AAA-based Infrastructure for Industrial Wireless Sensor Networks

Authors: Thomas Bartzsch (University of Applied Sciences Dresden, bartzsch@htw-dresden.de), Dirk Burggraf (University of Applied Sciences Dresden, burggraf@htw-dresden.de), Laura Cristina Gheorghe (University Politehnica of Bucharest, laura.gheorghe@cs.pub.ro), Alexis Olivereau (Commissariat à l'Energie Atomique France, alexis.olivereau@cea.fr), Nouha Oualha (Commissariat à l'Energie Atomique France, nouha.oualha@cea.fr), Emil Slusanschi (University Politehnica of Bucharest, emil.slusanschi@cs.pub.ro), Dan Tudose (University Politehnica of Bucharest, dan.tudose@cs.pub.ro), Markus Wehner (University of Applied Sciences Dresden, wehner@htw-dresden.de), Sven Zeisberg (University of Applied Sciences Dresden, zeisberg@htw-dresden.de)

1. Introduction

An Authentication, Authorization and Accounting (AAA) infrastructure is a well-known system that enables security-related services in multiple wide-scale Internet and telecommunications systems. AAA infrastructures are natively designed to provide node admission control (and are often extended towards the charging functionality) across multiple domains in commercial scenarios. Beyond these basic functionalities, they have also been enhanced to interact with a wide variety of telecommunications functions, such as fast mobility and QoS management, for which they can restrict access to subclasses of users or enable dedicated charging mechanisms. On the other hand, wireless sensor networks (WSNs) are often designed as quasi-autonomous systems in which authentication is managed by a proprietary mechanism. Recently, works on cellular-operated machine-to-machine (M2M) devices fleets have started to investigate how AAA infrastructures can be used, mainly for authentication purpose, in the field of wireless sensor networking.
This document presents novel WSN security services that can leverage on an AAA authentication system. In accordance with industrial scenarios defined in the "TWISNet[1]: Trustworthy Wireless Industrial Sensor Networks" project, it especially considers the initial large-scale deployment of manufactured sensors, the authentication and mobility of sensors when worn by an operator, the secure routing of sensor data and the operation of a sensor node owned by more than one peer (and therefore dependant on more than one AAA domain).

2. Problem statement

The security of a WSN integrated into an industrial environment can be supported by an AAA-based infrastructure deployed in a separate network (e.g., a cellular network). The AAA-based infrastructure that is considered in this document is the adaptation of the legacy Authentication, Authorization and Accounting infrastructure that empowers Internet and recent cellular security architectures to the industrial wireless sensor networks. This infrastructure initially aims at allowing secure network access for a node, e.g. consecutively to its deployment or mobility.
Several security challenges stem from the considered infrastructure (illustrated in Figure 2). These challenges are not just related to

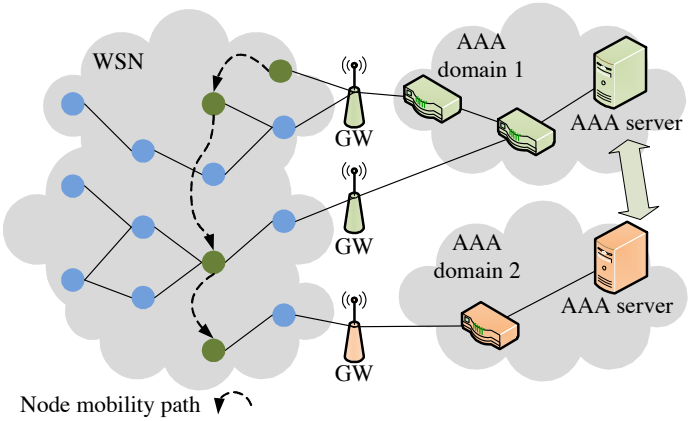

Figure 1: AAA-based infrastructure architecture

[1] TWISNet is partially funded by EU FP7 Research and Development programme.

the resource constraint inherent to sensors, but also to the security requirements in these networks supporting mobility of sensors within a multi-domain context. For instance, if nodes are mobile, they may move from one sensor network to another one. They, then, need to authenticate again to gain access to the network. They may have to authenticate through the AAA server of another administrative domain, if their home domain cannot be reached directly. To enable seamless communication of mobile nodes, the authentication procedure should support fast re-authentication adapted to a multi-domain context. Additionally, secure authentication between the node and its domain AAA server should be provided all the way through the foreign administrative domain. A node or a set of nodes may also be co-shared with different owners. This case raises the issue of secure sensor co-management in terms of information access and decision that should be agreed on by multiple owners.

