IoT Privacy in 5G Networks

Emanuele Catania and Aurelio La Corte
Department of Electric, Electronic and Computer Science Engineering,
Università degli Studi di Catania,
viale A. Doria 6, 95121 Catania, Italy

Keywords: Internet of Things, Ultra-Dense Networks, Privacy, Security, 5G.

Abstract: In the Internet of Things (IoT), objects, equipped with sensing, processing, storage and decision-making capabilities, actively interact with one another and with humans. Even if they have been conceived and programmed to make all their activities in security, several factors, such as weak implementations of communication protocols, metadata information exchange, and architectural flaws, could jeopardize security and privacy. Moreover, due to its complexity and attitude to change rapidly, and to the ultra-densification trend of the current communication infrastructure, new threats to the privacy might arise. After a brief introduction to IoT privacy issues, we describe how the evolution of the current wireless communication infrastructure toward the 5G generation network might undermine the privacy in the IoT. Then we propose a methodology of analysis, which looks at privacy threats from different perspectives and at various levels of abstraction.

1 INTRODUCTION

By definition, the Internet of Things is a composition of physical entities capable of sensing, computing and acting in response to the information they can acquire and manage (Sfar, et al., 2017). Thanks to this paradigm, "people and things can be connected anytime, anyplace, with anything and anyone, ideally using any path/network and any service" (Kende, 2014).

Mobility, scalability, interoperability and resource constraints characterize the million interconnected both wireless and wired devices of which the IoT is composed (Porambage, et al., 2016). Ubiquity is one of the key features that the communication infrastructure underlying the IoT should have. Undoubtedly, cellular networks, due to their diffusion, enable IoT implementation, also ensuring stable transmissions and acceptable delays. However, such networks have not been conceived to support machine-to-machine (M2M) communication (which are characterized by intermittent behavior and small-sized data packets). Furthermore, it has been foreseen that in the near future almost all data traffic supported by communication networks will be produced by smart devices (CISCO, 2016). Using only cellular network might not be sufficient to satisfy the M2M requirements, since during transmission, machine-type communications might easily exceed their uplink capacity.

In order to foster performance improvements of the current communication infrastructure, given also the prominent IoT diffusion trend, cellular networks will be cooperating with other wireless network technologies (e.g. WLAN, relay-assisted and device-to-device communications, wireless personal area networks, LTE-U). Ultra-dense networks (UDNs), namely hierarchical networks in which the density of access nodes is at least a magnitude greater than the density of users, will meet future communication requirements, providing a very high connectivity and data rate.

1.1 Motivation

Although the benefits that it may produce, the IoT may cause severe security implications. Inability or unwillingness of devices owner to update and fix devices' security flaws, limited capability of devices, and the lack of, or incompatibility among communication standards makes hard addressing the security challenges in the IoT (Mannilthodi & Kannimoola, 2017). Leakage of sensitive information is one of the most serious threats to the privacy. The

Catania, E. and La Corte, A.
IoT Privacy in 5G Networks.
DOI: 10.5220/0006710501230131
In *Proceedings of the 3rd International Conference on Internet of Things, Big Data and Security (IoTBDS 2018)*, pages 123-131
ISBN: 978-989-758-296-7

most spread devices in the IoT cannot implement strong security and cryptographic functions since they are equipped with computationally and resource limited micro-controllers (Malina, et al., 2016). For this reason, a growing body of literature has evaluated and proposed lightweight encryption algorithms and privacy-by-design methodologies.

Since it is an evolving, heterogeneous, and wide technological environment, it could be very hard guaranteeing the privacy to the whole IoT. A method for identifying privacy weaknesses fitting well to the complex IoT it would be desirable. Furthermore, new security challenges should be considered given the paradigmatic revolution that will overwhelm current communication networks soon.

