Secure sensor data transmission in 5G networks using pseudorandom number generators

Borja Bordel[1]* and Ramón Alcarria[2]
[1]Department of Telematics Systems Engineering
[2]Department of Topographic Engineering and Cartography
Universidad Politécnica de Madrid, Spain
{bbordel, ramon.alcarria}@dit.upm.es

Abstract

Future 5G networks face the challenge of supporting the global communications among the millions of devices making up the Internet-of-Things. Traditional 4G mobile devices have a high computational power, so applications based on the transmission of sensor data (accelerometers, GPS, etc.) may apply heavy end-to-end securing solutions. However, new 5G mobile components usually present reduced capabilities and a low clock speed. Therefore, new security solutions for sensor data transmission in streaming have to be developed. In this paper, it is described a light cryptography technology to secure sensor data during radio transmission in 5G networks. The proposed solution is based on pseudorandom number generators, which are specifically designed to fulfill the requirements of 5G systems. A simulation scenario and a first real deployment are developed in order to evaluate the performance of the contribution.

Keywords: 5G networks, cryptography, pseudorandom number generators, security, data transmission

1 Introduction

Future 5G networks will be designed to support communications between thousands of small, resource constraint devices [35]. These devices will be deployed in the context of a new technological paradigm, the Internet-of-Things (IoT), which is changing society at all. Traditional Internet services and applications (such as the web) will be dramatically modified and complemented with unimaginable businesses. From applications to Industry (the term Industry 4.0 was coined) [16], to enhanced home automation applications for water and energy saving [1], the impact of the IoT systems is growing day by day.

Any case, all future services will require the transmission of great amounts of data, sometimes with real-time requirements, between a pervasive hardware platform composed by several heterogeneous elements (usually sensor nodes) and a remote central server where service logic and other resources are hosted [35]. In that way, 5G solutions usually include proposals in order to address this challenge (which is probably the key challenge in 5G networks): fast handovers [33], new spectrum management techniques [4], advanced pricing [32], etc. In this line, new security techniques (as well as privacy preservation solutions) are usually also mentioned [38].

In fact, several of the future IoT applications will be actor-focused (based on people who are monitored, on personal information that is collected etc.) [5]. In that way, important personal information will be transmitted and managed by small resource constraint embedded devices that cannot execute complex standard security and privacy protection techniques due to their limited computational power and

Research Briefs on Information & Communication Technology Evolution (ReBICTE), Vol. 3, Article No. 11 (November 15, 2017)
*Corresponding author: E.T.S.I. Telecomunicación. Universidad Politécnica de Madrid. Avenida Complutense nº 30. 28040 - Madrid (Spain), Tel. (+34)-91-549-57-00 (ext. 3035)

low clock speed [7, 6]. So that, as indicated by various works [11, 8, 34], new and lighter security and cryptography solutions, adequate to be implemented into resource constraint devices are needed.

Therefore, the objective of this paper is to describe a light security (cryptographic) solution for protecting sensor data transmissions in IoT systems supported by 5G networks. The proposed technique is based on pseudorandom number generators [13], which are coordinated and synchronized by means of a negotiation protocol in order to establish a secure link between remote nodes and the base station. A hybrid cryptographic system (based both on symmetric and asymmetric techniques) being able to remove distortions due to time delays, multipath transmissions and node mobility of 5G systems is finally obtained.

The rest of the paper is organized as follows: Section 2 describes the state of the art on security provision technologies for resource constraint devices; Section 3 contains the main contribution; Section 4 presents a first experimental validation based on a simple initial prototype; and Section 5 concludes the paper.

2 State of the Art

Different proposals for security provision in systems based on resource constraint devices may be found. As in any other discipline related to security and cryptography, two main alternatives have been studied: asymmetric key schemes and symmetric key schemes.

Asymmetric solutions, as they require a higher computational power, are usually designed to employ physical effects in order to reduce the calculation effort. For example, authentication protocols based on Elliptic Curves (EC) considering physical phenomena such as vibrations or temperature [31] have been reported. In fact, in general EC has been proved to be usable in several different software implementations and hardware platforms; even some works confirm that cryptography in EC is well supported in current IoT devices [9, 24, 40](with some modifications). In this sense, some proposals based on the transmission of signed information and data (for example, using JSON objects) may be found [28].

However, as this approach still requires and important calculation time if implemented in resource constraint devices, some certificate-free solutions have been described. Collaborative solutions [17] or implicit certificates [30] are some examples of these technologies.

Any case, some regular Public Key Infrastructures (PKI) have been proposed for IoT systems, considering there is enough computation power in devices. Secure data transportation layers [29], authentication protocols [15] and asymmetric cryptographic schemes for streaming communications [10] have been communicated. Required changes to be applied to traditional PKI solutions in order to be applicable to IoT systems have been also investigated [39].

