Journal of Polish Safety and Reliability Association
Summer Safety and Reliability Seminars, Volume 5, Number 1, 2014

Porzeziński Michał
Gdansk University of Technology, Gdansk, Poland

The methods of secure data transmission in the KNX system

Keywords

security, KNX system, secure data transmission

Abstract

The article presents the demands concerning data security in distributed building automation systems and shows the need for providing additional mechanisms of secure communication in the KNX system. Three different methods developed for KNX data protection are discussed: EIBsec, KNX Data Security and the author's method. Their properties are compared and potential areas of application are presented.

1. Introduction

During last years a rapid increase in popularity of the home and building automation systems has been observed. The building automation systems are usually developed as distributed systems whose components, such as sensors and actuators, communicate with each other via a data network to carry out specific functions (*Figure 1*).

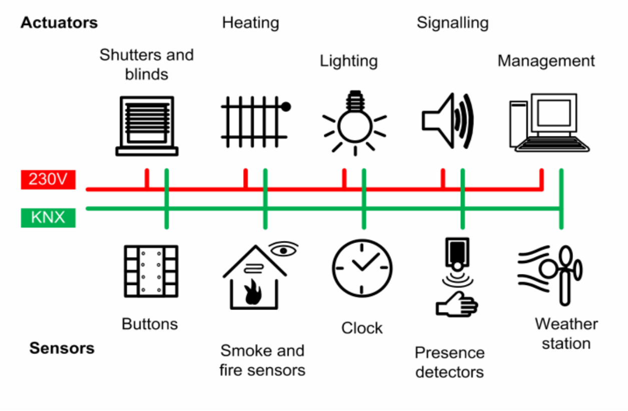

Figure 1. The idea of distributed building automation system.

Typical areas of building automation application are: lighting control, temperature control, air-conditioning and remote management [7]. These systems are successfully used for many years and they are sufficiently reliable to perform those functions.

Much greater demands are placed on systems implementing safety-related functions, such as Fire Alarm System, System Intrusion and Access Control System. They must be resistant not only to random disturbances, but also for the intentional attacks of third parties who want to disrupt their operation.

In order to allow the integration of these safety-related elements with existing building automation systems, it is necessary to use special mechanisms to protect transmitted data at the level of communication protocols.

Unfortunately, most of the existing building automation standards does not have such mechanisms or they are very weak [2]. The analyses carried out show that currently one of the most vulnerable to attacks building automation system is the KNX system [2].

This has contributed to the development of several methods to increase the security of the data transmitted in the KNX network. These methods and their limitations are analyzed in this article. They are compared to the author’s method which was developed to protect data transmitted from selected sensors to the building supervisory system.

2. The security demands

Regarding the functionality of the building automation systems the following general objectives of secure transmission channel can be formulated:

- data confidentiality,
- data integrity/authenticity,
- data freshness.

The data confidentiality requirement means that only authorized person should be able to read their original value.

The data integrity/authenticity requirement implies the presence of mechanisms for ensuring that the received information comes from a trusted sender and that the data has not been modified.

The verification of data freshness is needed for preventing the use of previously recorded data in the future. This verification is particularly important in industrial networks being applied to transmit control information. In such unprotected network the previously recorded data could be injected to the network to induce undesirable action.

Compliance with these requirements may be achieved by applying appropriate cryptographic algorithms such as encryption algorithms and hash functions based on the secret keys in combination with additional information such as a timestamp or sequence numbers to allow the data freshness verification.

The selection of appropriate algorithms is largely dependent on the communications protocols used in the network and its bandwidth. Usually the use of standard methods of data protection such as: SSL/TSL or IPsec is not possible due to connectionless multicast communication used in building automation system networks and due to the limited size of data frames. A big challenge is also to enable conflict-free coexistence the devices requiring protection of information and the standard devices in a single network.

For the building automation networks the ISO/IEC 24767-2 [5] standard can be used to select the appropriate methods of data protection. However, it does not specify the details of security algorithms, which must be tailored to the specifics of the communication protocol.

