Initial Key Distribution for Industrial Wireless Sensor Networks

Apala Ray*†, Johan Åkerberg*†, Mikael Gidlund* and Mats Björkman†
*ABB AB; Corporate Research
Email: firstname.lastname@se.abb.com
†Mälardalen University; School of Innovation, Design, and Technology
Email: firstname.lastname@mdh.se

***Abstract*—In any security design, the initial secret distribution for further key management solution is a major step. In industrial wireless sensor networks also, initial bootstrapping of the trust in the system is a major concern. The plant can be assumed to be a closed system, where only authenticated and trusted users are allowed to enter. However, wireless being the broadcast medium, wireless devices need to validate their identity to join the networks. So, there is a need for importing some initial secret key to the devices, so that they can be authenticated during the joining process. The standards for Industrial Wireless Sensor Networks (WirelessHART, ISA100.11a) also have left to the user the initial distribution of the key for joining during device provisioning. In this paper, the current industry practice and the pre-requisite of key distribution in industrial wireless sensor networks is discussed and an outline is presented for future research directions.**

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

I. Introduction

Industrial Control Systems, which include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and Programmable Logic Controllers (PLC), are typically used in Process Industries like pulp and paper, water and wastewater, food and beverages, mining etc. Originally industrial control systems were built as stand-alone systems, where all the components were not fully connected with the outside world, so security had less attention. Over the last few years, companies have been moving towards fast and cost effective decisions based on up-to-date information about the plant and the process at the management level which results in increasing interconnection between different automation systems. Industrial communication systems have unique requirements of performance and reliability issues that are somewhat different from general information system security. The outputs of control systems have a direct impact on the physical environment which lead to safety issues of humans and production environments [1]. The Fig. 1 is an example of a generic industrial automation networks. The network architecture of an industrial automation system is based on a hierarchical topology system model. The bottom of this hierarchy is the *automation system network*, which consists of a *field network* and a *control network*. The network topologies across different industrial plants may vary as different plants may have different integration strategies based on the plant policies, but as of now the Industrial Wireless Sensor Networks are targeting the field network level.

Since wireless is a broadcast medium, the security challenges are higher in industrial wireless sensor networks compared to the wired field and control network in the industrial automation. Although the wireless standards for industrial plants such as WirelessHART [2] and ISA100.11a [3] consider the required security aspect in terms of authentication, message integrity, node authentication and key exchanges, they however do not have a mechanism for bootstrapping the initial trust in the system which is instead left to the user to decide what technology to use. The trust is if device *A* is communicating with device *B*, then device *A* should be sure that it is communicating with device *B*, not any other device *C* and vice versa. If a wired scenario is considered in an industrial plant, the devices get connected to the network with a wire and it can be assumed that only trusted devices will be allowed to connect with the wire. However in wireless scenarios, this trust assumption might not hold true as wireless devices do not need to be connected with particular wires to join the network where the devices can be authenticated. When a wireless device transmits, the transmitted packet is broadcasted on the wireless medium and therefore it is required to establish an trust explicitly at initial phase before allowing any device to join the network inside the plant.

The "initial key pre distribution" is a well-known problem and the solutions which are available are not optimal for industrial plant for the following reasons. First of all, the plant down time costs money and it is not acceptable to create a secure system which may require additional time to establish security and as a consequence stop production in plants. A typical paper mill has 30 to 50000 sensors and actuators and out-of-band initial trust bootstrapping with a handheld device is an additional burden. Last but not least, a commissioning and maintenance engineer is responsible for commissioning and startup phase at several plants, so it is a non-trivial task to find the physical devices that are spread over large areas and not always visible. In this paper, we have evaluated the requirements of existing "initial key pre distribution" mechanisms and the current industry practice of distributing the initial key to the wireless devices from a new perspective of practical industrial point of view. The objective is to help to bridge the gap between a theoretical