Although, as seen, a great variety of proposals based on asymmetric cryptography for IoT systems have been proposed, due to their lower resource consumption, symmetric cryptography schemes are preferable [14].

If hash functions, sometimes employed in symmetric cryptography, are not considered as they show the same problems as previously cited PKIs (although some light hash functions have been reported [2]), two different encryption solutions may be found: block ciphers and stream ciphers.

In respect to block ciphers cyclic redundancy codes (CRC) are probably the most employed today in any scenario, even in IoT deployments [36]. This kind of ciphers, furthermore, are very common in IoT scenarios based on RFID technologies and other identity communication techniques (such as Bluetooth beacons) [25, 22], as transmitted packet are sparse and always present the same length. Moreover, hardware-supported (based on registers and other sequential logic circuits) have been also described [20].

Although block ciphers may be also based on pseudorandom number generators (PRNG), these solutions are more common if stream ciphers are considered. In particular, several proposals specifically

designed to be applied in IoT scenarios (made of Smart devices [19] or RFID tags [26, 21]) have been reported.

Finally, several proposals about protocols to security management may be also found [23]. Solutions for user [37] and devices [27] authentication have been described.

In comparison to these previous proposals based only on one cryptographic technique (symmetric or asymmetric) the proposed solution in this work mixes both approaches in a hybrid technology. The initialization procedure (performed only once, before operation time) is based on KPI. This process is employed to configure a light symmetric cipher based on a pseudorandom number generator, whose output may be employed as both, block and stream cipher.

3 A Light Security Solution for 5G Devices

A certain IoT scenario based on 5G technologies $\mathcal{S}_{iot}$ composed by a couple of element sets $\mathcal{S}_{iot} = \{B, N\}$ (see Figure 1). B is the set of 5G base stations, and N is the set of mobile nodes considered in the scenario. Without loss of generality, it may be considered that there is only one base station in the scenario, i.e. $card(B) = 1$.

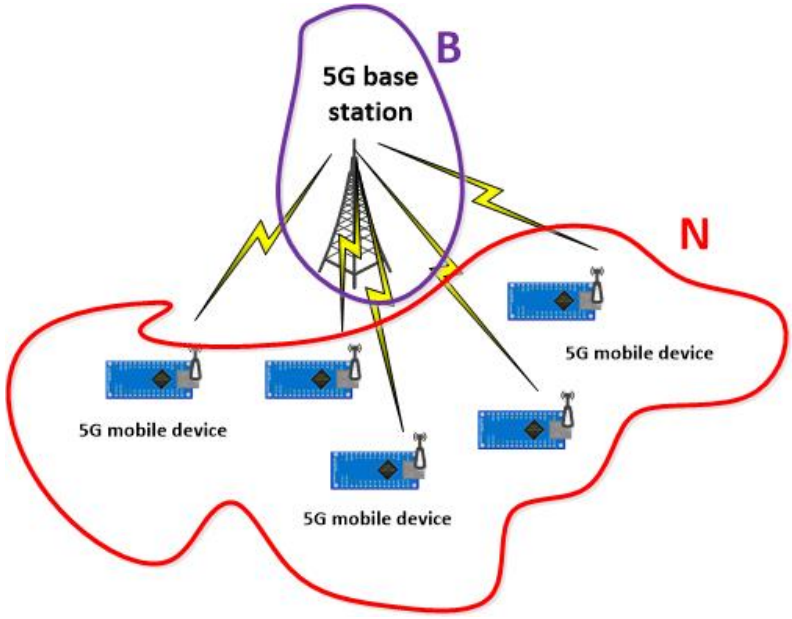

Figure 1: Study scenario

Then, two cryptographic functions are defined. $\mathcal{F}_{sym}$ represents a symmetric cipher based on a pseudorandom number generator, and $\mathcal{F}_{asym}$ describes a KPI, where the base station acts a central node (the element which distributed its public key).

In order to initialize the symmetric cipher a set of parameters $\mathcal{K}$ has to be communicated between transmitter and receptor. This set of parameters may be understood as the secret key of the cipher, as any entity provided with the same key can obtain the secured information from the encrypted message. In that way, the communication of these parameters has to be secure as well. Moreover, in order to confirm that the secure link is available, an acknowledgment message should be transmitted, following the requirements of 5G mobile networks.

