Identity Federation for Cellular Internet of Things

Bernardo Santos
Oslo & Akershus Oslo University College
Pilestredet 35, 0167 Oslo, Norway
bernardo.Santos@hioa.no

Van Thuan Do
Wolffia AS
1364 Fornebu, Norway
vt.do@wolffia.no

Boning Feng
Oslo & Akershus Oslo University College
Pilestredet 35, 0167 Oslo, Norway
boning.feng@hioa.no

Thanh van Do
Telenor Research & Oslo Akershus & Oslo University College
1331 Fornebu, Norway
thanh-van.do@telenor.com

ABSTRACT
Although the vision of 5G is to accommodate billions IoT devices and applications, its success depends very much on its ability to provide enhanced and affordable security. This paper introduces an Identity Federation solution which reuses the SIM authentication for cellular IoT devices enabling single-sign-on. The proposed solution alleviates the IoT provider's burden of device identity management at the same time as the operational costs are reduced considerably. The proposed solution is realized by open source software for LTE, identity management and IoT.

CCS Concepts
• Security and privacy→Authentication • Networks→Mobile networks.

Keywords
Mobile Identity Management, cross layer identity federation, Mobile network security, IoT security, Cyber security, cross layer security.

1. INTRODUCTION
Coined by Kevin Ashton of Procter & Gamble, later MIT's Auto-ID Center in 1999, the Internet of things aka IoT did not really take off until recently. However, its growth is at incredible rate and both the number and the variety of devices connected to the Internet are increasing at an ever accelerating pace. To meet the IoT demands the mobile industry put tremendous efforts in the elaboration of cellular IoT technologies such as Extended Coverage GSM for Internet of Things (EC-GSM-IoT), Long Term Evolution Machine Type Communications Category M1 (LTE MTC Cat M1, also referred to as LTE-M) and Narrowband IoT (NB-IoT) [1] which provide ubiquitous and mobile connectivity to low cost and low power devices while improving both outdoor and indoor penetration coverage. To ensure the success of IoT it is not sufficient to provide only efficient and low cost connections. It is necessary to be able to provide secure connectivity which is realized through strong authentication and encryption using the SIM (Subscriber Identity Module) card [2][3]. Unfortunately, the mentioned security measure is limited only to the authentication, access control and encryption towards the mobile network. The exchanged messages are indeed delivered in clear text to the IoT Platform by the mobile network. To have adequate protection the IoT Platform must have its own authentication, access control and encryption scheme, which is both technically and economically challenging. To overcome this rather severe limitation, this paper introduces a novel cross layer Identity Federation, which offers single-sign-on and confidentiality to the IoT vertical sectors such as heath, transport, logistics, automation, etc. using SIM authentication. This solution is developed within the scope of the H2020 SCOTT project [4] which is aiming at building trust in the Internet of Things. The paper starts with a comprehensive but not exhaustive review of related works. A brief review of identity management is then given before a description of state-of-the-art on cellular IoT Identity and Access Management. The central part of the paper is the proposed Identity Federation solution for cellular IoT, which is thoroughly described. Last but not least is the presentation of the secure 5G4IoT testbed. The paper concludes with some suggestions for further works.

2. RELATED WORKS
The usage of the SIM in the authentication and access control to the mobile network has proven to be both an affordable and trustable security measure. With the emergence of smart phones and mobile Internet applications there are several initiatives aiming at extending the usage of the SIM authentication to mobile Internet applications as Internet browsing, Web mail, Social networks, financial services, etc. The *Generic Bootstrapping Architecture (GBA)* [5][6] is a standard specified by the 3rd Generation Partnership Project (3GPP), which achieves the mentioned objective by introducing in the mobile network a new network element called *Bootstrapping Server Function (BSF)*, responsible for retrieving authentication vector from the *Home Subscriber Server (HSS)* and carrying out a mutual authentication of the mobile phone aka *User Equipment* (UE). The BSF provides the mobile Internet application aka *Network Application Function (NAF)* with encryption key Ks_NAF for the session between the NAF and the UE. The most serious limitation of this solution lies on the fact that

GBA requires the presence of the GBA client on the mobile phone, which is quite difficult because handset manufacturers do not have the incentive to implement it. To avoid the need for the BSF the Eureka Mobicome project has been proposing some solutions called *SIM strong authentication* that provides strong authentication from a regular browser on a regular mobile phone carrying a SIM/USIM [7][8]. However, these solutions do not address IoT, in which devices are communicating without the intervention of human beings. ETSI did promote the use of GBA in their M2M functional architecture [9] but they focus only on using the strong authentication of the SIM card. Indeed, they do not provide a comprehensive and flexible cellular IoT identity and access management, which enables both easy inclusion of IoT devices and strong authentication and confidentiality. This is precisely the objective of the solution described in this paper.