1.2 Contribution

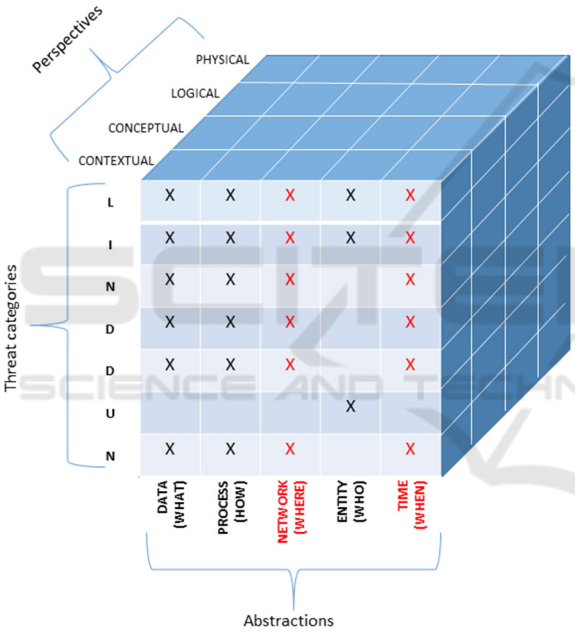

Figure 1: Privacy assessment and discovery methodology.

The present study has offered a framework for the exploration of privacy issues for the IoT. It introduces a methodology of analysis aiming at disclosing privacy weaknesses that might affect the IoT eco-system from different viewpoints. In particular, it is inspired by the popular Zachman framework and the LINDDUN framework. Among all the abstractions, the "Network" and the "Time" (see Figure 1) enrich the sets of observed information with respect to the LINDDUN framework.

We show how the proposed privacy threat analysis framework operates at different level of abstraction, thus highlighting privacy weaknesses from various perspectives. We describe an application example of our methodology to the IoT, starting from the most abstract level, namely the "Contextual" perspective. As to avoid being long-winded, we did not carry out a thorough analysis, thus deepening also the "Physical" viewpoint, but we stopped to the "Logical" is.

1.3 Paper Organization

Section 2 outlines the related works and describe the effect on the IoT privacy of communication infrastructure densification. Section 3 presents the proposed privacy assessment methodology. An example of application of the methodology on the IoT in ultra-dense cellular networks is presented in Section 4. Then, in the final section, the conclusion.

2 LITERATURE REVIEW

Wireless radio channels are widely used in M2M communications. Because of their limited resources, provide these devices with powerful, also computationally expensive, security capabilities are often infeasible. This makes M2M communications extremely vulnerable. Furthermore, attacks against information privacy become more effective as the underlying communication infrastructure is an ultra-dense network (Chen, et al., 2017). In this section, we introduce some background on IoT privacy and analyze the effect of the huge deployment of limited-resource devices in UDNs.

2.1 Privacy in the IoT

Because of design tradeoffs in term of cost, complexity, and energy required for fulfilling their operation, many devices in the IoT are usually resource-limited. To cope with unauthorized access, data theft, and eavesdropping, devices should be provided with authentication, authorization mechanisms, and data preservation capabilities, ensuring freshness, authenticity, confidentiality, and integrity of information. Privacy (i.e. unlinkability, data secrecy, and anonymity) has to be accurately preserved since personal and sensitive information could be stolen and abused by an adversary. Encryption is fundamental to provide sensitive data with a basic level of privacy. Indeed, it prevents that transmitted data can be intercepted and read by passive adversaries. Nevertheless, encrypting the information might mean make use of computationally expensive cryptographic primitives (e.g. pairing-

