Group Controller-based Authentication for Machine Type Communication Under LTE Network

Qi Pan¹,a*, Xiangming Wen¹,b, Zhaoming Lu¹,c, Huan Wu¹,d
¹Beijing Key Laboratory of Network System Architecture and Convergence
Beijing University of Posts and Telecommunications
Beijing, P.R. China, 100876

¹panqiouc@bupt.deu.cn, bXiangmingWen@bupt.edu.cn, c1zy0372@163.com, dwwuhan@bupt.edu.cn

Keywords: MTC, LTE, Group authentication, authentication and key agreement, congestion control

Abstract.
Machine Type Communication (MTC) in the cellular network with ubiquitous coverage and various applications has played an important role in our daily life. For security, MTC devices need to follow the Evolved Packet System-Authentication and Key Agreement (EPS-AKA) protocol to guarantee the secure requirements in the machine-to-machine (M2M) communications. However, a huge number of terminal devices tried to complete the authentication procedure simultaneously, which would bring a severe congestion and overload for the network. In this paper, we proposed an efficient, available and scalable group controller-based authentication and key agreement (GC-AKA) protocol for devices to ensure the safety in the long term evolution (LTE) network. Through a design of group controller and simplicity of devices' work in the authentication process, it would be more secure and efficient for resource-constrained devices in the communications between device and the cellular network, while providing simultaneous authentications for a mass of devices without congestion and overload in the network.

Introduction

Machine Type Communication (MTC) means information exchanges among miscellaneous objects or between the ubiquitous devices and servers without human interference.[1, 2] It has been discussed as a new type of communication, which may renew our living styles widely in our daily life, for instance, e-health, smart metering, intelligent transportation, smart grid and so on. However, unlike the traditional Human-to-Human (H2H) communications, billions of objects would generate a great deal of signaling consumption and data process information under different environments, resulting in an explosive increase in the data traffic flow in both the radio access network (RAN) and the core network (CN). [3]

In addition, wireless communication, in its nature, is always at a risk of eavesdropping or manipulation because data originally sent from/to a user may be received and unlawfully used by an unintended user. So bi-authentication is needed to protect the traffic from attack between the MTC devices and the network for the vulnerability of wireless communications. When thousands of devices carry on the authentication process almost simultaneously, it would lay a heavy burden on the network, which would produce an influence on the normal human-to-human (H2H) communications and even get the network collapse.

To solve the above problem for safety, there are plenty of researchers focusing on the solutions to overcome these authentication congestion deficiencies for the network. Jung et. al.[4] grouped multiple terminal devices for convenience, and selected a group header to communicate with the network on behalf of all the devices in the same group. Apparently, it can alleviate the congestion for the machine type communications, but it can’t resolve the authentication problem. Based on this idea, Cao et. al.[5] came up with a group-based authentication and key agreement (GR-AKA) for MTC in LTE networks, with which giant number of devices can simultaneously complete the authentication process and establish a safe session connection. However, it causes a heavy computation load on the devices and it is unreasonable and improper for the resource-constrained devices in the MTC scenarios. In addition, Li et. al.[6] proposed a group-based AKA protocol with dynamic policy
updating, by which an asynchronous secret share scheme combining with Diffie-Hellman key exchange scheme was chosen to implement distributed authentication and session key establishment in the LTE-A networks. However, this effective authentication scheme still costs lots of resources for computing and processing.

In this paper, we proposed an effective and dependable group controller-based authentication and key agreement (GC-AKA) mechanism for resource-constrained MTC devices based on those ideas above. The main contributions of this paper include:

1) Unlike other schemes with a group leader selected from the devices, we design a controller which has powerful and dependable ability of computation and communication as the aggregator of all the devices in the same group. Communications between devices and network have been replaced by the controller and network, which brings the load on the devices down for long service time and undertakes the resource-consuming encryption and security algorithm processing. In addition, with this controller, connection failures in M2M communications would be probably avoided as the group leader as a MTC device is more likely to go in trouble.

2) As MTC devices are always fixed or limited in restricted areas, we designed a ID table for controller for record of the devices’ identification information and reduce the message exchanges during authentication procedure for MTC devices. Apparently, it can reduce the resource consumption for devices. In addition, devices without request for network would enter into the sleeping mode for energy conservation, which prolong the work time for devices.

In the remaining of this article, network architecture will be introduced in Section II and then is the proposed authentication scheme. In addition, the security analysis would be detailed in Section IV and we draw our conclusion finally.