In particular, the establishment of a communication link (secure or not), as indicated by many different works, has to be preceded by a triple handshaking [12, 18]. This technological solution, however, has

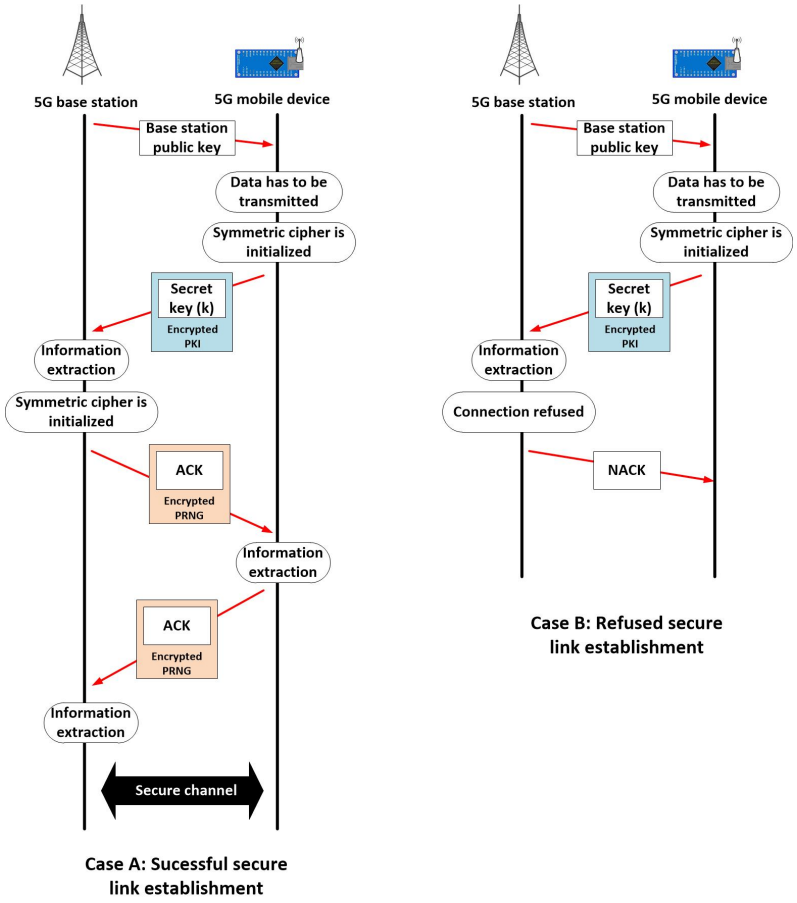

Figure 2: Message sequence chart (a) successful establishment (b) refused establishment

to be designed in the adequate way, as it may be an important mechanism employed by cyber-attackers in order to break the encryption [3].

Briefly, the proposed handshaking procedure is as follows. The 5G station has to broadcast its public key, in order to provide every mobile device with it. Then, if a sensor node wants to transmit data to the Internet it must initialize the symmetric cipher. The employed secret key is protected using the public key of the base station and it is transmitted. Then, the base station extract the secret key for the symmetric cipher and initializes it.

At this point, the base station constructs an acknowledgment message, which is secured using the symmetric cipher. When the remote sensor node receives this secure message, tries to recover the secret information. If possible, and it is an acknowledgment message, the remote sensor node sends the final confirmation using also the symmetric cryptographic solution. If an error occurs, a second iteration is performed. If at the end of this second interaction, the error persists or the base station refuse the communication, the secure link it is not stablished.

Figure 2(a) shows a message sequence chart describing a successful secure link establishment.

Although data format employed to transmit the secret key of the symmetric cipher it is independent from the proposed solution, as IoT devices tend to present constraint resources and a low computation power, light information representation mechanism (such as JSON) are preferred.

On the other hand, sometimes, see Figure 2(b), the base station might refuse the establishment of the secure link. In this case, a non-acknowledgment message is sent as plain text to the remote node, which