based cryptography), which could not be executed by every IoT device. In order to identify suitable cryptographic approaches to the IoT, Malina et al. (Malina, et al., 2016) measured the performance of the most used primitives (such as RSA, secure hashing algorithms and AES) on some of the most common micro-controllers (ARM, MSP430f X) equipping IoT devices. They found that while hashing and symmetric ciphering operations take few milliseconds and can also run on very limited microcontrollers, stronger approaches, such as RSA asymmetric signing (by a 2048-bit private key), can cause delays into hundreds of milliseconds, which are intolerable in real-time IoT applications. Processing of complex operations could be left to the cloud or to communication gateways, resulting in the reduction of both devices energy consumption and computation delays (Shariatmadari, et al., 2015). However, this method requires trustful gateways and secure communication among parties. A viable technique to protect entities (both devices and users) from being traced is hiding their real identity by means of pseudonyms. Anyway, as also suggested in (Bailey, 2012) and in (Shaik, et al., 2015), when attackers eavesdrop data packet within a sufficiently wide time window of observation, they might disclose real victims' identifier. As described later in this paper, when connected to an LTE network, IoT devices can decode messages broadcasted by the network to locate a specific subscriber. Such messages contain only temporary identifiers, but a passive adversary could be able to exploit decoded information to retrieve associations among temporary unique identifiers. Furthermore, colluding IoT users positioned in proximity of the occasionally visited locations by the IoT target (i.e. the victim), even though protected by a pseudonym, might reveal to the attacker the target's real identity and its private activities (Zhou, et al., 2017).

Here we argue that although the utilization of protection approaches in design and implementation stages, privacy objectives in the IoT could not be achieved because of its complexity. Then, a comprehensive understanding of motivations behind privacy weaknesses and resulting identification of appropriate mitigation actions in response to them requires an organic methodology capable of analyzing the wide and diverse IoT from distinct perspectives.

2.2 UDN and IoT Privacy

UDNs can effectively cope with the future networks data requirements, also provide energy and spectrum efficiency. Composed of heterogeneous nodes with different radio access technologies (e.g. LTE, Wi-Max, IEEE 802.15.x), transmit powers, and coverage area, UDNs are characterized by a multi-tier architecture. In detail, high-power nodes and low-power nodes, with large and small radio coverage, are placed respectively in macro-cell tiers and in small-cell tiers. Cellular communication infrastructure, if from one hand make it possible offer ubiquitous connectivity to the most devices, from the other hand is inefficient for transmitting small, infrequent data as required by M2M communications. Moreover, cellular network communications could make it possible to track entities involved in information exchange processes (Bailey, 2012), thus affecting their location privacy.

Spatial distribution of low-power nodes might influence the whole network security, as asserted in (Chen, et al., 2017). Specifically the probability of *positive secrecy rate*, that is the capacity deviation of the operating channel from the eavesdropper channel, increases as the density of low-power nodes growths (until a critical point, after which is not observed any enhancement in term if secrecy performance). Moreover, the higher the density of entities involved in communication processes, the higher is the risk of information eavesdropping (Yang, et al., 2015). Undeniably, while moving within a UDN, entities are likely to be subject to more handover processes than in the existing networks, making it possible for untrusted subjects to take part in the just mentioned processes. Albeit finding trusted security organizations responsible for credential distribution could solve the abovementioned problem (Swetina, et al., 2014), undesired network delays due to a large number of involved devices, in addition to high costs, make their adoption infeasible in practice. In consideration of this, physical layer security seems to be best suited for the 5G network with respect to cryptographic security. Indeed, the former approach, in addition to having high scalability, does not require complex operations to be fulfilled (differently than the cryptographic). Even computationally powerful adversaries, in fact, cannot compromise the network security (Yang, et al., 2015).

Despite scientific community has raised many concerns about UDN security and IoT security, no one to the best of our knowledge has studied the effect of network densification on the privacy of the IoT.