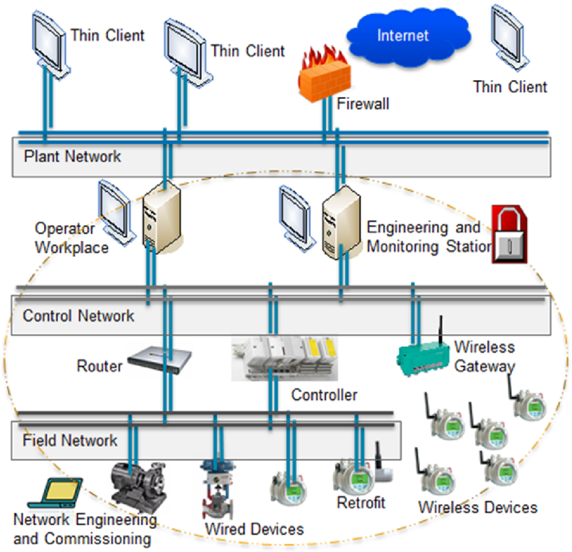

Fig. 1. Industrial Automation Network

approach and assumptions towards key distribution and its applicability in an industrial domain. In this paper, section 2 discusses the related work on key management. Then section 3 presents the industrial standard and the current practice of key distribution in Industrial Wireless Sensor Networks. Section 4 discusses the pre-requisite of key pre distribution solutions which can be applied in Industrial Wireless Sensor Networks. Section 5 describes the assessment of existing key distribution solutions for Industrial Wireless Sensor Networks. Finally, the conclusions are presented in section 6 and future work is outlined.

II. Related Work

The security issues in Industrial Wireless Sensor Networks have been extensively studied for the past few years and catering to the specific interest from Industries, WirelessHART [2], ISA100.11a [3] standards have been defined which also address the security issues in industrial plants. Those standards address security in terms of authentication, message integrity as well as node authentication and key exchanges. The WirelessHART and the ISA100.11a use the 128-bit Advance Encryption Standard (AES) encryption coupled with different keys depending on the layer of encryption. Those industrial standards utilize the security mechanisms included in the IEEE 802.15.4 [4] standard that ensures data integrity at the data link layer. The WirelessHART standard describes the roles of each security key however their management scheme is left to the users. In [5], security mechanisms provided by WirelessHART is also analyzed against well-known threats using a wireless medium. In [6], a survey focusing on security issues of the industrial standards by identifying potential attacks which could threaten the Industrial Wireless Sensor Networks and affect their operation is presented. In [7], a security analysis of WirelessHART, ISA 100 and ZigBee PRO has been done considering the critical aspect of supervisory control and data acquisition (SCADA) systems. In [8] security for industrial communication has been discussed in detail.

There are 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 [9], Camtepe and Yener covers 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 [10]–[14]. Generally it is shown in the surveys that that there is no one-size-fits-all solution for key distribution problems in Wireless Sensor Networks. There has been considerable work on key exchange on resource constrained sensor nodes based on public key cryptography also [15], [16]. The key distribution in Wireless Sensor Networks can be classified in different categories based on their application environment. In [17], existing key distribution scheme has been classified in five categories and security improvement of a hierarchical key distribution mechanism for large-scale Wireless Sensor Networks [18] has been shown. There has been some research done using the advantage of multi-path signal propagation as a source of randomness to generate secret keys [19]–[21]. In [22], a key deployment protocol using pair-wise ephemeral keys generated from physical layer information which subsequently enables an authenticated exchange of public keys has been shown. Each of the key distribution protocols has its own benefits and disadvantages, and moreover they can be suitable for particular application requirements. However, it is obvious 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 this paper, we will discuss the issues involved in the assumptions or pre-requisite of "key distribution" from an industrial perspective.

III. Industrial Standard and Current Practice on Key Management Workflow

In this section, the key management workflow for Industrial Automation Networks is presented in terms of Industrial Standard and Current Practice.

A. Key Management in WirelessHART standard

For industrial process automation and control systems, the WirelessHART standard, which is a mesh network communication protocol for wireless sensor networks, has been defined. Generally, in an automation plant involving wireless sensor networks, mainly the following types of system components are available [23].