3. BRIEFLY ABOUT IDENTITY MANAGEMENT

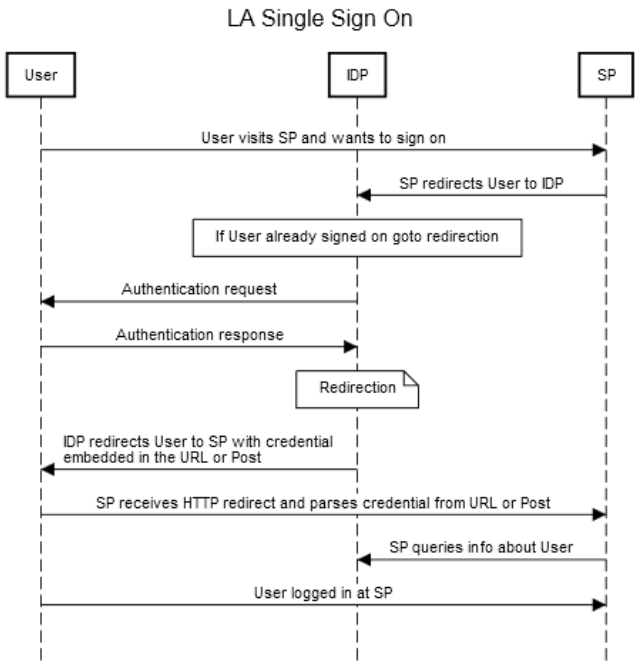
To get granted access to IoT applications or any digital service every user must have an identity that is recognizable by the IoT application or digital service provider. This identity is commonly known as user name or user account.

To ensure that the user is one he pretends to be authentication is needed and the user is usually asked to enter a password. As the number of services increases the number of passwords will grow at the same pace and the user meets the big challenge of remembering all the passwords. To make things worse for the users more and more service providers are forced to require stronger passwords, i.e. more complicated combinations of common and special symbols because of increased threats of attacks. This constitutes, however a burden for the service providers in terms of management and expenses.

To remedy the situation there are both standardized and proprietary solutions commonly known as single-sign-on [10], which both simplify the login or sign-on to the users and reduce the costs for service provider's identity management.

Liberty Alliance

To alleviate the identity burden of both the users and the Service Providers, the Liberty Alliance Project, established in 2001 and overtaken by the Kantara Initiative in 2009 introduced the notion of *Federated Network Identity* [11]. A new actor called *Identity Provider* is responsible of authenticating the users and federating user accounts at Service Providers that join the Identity Provider's *Circle of Trust*.



,

Figure 1 Liberty Alliance Single Sign On

As shown in Figure 1 upon attempt to sign on at an SP User is redirected to IDP. If User has not signed on at IDP authentication process is carried out and if it is successful User will be directed back with embedded credential to SP, which grants access to User

Users can federate their accounts with IDP. To preserve privacy, IDP and SPs exchange only opaque user handles instead of user names for example, mr3tTJ340ImN2ED.

OAuth 2.0 [12]

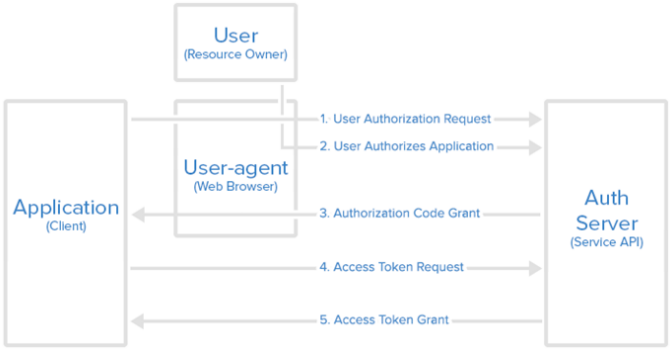


Figure 2 OAuth Authorisation Code Flow [13]

Although aiming at the same objectives, namely solving the user's problem of multiple passwords OAuth 2.0 takes an opposite approach by considering some user accounts such as Facebook, Google, Microsoft, Twitter, etc. as starting point. Indeed, users can select any of these accounts as their main account and use it at third party applications and websites without having to create new accounts and passwords.

