CEO WORLDWIDE
CONNECTING YOU WITH THE BEST CERTIFIED TALENT ON THE PLANET.

CEO Worldwide White Paper

The security challenges of the Industrial IOT Wireless Networks.

Didier Guiraud - Smart N Secure

Abstract

This paper will illustrate how important it is to ensure a very high level of security within all the upcoming Industrial IOT Wireless networks. It represents an absolute necessity that requires to be shared and understood at the highest executive levels of the Solution Providers and of all the Industrial Users.

These networks already are and will be more and more characterized by the need to implement bi-directional communications between devices without any human support or any access to any Server and/or Gateway/Data Concentrator Unit. This is setting up a huge difference in term of security architecture versus more traditional point-to-point or point-to-multipoint communications, alike the cellular communications that already are very well secured in case of sensitive transmissions or receptions, such as money transfers or cellular phone subscription management.

The Mesh communication architecture is one of the most promising to manage these IOT challenges mostly with bi-directional communications between devices independently from any external interactions. On top of that, each device (or node) of such Mesh Network is a relay for its direct neighbors during the transmissions or the receptions; the communications go from one node to the targeted node "hoping" from one neighbor node to the following one in order to cover the necessary distance and to ensure a very robust communication.

We will see that such Mesh network architecture, together with all its highly interesting capabilities, is also bringing numerous new challenges in terms of data and network securities. We will then observe how the new technologies enable the most comprehensive way to deal with each of those security weaknesses in order to facilitate a large deployment of such Industrial IOT solutions with a total security guaranteed.

Introduction and Problem Statement

The deployment of the Internet of Things in the Industry has been a reality for more than 10 years already and, each year several hundreds of millions of industrial "things" with an IP address are deployed worldwide for process automation, Smart Grid applications and for all those new areas in which the future of IOT will appear to be as broad as the Smart Cities and the Smart Health Care. However, all the smart nodes are so far essentially using a cellular communication solution analogous to the one used by your Smart phone. Hence, although it is a significantly mature technology, its point-to-multipoint approach is strongly limiting the "direct" node-to-node communication since all communications first need to reach a sever before being redirected to the targeted reception node.

Additionally, even if the security of such communications is now soundly managed, this architecture is suitable to connect a few points per concentrator and is not low power at all. The Mesh network architecture is adequate to connect thousands of points together independently from any external support or any interaction and is perfect to manage very low power operations, thus presenting a very important aspect of all the Node-to-Node or Machine-to-Machine applications.

State of the Art for security implementation

As mentioned above, most of the existing solutions are mainly extrapolated from what has been used for more than 20 years with the point-to-multipoint cellular phones or with the chip banking cards. These communication technologies work with systematic server control for any action and all the "intelligence" to ensure security of the network, to detect attacks and to neutralize them is localized at that server level. This system is operating correctly in these specific networks, but is power consuming, has a lot of latency and does not allow direct bi-directional communications between two nodes (devices) within the Network. That last configuration of node-to-node communication is occurring with no contact with the gateway nor with the server, and that is the main dimension of the Internet of Things which is going to be implemented for millions of nodes within thousands of Mesh networks in the Industry 4.0 world.

In most of all the existing solutions, each node is configured to provide data according to a specific duty cycle, often very light and neither has a lot of processing power nor a lot of memory space, as each node does operate as the "slave" of the server with or without the relay of any gateway.