Network Architecture

In this section, details about the system design would be represented.

As is shown in the figure 1, the network architecture was inherited from the typical 3GPP standard. Obviously, it can be divided into three domains: device domain, network domain and application domain. [2]

In the network architecture, devices are grouped for the similar characteristics, like adjacent locations. Devices in the same group and the group controller (GC) would communicate with each other via the short-range communication methods, such as IEEE802.15.4, Bluetooth Low Energy (BLE) and Wireless Location Area Network (WLAN). Devices with requirement for the Internet would inform the GC and GC would complete the authentication process with the concrete information of devices stored in GC. With such an effective GC design, the complicated and credible security algorithms can be processed in the GC, decreasing the computation load of the devices with a high-level security guarantee for the communication between group and the network.
The Proposed GC-AKA Scheme

In this section, we would describe details about the proposed GC-AKA protocol as solutions to the congestion for resource-constrained devices during the authentication procedure. Based on the concrete steps, the protocol can be divided into two stages: Information aggregating stage, group-based authentication and key agreement stage as shown in figure 2.

Information aggregating stage:
Firstly, when a device joined in this group, it would submit its authentication information to the controller for record. Afterwards GC would hold an ID table which keeps a record of the identification information of the devices within group for subsequent authentication, such as the IMSI, MTC_ID etc.

Afterwards, devices with attempts for the network would only send their identity MTC_ID to the group controller with the short-range communication methods. Through the simplicity of access request message for the devices, costs for devices would be decreased a lot.

Group-based authentication and key agreement stage:
Step 1: After the aggregation of devices’ access request in the group, GC would select related authentication information from the ID table and form an attach request vector (ARV) which contains authentication information for the devices which required for the network. Then the controller would send ARV to mobility management entity (MME) for mutual authentication.

Step 2: An MME, upon receipt of ARV, identifies the users using its IMSIs and requests authentication vector(s) (AVs) from a home subscriber server (HSS).

Step 3: The HSS then generates AV(s) using EPS-AKA algorithm, AV={RAND vector, XRES vector, AUTN_HSS vector, KASME vector}, in which the vector represented for relevant information for the whole devices in the requested queue, and forwards them to the MME.

Step 4: After storing the AVs, the MME uses part of them to perform mutual authentication with the devices. The MME forwards RAND vector and AUTN_HSS vector to GC, which then computes RES vector, AUTN_Ue vector and KASME vector using EPS-AKA algorithm for the devices.

Step 5: The group controller now compares the AUTN_Ue vector for the certain devices in its group and AUTN_HSS vector received from the MME for network authentication. Once authenticated, the RES vector computed in the controller is forwarded to the MME, which then compares the XRES vector received from the HSS and the RES vector received from the controller for user equipment (UE) authentication.

Step 6: If the device and network have authenticated each other, they share the same key KASME (KASME is not transferred between UE and MME, though). And then, MME would send authentication acknowledge to the controller as a declaration for the success of mutual authentication for the devices and network.
Step 7: The group controller would record the authentication results and send identification acknowledges to the corresponding devices for notification, which means the completion of the mutual authentication between devices and the network.

Security analysis

In this section, we would talk about the details about the robustness and security analysis of the proposed GC-AKA protocol, conforming its flexibility, availability and scalability in the machine type communications under LTE network.

With this presented effective GC-AKA protocol, a huge number of terminal devices can complete the mutual authentication procedure simultaneously with the network, while alleviating congestion and overload in the network. With a controller for communications between devices and network, it will be energy-efficient for resource-constrained MTC devices. Through amelioration of the protocol, terminal devices would undertake less work than before, reducing the consumption of the resources in the devices. What’s more, unlike the resource constrained MTC devices, the group controller can employ more secure algorithms in the transmission process, providing more secure data transmissions between controller and the network and protecting them from the common attack. In addition, with such an effective design of group controller, it would be more dependable and robust for the network for fear of the communication collapse for failure of group leaders.

Conclusion

In this paper, we proposed an efficient and novel GC-AKA protocol to alleviate the congestion and overload for the network during the authentication procedure before the data transmission. Through a design of group controller, we simplified the actual work of devices during the authentication process. It can not only authenticate lots of MTC devices at the same time, but also reduce the resource consumptions for the devices, which is vital for the resource-constrained devices and brings a longer service time. With powerful ability of computation and sufficient resources for communications, more encryption and security algorithms can be used in the controller, giving a secure data transmission between controller and the network.

References