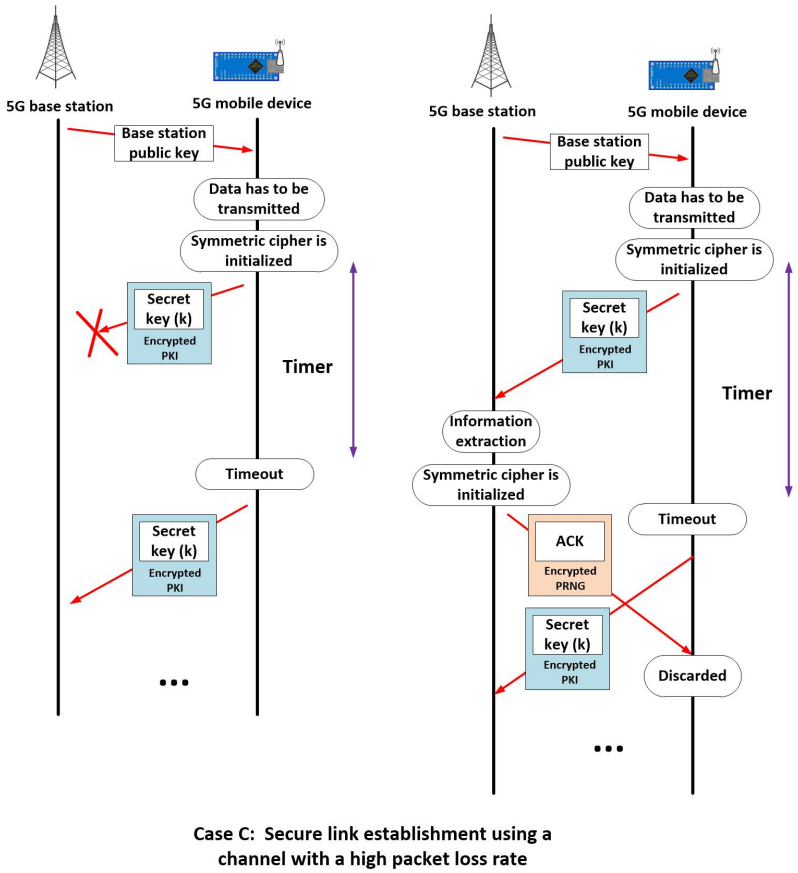

Figure 3: Message sequence chart: secure link establishment using a channel with a high packet loss rate

should store the acquired data and wait until the remote base station is available.

Nevertheless, fails in the secure link establishment procedure cannot be only due to refuse decisions in the base station. Problems due to a high packet loss rate in the communication channel (and other similar effects) may also affect this process. In that way, a technique in order to address these problems is required (see Figure 3 and Figure 4). Basically, if any problem occurs, a second iteration is performed. This second iteration may be trigger by a timer if no response of the base station is received before the timeout alert (Figure 3). As a communication channel with a great delay may be being employed, each message during the initialization procedure should include a transaction number (so that, any received message referring a past transaction is discarded), and the mentioned timer should be adapted to the conditions of the communication channel (in order to establish success secure connections).

However, other times, communication channel does not present a big delay but it is a very noisy medium and data packets get corrupted. In this case, a second interaction of the establishment procedure it is also triggered (see Figure 4).

Finally, if the triggered second interaction also causes an error, corrupted packets are received, or not response from the base station is received, the establishment procedure is canceled by the remote sensor node (see Figure 5).

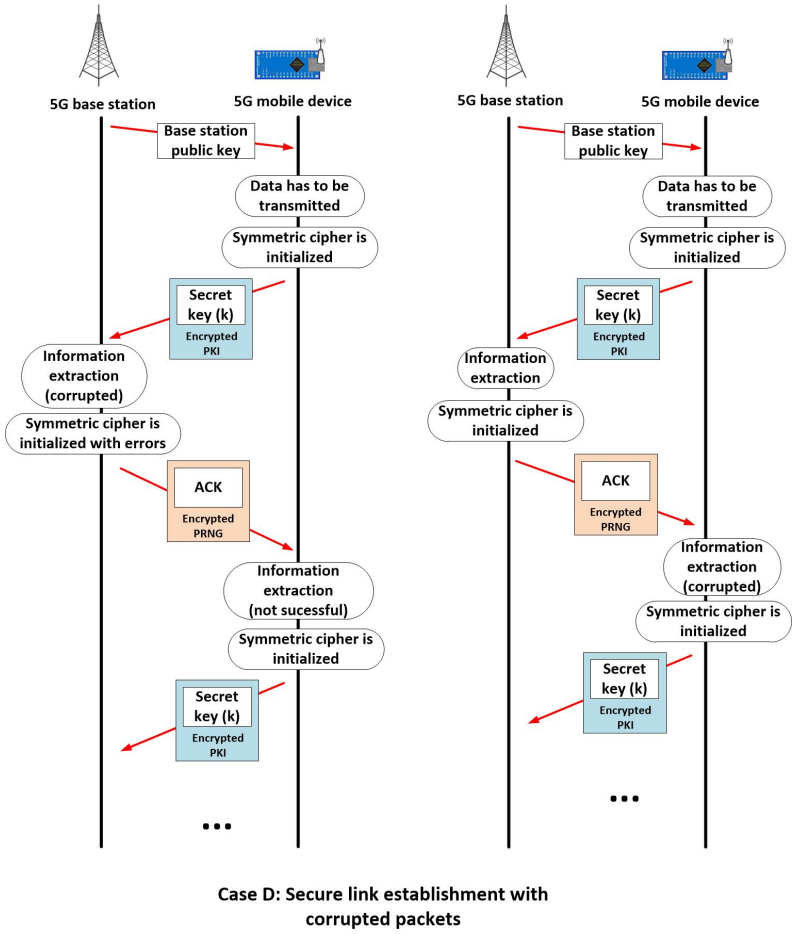

Figure 4: Message sequence chart: secure link establishment with corrupted packets