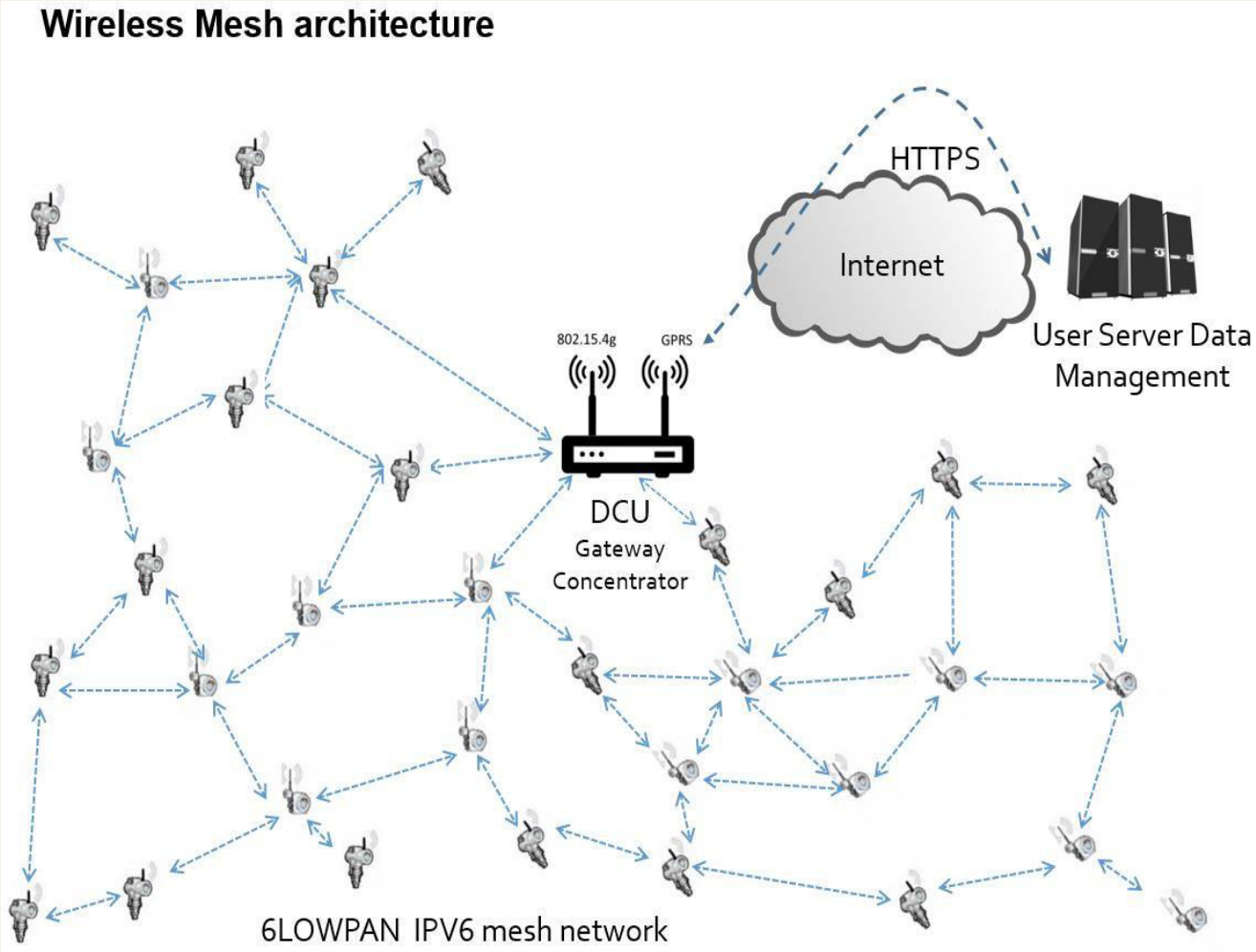
Besides, only the classical point-to-point type of Network attacks is pre-registered, and such Networks do not have any adequate defense against "smart" and/or "insider" attacks and it clearly does not have any way to manage them, before they could jeopardize the entire Network.

Necessary Security Solutions in case of real direct and bi-directional Node-to-Node wireless communications

The mesh topology provides a reliable and scalable network. Generally, each node of a mesh network is able to act as a relay to permit messages to "hop" from one node to another, where each node can directly or through "hops" communicate with another node of the mesh network. In this way, the nodes can be placed out of the range of the network gateway or concentrator. Nevertheless, this method requires sufficient intelligence (processor powers and memory sizes) in order to be able to manage those direct communications between nodes and the "hops" for all the neighbor nodes. We will also note that an important part of that intelligence must be able to manage efficiently and consistently all the security challenges of such a network.

