June 2022

ENTERPRISE ACCESS POLICIES UTILIZING 3GPP OPERATOR BARRING

Timothy P. Stammers

Bhavik Adhvaryu

Irfan Ali

ENTERPRISE ACCESS POLICIES UTILIZING 3GPP OPERATOR BARRING

AUTHORS:
Timothy P. Stammers
Bhavik Adhvaryu
Irfan Ali

ABSTRACT

Enterprises wish to provide access policies for private cellular networks that are tailored to a building's use. In support of such an enterprise use case, techniques are presented herein that apply 3rd Generation Partnership Project (3GPP) approaches for geographies, tracking areas, and access barring in innovative ways to realize a standards-compliant solution. Aspects of the presented techniques encompass novel floor-centric policies, whereby an enterprise may maintain a mapping of tracking areas to the floors of a building such that a floor may be uniquely determined by an association with one or more tracking areas. Under further aspects of the presented techniques, security and policy groups may comprise 'cellular home networks' to cater to visitor and guest scenarios in addition to, for example, international mobile subscriber identity (IMSI)-based groups. Under still further aspects of the presented techniques, the existing 3GPP subscription data attribute Operator-Barring may be leveraged to apply an enterprise access policy in a private cellular access network.

DETAILED DESCRIPTION

Enterprises wish to maintain network access policies that provide controls based on a set of physical locations. One example of such a scenario might encompass the floor of a building. Such an objective may be achieved using a location management system as the basis for identifying where a specific endpoint resides, such as a cloud-based location services platform for Wi-Fi access. The equivalent for private cellular networks would be the deployment of a 3GPP-compliant location determination system along with the integration of that location system with an enterprise’s location management system. Under such an approach, a further integration would involve applying the resulting enterprise policy during device access authentication and registration. However, such an approach can be a complex and expensive solution that is often better suited for the location or

proximity needs of, for example, safety scenarios where highly accurate location knowledge may be utilized.

In contrast, for policies that are based on a less granular location determination, use of the techniques presented herein (which will be described and illustrated in the below narrative) result in a cost-effective solution to the above-described challenge whilst maintaining a 3GPP-compliant approach for ascertaining location. Under aspects of the presented techniques, the level of complexity of the location-determining aspect is reduced and, consequently, the costs of deployment and operation are also reduced. Further, the delivery of policy details to the private cellular access network may make use of existing signaling interactions.

The techniques presented herein may be based on the premise that a floor of a building is associated with a unique tracking area within the private cellular network that serves the building. Such a tracking area may be provided to the cellular system during device access authentication and registration.

As one example, an enterprise may maintain a mapping of tracking areas to the floors of a building such that a floor may be uniquely determined through an association with one or more tracking areas. The enterprise may also maintain access policies by floor and may associate those policies to security groups. Those groups may comprise endpoints that are associated with an international mobile subscriber identity (IMSI) value. Further, the groups may comprise 'cellular home networks' to cater to visitor and guest scenarios.

During operation, when a device 'appears' in a given tracking area that is managed by the private cellular access network, the relevant policy for that tracking area may be applied. Such application may be based on the specific group membership of the device that identifies a policy set. The floor-specific policy for the device may be determined by using the tracking area.

A floor-specific policy, as described above, may be provided in cellular subscription data as an Operator-Barring attribute using existing 3GPP definitions. Typically, subscription data is relatively static. Under aspects of the techniques presented herein, a subscription data attribute may be modified depending upon the floor (i.e., the tracking area) in which a device authenticates and registers to reflect that access is either permitted or denied.

By using an existing 3GPP subscription data attribute, aspects of the techniques presented herein support an enterprise access policy that may be applied in a private cellular access network through the use of such an attribute. Figure 1, below, depicts elements of an exemplary system representation according to aspects of the techniques presented herein and reflective of the above discussion.