4 First Implementation and Experimental Validation

In order to validate the proposed solution as a valid technology for security provision in IoT scenarios based on 5G networks and resource constraint devices a first real implementation of our proposal was developed. The system was deployed using a couple of Arduino microcontrollers (see Figure 6) communicated by means of a serial port (UART). One of the microcontrollers was configured to act as base station, and the other one was employed to represent a standard 5G mobile IoT device.

Using Arduino programming language the proposed protocol was implemented. As asymmetric cipher was selected a light implementation of the RSA (Rivest, Shamir y Adleman) algorithm. The selected implemented is distributed with the AVR-Crypto-Lib library, and it is compatible with Atmel microcontrollers (the architecture of Arduino platform).

Besides as PRNG for the symmetric cipher it was selected the MeTuLR generator [25]. This scheme is based on logic operations that may performed in a very easy and fast way by Arduino microcontrollers and other similar low-power IoT development platforms and technologies.

The constructed prototype was forced to establish a secure link between both microcontrollers two hundred times. We found that, the proposed algorithm, only fails 2% of times.

However, the obtained results are dependent on the number of devices in the scenario, as (in the proposed solution) base stations may turn into bottlenecks if an appropriate network design and sizing it is not performed.

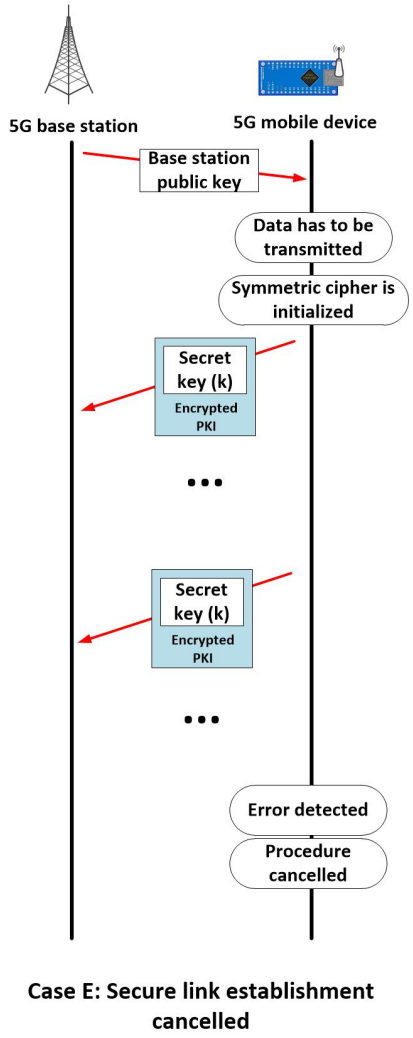

Figure 5: Message sequence chart: secure link establishment canceled

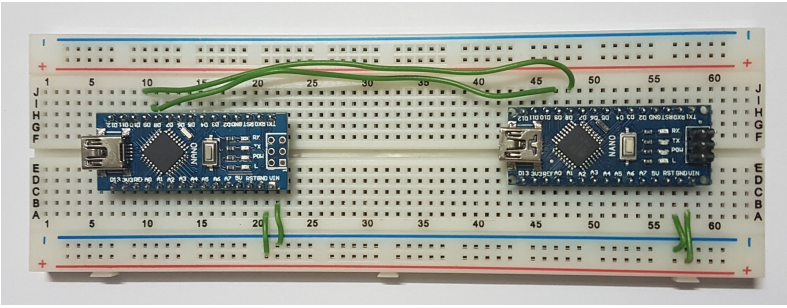

Figure 6: First implemented prototype

In order to evaluate this dependency, a simulation scenario was constructed using the NS3 simulator. In the planned simulation, base stations and mobile devices were provided with the proposed algorithm, configured in the same was as in the previously described prototype. During this experiment, the number of considered IoT devices in the simulation scenario was increased. Twelve simulation were performed

for each number of IoT devices. With the acquired information, the success rate in establishing the desired secure link was calculated. Figure 7 shows the obtained results.