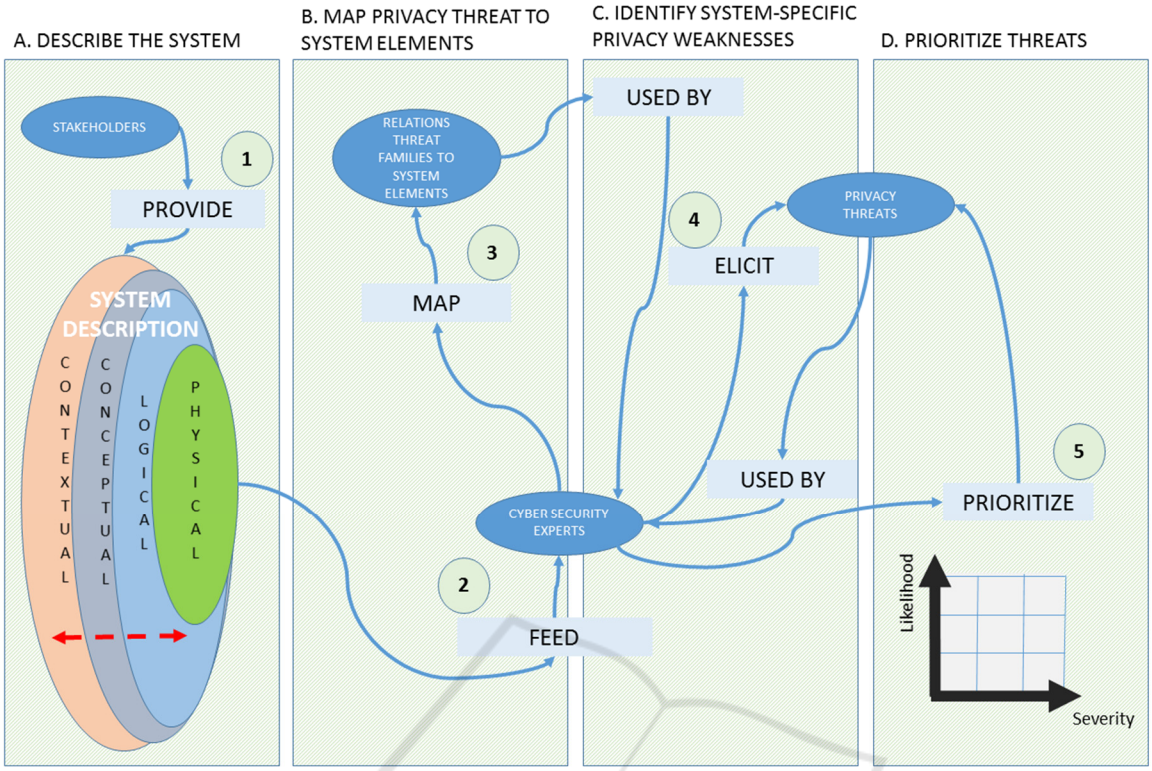

Figure 2: In this figure, we describe the proposed privacy threat modelling. We identified four main steps, namely "describe the system", "map privacy threats to system elements", "identify system-specific weaknesses", and "prioritize threats". Ellipses and rectangles represent respectively the entities involved and the actions they perform when interacting with each other in the privacy threats identification process.

3 METHODOLOGY

To tackle the problem of privacy in IoT, we propose an assessment methodology which combines the popular Zachman framework (ZF) (Zachman, 1987) with the LINDDUN framework (Wuyts, 2015). The proposed approach aims at providing a tool for acquiring awareness about, and then react to, privacy weaknesses that might affect the system from both microscopic and macroscopic perspectives. LINDDUN is mainly a methodological approach, which uses data flow diagrams to list entities, processes, data flows, and data stores. Then, by mean of further successive steps, it maps, elicits and prioritizes threats, guiding towards the identification of mitigation strategies and privacy enhancing technologies. The ZF allows logically organizing and classifying artifacts involved in the design and development of information systems. Different perspectives match with different aspects of the system, allowing decomposing the verification of privacy properties in small, though sometimes interdependent, modules. Privacy assessment on IoT applications is a large complex task that requires a systematic verification approach on both software and hardware. We remark that the LINDUNN framework is not aimed at the IoT domain. In addition to entities, data (flows) and data processes, knowledge on physical location in which event happens (e.g. authentications, data exchange) together with time information, might help to better understand motivations behind privacy issues and identify more suited privacy enhancing solutions. Here we give some explanation about the "Perspective" dimensions of our proposal.