OAuth is an open standard that allows users aka *Resource Owners* in OAuth framework, to share their accounts with third party applications aka *Client*. The Identity Provider role is removed and replaced by the Authorization Server that authenticates the users and sends authorization to the applications [13].

As shown in Figure 2 upon a visit at an application the user is requested to authorize the access to service resources i.e. his account information. The user clicks on the authorization code link presented by the application and must first log in to the service, to authenticate their identity (unless they are already logged in). Then they will be prompted by the service to authorize or deny the application access to their account.

If the user clicks "Authorize Application", the service redirects the user-agent to the application redirect URI, which was specified during the client registration, along with an authorization code. The application requests an access token from the API, by passing the authorization code along with authentication details, including the client secret, to the API token endpoint.

If the authorization is valid, the API will send a response containing the access token (and optionally, a refresh token) to the application. The application is now authorized and may use the token to access the user's account via the service API until the token expires or is revoked.

OpenID Connect

Since OAuth provides only an authorization framework OpenID Connect [14] is a standard built upon OAuth that goes one step further to offer single sign-on and identity provision on the internet.

It enables client applications to verify the identity of the user based on the authentication performed by an *OpenID Provider,* as well as to obtain basic profile information about the user in an interoperable and REST-like manner. OpenID Connect specifies a RESTful HTTP API, using JSON as a data format. Client apps receive the user's identity encoded in a secure J*SON Web Token (JWT)* called *ID token*.

The OpenID Connect authentication flow is quite similar to the LA single sign on. The service provider now called Relying Party initiates user authentication by redirecting the browser to the OpenID Provider (OP). The OpenID authentication request is essentially an OAuth 2.0 authorisation request to access the user's identity, indicated by an open id value in the scope parameter. The OP will check whether the user has a valid session i.e. a cookie in the browser. If not, the user will be asked to log in and thereafter to consent to sign on to the RP. The OP will redirect the browser back to the RP with an authorization code. This authorisation code is an intermediate credential, which encodes the authorisation obtained previously. It is therefore opaque to the RP and only has meaning to the OP server. To retrieve the ID token the RP must submit this code to the OP.

Currently OpenID Connect is definitely the most popular Identity Management which is used by several identity provider such as Facebook, Google, Twitter and even mobile operators in their *Mobile Connect*, a secure log-in solution using mobile phones. It is worth noting that OpenID Connect does not provide identity federation, i.e. federation of the SP's identity with the IDP's identity but promote the usage of the IDP's identity at the service provider. Further, it is not used in identity management for cellular IoT.

4. STATE OF THE ART ON CELLULAR IOT IDENTITY AND ACCESS MANAGEMENT

As shown in Figure 3 a current cellular IoT device can be conceptually divided into two co-existing but independent components operating respectively on the network layer and on the IoT application layer

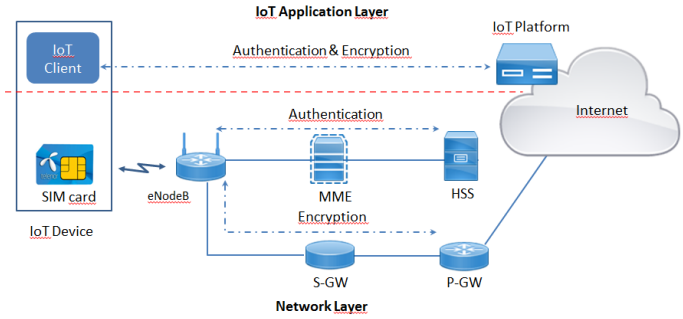


Figure 3 Authentication and Access Control of current IoT devices

On the network, the IoT device is identified by the combination of two identities: *IMEI* (International Mobile Equipment Identity) that uniquely identifies the device and *IMSI (*International Mobile Subscriber Identity) that resides in the SIM card and uniquely identifies the subscriber to the mobile network. Upon device power on a mutual authentication using AKA (Authentication and Key Agreement) protocol [15] is carried out between the mobile network Home Subscriber System (HSS) and the IoT device and upon success the device is allowed to connect the mobile network and to access to all the subscribed services. To ensure confidentiality and integrity encryption is done in the radio access link using the cipher key exchanged in the authentication. In the IoT case, the device will require a data connection and get allocated a PDP (packet data protocol) context which includes the mobile device IP address.