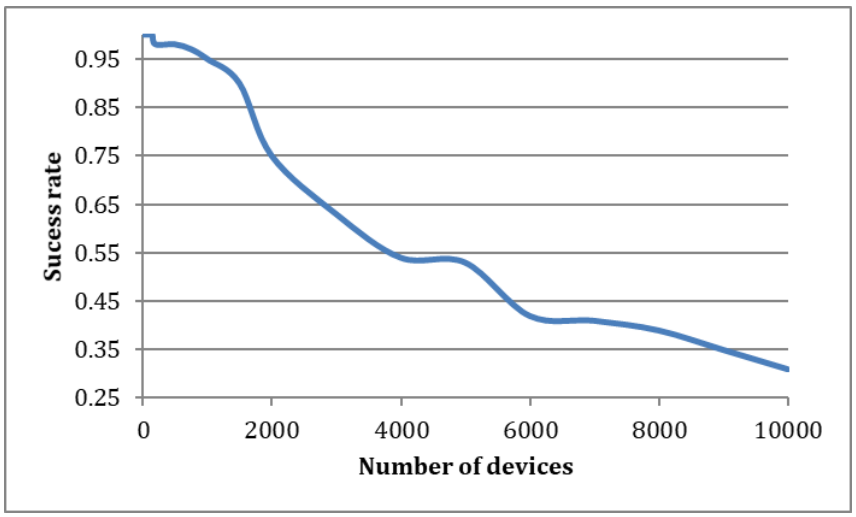

Figure 7: Success rate. Simulation results

As can be seen, success rate is around 100% until the number of considered devices reaches a thousand. At this moment, the success rate is around 90%. From this point, the high number of devices communicating with a same base station causes transmission delays going up, and each time it is more complicated for mobile devices to establish a secure link with the 5G station. If ten thousands devices are considered, the success rate descends to 30% (approximately). However, it is not planned the future 5G networks to present this great device density inside a unique cell. Therefore, the obtained results are a first evidence that the proposed technology is a valid solution for security provision in IoT systems based on 5G mobile networks.

5 Conclusion and Future Works

This paper describes a light solution for security provision in IoT scenarios based on 5G networks. Future engineered systems will be based on pervasive hardware platforms made of resource constraint devices, which cannot support traditional heavy encryption algorithms. In that way, new and adequate techniques are needed. The proposed solution includes a initialization protocol based on asymmetric cryptography and a symmetric cipher based on pseudorandom number generators. The described contribution, thus, enables IoT devices to establish a secure link between themselves and 5G base stations.

In order to evaluate the performance of the proposed technology, a first prototype based on Arduino microcontrollers has been constructed, and a simulation scenario has been employed to determine the scalability and the operation limits of the presented solution. Obtained results are a first evidence of the validity of the described security solution.

Future works should consider enhanced prototypes (including, for example, wireless communication) and address some practical problems not treated in this first work. For example, in order to determine the security level of the entire proposal, details about the selected pseudorandom number generator (such as the employed seeds) should be considered, as resource constraint devices may also impose restrictions in this sense.

Acknowledgments

The research leading to these results has received funding from the Ministry of Economy and Competitiveness through the INPAINK (RTC-2016-4881-7) and SEMOLA (TEC2015-68284-R) projects, and from the Centre for the Development of Industrial Technology (CDTI) through PERIMETER SECURITY project (ITC-20161228). Borja Bordel has received funding from the Ministry of Education through the FPU program (grant number FPU15/03977).

References

[1] R. Alcarria, B. Bordel, D. Martín, and D. Sanchez De Rivera. Rule-based monitoring and coordination of resource consumption in smart communities. *IEEE Transactions on Consumer Electronics*, 63(2):191–199, May 2017.

[2] J.-P. Aumasson, L. Henzen, W. Meier, and M. Naya-Plasencia. Quark: A lightweight hash. *Journal of Cryptology*, 26(2):313–339, April 2013.

[3] K. Bhargavan, A. D. Lavaud, C. Fournet, A. Pironti, and P. Y. Strub. Triple Handshakes and Cookie Cutters: Breaking and Fixing Authentication over TLS. In *Proc. of the 2014 IEEE Symposium on Security and Privacy (SP'14), San Jose, California, USA*, pages 98–113. IEEE, May 2014.

[4] N. Bhushan, Junyi Li, D. Malladi, R. Gilmore, D. Brenner, A. Damnjanovic, R. Sukhavasi, C. Patel, and S. Geirhofer. Network densification: the dominant theme for wireless evolution into 5G. *IEEE Communications Magazine*, 52(2):82–89, February 2014.

[5] B. Bordel, R. Alcarria, D. Martín, T. Robles, and D. S. de Rivera. Self-configuration in humanized Cyber-Physical Systems. *Journal of Ambient Intelligence and Humanized Computing*, 8(4):485–496, August 2017.