- Contextual (i.e., what the system should do): refers to the description of information, processes, locations, involved entities, events, and motivations. It gives an overall, also non-detailed, view of purposes, extents, and relationships among elements of the IoT eco-system or its subsystems.
- Conceptual (i.e., how the system should operate): less abstract and more descriptive with respect to the former

perspective, gives an overview of models, semantic relationships, and processes
- Logical: indicates processing structure, how applications are architected, rules and information models.
- Physical: the most concrete as compared to the aforementioned perspectives, aims at analyzing the IoT from technical points of view (technology constrained models) providing information on physical quantities and parameters.

Each perspective aims at identifying privacy threats by analyzing the system from different viewpoints and may be ground for investigations into the threats causes. Disclosed threats on one perspective, can be reported and investigated from other perspectives. This implies that also threats can be described according to more viewpoints. Moreover, information, processes, locations, entities, and event (see Table 1) can be related to each other.

Table 1: In this table contextual and conceptual information are retrieved using a taxonomy on the IoT (Yaqoob, et al., 2017) and a smartphone data taxonomy (Mylonas, et al., 2012).

#	Data	Processes	Network/Location	Entities	Time/Events
Contextual (What)	▪ Measured and elaborated data	▪ Communication and acquisition of information ▪ Requiring for and feeding a service	▪ Buildings ▪ Public areas ▪ Private areas ▪ Wired network ▪ Wireless networks	▪ Things	▪ Synchronous and asynchronous events
Conceptual (How)	▪ Messages (content, metadata) ▪ Connection (re)configuration ▪ Electronic addresses (of entities) ▪ Services	▪ Searching (entities, services, etc.) ▪ Notification ▪ Decentralized data processing, auditing and information sharing ▪ Realtime messaging ▪ Connection management and control	▪ Wireless communication systems and infrastructures (e.g., LTE – LTE/A – LTE/U, IEEE 802.11 x, IEEE 802.15 x, WiMax, ZigBee, etc.) ▪ Ethernet (real-time Ethernet, EtherCAT), PLC, MoCA	▪ Smartphones ▪ Vehicles ▪ Laptops ▪ Sensors ▪ Access Points ▪ Users ▪ Smart home systems ▪ Smart healthcare systems ▪ Intelligent building systems ▪ Smart meters ▪ Etc.	▪ Decentralized communication ▪ Event notification ▪ Real-time-analysis ▪ Peer-to-peer communication ▪ Decentralized auditing ▪ Decentralized file sharing
Logical (LTE only)	▪ GUTI ▪ MSISDN ▪ RRC Message Body ▪ RRC keys ▪ Resource configuration ▪ Report (measurement and link failure) ▪ S-TMSI ▪ IMSI	▪ RRC connection establishment ▪ RRC connection release ▪ Broadcast of system information ▪ RRC connection reestablishment (NB-IoT only) ▪ Radio link establishment ▪ RRC key sharing ▪ Paging	▪ TA ▪ eNB Location ▪ Device Location ▪ MME ▪ HHS	▪ eNB ▪ Relay ▪ Device's LTE network Interface ▪ Mobility Management Entity ▪ Home Subscriber Server	▪ Paging Triggering ▪ Initial security activation ▪ Establishment of signal radio bearer ▪ Establishment of data radio bearer ▪ Handover ▪ Configuration of lower protocol layers

For example, connection (re)configuration information may be related to the connection management and control processes. Privacy threats can be grouped into seven families, that is linkability, identifiability, non-repudiation, detectability, distinguishability, unawareness (of information content), and non-compliance to policy.

