June 19, 2018

HUMAN USAGE DESCRIPTION FOR 5G NETWORK ENDPOINTS

M. David Hanes

Chuck Byers

Joe Clarke

Gonzalo Salgueiro

HUMAN USAGE DESCRIPTION FOR 5G NETWORK ENDPOINTS

AUTHORS:
M. David Hanes
Chuck Byers
Joe Clarke
Gonzalo Salgueiro

ABSTRACT

Just as Manufacturers Usage Description (MUD) defines security and access control for "things," Human Usage Description (HUD) does the same for humans by associating a user and all of their devices in a database. With such a database, a 5G provider has insights into user behavior on the network in context with the user device. This allows for more accurate Quality of Experience (QoE) and network slicing at the user device level, common licensing and security across multiple devices, next generation media consumption, and revenue generation through targeted advertising.

DETAILED DESCRIPTION

Manufacturer Usage Description (MUD) is disclosed in an Internet Engineering Task Force (IETF) specification that provides security and access control for "things." This allows a network to properly handle the security aspect and potentially other aspects, such as Quality of Experience (QoE), for Internet of Things (IoT) devices. However, there is no application of MUD to humans and their devices. For example, there is no centralized repository of user behaviors and devices to provide users with better experiences. Many opportunities exist if information similar to that found in MUD repositories is applied to humans. This can be remedied by applying the concept of MUD to humans and their devices (referred to herein as "Human Usage Description" or "HUD").

MUD is dedicated to IoT devices. HUD deals with humans and their devices. While MUD is currently focused on security and access control, HUD covers this and also address QoE. The combination of MUD and HUD offers new possibilities in network performance, efficiency, and feature richness.

Like MUD, HUD depends on an identifier or reference for the person and their device. MUD uses a Uniform Resource Identifier (URI) that is emitted by all devices of a certain type that points to a manufacturer's security policy and access control configuration.

Published by Technical Disclosure Commons, 2018

With HUD, the emission of a URI is not necessary. Instead, the subscriber phone number, International Mobile Equipment Identity (IMEI), Media Access Control (MAC) address, and so on is leveraged depending on the device type and how it is connecting to a 5G network. This is different than MUD because HUD is looking at unique identifiers for each device instead of a class of devices.

MUD uses an online database that is explicitly referenced by the emitted URI. With HUD, there is a similar database (referred to herein as a "HUD database") that is maintained by the 5G network provider or service bureau. However, instead of URI lookups, the unique identifiers are used (e.g., subscriber number, IMEI, Layer 2 (L2) address, network ingress point, geolocation, etc.). This allows for unique devices to be profiled and correlated to a specific user.

Figure 1 below illustrates a high level overview of an example system.

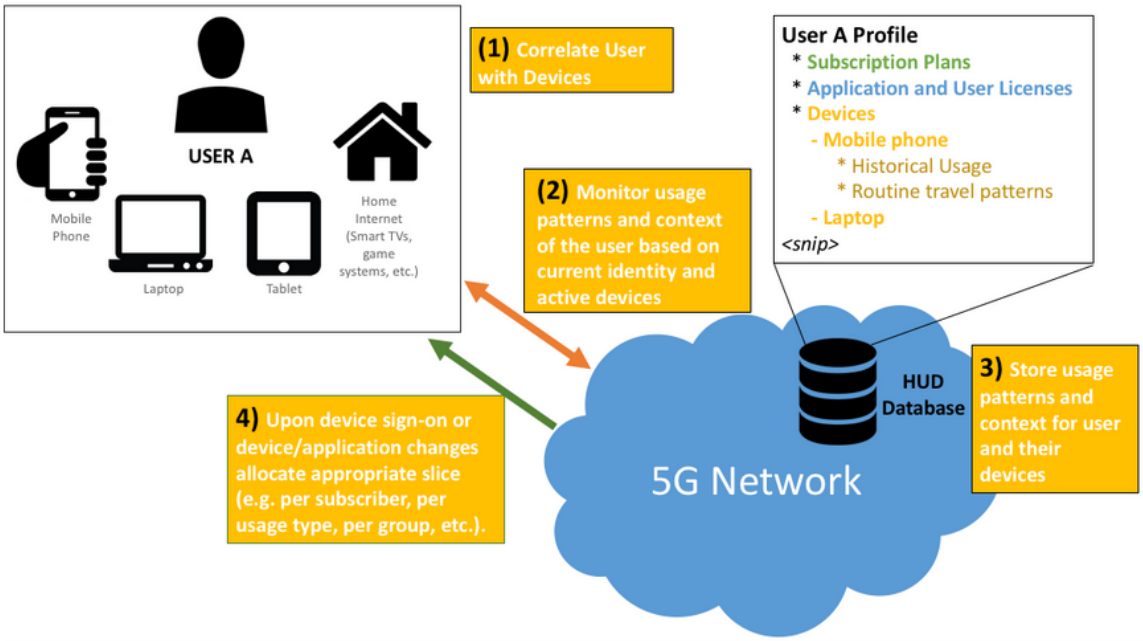

Figure 1

Step 1 involves correlating the user and devices in order to ultimately populate the HUD database using various methods. This may be based on, for example, subscriber number, IMEI, L2 address, and other unique identifiers. Subscription plans and premium services are already known by the provider. Security preferences and options can be defined by the user or implemented through subscription plans. Privacy preferences may be selected by users, employers, or governments. Historical usage by device is archived

and profiled. This may also use biometric authentication, user knowledge (e.g., Personal Identification Number (PIN) and password authentication, and items in the user's possession (e.g., authentication tokens, wearables with network credentials, key fobs, blockchain devices, etc.). These methods and the orchestration between them allow for the contextual connection of a user with multiple devices.