Now that connection has been established on the network layer communications can now be started on the IoT Application layer. To prevent malicious attacks an authentication must be performed between the IoT client and the IoT Platform. End-to-end Encryption can also be used to ensure confidentiality. The IoT device must have a unique Identity, IoT_dev_ID recognizable to the IoT platform which

must be equipped with a sufficiently strong authentication function and an adequate IdM system. These requirements incur considerable expenses and also demand IT expertise from the IoT provider. To alleviate the burden of authentication to the IoT provider we propose an Identity Federation solution that will be described in detail in the section.

5. THE PROPOSED IDENTITY FEDERATION FOR CELLULAR IoT

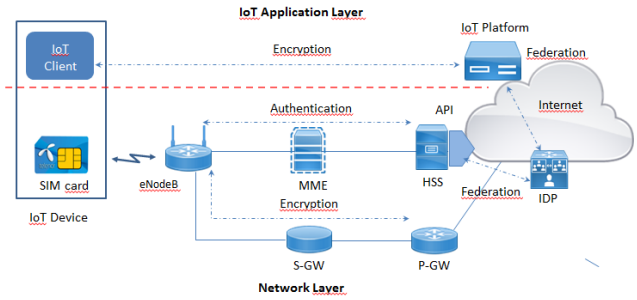


Figure 4 The architecture of Identity Federation for Cellular IoT

As shown in Figure 4 a new network entity called *Identity Provider (IDP)* is introduced. The mission of the IDP is to bridge the gap between the IoT Application layer and the Network layer and hence to enable single sign on of IoT devices.

A *SIR API (Subscriber Information Retrieval Application Programming Interface)* is implemented on the Home Subscriber Server (HSS). The interface between the HSS is the standard Diameter-based S6m [16] which supports at least of the following procedure:

Subscriber Information Retrieval

To illustrate the configuration, federation, authentication and authorization of an IoT system let us consider a small surveillance IoT system with 3 cameras, 1 smoke detector and 3 contact sensors.

Configuration and federation

Seven IoT subscriptions with 7 SIM cards have been acquired from a mobile operator. Each device gets assigned a SIM card containing an IMSI and one identity corresponding to their location. The IoT platform carries out an identity federation which results to a federation of device identities and mobile identities is shown in Table 1.

Device_ID	IMSI
Camera_ Front_Door	$IMSI_1$
Camera_ Backyard	$IMSI_2$
Camera_ Garage	$IMSI_3$
Smoke_Detector	$IMSI_4$
Contact_ Front_Door	$IMSI_5$
Contact_ Balcony_Door	$IMSI_6$
Contact_ Back_Door	$IMSI_7$

Table 1 Identity Federation Table

Authentication and authorization

When all the devices get installed their SIM and are properly mounted at their location the power is turned on.

At the network layer a mutual authentication process is carried out between the SIM of the IoT device and the mobile network HSS. Upon successful authentication, the IoT device is authorized to access the mobile network and gets granted an Internet connection.