[6] B. Bordel, R. Alcarria, T. Robles, and D. Martín. Cyber–physical systems: Extending pervasive sensing from control theory to the internet of things. *Pervasive and Mobile Computing*, 40:156 – 184, September 2017.

[7] B. Bordel Sánchez, R. Alcarria, D. Martín, and T. Robles. TF4SM: A Framework for Developing Traceability Solutions in Small Manufacturing Companies. *Sensors*, 15(12):29478–29510, November 2015.

[8] W. Chin, Z. Fan, and R. Haines. Emerging technologies and research challenges for 5G wireless networks. *IEEE Wireless Communications*, 21(2):106–112, April 2014.

[9] A. Corporation. Ecc-based devices. `http://www.atmel.com/products/security-ics/cryptoauthentication/ecc-256.aspx` [Online; Accessed on Octobert 3,2017].

[10] C. Doukas, I. Maglogiannis, V. Koufi, F. Malamateniou, and G. Vassilacopoulos. Enabling data protection through PKI encryption in IoT m-Health devices. In *Proc. of the 12th IEEE International Conference on Bioinformatics & Bioengineering (BIBE'12), Larnaca, Cyprus*, pages 25–29. IEEE, November 2012.

[11] X. Duan and X. Wang. Authentication handover and privacy protection in 5G hetnets using software-defined networking. *IEEE Communications Magazine*, 53(4):28–35, apr 2015.

[12] J. Gu and Z. Xue. An Improved Efficient Secret Handshakes Scheme with Unlinkability. *IEEE Communications Letters*, 15(2):259–261, February 2011.

[13] L. Hernández Encinas, F. Montoya, and A. Orue. Trifork, a new pseudorandom number generator based on lagged fibonacci maps. *Journal of Computer Science and Engineering*, 2(2):46–51, 2010.

[14] M. Katagi and S. Moriai. Lightweight Cryptography for the Internet of Things, May 2012. `https://www.iab.org/wp-content/IAB-uploads/2011/03/Kaftan.pdf` [Online; Accessed on October 3, 2017].

[15] M. B. Krishna and J. J. P. C. Rodrigues. Two-phase incentive-based secure key system for data management in internet of things. In *Proc. of the 2017 IEEE International Conference on Communications (ICC'17), Paris, France*, pages 1–6. IEEE, May 2017.

[16] H. Lasi, P. Fettke, T. Feld, and M. Hoffmann. Industry 4.0. *Business & Information Systems Engineering*, 6(4):239–242, October 2014.

[17] M. Lavanya and V. Natarajan. Certificate-free collaborative key agreement based on IKEv2 for IoT. In *Proc. of the 3rd International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB'17), Chennai, India*, pages 397–400. IEEE, February 2017.

[18] X. Li, J. Xu, Z. Zhang, D. Feng, and H. Hu. Multiple Handshakes Security of TLS 1.3 Candidates. In *Proc. of the 2016 IEEE Symposium on Security and Privacy (SP'16), San Jose, California, USA*, pages 486–505. IEEE, May 2016.

[19] K. Mandal, X. Fan, and G. Gong. Design and Implementation of Warbler Family of Lightweight Pseudorandom Number Generators for Smart Devices. *ACM Transactions on Embedded Computing Systems*, 15(1):1–28, February 2016.

[20] H. Martin, P. Peris-Lopez, J. E. Tapiador, and E. San Millan. An Estimator for the ASIC Footprint Area of Lightweight Cryptographic Algorithms. *IEEE Transactions on Industrial Informatics*, 10(2):1216–1225, May 2014.

[21] J. Melia-Segui, J. Garcia-Alfaro, and J. Herrera-Joancomarti. Multiple-polynomial LFSR based pseudorandom number generator for EPC Gen2 RFID tags. In *Proc. of the 37th Annual Conference of the IEEE Industrial Electronics Society (IECON'11), Melbourne, Victoria, Australia*, pages 3820–3825. IEEE, November 2011.

[22] M. Merhi, J. C. Hernandez-Castro, and P. Peris-Lopez. Studying the pseudo random number generator of a low-cost RFID tag. In *Proc. of the 2011 IEEE International Conference on RFID-Technologies and Applications (RFID-TA'11), Sitges, Spain*, pages 381–385. IEEE, September 2011.

[23] K. T. Nguyen, M. Laurent, and N. Oualha. Survey on secure communication protocols for the internet of things. *Ad Hoc Networks*, 32:17 – 31, September 2015.

[24] Openmote.org. Openmote cc2538. `http://www.openmote.com/hardware/openmote-cc2538-en.html` [Online; Accessed on October 3, 2017].