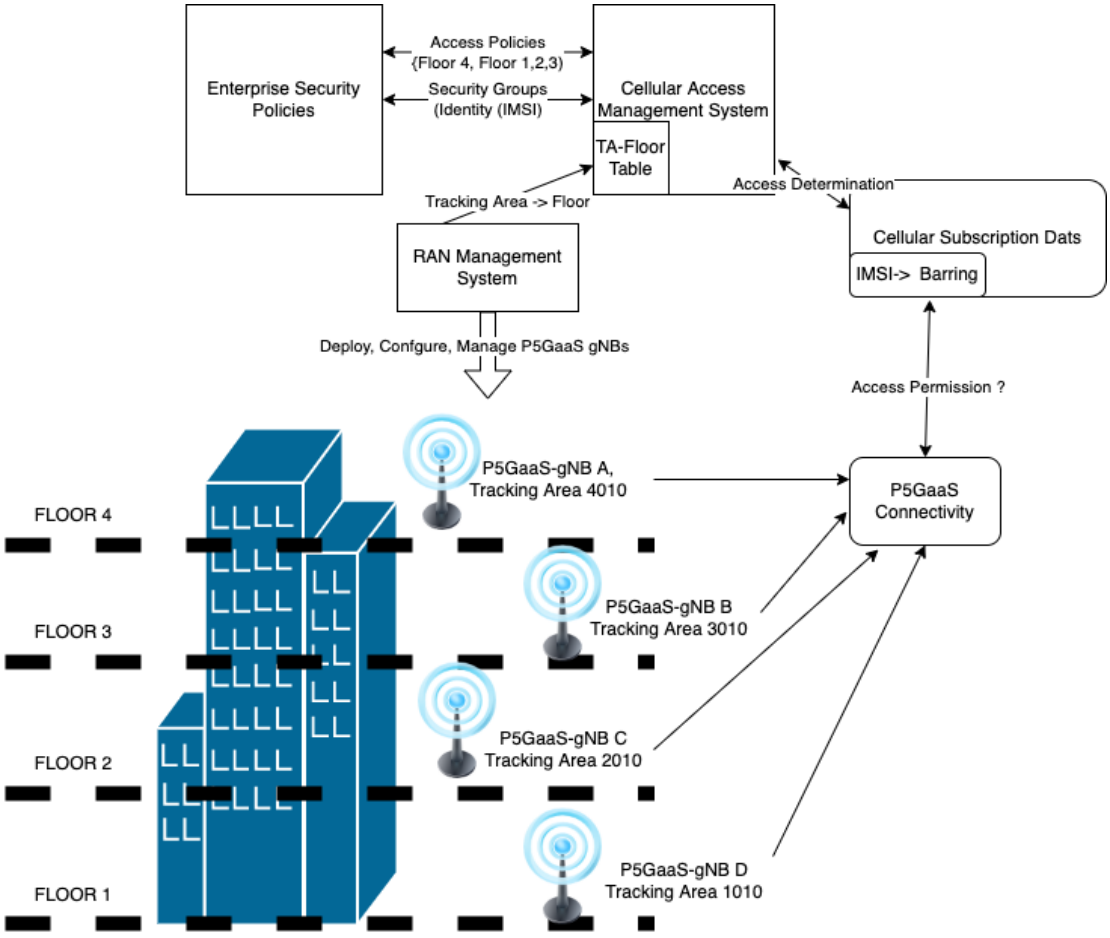

Figure 1: Exemplary System Representation

A sample message flow for a device accessing its home network (according to aspects of the techniques presented herein) is shown in Figure 2, below. The techniques presented herein may be extended to policies for visitor and guest access. While that scenario is not depicted in the system representation that was presented in Figure 1, above, basic message flows for such a scenario are presented in Figure 3, below.

