Radiocommunication Study Groups

Received: 16 February 2016

Subject: Resolution ITU-R 66 and WRC-19 agenda item 9.1, issue 9.1.8

Document 5D/XX-E
16 February 2016
English only

FRANCE, xxxx

PROPOSAL FOR STUDIES RELATED TO THE SECURITY OF MACHINE-TYPE COMMUNICATIONS AND INTERNET OF THINGS

1 Introduction

In order to address evolving user needs, ITU-R is currently working on the future development of "Internet of Things" (IoT) under resolution ITU-R 66 adopted by the year 2015 Assembly of Radio communications (RA-15). Furthermore, WRC-15 agreed on a new issue 9.1.8 to the WRC-19 related to Studies on the technical and operational aspects of radio networks and systems, as well as spectrum needed, including possible harmonized use of spectrum to support the implementation of narrowband and broadband machine-type communication infrastructures, in order to develop Recommendations, Reports and/or Handbooks, as appropriate, and to take appropriate actions within the ITU Radio communication Sector (ITU-R) scope of work.

The report "Harnessing of the Internet of Thing for Global Developments" (by ITU and CISCO) points out numerous applications and explicates several operational and technical challenges relevant to the massive deployment of machine type communications and of Internet of Thing (IoT), including security, privacy and policy considerations. Particularly, the expected increasing deployment of such systems should remain dependent on the security and privacy of stakeholders and of the trust in confidentiality of professional and private users of radio devices. Nevertheless, regarding the economy and the engineering of machine type communications, there would be great advantage to enable massive radio access without User Identity Module (UIM-less), and to keep the use of UIM for communication services of higher level.

For instance, it seems that machine type communications and associated RAT for M2M and IoT can take benefits from the definition and study of key-free mechanisms for improving the reliability, the security, the privacy and the confidentiality of the physical layer of radio communications, as a complement of existing UIM-based identity authentication and cipher schemes. In this context, some existing studies address technical aspects of key-free security mechanisms and UIM-less RATs based on extraction of radio channel randomness and on physical layer security (PHYSEC).

2 Proposals

Frances proposes to consider a possible new report in response to the WRC-19 issue 9.1.8, addressing the security of machine type communications.

The WP 5D is invited to consider existing material as listed in the annex 1 and to initiate a new report whose outline is proposed in annex 2.

Annex 1

EXISTING MATERIAL RELATED TO THE SECURITY OF MACHINE TYPE COMMUNICATIONS

A.1.1- "Active and passive eavesdropper threats within public and private civilian wireless networks - existing and potential future countermeasures – an overview"

Abstract— The paper aims at providing an overview of threats that may deteriorate security level and trust in public wireless networks, because of eavesdropper and hacking technologies that operate at the radio interface, and aims at providing an introduction to relevant counter-measures that deal with "physical based" security in a large sense (Physec). It highlights selected promising Physec technologies that are expected in the future years by mixing classical protections and advanced issues of information-theoretic security, secrecy coding and cooperative jamming.

«http://www.phylaws-ict.org/?page_id=92» [On line]

A.1.2- "PHYSEC concepts for wireless public networks - introduction state of the art perspectives"

Abstract— The paper aims at providing elements about advances in physical security (physec) and about relevant application perspectives in public wireless networks. After a short introduction of existing protections of communications signals, it introduces several notions relevant to information theory and point out the main physec concepts. Then, it discusses their theoretic advantages and the current knowledge about secrecy codes. Finally, the paper highlights practical implantation perspectives of physec in existing and future public radio-networks, as stand-alone added modules operating at the physical player, or as added algorithm combined with classical solutions in order to upgrade and/or to simplify existing security procedures.

«http://www.phylaws-ict.org/?page_id=92» [On line]

A.1.3- "Perspectives of Physical Layer Security (Physec) for the improvement of the subscriber privacy and communication confidentiality at the Air Interface - Results for WLANs, IoT and radiocells"

Abstract— Physical layer security (PHYSEC) is a promising new security approach in the context of the IoT and ubiquitously connected systems. PHYSEC exploits the intrinsic randomness of the radio channel between several nodes to establish cryptographic keys in a plug-and-play manner, to achieve information-theoretic security without complex ciphers, and to securely pair devices. Each of these opportunities has been successfully demonstrated by the German research project Prophylaxe for application to the Internet of Things (Wi-Fi and IEEE 802.15.4) and by the European project Phylaws for application to Wi-Fi and to Radio-cells (LTE).