For the sake of completeness, we report the definition of threat categories, as indicated in (Wuyts, 2015). Linkability occurs when two entities can be related to each other. Identifiability refers to a capability of an adversary to infer the identity of an entity. Non-repudiation stands for the inability of a subject to demonstrate that he/she could not carry out a specific action. Detectability implies that it possible detect whether an entity exists or not. Disclosure of information happens when protected individuals information can be accessed by unauthorized entities. Unawareness is related to unconsciousness about supplied information to the system. To conclude, non-compliance refers to the inability of the system to be compliant with regulations, policies, and agreements with users.

4 PRIVACY THREAT ANALYSIS

Most of the IoT applications require both data and communications security, in addition to ubiquitous connectivity. In order to be compliant with the proposed methodology, abstractions (see Figure 1) should be listed and analyzed from every perspective. As to provide an example of a use of the proposed method, in this paper privacy analyses covered only three of the four perspectives (omitting the Physical one).

4.1 Contextual and Conceptual Perspectives

Contextual perspective allows observing and tackling the privacy problem from a very non-concrete point of view. A high-level architectural representation of systems, in addition of delimiting the boundaries of analysis, might allow identifying the critical elements involved in communication processes. In Figure 3, we provide an example of system representation from this perspective. Vehicles, smartphones, laptops, smart homes and their appliances, access points, and users are some example of interconnected entities within the network. Access points to communication networks may be deployed in public or in private areas. Privacy specifications might depend on application fields and on protection objectives.

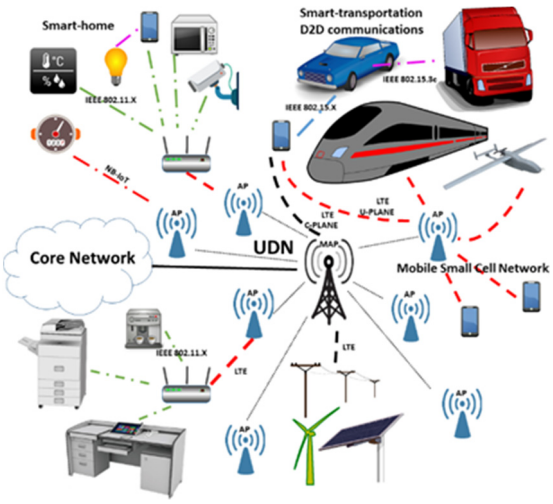

Figure 3: Communication technologies in the IoT.

For example, in smart home systems, privacy objectives could be concealing presence or absence of persons, consumption habits, and appliances installed inside houses. In pay-as-you-drive insurance, black-box car insurance, and car-sharing services, because of routes and driver's guide style monitoring, users could be exposed to linkability, identifiabiliy and disclosure of information threats (to give just some examples). For the listed cases, avoiding fine-grained information communication (also via secure media) might reduce the risk of private information disclosure. When a device communicate sensed data to a remote service (see Table 1), linkability, identifiability, detectability, and disclosure of information threats might violate the system. Issues might derive from devices settings and from identifiability of remote services to which they connect. Problems might become more serious when the aforementioned settings and service are set by the manufacturers and cannot be altered by end users. As an instance, it could be possible, through traffic analysis, identifying installed smart appliances within a home. Hence, adversaries, by exploiting known vulnerabilities of them, could steal or infer private users' information.

The just discussed problems may be reported to the more specific conceptual perspective. Both wired and wireless communications can be considered, though we only deepen the latter because more exposed to eavesdropping. The communication infrastructure taken into consideration is multi-tier, ultra-dense and heterogeneous. Several wireless communication technologies and protocols can be analyzed, such as IEEE 802.11x, IEEE 802.15.x, WiMax, ZigBee, and LTE/LTE-A/LTE-U. Attackers, to launch an attack against users' privacy,

Table 2: In this table, we report the definitions of some entities, protocols, and procedures involved during the UE-to-Core network communications (LTE).

