Secure Access to IOT Network: An Application-based Group Key Approach

Samita Chakrabarti, Wassim Haddad
{firstname.lastname}@ericsson.com

Abstract

In this position paper, we describe a per-application secure network access and key distribution mechanism between the 'Internet Of Things' infrastructure and application users. Our suggested mechanism uses existing IETF protocols as a basis.

Introduction

The *Internet Of Things* provides a view of a web that is made from connecting machines of different capacities and applications. Sometimes, these connected devices form their own network with the ability to communicate with other device(s) on the Internet via one or more gateways, by accessing and/or sending information outside their own homogeneous network. Handling communication through IP network among a plurality of new and existing devices poses significant challenges to the capacity of today's existing Internet infrastructure, in terms of power and application usages, IP source and destination address identification as well as providing security to these devices.

Among these ubiquitous devices, sensors and actuators collect information, which in turn would trigger critical chain of events without human intervention, such as remote operation of household equipments or controlling electricity distribution systems. Therefore, security is an essential component of the machine-to-machine (m2m) communication especially that related threats and attacks such as denial-of-service, associated with low-power and/or low-capacity wireless devices are higher than for current wireless devices.

In this position paper, we focus on simple and efficient secure key distribution based on the node's particular role(s) and application(s) in the associated network, and discuss the case when the node has more than one interface. Our suggested mechanism uses existing IETF protocols as a basis.

General Assumptions and Goals

The suggested mechanism is based on the following assumptions:

1. The description of the proposal assumes that sets of different applications are running for different groups of IOT nodes. Thus, each node that is member of a particular application group possesses the same group key by which all members are authenticated to each other.
2. Node mobility across application groups is out of scope.
3. User node has typically more than one interface, and each interface may be tied to a different set of applications. A typical user node would be a smart phone/tabled equipped with a ZigBee interface. In addition, the application user should have at least one additional interface connected to the regular IP-network via wireless and/or wired interface, e.g., WLAN, 4G, etc.
4. All nodes in a particular application group may be served by their respective access router (AR) node, which sits between the 'Internet Of Things' network and the regular IP Network.

5. This access router (AR) node may be accessible by the user-node for group key association
6. The same AR may be used by the IOT network as a gateway to access the authentication server and/or a particular certificate database to obtain the same group-key for the IOT nodes.
7. A group-key is stored in a Database with a one-to-one mapping with a registered application and user specific information. The specific information is accessed only when the user requests a group key. However, in order to receive the application group key, the IOT node must be first authenticated in its own network.

Abbreviations

- IOT = Internet Of Things made of low-power devices such as sensors, actuators and radio devices
- AR = Access Router
- SeND = Secure Neighbor Discovery (IPv6)
- PANA = Protocol for Carrying Authentication for Network Access
- M2M = Machine-to-Machine
- RtSol = IPv6 Router Solicitation Message
- RtAdv = IPv6 Router Advertisement Message
- GK = Group-Key
- GK[X] = Group Key for accessing the application X
- Cert DB = Certificate Database
- GK DB = GK Database
- PK[a] = Parameter 'a' encrypted with public key PK

Description

Our main focus is to enable a user node to securely obtain one or more per-application group-key(s) in order to access information in the IOT network based on the selected and authorized application(s).

There are two ways a user node may attach to an IOT network. The first one is via the IOT network access gateway and the second one is via a direct communication with IOT nodes using an IOT-supported interface (e.g., ZigBee, HomePlug, etc.). In order to cover both scenarios, the authorized GK(s) are sent to the user node via the interface used to attach to the regular IPv6 network, e.g., via WLAN, LTE, Bluetooth. This also means that the IOT interface will not intervene when fetching the set of GK(s). Instead, IOT interface will only use GK(s) to securely communicate with low power devices associated with the selected application(s). It follows that such communication cannot occur if the user node cannot be authenticated prior/during attachment to the network.

In the following, we detail our solution by following a particular user node as it goes first through the access network attachment procedure then requests secure access to two different applications provided by the IOT network.

We start by assuming that each user/machine has a certificate that is pre-associated with selected/authorized applications provided by the IOT infrastructure. These certificates and associated apps are stored in a database that can be queried by the access network infrastructure nodes. In addition, GKs that are distributed to the IOT nodes, i.e., depending on the offered services, are also stored in a database, which can be accessed by access routers located within the IOT network using AAA Radius [RADIUS], PANA Relay (PANA-RLY) protocols.

The first step in our solution consists of attaching and authenticating to the network access infrastructure. For this, we assume that SeND protocol [SEND] is deployed to secure the attachment procedure. Note that the attachment to the access network occurs through an interface that is different from the IOT-enabled interface as we consider that data provided by IOT nodes will have to be sent to other remote nodes using a different interface and a secure connection.

In addition, the user node attaching to the network should send its certificate in the RtSol message.

Upon receiving a RtSol message carrying a valid certificate, the AR queries a special database and fetches the associated applications authorized for this particular certificate. Then, the AR fetches the GK associated with each authorized service and sends in response, a unicast RtAdv message to the attaching node. Such message will carry the GKs needed to access each authorized service. For this purpose, the AR must encrypt each GK using the node's public key (i.e., in addition to signing the message).

Note that the node may specify which service(s) it wants to use in a new option carried in the RtSol message. In this case, the AR will only fetch the GK(s) associated with these services.

After completing the attachment procedure, the user node has already been authenticated and obtained the necessary GKs. User node binds each GK to the associated application and stores it in its cache memory. A lifetime may be associated with each GK that would allow a periodical refresh of the group keys (i.e., using SeND).

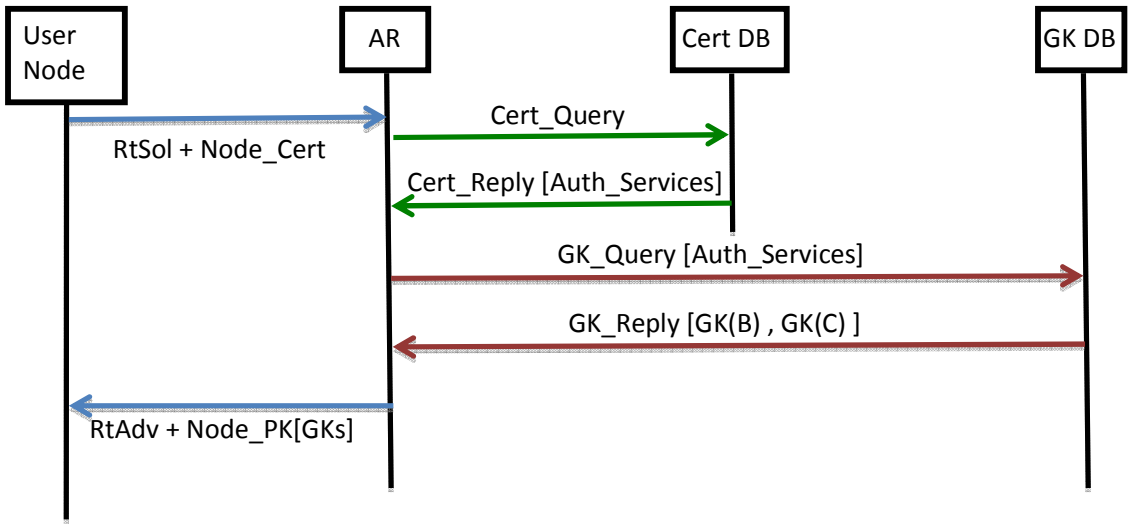

Figure 1: Messages exchange on the LAN side interface

Group keys are used only by the user node's IOT interface, in order to securely query specific IOT nodes offering the requested service(s). This is the case when the user node is directly accessing IOT devices. However, if the user node sits outside the IOT network, then it can use the regular IP-network interface to communicate with specific IOT devices via the IOT access gateway.

Deployment Scenarios

A typical deployment example is using a smart phone/tablet equipped with a ZigBee-interface to monitor home-energy consumption, monitor/regulate temperature/humidity of a section of a building remotely and securely.

Conclusion

The suggested proposal for secure access to the application group IOT nodes will require adding new options to the IPv6 Neighbor Discovery [ND] protocol for the purpose of carrying group-key and associated information. Depending on the scenarios and IOT network usage, PANA-RELAY [PANA-RLY] and 6LoWPAN Neighbor Discovery [6lowpan-ND] may need to offer additional information for application-based group key (GK) dissemination to the IOT network nodes.

References

[ND]	IPv6 Neighbor Discovery Protocol (RFC 4861)
[PANA-RLY]	PANA Relay Element (draft-ohba-pana-relay-03.txt)
[6lowpan-ND]	IPv6 Neighbor Discovery for Low Power and Lossy Networks (draft-ietf-6lowpan-nd-15.txt)
[SeND]	Secure Neighbor Discovery (RFC 3971)
[RADIUS]	RADIUS Accounting (RFC 2866)