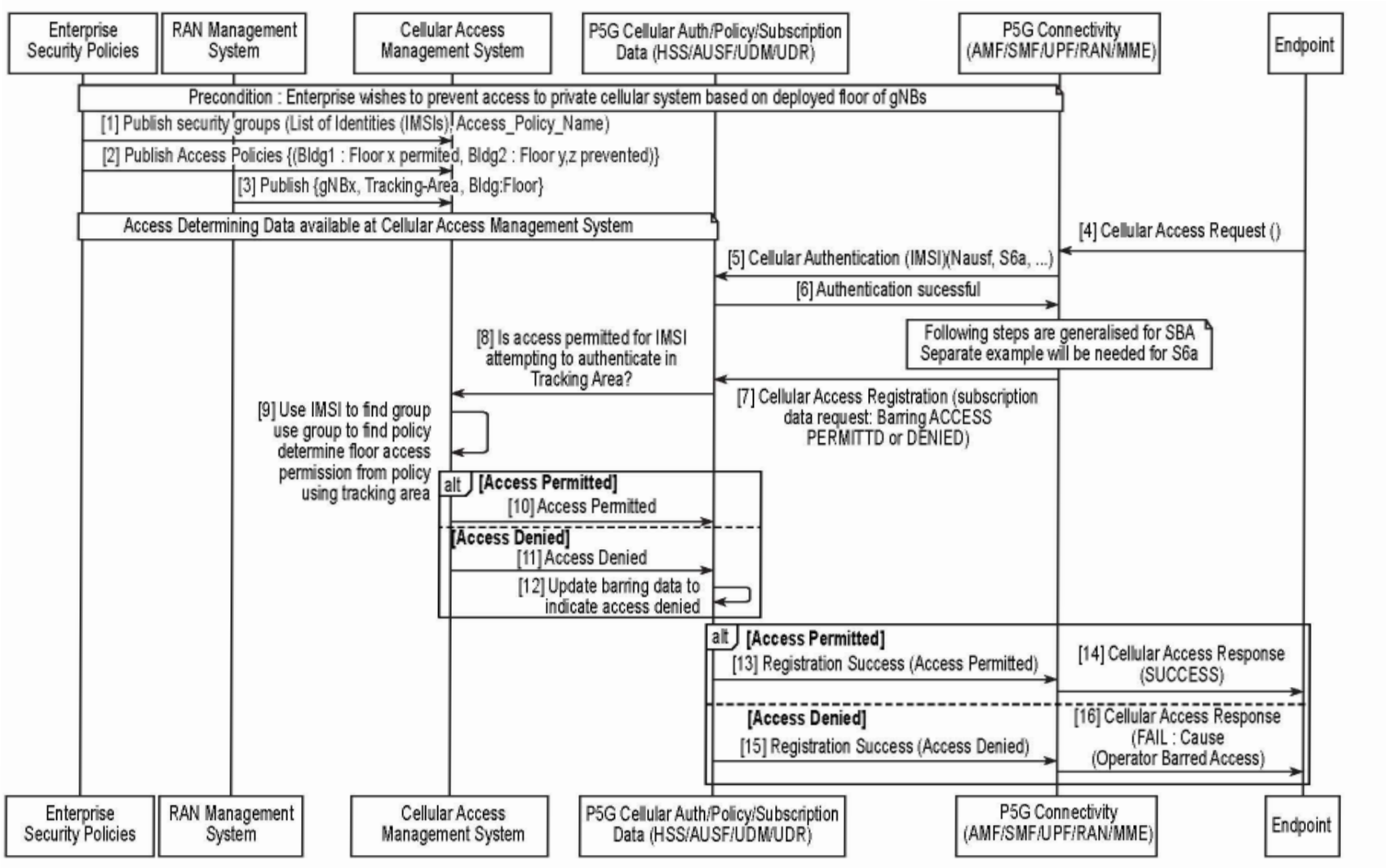

Figure 2: Cellular Access Barring by Security Group – Home Scenario

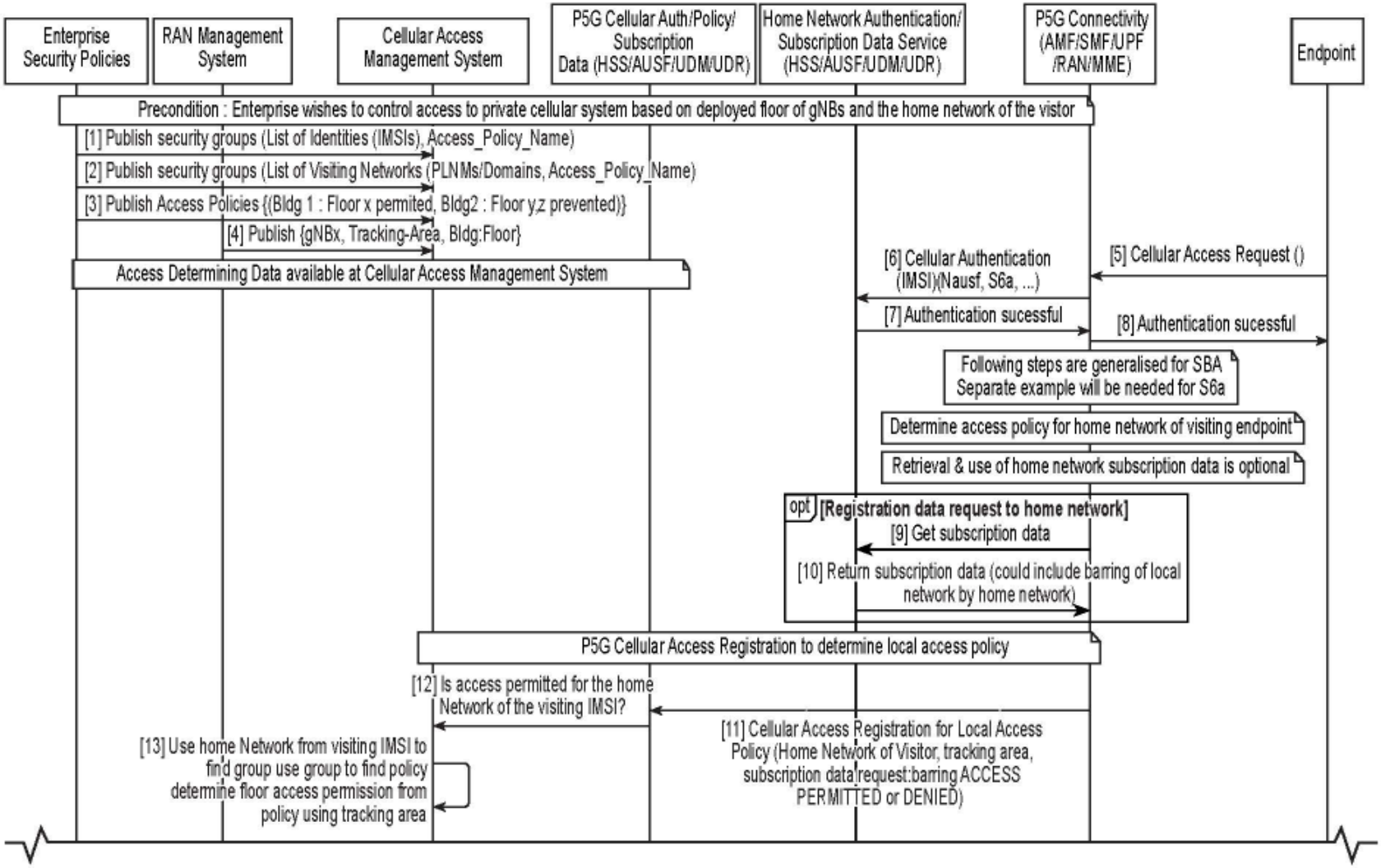

Figure 3: Cellular Access Barring by Security Group – Visitor Scenario

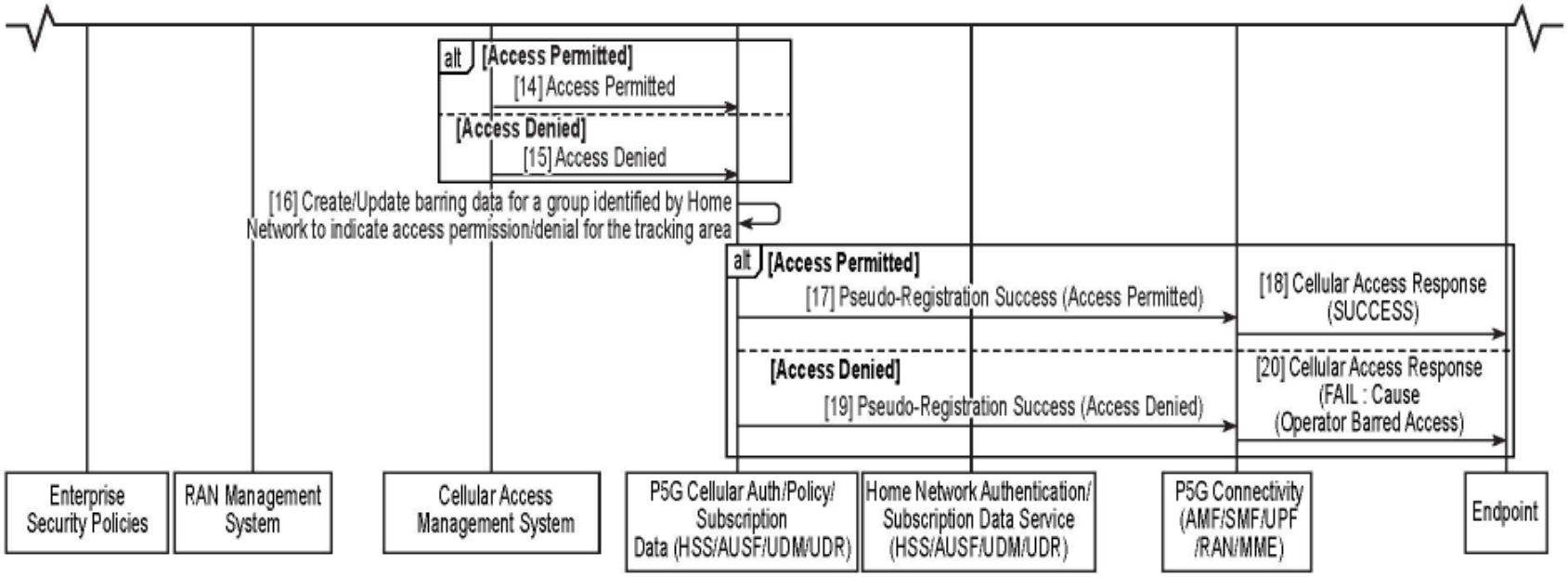

Figure 3: Cellular Access Barring by Security Group – Visitor Scenario (Cont.)

The primary difference between the message flows for a home scenario (as depicted in Figure 2) and a visitor scenario (as depicted in Figure 3) is that for home devices the access policy may be determined as part of the authentication and registration process with the home network. For visitors and guests, as the authentication and registration are performed with the home network of the visitor, and not the enterprise private cellular network, additional steps are involved, which provide for intercepting subscription data returned from the home network and determining an enterprise access policy based on the subscription data. Operator-Barring data in the home network subscription data may be overwritten, as appropriate, to reflect the enterprise access policy.

As described and illustrated in the above narrative, the techniques presented herein provide a number of innovative features. First, an enterprise may maintain a mapping of tracking areas to the floors of a building such that a floor may be uniquely determined by an association with one or more tracking areas. Second, security and policy groups may comprise 'cellular home networks' to cater to visitor and guest scenarios in addition to, for example, IMSI-based groups. Third, an existing 3GPP subscription data attribute (i.e., Operator-Barring) may be leveraged to apply an enterprise access policy in a private cellular access network.

In summary, techniques have been presented herein that apply 3GPP approaches for geographies, tracking areas, and access barring in innovative ways to realize a standards-compliant solution. These techniques can be applied to 5G, 4G, 3G and even 2G networks. For 3G and 2G systems, the equivalent concept of tracking area is routing areas. Aspects of the presented techniques encompass novel floor-centric policies; support security and policy groups that cater to visitor and guest scenarios in addition to IMSI-based groups; and leverage an existing 3GPP subscription data attribute to apply an enterprise access policy in a private cellular access network.