3. Bootstrapping

Bootstrapping is a procedure that occurs after node's manufacturing and prior to node's operation. It is meant to provide a node with the parameters (e.g. cryptographic material, essential peers' identifiers and addresses) that will be required to operate. Bootstrapping cannot happen without initial knowledge: a manufactured node is assumed to be provided with an initial cryptographic material, which will be used during the bootstrapping phase.
In accordance with ETSI M2M specification, we propose to instantiate the bootstrapping procedure as a specific case of network entry authentication, and to base it on EAP-TLS. We propose however to have EAP-TLS derive, through its non-exported EMSK key material, the long-term shared secret used in subsequent EAP-PSK authentications.
As per the bootstrapping itself, we let it occur as multiple expanding rings centred on the AAA clients of the authenticating EAP-TLS –capable AAA server. The first nodes to be bootstrapped are those that are one IP hop away from the PAA. Once bootstrapped, these nodes acquire the PANA Relay Element functionality. Their immediate neighbours can then perform their own bootstrapping procedure through them.

4. Authentication and access control

Once the initial bootstrapping procedure has been performed, subsequent network accesses should be controlled through a lightweight authentication procedure between sensor nodes and the AAA server. Since authentication is performed more often than bootstrapping, resource constrains at the devices limit the choice of the EAP method, for instance, EAP-PSK is favored to EAP-TLS.
The authentication procedure should manage the different ways in which sensor nodes may access the network. If the mobile node cannot access the gateway directly and does not have yet an IP address, the first intermediary node in the path to the gateway may play the role of a PANA Relay Element (PRE). In the scenario where the mobile sensor node is not able to reach the network directly via its administrative domain but only through a foreign administrative domain, the foreign AAA server will forward the EAP request messages to the node home AAA server and the EAP response messages back to the node through the foreign gateway. To support fast re-authentication, existing extensions to EAP have been proposed that can be used in single or multi-domain AAA-based infrastructure settings, like for instance, the EAP Re-authentication Protocol (ERP) and the Authenticated Anticipatory Keying (AAK) scheme.
A main security issue may emerge if the node connects to the network through a node from the same domain as itself. Both nodes require building a link-layer security association. Obviously, the security association should be established with cryptographic keying material not shared with foreign domain entities. Otherwise, the communication between both nodes may be prone to identity spoofing attacks allowing foreign domain entities to route their messages through the nodes or to launch denial-of-service attacks against them.

5. Secure routing

In this kind of sensor network, at least four types of devices are involved in the communication process, namely end nodes, routers, a gateway and a server. Data should be delivered to the server that centralizes and analyzes information from the whole network. Routers have the main purpose of forwarding data packets toward the gateway. They run a routing protocol, which computes the best path towards the gateway.

In single-domain AAA-based infrastructure, the gateway receives data packets from the network and relays them to the appropriate server. It can perform aggregation upon the data received from the network. The gateway has a high level of processing and memory resources and unlimited power. The server has the purpose of analyzing and storing all information received from the sensor network. The server has very high or unlimited resources to process all data coming from a network of any size.

In multi-domain AAA-based infrastructures, the gateway receives data packets from the network, stores all data, and sends it to the (or multiple) server(s) on demand. It can perform aggregation upon the data received from the network. In this case, the gateway has virtually unlimited resources. The server has the purpose of analyzing all information received from the gateway. The server has very high or unlimited resources. This means that it has enough resources to process all data coming from a network of any size. In following, only the multi-domain infrastructure is described.

We propose a 3-level security with the following characteristics. The communication between the end nodes and the gateway is secured by symmetric keys K_D which are unique for each end. Additionally, symmetric keys K_R are used by the routers that are also only known to the gateway. Finally, an asymmetric keying scheme is employed between the gateway and the servers. In addition, a network key K_N is used by the gateway to send messages to the whole network and a key K_{AR} is used to send messages to all routers only.

6. Sensor co-management

The Sensor Co-Management (SCM) module enables the monitoring of several parameters that characterize the sensor network, such as load, link quality, processor and radio usage on the nodes. The module also allows the execution of tasks such as enabling sensing or actuation, changing the sampling rate.

In order for a command to be executed on a Sensor, certain requirements must be satisfied: the user sending the command is authenticated, the user has the required permissions for executing that command, and the target node is authenticated to the AAA server.

In a single-domain AAA-based infrastructure, the Sensor authenticates itself to the AAA server through the Gateway and moves inside a single domain. Only one AAA server is involved, therefore, SCM interacts directly with this server in order to obtain the list of authenticated devices.

In multi-domain AAA-based infrastructure, it is possible to have two AAA servers, associated to each domain. SCM has a list of associations between AAA servers and Gateways. In this case, the command can specify one or more domains. For each specified domain, the SCM module interrogates the associated AAA server for authenticated devices.

7. Conclusion

This document describes the realization of an AAA-based infrastructure used to support the security of an industrial wireless sensor network. The issues associated with the scarcity of sensor resources and their mobility are addressed. From the AAA-based infrastructure side, the multiple administrative domain aspect is also taken into consideration.

As future work, we plan to enhance the AAA-based infrastructure empowerment to the industrial wireless sensor network by considering authorization and accounting services.