Of course, in order to achieve that level of intelligence, with a minimum level of latency and a minimum level of power consumption, it is essential to use the most advanced wireless communication IEEE (Institute of Electrical and Electronics Engineers) standards, such as the Smart Utility Networks (802.15.4g) with efficient and modern RF modulations at the hardware level in combination with the most advanced IETF (Internet Engineering Task Force) software protocols such as 6LoWPAN, IPV6 and RPL.

CEO Worldwide White Paper



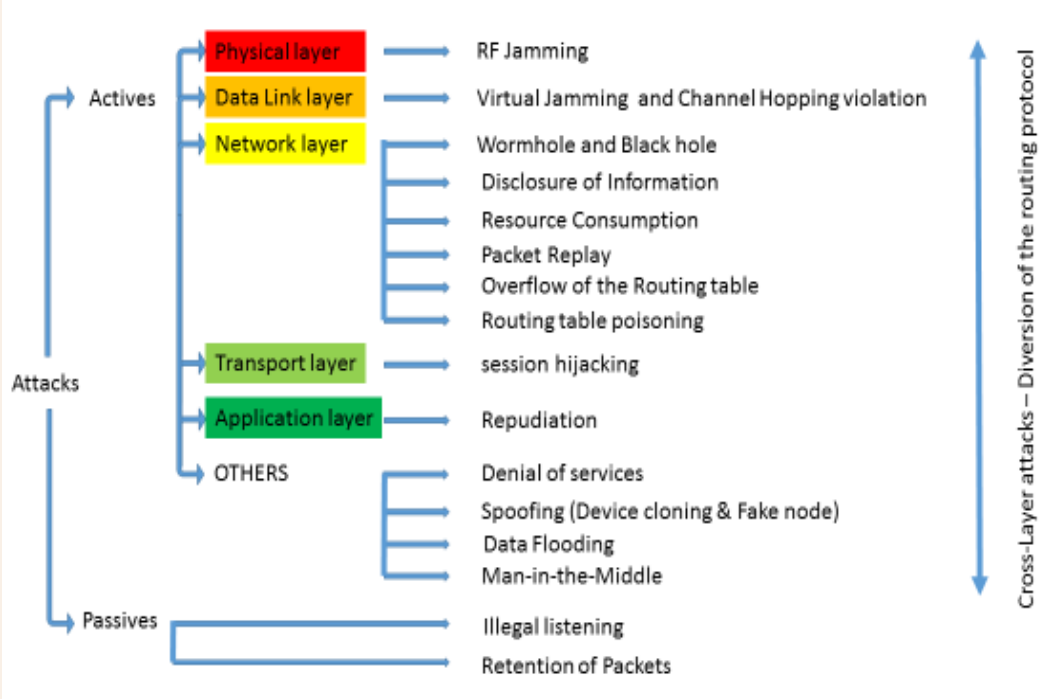
Potential Threats

In contemplation of understanding the large spectrum of potential attacks and/or threats that can jeopardize a wireless Mesh network, it is necessary to first have a notably high level view on the standard architecture to achieve any kind of communication between two nodes, which is called the ISO Model and which can be represented in a quite simplified way, as follows:

CEO Worldwide White Paper

OSI Layers			
Layers		Protocol data unit	Function
Host Layers	Application	Data	High-level Application Programming Interfaces, Translation between a networking service and an application, Managing communication sessions.
	Transport	Segment/Datagram	Reliable transmission of data segments between points on a network, including segmentation, acknowledgement and multiplexing.
Media Layers	Network	Packet	Structuring and managing a multi-nodes network, including addressing, routing and traffic control
	Data Link	Frame	Reliable transmission of data frames between two nodes connected by a physical layer
	Physical	Bit	Transmission and reception of raw bit streams over a physical medium

Having that in mind, it will be much easier to perceive the challenges arising from setting up a comprehensive security architecture for a wireless Mesh network **with the below exhaustive description of all potential attacks** (at least, until a new type of attack appears):