The major component is the Gateway which has the capability of sending and receiving data with field devices. The gateway is a network device which has at least one interface like serial or ethernet to connect to the Engineering or Monitoring station or Operator Workplace. These gateway types of devices act as access points which connect Wireless Sensor Networks to industrial automation networks. The assumption for the gateway component is that the gateway should have connectivity with a component that can store and generate keys and the gateway is physically protected. The next components are sensors/devices which are connected to the processes in an Industrial Plant. They characterize or control the process and they are the producer and consumer of wireless packets in the Industrial Wireless Sensor Networks. The device can be battery powered or line powered. As per standard WirelessHART, there is another component called Handheld device which is used for out-of-band communication to distribute keys to sensors/devices. These are used in the installation, control, monitoring and maintenance of network devices.

For security, the WirelessHART standard has defined four security keys which help to ensure confidentiality and integrity both in Network and Media access control (MAC) levels. The security keys are Universal Key, Join Key, Network Key and Session Key. The standard describes the roles of each security key but their management scheme is left to the users. The following section describes how the joining process happens in the network.

1) Before the deployment phase, the device is pre-configured with a “Join Key”, which is used to verify whether the device is allowed to join the network.
2) The gateway transmits Advertisement Packets. The other devices which have already joined in the network also transmit Advertisement Packets, which are encrypted with a Universal Key.
3) The field device which is in the process of joining in the network, after booting up, listens to the Advertisement Packets from the Network.
4) When it finds some Advertisement Packet, it sends a “Join Me” request which is encrypted with the Join Key.
5) After receiving the Join request the gateway verifies whether the device has the correct key to join the network. When other active devices in the network receive the “Join” request, they forward the request to the gateway for authentication.
6) When the device is verified, the gateway adds the device to its active device list with its unique ID and allocates a Network Key and a Session key which will be used for further communication. The Network Key, which is common for a particular network, is used to generate the Message Integrity Code (MIC) of the network layer and the Session Key is a unique key between two devices only and it is generated by the network manager to encrypt critical data packets.
7) These Network and Session keys are managed by the gateway/ security or key manager and can be updated during the operational time of the plant as per security policies.

B. *Current Practice in Key Management*

Before discussing the current practices in key management, the major security objectives for an industrial plant are explained which provides a framework for categorizing and reviewing the issues involved in distributing an initial secret key to the devices in an industrial plant. The security objectives are:

- Availability: For Industrial Wireless Sensor Networks, during operational phase of plant life cycle, the data from the sensor devices should be available to the operator work place or engineering or monitoring station within the update period as fixed by industrial application. Also during the maintenance phase of the plant life cycle, if a device needs to be replaced, the downtime should not be more compared to normal replacement time.
- Data integrity: For Industrial Wireless Sensor Networks, sensor values or control commands should be protected against undetected modification of information by unauthorized persons or systems, which implies that it should not be possible to tamper with the data communication between device/sensor to gateway and gateway to sensor device.
- Confidentiality: The information should not be disclosed to unauthorized persons or systems. The data should be encrypted such that no one should be able to read the content of the message that is transmitted in the wireless networks.
- Authentication: Authentication is related to determining the true identity of communicating parties. In Industrial Wireless Sensor Networks, the sensor device should receive data only from authenticated devices and vice versa.

Though as per the WirelessHART or ISA100a standard, the initial key management scheme can be chosen by the users but as per normal practice in industry, the key management is based on key pre-distribution. There are two different scenarios for key pre-distribution. The first scenario is related to Green Field which corresponds to a plant where the infrastructure is newly built and the wireless devices need to be installed in the plant. To create a network, the field devices are required to be joined with the wireless gateway which has connectivity to the upper level of the Industrial Network. For this, the devices are pre-configured with a “Key” for initial bootstrapping. This key is used to verify whether the devices are allowed to join in the network and both the Gateway and the device or devices should have the same key.

