**IEEE P802.24**

|  |  |
| --- | --- |
| Project | IEEE P802.24 Vertical Applications TAG, Smart Grid Task Group |
| Title | **802.24 question for ECSG Privacy.docx** |
| Date Submitted | [16 September, 2014] |
| Source | [Tim Godfrey][EPRI] | Voice: E-mail: [] |
| Re: | Discussion on MAC Address Privacy issues for Smart Grid devices |
| Abstract | [Working document] |
| Purpose |  |
| Notice | This document has been prepared to assist the IEEE P802.24. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein. |
| Release | The contributor acknowledges and accepts that this contribution becomes the property of IEEE and may be made publicly available by P802.24. |

**802.24 discussion on ECSG for Privacy**

Do the privacy concerned identified by the ECSG for privacy have any impact on Smart Grid networks?

Discussion:

 Most Smart Grid systems do not run on public networks

 Is the visibility of MAC addresses an issue?

 Divide problem into utility owned devices and consumer owned devices

Identify of Device – In what scenario do we care about hiding this?

Is there any further value to an attacker of having a fixed MAC address once they have decoded the signal to the point of being able to read the MAC address?

Location of Device - In what scenario do we care about hiding this? (The limited range of the signal provides localization)

Does the combination of knowing the device identity and location provide any attack vector?

The ECSG use case is consumer-level tracking of mobile Wi-Fi devices in a store scenarios.

Initial Conclusion: We don’t see the same problem in the grid space.

Considering another perspective:

Would widespread adoption of a MAC privacy solution cause a problem for grid devices?

MAC Addresses are often used as an equipment identifier. If MAC addresses become more dynamic, it might require the establishment of a new type of device identifier.

If all MAC addresses are dynamic, there would be a potential for address conflicts. Any solution would need to include a mechanism for avoiding address conflicts. Assuming MAC privacy is through randomization – if the solution is different, then the problem would not exist,

There may be a possibility for conflict with networks that use both long and short addresses. Also with protocols that derive the IP address from MAC address.

Potentially a “NAT-like” function could assign MAC addresses. Or MAC addresses could be encrypted. Or a defined way of assigning MAC addresses could be defined.

If locally administered addresses are used, there is a problem if multiple local administrators are in the same area of a wireless network.

It was noted that there are unique signatures of any RF transmitter and antenna system that can be tracked, independent of the MAC Address. (Granted, it would require more technical sophistication and presumably cost to take advantage of these techniques compared to sniffing the MAC address)

MAC address privacy could have limited applicability to utility field workers and their wireless devices.

**Question to ECSG** – Given that most utility Smart Grid devices are at fixed locations, does the Privacy ECSG envision a use case for MAC address privacy for fixed devices?

802.24 would like to discuss this with the ECSG at the November 2014 meeting.