«http://www.phylaws-ict.org/?page_id=58» [On line]

A.1.4- "Analysis of threats, countermeasures and self-protection techniques"

Overview— This document surveys Physical Layer Security (Physec) threats and potential countermeasures. The purpose of the document is to achieve a wide understanding on the security threats and existing solutions as well as on the possibilities in the physical communication layer in

the scope of existing and emerging wireless standards. This document is organized in the following manner. Section 2 lists and defines the main concepts and terms, which are relevant for the document, and illustrates the scope of the document. Section 3 surveys on security attacks against wireless systems. It starts by an analysis and survey of consequences of lacking security, then classifies attacks, as well as gives brief explanations and references for more detailed attack descriptions. Section 4 surveys and analyses the security countermeasures and lists numerous references. Section 5 analyses how 2/3/4G and WLAN standards are vulnerable against the identified attacks and what kind of Physec based security countermeasures could be utilized.

«http://www.phylaws-ict.org/?page_id=48» [On line]

A.1.5- "New opportunities provided by modern waveforms new security protocols and sensing/measure of radio environments"

Overview— This document surveys opportunities for Physical layer Security (Physec) improvements in existing and emerging public wireless standards. It particularly surveys versatile radio access protocols for the first access stages, cognitive and opportunist RATs, advanced front end processing for spectrum sensing, CIR measurement and adaptive configuration of modulation and coding schemes, antenna processing into MISO and MIMO technologies and their relevant modulations and space time block coding schemes, Full-Duplex technologies (including self-interference mitigation techniques) and advanced Radio Protocols for Identification Friend or Foe (IFF). This document deepens technical considerations relevant to future implementations of security-upgrades of existing and new wireless standards, based on Physec concepts. It also identifies the most promising solutions for future works. The content of the document is relevant to both existing and new wireless standards

«http://www.phylaws-ict.org/?page_id=48» [On line]

A.1.6- EC project PHYLAWS

Overview— **PHYLAWS** stands for **PHY**sical **LA**yer **W**ireless **S**ecurity and address the enhancement of privacy at the radio interface of wireless networks Physical Layer Security (Physec) and Design of Trustworthy Wave Forms and Radio Access Protocols in realistic Test cases: WiFi (experiments) and LTE (simulation).

Its main objectives are the design and the efficiency proof of new privacy concepts for wireless communications that exploit propagation properties of radio channels ; then the search for realistic terminal and node embedded implantations in existing and in future Radio Access Technologies.

«http://www.phylaws-ict.org» [On line]

A.1.7- BMBF project PROPHYLAXE,

Overview— Providing Physical Layer Security for the Internet of Things, prophylaxes is a strategic research project supported by the German Ministry of Education and Research (BMBF) within BMBF program "IT-Sicherheitsforschung", 4th call, which makes use of Physical Layer Security to foster new applications for the IoT.

«http://www.ict-prophylaxe.de» [On line]

Annex 2

PROPOSAL FOR SUMMARY OF NEW REPORT RELATED TO THE SECURITY OF MACHINE TYPE COMMUNICATIONS

1. NEED FOR SECURITY OF MACHINE TYPE COMMUNICATIONS
2. SECURITY OF THE PHYSICAL LAYER
   - 2.1. SIM based security
   - 2.2. UIM based security
   - 2.3. Physical layer based security
     - 2.3.1. Extraction of radio-channel randomness and exploitation
       - 2.3.1.1. Radio-channel randomness parameters to be measured
       - 2.3.1.2. Performance and tolerances.
       - 2.3.1.3. Radio propagation characteristics in the SHF/EHF band
       - 2.3.1.4. Particular cases of Time Division Duplexing and of Frequency Division Duplexing.
     - 2.3.2. Use of radio-channel randomness for security and privacy of the physical layer into the M2M/IoT Radio Access Technologies
       - 2.3.2.1. Definition of use cases
         - 2.3.2.1.1. Integrity and confidentiality of signalling information;
         - 2.3.2.1.2. Identity authentication and identity confidentiality of terminal/node/user/UIM; verification of UIM Holder;
         - 2.3.2.1.3. Integrity and confidentiality of user data transmission (including DMTF).
       - 2.3.2.2. Study of security and privacy schemes based on physical layer security
       - 2.3.2.3. Study of their usage for the protection of signalling and access messages (as a complement of identity authentication and cipher mechanisms that are already implanted into RATs).
       - 2.3.2.4. Study of advanced concepts: remote control of security schemes, management of security information into the protocol layers.
3. SECURITY OF THE UPPER LAYER