The second scenario is related to device replacement. When a field device breaks down in a plant at odd hours, it is required to be replaced immediately with a new device so that the plant activity can resume quickly. The normal practice to replace a device is that the device which is going to replace the broken device is taken out from the store room and the operator has the correct “Key” for initial bootstrapping. The new field device is configured with the “Key” for initial bootstrapping. The operator configures the device so that it will do the same work as the broken device was supposed to do. The gateway may check whether the new device is a replacement of an existing device.

In the existing scenario for WirelessHART, symmetric key cryptography is used where the secret key is required to be shared between the device and the gateway prior to the communication. Here, the key distribution in both cases is normally done through an out-of-band channel. One of the ways key distribution can be done is through the serial port of the device or using Frequency Shift Keying (FSK) modem through a handheld device. When out-of-band communication is used for initial key distribution, the device which is going to be used as the out-of-band option and the device which is going to be commissioned, should maintain a secured connectivity so that an attacker cannot listen, inject, or capture packets during the process.

Now every device in the same network can have a unique or same initial key for bootstrapping. In the first case, there will be a unique initial key for bootstrapping of every device in the network and every device will be configured with a unique key and the gateway/key manager should generate and maintain individual keys for every device in the network. The gateway should also have a list of keys for every device along with their unique identity. The device which is used for out-of-band key distribution should also have a list of keys corresponding to the device. The gateway/key manager will be responsible for maintaining the old keys which has become compromised, so that the same key is not used in future. The gateway/key manager is also responsible for updating keys if some keys are leaked. The gateway/key manager itself must be secured to keep all the keys secret.

In the second case there will be the same initial key for bootstrapping of every device in the same network. In this case, any device which is going to be part of that particular network will be configured with the same key. The gateway/key manager should generate and maintain this initial key.

IV. Assessment of current practice key distribution in Industrial Wireless Sensor Networks

This section assesses the current industry practice and standard state-of-the-art approach of key distribution in an Industrial Wireless Sensor Networks. As mentioned earlier, the major expectation of industries for wireless sensor networks is the availability of the plant. The data from the sensor devices should be available to the operator work place or engineering or monitoring station within the update period as outlined by the industrial application. Also during the maintenance phase of the plant life cycle, if a device needs to be replaced, the downtime should not be more compared to the normal replacement time. Similarly, when a new sensor device is being introduced, minimal manual intervention is expected. Therefore, once one device is compromised, it should not take more time to detect and remove the device from the system compared to the current practice. The compromise of one or a small group of devices should not require the entire system to upgrade its security credentials and at the same time the system downtime should not be high due to compromising one or a small set of sensor devices. However, in reality the state-of-the-art initial key distribution does not pay enough attention to the use case of adding a new sensor device or exchange of a broken device inside a plant.

In the WirelessHART standard, the initial join key is symmetric and as per current practice the initial key can be used in two different scenarios. In the first scenario, every device will have an unique initial key for the network. In this scenario, during device replacement if the replaced device is a new device which has not yet configured to deploy in the plant, the downtime will be high. The reason is a new key for the device has to be generated, put in the gateway, and using out-of-band communication the device needs to be configured. In general, if there are many devices that need to be configured, the initial key distribution is a time consuming process because the current practice of using out-of-band communication is a serial process. The unique initial key needs to be stored in the Gateway also. Therefore before deploying the device inside the plant, it needs an extra manual step to configure the gateway with the initial key of the device. However, considering the security property in the initial network bootstrapping, the system resilience is acceptable when one device is compromised. Then the entire system will not be compromised as the network will not accept any new device unless it has a unique initial key for joining in the network. Therefore, if one device is compromised, only that device is required to be taken out and other field devices will not require any update. In addition, the leaking of a secret initial key will not affect the network as all the devices are expected to have a unique initial key. However an attacker can clone the compromised device and still send a packet.