#	Symbol	Description
Paging		Refers to the process in which the mobility management entity (MME) needs to locate an UE in a particular area and to deliver network services, such as incoming calls.
Radio Resource Control	(RRC)	Includes a set of functions to manage connectivity between UE and eNB, that is broadcasted information (sent by eNBs over a broadcast channel) and UE measurement reports or radio link failure (RLF) sent by UEs
Access Stratum	(AS)	Is a functional layer within LTE protocol stack, responsible for radio resource management and data transportation over the wireless channel
Access Stratum Security Context		The purpose of AS security context is to deliver RRC messages between an UE and an access point (eNB) through the control plane, and IP packets through the user plane using AS security keys.
Radio Link Failure report	(RLF)	It allow detecting connection failures caused by intra-LTE mobility and intersystem handovers between LTE, GSM, and 3G networks.
Measurement report		It includes throughput measurements, latency, reference signal received power (RSRP), received signal strength indicator (RSSI), as well as information about dropped calls and, sometimes, latitude and longitude.

could exploit weaknesses and known vulnerabilities in wireless technologies and in devices' interfaces to wireless networks. For instance, in LTE networks the subscribers' unique identifier is masked by using pseudonyms. Since during paging processes (as described in the next section) such information can be broadcasted in clear text, adversaries can link subscriber identity to a specific geographical area. In order to protect them from being identified, such associations should neither be publicly available nor it should be possible infer any correlation among them. Even if generally useful for protecting security and privacy of information, as the cellular network evolves toward the ultra-dense paradigm, current cryptographic approaches (as described before, in Section 2.2) might not be still suitable to satisfy protection requirements or could not be implemented due to devices' limited characteristics. Cryptographic operations should be lightened, leading, however, to a reduction of effectiveness protection. Indeed, simplifying current cryptographic techniques might allow even non-powerful adversaries to succeed in breaking cryptography.

4.2 Logical Perspective

The Logical is further specialized and require more effort to be analyzed with respect to the previous viewpoints. For this reason, in this paper, only LTE communications are considered. Exploiting LTE network as a part of the IoT communication infrastructure, besides of producing economic benefits and providing pervasive connectivity, also offers security of communications since it integrates various authentication and encryption algorithms (e.g., EPS AKA, SNOW 3G, MILENAGE). As asserted in (Shariatmadari, et al., 2015), some security arrangements to the IoT might include embedding a SIM card into devices. Anyway, but despite this, devices' security and privacy might be at risk. Indeed this means sending signal measurements to a central unit (i.e. a server), thus making them radio-frequency finger-printable. In this section, we provide some background about LTE communications. Let us briefly introduce the concept of access stratum (AS) security. The AS security keys are generated every time a new radio link is established (that is when a mobile device moves from IDLE state to CONNECTED state). When the AS security setup is completed, the mobile device (UE) and the eNodeB (eNB) share an RRC integrity key, an RRC encryption key, and a user plane encryption key. In order to locate an UE and serve him/her with network services, the network can trigger Paging Messages (see Table 2 for further details). The Mobility Management Entity (MME) generates a paging message and forwards it to several eNBs within a tracking area (TA). Thus, all eNBs within the paged TA broadcast a radio resource control (RRC) paging message to locate the UE (3GPP, 2016). Paging messages contain identities of UEs such as serving temporary mobile subscriber identities (S-TMSI(s)). S-TMSI is a temporary identifier and it is part of a global unique temporary identifier (GUTI). When it is in the IDLE state, the UE decodes RRC paging messages and searches for its IMSI in it. If its IMSI matches, it initiates a new Attach procedure to receive a GUTI. RRC messages