[25] M. H. Özcanhan, G. Dalkiliç, and M. C. Gürle. An Ultra-Light PRNG for RFID Tags. In *Computer and Information Sciences III*, pages 231–238. Springer London, 2013.

[26] A. Peinado, J. Munilla, and A. Fúster-Sabater. EPCGen2 Pseudorandom Number Generators: Analysis of J3Gen. *Sensors*, 14(4):6500–6515, April 2014.

[27] P. Peris-Lopez, J. Hernandez-Castro, J. Estevez-Tapiador, and A. Ribagorda. An ultra light authentication protocol resistant to passive attacks under the gen-2 specification. *Journal of Information Science and Engineering*, 25(1):33–57, 2009.

[28] H. C. Pohls. JSON Sensor Signatures (JSS): End-to-End Integrity Protection from Constrained Device to IoT Application. In *Proc. of the 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS'15), Blumenau, Brazil*, pages 306–312. IEEE, July 2015.

[29] P. Porambage, E. Harjula, A. Gurtov, P. Kumar, and M. Ylianttila. Certificate based keying scheme for DTLS secured IoT, 2013. `https://tools.ietf.org/html/draft-pporamba-dtls-certkey-01` [Online; Accessed on October 3, 2017].

[30] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila. PAuthKey: A Pervasive Authentication Protocol and Key Establishment Scheme for Wireless Sensor Networks in Distributed IoT Applications. *International Journal of Distributed Sensor Networks*, 10(7):357430, July 2014.

[31] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila. Two-phase authentication protocol for wireless sensor networks in distributed IoT applications. In *Proc. of the 2014 IEEE Wireless Communications and Networking Conference (WCNC'14), Istanbul, Turkey*, pages 2728–2733. IEEE, April 2014.

[32] M. Qiu, D. Cao, H. Su, and K. Gai. Data transfer minimization for financial derivative pricing using Monte Carlo simulation with GPU in 5G. *International Journal of Communication Systems*, 29(16):2364–2374, October 2016.

[33] B. B. Sanchez, A. Sanchez-Picot, and D. S. D. Rivera. Using 5G Technologies in the Internet of Things Handovers, Problems and Challenges. In *Proc. of the 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS'15), Blumenau, Brazil*, pages 364–369. IEEE, July 2015.

[34] A. R. Sfar, E. Natalizio, Y. Challal, and Z. Chtourou. A roadmap for security challenges in internet of things. *Digital Communications and Networks*, pages 1–20, April 2017.

[35] Shanzhi Chen and Jian Zhao. The requirements, challenges, and technologies for 5G of terrestrial mobile telecommunication. *IEEE Communications Magazine*, 52(5):36–43, May 2014.

[36] Z. Sohrabi-Bonab, M. R. Alagheband, and M. R. Aref. Formal cryptanalysis of a CRC-based RFID authentication protocol. In *Proc. of the 22nd Iranian Conference on Electrical Engineering (ICEE'14), Tehran, Iran*,

pages 1642–1647. IEEE, May 2014.

[37] M. Turkanović, B. Brumen, and M. Hölbl. A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the internet of things notion. *Ad Hoc Networks*, 20:96 – 112, September 2014.

[38] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. D. Renzo. Safeguarding 5G wireless communication networks using physical layer security. *IEEE Communications Magazine*, 53(4):20–27, April 2015.

[39] Zhihua Li, Xi Yin, Zhenmin Geng, Haitao Zhang, Pengfei Li, Ya Sun, Huawei Zhang, and Lin Li. Research on PKI-like Protocol for the Internet of Things. In *Proc. of the 5th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA'13), Hong Kong, China*, pages 915–918. IEEE, January 2013.

[40] Zolertia. Zolertia remote. `http://zolertia.io/product/hardware/re-mote` [Online; Accessed on October 3, 2017].

Author Biography

Borja Bordel received the B.S. degree in telecommunication engineering in 2012 and the M.S. telecommunication engineering in 2014, both from Technical University of Madrid. He is currently pursuing the Ph.D. degree in telematics engineering at Telecommunication Engineering School, UPM. His research interests include Cyber-Physical Systems, Wireless Sensor Networks, Radio Access Technologies, Communication Protocols and Complex Systems.

Ramón Alcarria received his M.S. and Ph.D. degrees in Telecommunication Engineering from the Technical University of Madrid in 2008 and 2013 respectively. Currently, he is an assistant professor at the E.T.S.I Topography of the Technical University of Madrid. He has been involved in several R&D European and National projects related to Future Internet, Internet of Things and Service Composition. His research interests are Service Architectures, Sensor Networks, Human-computer interaction and Prosumer Environments.