In the second scenario, the same initial key is used for joining every device in the same network. In this scenario, the downtime may not be high as the device is required to be configured with a key which is used by all devices in the network. However the system resilience is too low as one device is compromised, the entire system will be compromised and all devices in the network will require a key update. Even though during device commissioning only concerned devices need to be configured with the initial key which could potentially make the workflow for the user easier but once a device is compromised, all the devices in the network have to be updated which will lead to downtime of the entire plant. In addition, if the initial key is compromised, the attacker can get access to the whole network because all the devices use the same initial key to join the network.

Though it is possible to use public key cryptography for setting up the key distribution, it is still expensive and slow compared to the symmetric key approach. Public key cryptography also requires large storage space as master device needs to maintain the public key of every slave device. However in symmetric key cryptography all the devices in the network can have the same key though it requires a strong security assumption and provides a weaker system resilience.

V. Key Distribution Pre-requisite and Assessment

This section classifies the existing key distribution mechanism based on encryption techniques and discusses the pre-requisite of key pre-distribution for wireless devices in Industrial Wireless Sensor Networks. In general, the Industrial Wireless Sensor Networks utilize the concept of shared key pre-distribution, so the design of security in an industrial plant requires an efficient way of distributing the initial secret key in the plant.

Normally, there are two types of algorithms which are used for encryption: Asymmetric Keys and Symmetric Keys. In each case, the goal is to fix an initial key between a master and a slave device. When the slave device needs to join a network which is managed by a master device, this secret key will be used by the master device to authenticate the slave device.

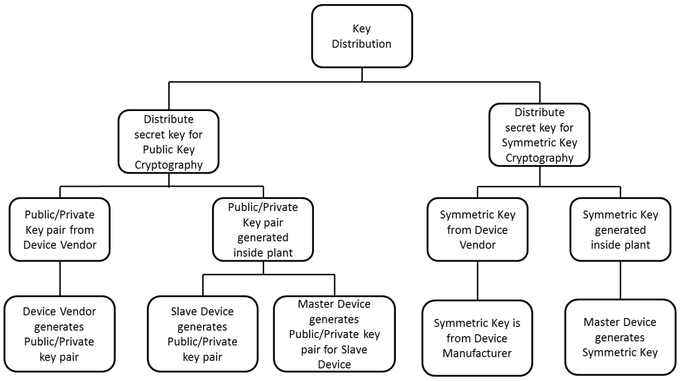
Key Distribution
Distribute secret key for Public Key Cryptography
Distribute secret key for Symmetric Key Cryptography
Public/Private Key pair from Device Vendor
Public/Private Key pair generated inside plant
Symmetric Key from Device Vendor
Symmetric Key generated inside plant
Device Vendor generates Public/Private key pair
Slave Device generates Public/Private key pair
Master Device generates Public/Private key pair for Slave Device
Symmetric Key is from Device Manufacturer
Master Device generates Symmetric Key

Fig. 2. Classification of Key Pre Distribution

When public key cryptography is used, the public key of the slave device needs to be shared with the master device and the private key of slave device is also required to be ported inside the device. When the symmetric key cryptography is used as a solution methodology, the initial symmetric secret key will be the symmetric key and this needs to be distributed between the master and the slave device or devices. From the classification shown in Fig. 2, we can group the initial key distribution in five possible ways.

1) Device Manufacturer generates Public/Private key pair
2) Slave device generates Public/Private key pair
3) Master Device generates Public/Private key pair for Slave Device
4) Symmetric Key is from Device Manufacturer
5) Master Device generates Symmetric Key