3. The KNX standard

The KNX is a distributed building automation system standard managed by the KNX Association based in Brussels [4]. It is the continuation of a previous standard originally developed at Siemens and known as the European Installation Bus (EIB). Currently, it is the international standard ISO/IEC 14543-3 also published as the European standards EN 50090 and EN 13321.

The KNX system consists of modules performing the typical building automation functions and communicating each other using one of the approved by KNX communication media (TP10, PL110, RF, KNX/IP).

The most common communication medium is a twisted-pair (TP10) which is used simultaneously to supply low power KNX devices such as push buttons modules and sensors. The data are transmitted between nodes as a sequence of bits in the form of so-called telegram shown in *Figure 2.*

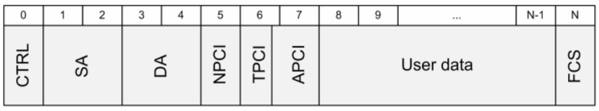

Figure 2. The structure of the KNX telegram.

CTRL is the control field which decides also about the priority of the telegram. SA and DA are respectively 2-octet sender address and destination address. Next fields are: the control information field associated with the transport layer (TCPI), the application layer control field (ACPI) and the User data. At the end of the message the frame check sequence (FCS) is attached. The maximum telegram length is 23 octets. It means that the maximum size of the user data is 14 octets. The latest version of the KNX standard (2.1) also provides the ability to use the extended frame, which can carry up to 254 bytes, but as yet it is not widely used.

The same telegram structure is used both during group (multicast) communication and during connection-oriented (unicast) communication.

Connection-oriented communication is used mainly for remote configuration of KNX modules. In this mode of communication, it is necessary to establish earlier a logical session between the nodes exchanging data. During this operation a 4-octet authorization code can be send, which should be verified by receiver. However, this code is sent in plain text, which is a major weakness of this security. The attacker who intercepts the authorization code is able to change the configuration and even delete the application program of any module.

KNX group communication is essentially an event driven unidirectional communication. It allows KNX modules to transmit the information about their communication objects status changes. Although the acknowledgment of receipt of the telegram is generated, but this is done only at the data link layer and the application layer does not take part in this process. This mode does not provide any security mechanisms. The telegram of any content can be send by using commonly available diagnostic software, which means the possibility of controlling any KNX device.

It follows that the KNX standard does not offer any mechanisms to guarantee data confidentiality, data integrity nor data freshness. This justifies the need to develop additional security mechanisms to protect data transmitted in the KNX bus.

4. The methods of secure communications in KNX network

The proposals of three different methods which meet the demands of the KNX network data security are presented below. The description is focused on the method of securing the data transmitted in group communication mode, which is the KNX network primary communication mode.

4.1. The EIBsec protocol

EIBsec protocol is the first protocol which has been developed to eliminate the security weaknesses of the standard KNX/EIB protocol [3]. For data encryption the well-known symmetric encryption algorithm AES (Advanced Encryption Standard) is used. Moreover, it is assumed that each network segment contains a special device called ACU (Advanced Coupler Unit) which performs active role in the process of session establishment and group key retrieval [3]. In case of the group communication mode EIBsec protocol works in so-called counter mode, shown in *Figure 3*.

