An efficient authentication protocol for 5G

Markus Ahlström, Simon Holmberg, *Lund University*

2016-09-07

Machine to machine (M2M) devices will in the future authenticate to 5G networks in a more efficient way than they do to 3G and 4G networks today – at least if they will use a new cryptographic protocol developed at SICS Swedish ICT.

A new group-based authentication protocol

Around the year 2020, mobile network operators will begin to release 5G telecommunications networks. While the visions for 5G are clear – among them, a massive amount of M2M devices – the protocols for 5G are not yet standardized. One protocol that could possibly be included in the 5G standards is the aforementioned authentication protocol. It belongs to a breed of authentication protocols that aim to make authentication more efficient by letting devices form groups.

Although all group-based authentication protocols have the grouping in common, they differ a lot in terms of the actual techniques used and in what ways they perform better than the current standards. This became apparent to us when, in the beginning of the degree project, we evaluated some of the existing group-based authentication proposals. The conclusion of the evaluation was that the existing proposals all had some major disadvantage.

Based on the results of the evaluation, the new protocol was developed by researchers at SICS. Our task was to implement it and to evaluate its performance. In short, the protocol works by deriving several different authentication parameters, belonging to different members of the group, from a root value, so that only the root value needs to be sent from the group's home network to the roaming network.

Implementation and performance evaluation

Mobile telecommunications networks are complex and governed by a plethora of protocols, which are standardized by telecommunication associations from all over the world. As a consequence, implementing the new protocol from scratch would be nearly impossible. Instead, our approach was to adopt an existing platform which followed these rules and modify it to include the new group-based protocol. In our project we investigated eight platforms and found the best one: OpenAirInterface.

The result of modifying OpenAirInterface is a plausible and practical implementation of the new protocol, including a specification of how the protocol could actually be implemented in real systems. Furthermore, our implementation enabled us to test and measure the performance of the new protocol.

In our performance evaluation of the protocol we focused on bandwidth consumption and latency. The result of our evaluation shows that the new protocol fares much better than today's systems, especially when the system is under the load of thousands of M2M devices. Specifically, we found that the total bandwidth of the system is reduced already when there are three devices authenticating in a single group. Our evaluation of the latency was based on the roaming scenario – when a group is far away from its home network. We found that the new protocol decreased latency in this scenario significantly.

In conclusion, this new protocol may definitely be worth implementing in 5G, and what better way to do it but as specified in our master's thesis?