Written by Didier Guiraud, iCEO # 68831

Contact us! Phone: *+44 203 137 2581* Email: *search@ceo-worldwide.com*

Website: *www.ceo-worldwide.com*

CEO Worldwide Ltd - 9 Queen's Yard - White Post Lane, London E9 5EN, ENGLAND

Here, the goal is not to be familiar with each of these attacks but to get a clear understanding of their large spectrum, and that if only one of them is successful, the Mesh Network will at least work very slowly, and in the worst case, the same Mesh Network, could be used against its normal users.

As a matter of fact, a wireless Mesh network is not by construction a closed system, and the limitation of the trusted zone of such system cannot be traced with unbroken lines, due to the open nature of the wireless medium and to the operation of the connected nodes without human intervention.

At very high level, we will see below that a lot of technical solutions exist to secure such a network and that certain IETF initiatives are ongoing to provide stronger and smarter protections in front of always tougher and smarter attacks.

Yet it is clear that to build a secure system, security engineering should be incorporated into the system design process in its early stage. If the security concerns associated with the architecture are not addressed beforehand, the risk of future security issues, which are time consuming and costly to fix, is clear-cut.

Security Architecture

In order to get the full benefit of all the security developments done through those last ten years in the area of the securization of the wireless Mesh network by a large variety of actors (Large Enterprises, Start-UPs, Universities and State Laboratories…) under the global synchronization of the IEEE or the IETF, the wiser approach is to focus on all the Protocols in that area provided by IETF, by the NIST (National Institute of Standards and technologies) and by IEEE. As a matter of fact, we will subsequently see that all the technologies are available, correctly proven and, up to now, extremely efficient to guarantee the authentication, the integrity, the none-repudiation, the confidentiality, the authorization, and the availability, as well as an access control, a real time operation, a default tolerance and the relevant flexibility necessary all together for the management of a very efficient open system and in particular in all the advanced Industrial applications.

In the interest of building the optimal secured architecture to manage all the different attacks described above, the wireless Mesh Network security architecture is specified to use IETF-defined security and networking protocols for use with the Smart Utility Network IEEE standard based. The security architecture will cover the following security services:

- **Data encryption/decryption**
- **Authentication and key management**
- **Network access control**
- **Routing security**
- **Application-layer / Data security**

Data encryption/decryption

The use of an AES128,192 or 256 standard encryption algorithm is a must and most preferably that algorithm should be hardcoded in hardware so that its protection against hacking is significantly strengthened and the associated power consumption at the level of each node is substantially decreased.

Authentication and key management

The IEEE 802.1x standard is a much optimized solution to certify the security of a wireless Mesh architecture and to establish all the communication layers in the best secured way. This IEEE standard enables the authentication of all the nodes that are willing to join a Mesh network, using the EAP (Extensible Authentication Protocol) that allows the transportation of all the identification information of all the nodes in a strongly secured way, according to the Protocol for Carrying Authentication for Network Access (PANA).

Network key

The security of the network relies on the use of a random 16-byte (128 bits) network key delivered to the node after its successful authentication. The network key can be managed either by the authentication server or by the DCU. If the network key is managed by the authentication server, the network key can be distributed using a secure channel established to provide channel bindings. In optimized security architecture, the network key is managed by the DCU, and is delivered to the node using secure PANA payloads. The DCU is then responsible of the network key update and maintenance.

The network key is updated once the key expires, or once a network access is revoked to a node (forward secrecy). It may also be updated if a new device joins the network (back ward secrecy). Alternatively, it can be updated following a random approach so that any passive attack is made powerless/ineffective.

Each network key is associated with a sequence of numbers that permits to specify which network key is active in the network, and each Network layer are using specific keys.

Network Key Secure distribution

Upon successful EAP authentication, the EAP method derives two keys: The Master Session Key (MSK) and the Extended Master Session Key (EMSK), at both EAP peer and EAP authentication server. The EAP authenticator is provided with the MSK by the authentication server. The EMSK is kept secret the EAP peer and the authentication server.