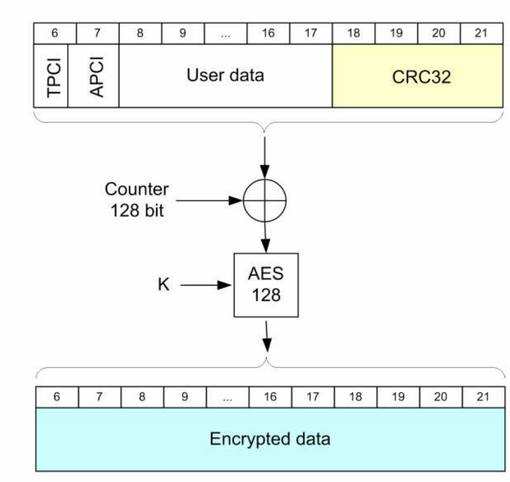

Figure 3. Encryption in EIBsec method

White background means plain text. Yellow background means plain text specific for the security method and blue background the encrypted data.
The only 10 octets of user data can be used in this method. The last 4 octets contain the CRC32 checksum [6] calculated over the plain text of user data. The message block is XOR-ed with counter value and encrypted using 128-bit AES algorithm. Counter is used to provide protection against replay attacks and is incremented after each transmission.
The recipient of information makes the reverse operation: decrypts the transmitted block, performs XOR operation with its own local counter and verifies the checksum CRC32. If the CRC sequence is correct receiver accepts data and increments its own counter. If the counters lose synchronization due to a loss of previous message a small number of counter variations can be tested. If the approach fails, the current counter value must be retrieved from the ACU.
The presented method allows the co-existence in one network both standard devices and devices using the EIBsec protocol. Unfortunately, encrypting the TCPI and ACPI fields causes the telegrams EIBsec will not be properly processed by the standard KNX protocol stack and existing diagnostic tools. The other limitation of this method is the need of use the ACU in each KNX network segment. Another problem is the communication of devices belonging to different network segment that requires the mutual cooperation of both ACU.

4.2. The KNX Data Security protocol

Another method, which has been recently presented by the KNX Association as a draft of the KNX standard is the KNX Data Security protocol [1]. The idea of its security mechanism is shown in *Figure 4*.

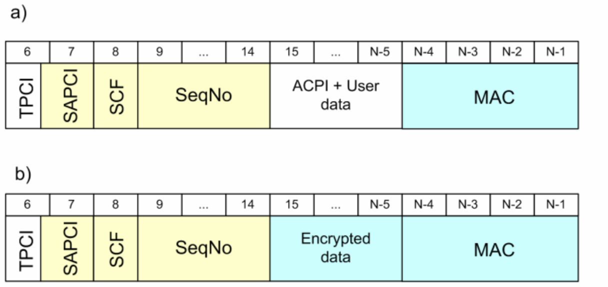

Figure 4. Data frames of the KNX Data Security protocol

There are two modes of operation: a) with data authentication only and b) with data authentication and confidentiality. SAPCI and SCF are the control fields with the information about security method. The SeqNo is 6-octet sequence number used for data freshness verification. MAC is the Message Authentication Code. To calculate the MAC value the CCM [8] method is used, which combines the CBC-MAC [10] authentication method with CTR-AES cipher using the same encryption key. Details of the algorithm are presented in [1]. Depending on the selected mode only the the MAC value is calculated or user data field is also encrypted.
The advantages of this method are: the possibility of transmission telegrams of varying data length and encapsulating complete APDU frames. However, the very small size of the user data field (2 octets in case of using standard frame) and complex encryption algorithm may be a limitation of this method.

4.2. The Author's method

The Author's method of secure data transmission in the KNX network has been developed for remote monitoring system and has been presented in [9].

The conception of this method is shown in *Figure 5*.

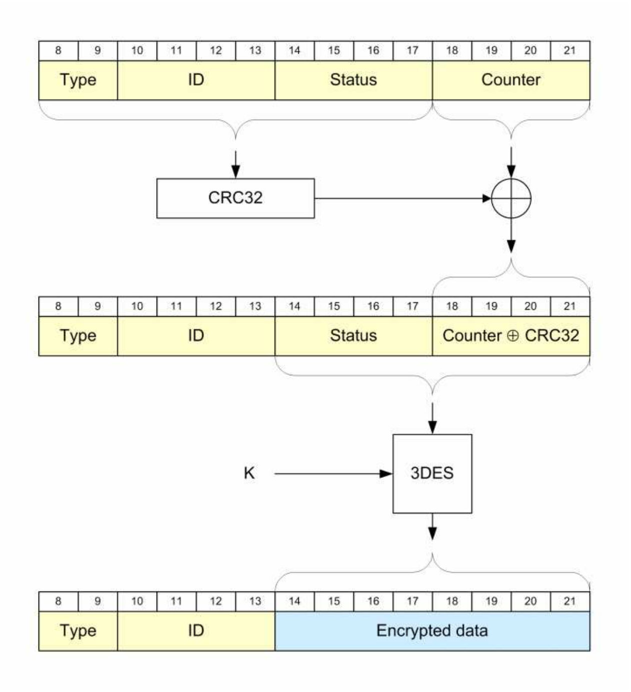

Figure 5. The Author's method of secure data transmission

Secured information is sent as a single 14-octet block of data. The Type field determines the format of the message. The ID is a 32-bit identifier of the sender, which allows its identification and is independent of the KNX address. This identifier, which is sent in plain text, allows the receiver to select the encryption key needed to decrypt the rest of the message.