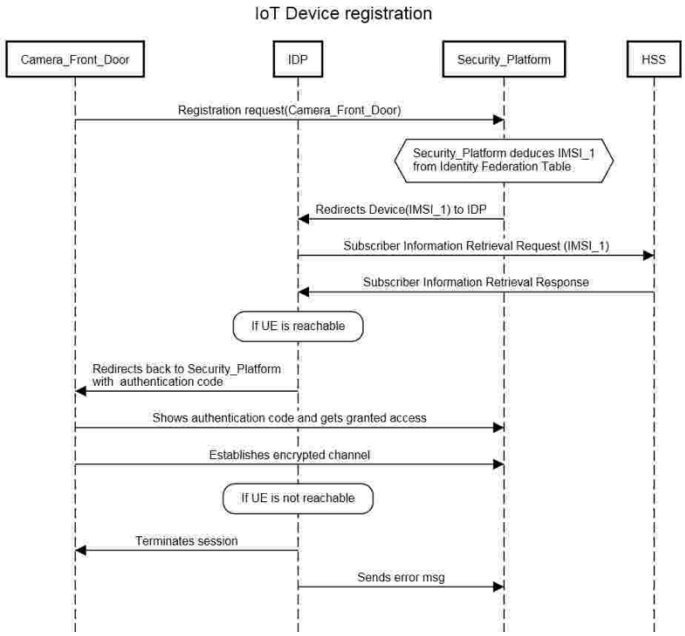


Figure 5 IoT Device Registration and Authentication

The IoT devices can now initiate the registration at the IoT platform. Each device will perform the same sequence of actions as Camera_Front_Door shown in Figure 5. Camera_Front_Door sends a registration_request to the Security_Platform and gets redirected to the IDP. The IDP invokes Subscriber_Information_Retrieval_Request (IMSI_1) at the HSS and receives a Subscriber Information Retrieval Response which contains information about whether the User Equipment (device) is registered to any serving node. If it is the case, the device has been successfully authenticated and the IDP can re-direct Camera_Front_Door with an authorisation code back to the Security_Platform. which grants access to Camera_Front_Door. Further, an encrypted channel can be

established between Camera_Front_Door and the Security_Platform.

In the case that the UE is not registered to any serving server an anomaly has occurred. It could be an attack or simply a fault situation. To prevent any further damage the IDP will terminate the session with Camera_Front_Door and send an error message to the Security_Platform. Further actions should be carried out to find out what has happened to Camera_Front_Door.

6. IMPLEMENTATION

To verify the feasibility of the proposed Identity Federation for IoT devices a 4G LTE (Long Term Evolution) has established at the Secure 5G4IoT Lab at the Oslo & Akershus University College using the open source software OpenAirInterface developed by EURECOM [17].

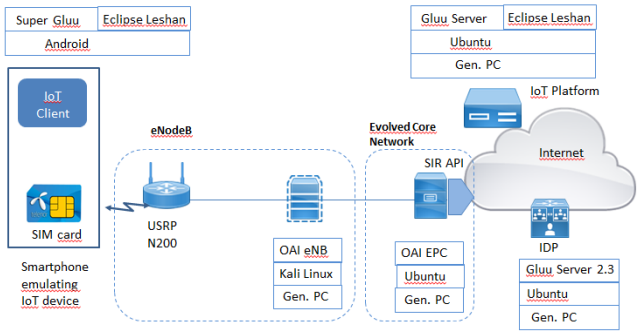


Figure 6 The Secure 5G4IoT Testbed

As shown in Figure 6 the LTE base station *eNodeB* is realised by:

- a generic PC running Kali Linux and OpenAirInterface eNB connected to
- a USRP (Universal Software Radio Peripheral) N200, software-defined radios designed and sold by Ettus Research [18]

The whole *Evolved Packet Core* is realized by:

- a generic PC running Ubuntu and OpenAirInterface, which includes a *HSS* and a *Subscriber Information Retrieval API*

The Identity Provider (IDP) server is implemented by:

- a generic PC running Ubuntu and Gluu server 2.3 [19], which is an open source identity provider server software

The IoT Platform is realized by:

- a generic PC running Ubuntu and Gluu server 2.3 and also a lightweight M2M server open source using Eclipse Leshan [20]

Due to the lack of cellular IoT devices an Android smartphone is used to emulate on by installing Super Gluu and an Eclipe Leshan client.

7. CONCLUSION

In this paper an Identity Federation solution which allows the reuse of the SIM authentication carried out on the network layer for IoT applications and hence providing single sign on is presented. The proposed solution is proven to be feasible by making use of state-of-the-art open source software such OpenAirInterface, OpenID Connect and Eclipse IoT [21]. With the proposed solution, IoT security will be enhanced while operational costs will be considerably reduced. The solution will pave the way for support of billions of IoT devices and application with the coming 5G mobile networks. As further work, it is definitely relevant to initiate the development of cellular IoT devices and gateway, which can execute both a IoT client and an Identity client. Another further work will be the design and implementation of a cross layer security solution aiming at improving security of IoT systems by combining security measures deployed at both the mobile network layer and the IoT application layer.