Fig 3. shows a generic algorithm for initial key distribution. The device manufactures is denoted as *DM*, master device is denoted as *M* and the slave device is denoted as *S*.

```
procedure InitialKeyDeployment
    if Asymmetric Key based then
        if Key generated in manufacturing unit then
            % Scenario 1
            $DM \rightarrow S : K_{pr(S)}$ % Trusted and Secured
            $DM \rightarrow M : K_{pub(S)}$ % Trusted
        else if Key generated in plant then
            if Slave Device generates then
                % Scenario 2
                $S \rightarrow M : K_{pub(S)}$ % Trusted
            else if Master Device generates then
                % Scenario 3
                $M \rightarrow S : K_{pr(S)}$ % Trusted and Secured
                $M \rightarrow S : K_{pub(S)}$ % Trusted
            end if
        end if
        $S \rightarrow M : \{JoinRequest\}_{K_{pr(S)}}$
        $M \rightarrow S : \{KeyEstablishment\}_{K_{pub(S)}}$
    else if Symmetric Key based then
        if Key generated in manufacturing unit then
            % Scenario 4
            $DM \rightarrow S : K_{MS}$ % Trusted and Secured
            $DM \rightarrow M : K_{MS}$ % Trusted and Secured
        else if Key generated in plant then
            % Scenario 5
            $M \rightarrow S : K_{MS}$ % Trusted and Secured
        end if
        $S \rightarrow M : \{JoinRequest\}_{K_{MS}}$
        $M \rightarrow S : \{KeyEstablishment\}_{K_{MS}}$
    end if
end procedure
```

Fig. 3. Pre-requisite of Initial Key Deployment

The *Trusted Channel* is the medium where communicating parties are authenticated, though the transmitting messages can be public. The *Secured Channel* is the medium where no one can hear the exchanged messages except communicating parties. From the algorithm we can see that in scenario 1, the private key of the slave device $K_{pr(S)}$ is stored within the device during manufacturing using *trusted and secured channel* and when the device is brought to the plant the public key of it $K_{pub(S)}$ is given to the master device using a *trusted channel*. In scenario 2, the slave device computes public-private key pair, stores private key $K_{pr(S)}$ within itself and transmits its public key $K_{pr(S)}$ to the master device. During scenario 3, the master device generates the public/private key pair for the slave device. The private key of the slave device $K_{pr(S)}$ is stored inside the device using a *trusted and secured channel* and the private key of the slave device $K_{pub(S)}$ is stored inside the device using a *trusted channel*. In scenario 4 the Symmetric Key of the slave device K_{MS} is stored within the device during manufacturing using *trusted and secured channel* and when the device is brought to the plant this symmetric key K_{MS} is given to the master device using *trusted and secured channel*. In scenario 5 the Symmetric Key of the slave device K_{MS} is stored within the device by the master device using *trusted and secured channel*. Therefore, it can be seen that given any key distribution mechanism the primary requirement is to establish a trusted channel inside that plant. When the device is brought inside the plant, it is required to be identified as the original device before connected to the network.

VI. Conclusion and Future Work

The key management in Wireless Sensor Networks have been studied for a long time though there are still open issues which need to be investigated further. In this paper, we have identified the possible solutions and issues of distributing initial keys to an industrial plant network. It is found that a initial key which is going to be used in a key management system requires a trusted, or trusted and secured channel. In symmetric key cryptography, there is a need for a trusted and secured channel where no one can listen when the initial key is going to be distributed. In public key cryptography, there is a need for only a trusted channel when the public key is transmitted between two communicating parties. However, when the private-public key pair is generated from a central security server inside the plant, there is also a requirement of a secured channel where no one can listen. On the other hand, if the vendor puts the secret key in the device during manufacturing, there is a risk of failure if the keys are required to be updated by security policies and in similar way a trusted channel is required to be established. We have also discussed the current practice in industrial plants where the symmetric key is used and pointed out that it will be difficult for any plant to distribute the initial secret as it will be time consuming and need a secured infrastructure to distribute keys. This leads to a solution requirement of investing further how initial trust to the device can be distributed considering the plant environment. If we consider the scenario of distributing the initial key by utilizing the unique identity of the device, or wireless channel characteristic, it might be possible to have a solution for initial trust establishment in the plant. Moreover, the existence of a generic key manager in a plant environment might help to maintain a unique policy in the plant. Such scenarios will be considered in our future work in this area.

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, Västrås, Sweden) as well as by the ABB Industrial Communication and Electronics Program.

References

[1] K. A. Stouffer, J. A. Falco, and K. A. Scarfone, “Guide to industrial control systems (ics) security,” Gaithersburg, MD, United States, Tech. Rep., 2011.

[2] *HART Communication Foundation (HCF)*, Std. [Online]. Available: http://www.hartcomm2.org/index.html

[3] *An ISA Standard Wireless systems for i ndustrial automation: Process control and related applications*, ISA Std. ISA-100.11a-2009, 2009.

[4] *Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (LR-WPANs)*, IEEE Computer Society Std. 802.15.4, 2007.

[5] S. Raza, A. Slabbert, T. Voigt, and K. Landerns, “Security considerations for the wirelesshart protocol,” in *International Conference on Emerging Technologies and Factory Automation (ETFA 2009)*, Mallorca, Spain, sep 2009.

[6] D. Christin, P. S. Mogre, and M. Hollick, “Survey on wireless sensor network technologies for industrial automation: The security and quality of service perspectives,” *Etude de la notion de pile application l’analyse syntaxique.*, pp. 96–125, 2010.

[7] C. Alcaraz and J. Lopez, “A security analysis for wireless sensor mesh networks in highly critical systems,” *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on*, vol. 40, no. 4, pp. 419 –428, july 2010.

[8] D. Dzung, M. Naedele, T. P. V. Hoff, and M. Crecatin, “Security for industrial communication systems,” *Proceedings of the IEEE,*, vol. 93, no. 6, pp. 1152–1177, 2005.

[9] S. Camtepe, “Key distribution mechanisms for wireless sensor networks: a survey,” Tech. Rep., 2005.

[10] Sun D-M; He B;, “Review of Key Management Mechanisms in Wireless Sensor Networks,” *Review of key management mechanisms in wireless sensor networks. Acta Automatica Sinica 2006*, vol. 32, no. 6, 2006.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] D. J. Malan, M. Welsh, and M. D. Smith, “A public-key infrastructure for key distribution in tinyos based on elliptic curve cryptography,” in *IEEE Sensor and Ad Hoc Communications and Networks (SECON 2004)*, 2004.

[16] G. Gaubatz, J. P. Kaps, and B. Sunar, “Public key cryptography in sensor networks,” in *1st European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS 2004)*, 2004.

[17] K. Xue, P. Hong, H. Lu, B. Zhu, and L. Li, “Security improvement on an efficient key distribution mechanism for large-scale wireless sensor network,” in *Anti-counterfeiting, Security and Identification, 2008. ASID 2008. 2nd International Conference on*, aug. 2008, pp. 140 –143.

[18] Y. Cheng and D. P. Agrawal, “An improved key distribution mechanism for large-scale hierarchical wireless sensor networks,” *Ad Hoc Networks*, vol. 5, no. 1, pp. 35 – 48, 2007.

[19] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, “Radio-telepathy: extracting a secret key from an unauthenticated wireless channel,” in *Proceedings of the 14th ACM international conference on Mobile computing and networking*, ser. MobiCom ’08. New York, NY, USA: ACM, 2008, pp. 128–139.

[20] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, “On the effectiveness of secret key extraction from wireless signal strength in real environments,” in *Proceedings of the 15th annual international conference on Mobile computing and networking*, ser. MobiCom ’09. New York, NY, USA: ACM, 2009, pp. 321–332.

[21] M. Wilhelm, I. Martinovic, and J. B. Schmitt, “Secret keys from entangled sensor motes: implementation and analysis,” in *Proceedings of the third ACM conference on Wireless network security*, ser. WiSec ’10. New York, NY, USA: ACM, 2010, pp. 139–144.

[22] M. Wilhelm, I. Martinovic, E. Uzun, and J. B. Schmitt, “SUDOKU: Secure and usable deployment of keys on wireless sensors,” in *Proceedings of the 6th Annual Workshop on Secure Network Protocols (NPSec ’10).* IEEE, oct 2010, pp. 1–6.

[23] *WirelessHART Device Specification - HCF SPEC-290*, HART Communication Foundation (HCF) Std. Revision 1.1, May 2008.