case, the master device verifies the encrypted APARAM with private key of employee and then the network related parameters are downloaded for further communication.

IV. Assessment of the initial trust establishment workflow

In this paper, we have proposed a workflow for efficient, user friendly device commissioning with the initial trust establishment. In this section we will consider whether this workflow suffice primarily the three objectives of device identification, device authentication and user friendliness, as mentioned earlier.

Device identification: In our proposed workflow of device commissioning with initial trust establishment, we can see that the commissioning engineer or maintenance engineer will have direct access to the devices while commissioning. Therefore, the engineer can verify that the device which is going to be deployed is not tampered. He can also check that the device is connected to the correct physical entity.

Device authentication: In addition to that, the hierarchical authentication mechanisms ensure that the trust from the employee is transferred to the industrial devices. When the trusted employee has correct ID and correct passcode, the certificate can be transferred to the device through the commissioning device. Therefore, the master device will know the device is commissioned by authorized person.

User friendliness: Moreover, this commissioning or maintenance does not need any extra time consuming steps. The commissioning or maintenance engineer will have their ID card. Therefore when any devices need to be configured, the engineer is required to use the commissioning device for swiping his ID card. The authentication for the card and employee is done based on asymmetric crpto.

As explained in [9], maintaining unique key or keys for slave devices from a central database is not recommended as it assumes strong security assumptions. In our workflow, we can see that in the commissioning phase, the commissioning engineer is not required to synchronize the security keys from server for each device. The commissioning engineer is not required to find out the information for specific device from a central server. Instead, using the ID card of the engineer, the device can be configured for network access. In maintenance phase also, the device can be taken out from the store room and using the commissioning device the trust of the employee will be transferred to the device without time consuming effort of manual device configuration.

In addition to that, this workflow also optionally supports the commissioning/ maintenance engineer to download the required configuration data in the device as well. As explained, if the plant infrastructure has a central database with the required tag-names for the devices to be commissioned, the commissioning device can download the information from there. In other scenario, the commissioning engineer enters manually the tag data according to the plant documentation as used in currently practice. Both the features have their own advantage or disadvantage. In first scenario the configuration data is downloaded from a central server. It improves consistency and reduces manual errors; however it limits the flexibility of adding new devices and requires an online server always. The second scenario of manual entry does not provide the consistency at the same level as the first scenario provides. However, it is good enough considering the current state of practice inside the plants. The commissioning device downloads the configuration data for the slave device along with encrypted APARAM (authentication parameter). If the configuration is not required to be uploaded to the slave device, the network access data is downloaded with encrypted APARAM. This provides a generic and protocol independent addressing scheme since protocol dependent parameters can be discovered based on the initial trust and its embedded discovery and the control parameters which were programmed. In addition to that, it enables automatic scanning of the network to know which the devices are commissioned and thus reduce the manual labor of finding the devices and verifying its identity. It improves the current practice, as today it takes

several persons over several days to verify if the devices are commissioned properly.

In our workflow, we have used commissioning device to read the data from the ID card of commissioning engineer. In near future, with the technology advancement, if the device which is going to be commissioned has capability to read the employee trust from the ID card of the employee and create network access request using the signed certificate of employee, this proposed workflow will be applicable to that scenario too. Therefore, this proposed approach has flexibility to adapt new technology innovation in future.

V. Conclusion and future work

The goal of this paper was to introduce how reusing the trust prevailed in the industrial plant between employees, the devices can get network access without any prior secret sharing. As pointed out in [9], an initial key which is going to be used in a key management system in industrial plant requires a trusted, or trusted and secured channel, which leads to a solution requirement of investing further how initial trust to the device can be distributed considering the plant environment.

In this paper, we have presented a workflow for initial trust establishment. We started by introducing the objectives of initial trust establishment workflow along with the system components and their assumptions. Then we proposed our workflow and assessed with the objectives of the workflow for initial trust establishment. It is found that the devices can be commissioned by a generic and protocol independent addressing scheme since protocol dependent parameters can be downloaded based on the initial trust. This workflow is flexible to optionally support the commissioning engineer to download the required configuration data in the device as well as during initial trust establishment. This step also has both the option of downloading the data from a central server or configure manually. Thus, it provides the adaptability of the workflow for different plant environment. This proposed workflow enables to automatically scan the network to know which devices are commissioned and thus reduce the manual labor of finding devices and verifying its identity. It improves the current practice, as today it takes several persons over several days to verify if the devices are commissioned properly. This workflow has also taken into consideration the technology advancement. In the proposed workflow, the commissioning device is used for the device configuration. In future, if the device itself has capability to read information from the employee card and create network access request, the same workflow can be reused.

As future work, we are planning to work on a detailed security analysis and the demonstrating the practicability of this workflow.

Acknowledgment

This work has been supported by the Swedish Knowledge Foundation (KKS) through ITS-EASY, Embedded Software and Systems Industrial Research School, affiliated with the School of Innovation, Design and Engineering (IDT) at Mälardalen University (MDH, Västerås, Sweden) as well as by the ABB Industrial Communication and Electronics Program.

References

[1] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," in *Technical Report 39, Digital Systems Research Center*, 1989.

[2] J. A. Clark and J. L. Jacob, "A survey of authentication protocol literature: Version 1.0," 1997.

[3] S. Camtepe, "Key distribution mechanisms for wireless sensor networks: a survey," Tech. Rep., 2005.

[4] Sun D-M; He B;, "Review of Key Management Mechanisms in Wireless Sensor Networks," *Acta Automatica Sinica 2006*, vol. 32, no. 6, 2006.

[5] H. Lee, Y. H. Kim, D. H. Lee, and J. Lim, "Classification of Key Management Schemes for Wireless Sensor Networks," in *The 2007 InternationalWorkshop on Application and Security service inWeb and pervAsive eNvironments (ASWAN 07)*, 2007, pp. 664–673.

[6] Y. Xiao, V. K. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway, "A survey of key management schemes in wireless sensor networks," *Computer Communications*, vol. 30, no. 11-12, pp. 2314–2341, Sep. 2007.

[7] A. Barati, M. Dehghan, H. Barati, and A. A. Mazreah, "Key Management Mechanisms in Wireless Sensor Networks," *2008 Second International Conference on Sensor Technologies and Applications (sensorcomm 2008)*, pp. 81–86, 2008.

[8] M. A. Simplício, Jr., P. S. L. M. Barreto, C. B. Margi, and T. C. M. B. Carvalho, "A survey on key management mechanisms for distributed wireless sensor networks," *Comput. Netw.*, vol. 54, no. 15, pp. 2591–2612, Oct. 2010.

[9] A. Ray, M. Björkman, J. Åkerberg, and M. Gidlund, "Initial key distribution for industrial wireless sensor networks," in *IEEE International Conference on Industrial Technology (ICIT 2013)*, February 2013.

[10] J. Åkerberg, M. Gidlund, T. Lennvall, J. Neander, and M. Björkman, "Integration of wirelesshart networks in distributed control systems using profinet io," in *8th IEEE International Conference on Industrial Informatics (INDIN)*, July 2010.