also indicate UEs which information it should be returned in response (either Measurement report or RLF report). Narrowband IoT (NB-IoT) functionality is specified in the LTE technical specifications (3GPP, 2016). In (Ratasuk, et al., 2016) authors describe two optimizations introduced for small data transmission, namely the RRC connection suspend/resume procedure and data transmission using control plane signaling. As reported by NB-IoT specifications (3GPP, 2017) M2M communications are not provided with measurements reporting and handover management. Until serving eNB does not release the connection or a link failure happens, UEs stay in the connected mode. When the connection is interrupted, they go to the idle state and then trigger RRC connection reestablishment procedure. Paging processes, if triggered when users are in IDLE state, could allow relating IMSIs and GUTIs to TAs (Kune, et al., 2012) (3GPP, 2017). In fact, in its first phase, RRC paging lacks encryption protection (Shaik, et al., 2015). Moreover, correlations among TAs and eNBs can be disclosed.

In summary, our work has presented a methodology of analysis for identifying privacy threats in the IoT with a view to 5G networks implementation. The paradigm shift of wireless networks toward the 5G evolution will result in employment of ultra-dense networks as to provide, among all benefits, high data rate and low communication latencies. Anyway, this network transformation may seriously undermine, to some extent, the privacy of devices and users. The proposed methodology extends and the LINDDUN frameworks by introducing temporal and location information to the threats identification process. Moreover, taking a cue from the popular Zachman framework, it also addresses the privacy weaknesses identification by investigating the entangled IoT from four different points of view, namely contextual, conceptual, logical, and physical.

The current paper lacks a comparative evaluation and validation. Anyway, we planned to provide these enhancements in the future.

5 CONCLUSION

We have presented a privacy assessment methodology, which aims at discovering privacy threats in the IoT through a systematic approach. Our technique extends the LINDUNN framework by introducing temporal and location information to the threats identification processes. Moreover, it draws on from the Zachman framework, thus observing privacy issues from various viewpoints.

An application example of our methodology has been discussed. However, in order to be brief, it has not been conducted a thorough investigation. We foresee to provide supplementary information in future works. Further studies, which consider different IoT architectures, will need to be undertaken. Although our approach has been thought to a specific case of the IoT, hopefully, it could be also applied to other technological systems in which privacy is critical. The prospect of being able to do deliver secure and privacy-preserving services in many contexts, serves as a continuous stimulus for future research.

REFERENCES

3GPP, 2016. Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description. Issue TS 36.300.

3GPP, 2017. *Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification.* s.l.:s.n.

Bailey, D. A., 2012. Moving 2 mishap: M2M's impact on privacy and safety. *IEEE Security Privacy,* 10(1), pp. 84-87.

Chen, S. et al., 2017. Machine-to-Machine Communications in Ultra-Dense Networks-A Survey. *IEEE Communications Surveys & Tutorials*.

CISCO, 2016. Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2015--2020 White Paper. *Cisco Public Information.*

Kende, M., 2014. Internet society global internet report 2014. *Internet Society*, 15 July.

Kune, D. F., Koelndorfer, J., Hopper, N. & Kim, Y., 2012. *Location leaks on the GSM Air Interface.* s.l., s.n.

Malina, L., Hajny, J., Fujdiak, R. & Hosek, J., 2016. On perspective of security and privacy-preserving solutions in the internet of things. *Computer Networks,* Volume 102, pp. 83 - 95.

Mannilthodi, N. & Kannimoola, J. M., 2017. *Secure IoT: An Improbable Reality.* s.l., SciTePress, pp. 338-343.

Mylonas, A. et al., 2012. *Smartphone forensics: A proactive investigation scheme for evidence acquisition.* s.l., Springer.

Porambage, P. et al., 2016. The Quest for Privacy in the Internet of Things. *IEEE Cloud Computing,* 3(2), pp. 36-45.

Ratasuk, R. et al., 2016. Overview of narrowband IoT in LTE Rel-13. *2016 IEEE Conference on Standards for Communications and Networking (CSCN),* pp. 1-7.

Sfar, A. R., Natalizio, E., Challal, