June 25, 2018

IOT DEVICE POLICY MANAGEMENT FRAMEWORK IN 5G/4G CELLULAR NETWORKS

Santosh Patil

Mark Grayson

Byju Pularikkal

Swami Anantha

Sourav Chakraborty

IOT DEVICE POLICY MANAGEMENT FRAMEWORK IN 5G/4G CELLULAR NETWORKS

AUTHORS:
Santosh Patil
Mark Grayson
Byju Pularikkal
Swami Anantha
Sourav Chakraborty

ABSTRACT

The embodiments presented herein relate to a framework for sharing Manufacturer Usage Description (MUD) Uniform Resource Identifiers (URIs) in 5G/4G cellular networks, and mechanisms to apply policies based on MUD profiles for Internet of Things (IoT) devices connected to a 5G/4G cellular network. The proposal uses Protocol Configuration Options (PCO) parameters within 4G/5G cellular signaling to share MUD URIs from devices to cellular core network elements, which can apply additional policies for IoT devices. This proposal enables MUD integration into 5G/4G Core network with 3rd Generation Partnership Project (3GPP)-defined PCO Industrial Ethernet (IE) and provides a framework for uniform IoT device policies through a MUD in enterprise as well as Service Provider (SP) cellular networks.

DETAILED DESCRIPTION

In order to support IoT devices on a 4G or 5G network, it is important to establish proper policies to ensure security for IoT devices. Many IoT devices do not authenticate themselves to a network, as they do not have the capability to authenticate using IEEE 802.1X or other strong authentication methods. However, a network may benefit from the ability to determine the particular types or classes of devices that are connecting to it, so that the network can apply a particular policy to the device based on its class.

Manufacturer Usage Description (MUD), which is currently being standardized and implemented, is an example of a mechanism by which a device may identify its class. When MUD is used, an IoT device may state its device class in the form of a URI, which a network can resolve to learn the identity and any manufacturer-derived policies associated with that device. In an enterprise network, network management systems can use MUD profiles from IoT devices to apply appropriate network policies in terms of QoS and security/firewall policies for particular IoT devices. Although many IoT devices have a cellular interface and can directly connect to the 5G/4G cellular network, 3ggp or other standards do not address how to apply policies based on these MUD profiles. The embodiments presented herein provide a mechanisms for sharing MUD URIs in 5G/4G cellular networks, as well as mechanisms to apply policies based on MUD profiles.

First, a device may share its MUD URI with a cellular network. When MUD is used, the IoT device can emit a claim of its device class in the form of a URI. By using an enhanced Protocol Configuration Options (PCO) parameter to send MUD URI information from device to a Packet Data Network Gateway (PGW) so that the PGW can use this information to apply policies. Policies can be applied to each IoT device based on its MUD profile. A PGW or Policy and Charging Rules Function (PCRF) can be used to contact a MUD server and retrieve the MUD profile for the device. Using the MUD profile, QoS and QCI can be applied to the IoT device's cellular connection, and firewall policies can be applied based on the ports and protocols used by the IoT device.

When MUD is used, an IoT device emits a claim of device class in the form of a URI. In an enterprise network where IoT devices are connected to an enterprise switch or IoT gateway router, a device may broadcast its MUD URI to a switch, or the MUD URI can be shared as part of the DHCP options handled by an enterprise DHCP server. An IoS device may broadcast its MUD URI similarly in setting in which LLDP is used. Figure 1 illustrates an example of a MUD URI.

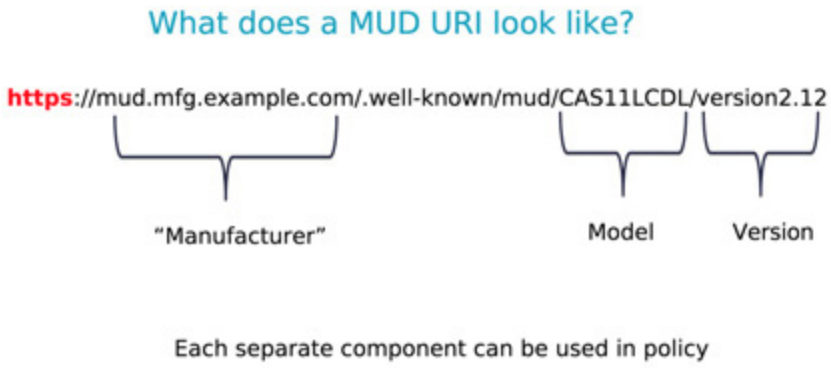

Figure 1

In the case of a 5G/4G cellular network, there is no official mechanism specified for a device to share URI information with a PGW. However, a modified Protocol Configuration option (PCO) parameter may be used to share URI information from a device to a PGW. PCO is typically used in LTE networks as a means by which devices can indirectly exchange information with a PGW. The information that is exchanged is typically related to particular Public Data Network (PDN) connections, such as PCO information that includes the address of a DNS server. The PCO parameter can be enhanced to include a MUD URI field, enabling an IoT device to share its URI information with a PGW.

Since PCO is a component of NAS messaging, this component can be carried by many different messages, such as by a PDN Connectivity Request or an Activate Default EPS Bearer Context Request. PCO details are defined in 3GPP specification 24008, section 10.5.6.3. Figure 2 provides an illustration of these PCO details.

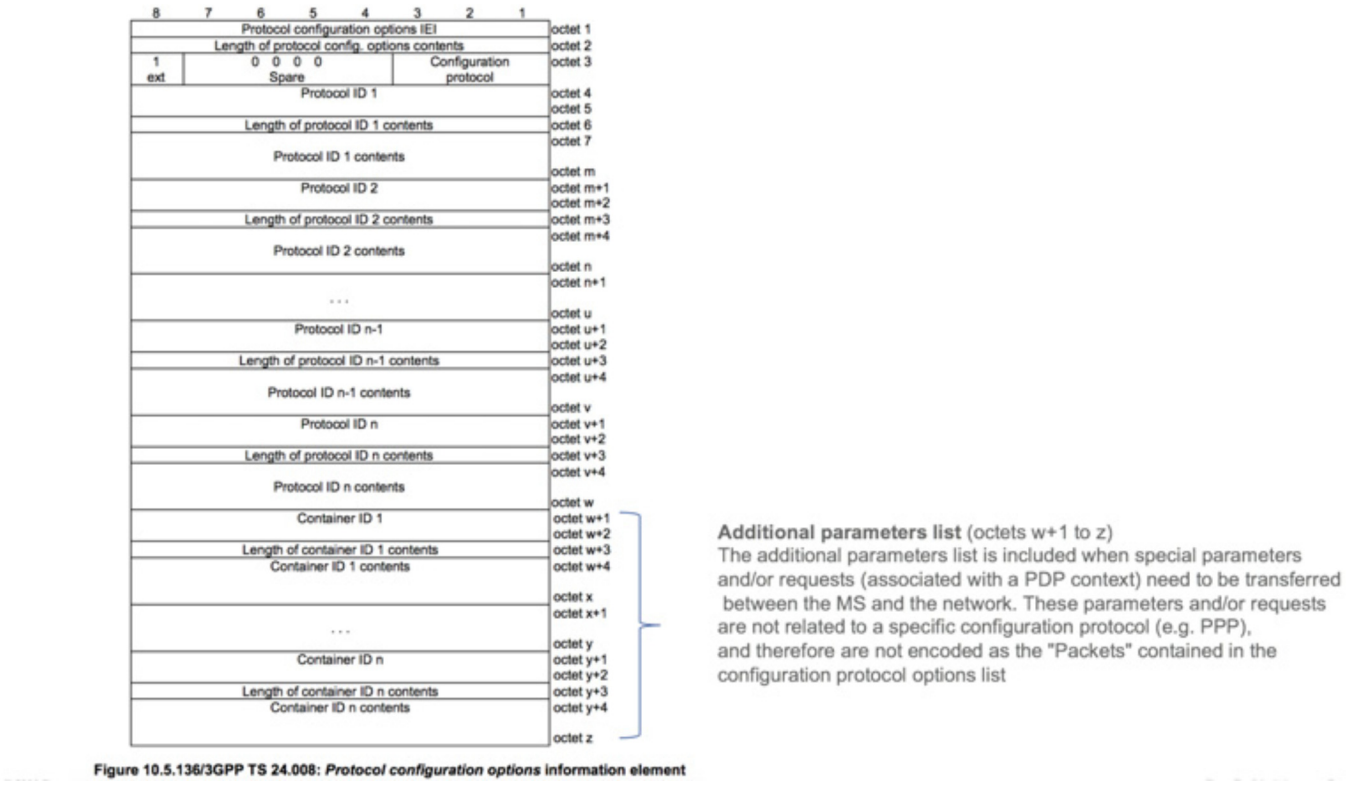

Figure 10.5.136/3GPP TS 24.008: *Protocol configuration options* information element

Figure 2

In PCO, Octets W+1 to Z may be used for an additional parameter. We are proposing to modify an mobile subscriber (MS)-to-network-direction parameter in this additional list to accommodate MUD URI information from the device to the PGW. See Table 1:

MS-to-network-direction parameters may include:

- 0001H (P-CSCF IPv6 Address Request);
- 0002H (IM CN Subsystem Signaling Flag);
- 0003H (DNS Server IPv6 Address Request);
- 0004H (Not Supported);
- 0005H (MS Support of Network Requested Bearer Control indicator);
- 0006H (Reserved);
- 0007H (DSMIPv6 Home Agent Address Request;
- 0008H (DSMIPv6 Home Network Prefix Request);
- 0009H (DSMIPv6 IPv4 Home Agent Address Request);
- 000AH (IP address allocation via NAS signaling);
- 000BH (IPv4 address allocation via DHCPv4);
- 000CH (P-CSCF IPv4 Address Request);
- 000DH (DNS Server IPv4 Address Request);
- 000EH (MSISDN Request);
- 000FH (IFOM-Support-Request);
- 0010H (IPv4 Link MTU Request);
- 0011H (Device MUD URI);
- FF00H to FFFFH (reserved for operator-specific use)

Table 1

The 0011H field may be enhanced to add MUD URI information. IoT devices can send MUD URI through this PCO IE during a PDN connectivity request call flow, and a PGW can use this information to retrieve MUD profile information.

Based on the MUD URI information received in a PDN connectivity request, a PGW can directly contact a MUD server of the manufacturer based on the URI, or the PGW can ask a PCRF to contact a MUD server to retrieve the MUD profile information for the IoT device. Based on the received MUD profile information, the PGW can apply policies for the IoT device's PDN connection. Policies can be established in terms of QoS or QCI assignment, and policies may include firewall rules based on specific ports or protocols.

As part of a PDN connectivity response, a PGW provides allowed QoS/QCI levels. For IoT devices, PGW can use a MUD profile information to map QoS/QCI to be allowed

for the IoT device based on factors such as the specified data rate and quality of service expectation in MUD profile. Based on the MUD profile, a PGW can retrieve information about the destination IPs, ports, and protocols that should be allowed or used by a specific IoT device. The PGW can use this information to enact policies as part of a PDN connectivity response, and the PGW may update the PCRF with those policies. For example, Table 2 provides an example of code for a MUD profile specifying a destination port 53 that needs to be allowed for this IoT device.

```
"ace": [
        {
        "name": "ent0-frdev",
        "matches": {
                "ietf-mud:mud": {
                        "controller": "urn:ietf:params:mud:dns"
                },
                "ipv4": {
                        "protocol": 17
                },
                "udp": {
                        "destination-port": {
                                "operator": "eq",
                                "port": 53
                        }
                }
        },
        "actions": {
                "forwarding": "accept"
        }
},
```

Table 2

Note that same mechanism may also be applied to a 5G or 3G cellular network infrastructure.

Regarding security concerns, MUD specification draft-ietf-opsawg-mud-13 states: “[b]ased on how a MUD URL is emitted, a Thing may be able to lie about what it is, thus

gaining additional network access. There are several means to limit risk in this case." Furthermore, "the MUD URL can act as a classifier that can be proven or disproven. Fingerprinting may have other advantages as well: when 802.1AR certificates are used, because they themselves cannot change, fingerprinting offers the opportunity to add artifacts to the MUD URL. The meaning of such artifacts is left as future work."
Fingerprinting, IMEISV, and/or other derived information may be used to authenticate a MUD URI signaled over PCO parameters.

In summary, the embodiments presented herein offer the benefits of MUD integration into 5G/4G core networks with 3GPP-defined PCO IE, and the capability to maintain uniform IoT device policies through the MUD in enterprise as well as SP cellular networks.