Once the association between the user and their devices has been made, the method may proceed to step 2 where the usage patterns are monitored. Instead of simply viewing each device on its own, the user's usage and behaviors across all devices is monitored together, optionally with automated / machine learning systems that optimize the user experience.

Step 3 involves a database in the 5G network where the context of a user and their devices combined with usage patterns and behaviors are stored and analyzed. With such a database that correlates all of a user's devices, the 5G provider has insights into a user's behavior on the network in context with the device that they are using. For example, when on a mobile phone, a user may predominantly use texting, social media, and email, with occasional web browsing. However, when on a laptop, the user may play video games or stream high-definition or 4K movies. Here, the resources consumed from the network greatly change for this user based on the device being used. Additionally, the provider can correlate usage with location as the user most likely has similar data usage patterns at locations frequented by the user.

Meanwhile, another user may use a mobile phone for virtual or augmented reality, and as such their usage profile and demand for network resources may be much greater. A HUD database allows the 5G network to understand the usage patterns and network resources needed for any user based on the context of the device they are using. This may be combined with machine learning techniques to constantly update a user's profile as usage patterns change and evolve. Ultimately, the 5G provider may be able to predict the usage and the possibility of resource contention on any node based on the connected user devices.

From a provider perspective, this user and device context combined with usage and behaviors allows the provider to better place the subscriber or user in an appropriate network slice. This is highlighted in step 4, and may ensure a specific QoE and offer tiered

service levels. For example, providers may want to offer an entry level of service that is free but have advertisements to generate revenue. This may be offered across all user devices or specific ones. A user's work laptop may not be a device where this would apply but a tablet used for email and web browsing may. Bring Your Own Device (BYOD) users may be allocated specialized slices. Only by tracking a device in the context of the user can such decisions be made intelligently.

Correlating all devices to a single user in a HUD database also provides security and privacy benefits, licensing across multiple devices, and next generation media consumption using multiple screens and devices. For example, if a user is viewing a sporting event (e.g., a football game on a large video screen), they may want to use their private smart phones and tablets to supplement their viewing experience (e.g., by looking up player statistics for replays of past games on their tablet), or transfer their viewing streams between devices. Only by establishing the association of a device to a user can the proper context be generated regarding future usage of a user device. In one example, the user may simultaneously want to shop for merchandise and engage in social media on their phone. Using HUD, the preferences for each user's capabilities on each device may be determined as being correlated with activities happening concurrently or in the past on others of their devices. With this context, the necessary applications may be automatically configured, and the network may be optimized for all the data flows supporting this rich environment.

With a HUD database that associates users and their devices, certain functions may also be provided to a user. For example, an enterprise may purchase a higher QoE for its employees from a 5G provider when their slice indicates the employees have entered a Virtual Private Network (VPN) of the enterprise or access enterprise resources. The enterprise may also want its customers to have a better QoE when browsing or downloading software from its website. Users may be designated as enterprise employees or customers and a better QoE may be provided no matter which of their devices are being used. Additionally, personal mobile phones are often used at work as well. With the context described herein, a user may be switched from a corporate BYOD slice during business hours to a personal/group/household slice after hours, for example.

In another embodiment, the user may have access to elements of their HUD profile and restrict certain websites and/or content (e.g., for children who may be using their devices). Users may even specify their exact usage patterns if they want to guarantee certain experiences, or pay to upgrade their experience for an important event (e.g., video streaming of an important presentation, wedding, or graduation).

The central HUD database may be strongly encrypted, and only the relevant portions of it may be securely sent to the Internet. Updates to the HUD may be managed in ways that insures data integrity and privacy.

Knowing the context of users and their devices along with the behaviors and usage patterns may provide the information needed for a provider to allocate the proper network slice. A subscriber database functionality is described herein, but this database is not simply a listing of unique subscriber identifiers and their attributes. Instead, examined is an overlay (a subscriber database organized around a user and their devices). This type of database allows for a contextual correlation between users and devices.

The additional context may be applied to new services and even network slicing. This incorporates slicing based on the contextual user/device behavior and usage. Creating a slice per subscriber may allow providers to target services, advertising, and applications to a single user across all devices, thereby providing the capability to track the context of a user across the multiple devices that are correlated with that user.

In summary, just as MUD defines security and access control for “things,” HUD does the same for humans by associating a user and all of their devices in a database. With such a database, a 5G provider has insights into user behavior on the network in context with the user device. This allows for more accurate QoE and network slicing at the user device level, common licensing and security across multiple devices, next generation media consumption, and revenue generation through targeted advertising.