The next 32-bit field contains the status of the sensor forwarded to the monitoring station. This field may be e.g. the 32-bit floating point number containing the measurement result or the set of alarm bits. The last field is 32-bit counter used for verifying the freshness of data. The counter is XOR-ed with the CRC32 signature calculated over the first 10 octets of the message. Then the last eight octets, containing the Status filed and XOR-ed Counter field, are encrypted using 3DES algorithm.

The KNX node being the recipient of the message shall reverse the process. It finds the appropriate cryptographic key on the basis of received ID and makes decrypting the cryptogram. Then the CRC32 signature is calculated which allows getting the initial value of the counter. Packets can be accepted if the resulting counter value is equal to the local counter value. Then the local counter is incremented so that the receiver is synchronized with the sender.

If the telegram does not reach the destination due to noise or transmission interferences the counters can lose the synchronization. In this case it is possible to restore the synchronization after receiving two consecutive telegrams with counter value higher than the local counter value.

The main advantage of proposed method is using the standard KNX data type (DPPT 16) which allows placing the security layer above the application layer of the KNX protocol stack.

Thanks to above the commercially available ready-made components and software libraries can be used without any change. The added layer can also act as a safety layer which perform additional data checking required by the PN-EN 61784-3 standard.

5. Conclusion

The developed methods of secure data transmission are the response to the lack of sufficient security mechanisms in the standard KNX protocol.

The proposed EIBsec and KNX Data Security methods are comprehensive methods which can be used for securing most of the KNX data transfers. However, both require modifications to the KNX protocol stack below the application layer. For this reason it is not possible to use a standard KNX stack in devices which require such secure data transmission. This probably will change when the KNX Data Security protocol becomes the KNX standard and a new certified stacks are developed.

In Author's method the additional security layer is placed above the application layer of the standard KNX stack and the standard KNX data type is used for protecting data transmission. Thus, the method is not suitable for protecting all data exchanged during the KNX system operation. However, it may be successfully used for securing the data exchanged between dedicated sensors and supervisory system. Thanks to this it is possible to use standard KNX components and standard KNX diagnostic tools. The added layer can also be used as a safety layer in the sense of PN-EN 61784-3 standard enabling the fulfillment of formal requirements for systems performing safety-related functions.

References

[1] Application Note 158/13 v02 (2013), KNX Standard v.2.1. KNX Association.

[2] Granzer, W. & Kastner, W. (2010). Security Analysis of Open Building Automation Systems. *Proc. 29th International Conference on Computer Safety, Reliability and Security (SAFECOMP '10)*, 303-316.

[3] Granzer, W., Kastner, W., Neugschwandtner, G. & Praus, F. (2006). Security in networked building automation systems. *Proc. WFCS*, 283–292

[4] http://www.knx.org (2014). The official webpage of the KNX Association.

[5] ISO/IEC 24767-2 (2009). Home network security/Secure communication protocol middleware (SCPM)

[6] Koopman, P. (2002). 32-bit cyclic redundancy codes for internet applications, *Int. Conf. Dependable Systems and Networks (DSN)*, Washington DC, 459-468.

[7] Merz, H., Hansemann, T. & Hubner, C. (2009). Building Automation. Communication Systems with EIB/KNX, LON and BACnet. *Springer Series on Signals and Communication Technology*.

[8] NIST SP 800-38C (2004). Recommendation for Block Cipher modes of Operation: The CCM Mode for Authentication and Confidentiality

[9] Porzeziński, M. (2013). Koncepcja metody bezpiecznej transmisji danych w sieci KNX na potrzeby systemu nadzoru. *PAR* 10, 96-101

[10] RFC 3610 (2003). Counter with CBC-MAC (CCM)