8. REFERENCES

[1] GSMA: 3GPP Low Power Wide Area Technologies: White paper 2.0, 2017

[2] 3GPP: TS 11.11 Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) Interface, ver 8.14.0, 12-06-2007

[3] 3GPP: TS 31.102 Characteristics of the Universal Subscriber Identity Module (USIM) application ver 16-06-2017

[4] SCOTT: Secure Connected Trustable Things- https://scottproject.eu

[5] 3rd Generation Partnership Project: 3GPP TS 33.220 V8.2.0 (2007-12) Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA) Generic bootstrapping architecture (Release 8)

[6] Timo Olkkonen: Generic Authentication Architecture, Helsinki University of Technology - http://www.tml.tkk.fi/Publications/C/22/papers/Olkkonen_final.pdf

[7] Do Van Thanh, Tore Jønvik, Do Van Thuan & Ivar Jørstad: Enhancing Internet service security using GSM SIM authentication, Proceedings of the IEEE Globecom2006 conference – ISBN 1-4244-0357-X – San Francisco, USA, Nov 27 - Dec 1, 2006

[8] Do van Thanh, Tore Jønvik, Boning Feng, Do van Thuan & Ivar Jørstad: Simple Strong Authentication for Internet Applications using mobile phones, Proceedings of IEEE Global Communications Conference (IEEE GLOBECOM 2008), ISBN 978-1-4244-2324-8, New Orleans, LA, USA, Nov 30 – Dec 4, 2008

[9] ETSI: TS 102 921 Machine-to-Machine communications (M2M); mIa, dIa and mId interfaces, V2.1.1 (2013-12)

[10] Telektronikk 3/4 2007: Identity Management – Guest Editorial Do van Thanh – ISSN 0085-7130 - https://www.telenor.com/wp-content/uploads/2012/05/T07_3-4.pdf

[11] Liberty Alliance: ID-FF Architecture Overview – vers. 1.2-errata-v1.0.

[12] IETF Request for Comments: 6749: The OAuth 2.0 Authorization Framework, October 2012

[13] Anicas Mitchell: An Introduction to OAuth 2, posted Jul 21, 2014 - https://www.digitalocean.com/community/tutorials/an-introduction-to-oauth-2

[14] OpenID Connect: http://openid.net/connect/

[15] ETSI: TS 133 102 v3.6.0 (2000-10) Universal Mobile Telecommunications System (UMTS); 3G Security; Security Architecture

[16] 3GPP: TS 29.336 V15.0.0 (2017-09) Technical Specification 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Home Subscriber Server (HSS) diameter interfaces for interworking with packet data networks and applications (Release 15)

[17] The OpenAirInterfaceTM Software Alliance (OSA) http://www.openairinterface.org/

[18] Ettus Researcjh: https://www.ettus.com/

[19] Gluu: https://www.gluu.org/

[20] Leshan: https://eclipse.org/leshan/

[21] Open Source for IoT: https://iot.eclipse.org/

Acknowledgement:

This paper is a result of the SCOTT project (www.scott-project.eu) which has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement No 737422. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Spain, Finland, Ireland, Sweden, Germany, Poland, Portugal, Netherlands, Belgium, Norway

Columns on Last Page Should Be Made As Close As Possible to Equal Length

The latest Infoblox Security Assessment Report reveals 40 per cent of the files it tested showed evidence of DNS tunnelling. That's nearly half of the enterprise networks that were tested by Infoblox returning evidence of a threat that can mean active malware or ongoing data exfiltration within the network.

For more than a decade now the bad guys have been looking at ways of using DNS to exfiltrate data. Port 53 manipulation, also known as DNS Tunneling, allows data to be directed through this established path for malicious purposes. Perhaps this shouldn't be surprising, given the inherently trusted nature of DNS.

Authors' background

Your Name	Title*	Research Field	Personal website
Bernardo Santos	PhD Candidate	5G/IoT/Security	
Van Thuan Do	Senior Scientist	IoT	
Boning Feng	Assoc. Professor	Resilience/Robustness	
Thanh van Do	Full Professor	Mobile & Cyber security	www.item.ntnu/~thanhvan

***This form helps us to understand your paper better, the form itself will not be published.**

***Title can be chosen from: master student, Phd candidate, assistant professor, lecture, senior lecture, associate professor, full professor**