Network Access Control

The offered solution for network access control relies on cryptographic filtering using the security suites of the IEEE 802.1x. The node is provided with a network key received from the DCU after successful authentication. The network key is then used to derive a network-shared Data Link key.

To provide integrity protection, the node sends packets with a Message Integrity Code (MIC) appended to each Data Link-layer frame. An auxiliary security header is included in the Data Link header that specifies, in particular, a frame counter field that offers a protection against replay attacks. To provide confidentiality protection, the data payloads, as well as the MIC if included, are encrypted.

CEO Worldwide White Paper

Routing Security

The routing should be managed by the RPL (IPV6 Routing Protocol for Low power and Lousy Networks) protocol, which is standardized according to the IETF, and which is also leveraging the deployment of the AES 256 encryption hardware coded algorithm. The IETF 6LowPAN Mesh network protocol is also leveraging its neighbor discovery security countermeasures.

Application-Layer / Data Security

The Application level is fully managed by the CoAP (Constrained Application Protocol), fully adapted to the wireless communication between nodes, and fully secured by the DTLS protocol (Datagram Transport Layer Security) and the IPSec protocol (Internet Protocol Security).

Security Protocol schematic presentation

Conclusion

We have seen that the wide range of IEEE and IETF security protocols are already able to bring a very high level of security in operation with large Wireless Mesh network.

Beyond that, a lot of ongoing works are being done around the optimized combination of all those IETF standards and the important corresponding level of intelligence that should be available at each node level. As of today, with individual nodes equipped with a 32bits processor, hardcoded AES 256 encryption and with more than 4 Mbits of Flash memory, it is already possible to make available an embedded Smart IDS "Intrusion Detection System".

That IDS is capable of detecting, without any external support, a suspicious node or a group of suspicious nodes, which are running smart and recurrent attacks. These attacks are characterized by systematic and multiple different attack strategies against the neighbor nodes and/or the entire network in order to build by combining all the responses of the defense system, the right attack strategy to work around it and ultimately get hold of a part of the network, or of the complete network.

Written by Didier Guiraud, iCEO # 68831

Contact us! **Phone:** *+44 203 137 2581* **Email:** *search@ceo-worldwide.com*

Website: *www.ceo-worldwide.com*

CEO Worldwide Ltd - 9 Queen's Yard - White Post Lane, London E9 5EN, ENGLAND

The IDS is identifying the suspicious nodes, from which a large number of different and unsuccessful attacks are operated and doing so, is "learning" out that newly combined "smart attacks", while isolating all the contaminated nodes from the overall network, before one of these "smart attacks" eventually finds a way to break into the system.

Once the contaminated nodes are fully isolated from the network, the rest of the network can continue to operate as usual, and the IDS is resetting, still without any external support, the "contaminated" or "fake" nodes to normal configuration, before re-introducing them into the network to bring it back to its entire configuration.

That IDS, within the limits of the level of intelligence available on each node (Processing power and memory space) can then learn new types of attacks while it is neutralizing them, and therefore be each time more rapid and more efficient in isolating "contaminated" or "fake" nodes.

Thereupon, although it is sure that the issues with the next generation of wireless Mesh Network attacks will be more and more challenging to be neutralized and fixed, a huge counter measure arsenal is already available, and is strengthened every day.

Indeed, it is possible to say that on the one hand, the existing IETF and IEEE toolboxes have not been used at their maximum yet, and that on the other hand, many highly interesting ongoing works, to optimize the efficiency of the existing security protocols, could let us foresee a very bright future for the security and efficiency of the Industrial IOT.

Written by Didier Guiraud, iCEO # 68831

Contact us! Phone: *+44 203 137 2581* Email: *search@ceo-worldwide.com*

Website: *www.ceo-worldwide.com*

CEO Worldwide Ltd - 9 Queen's Yard - White Post Lane, London E9 5EN, ENGLAND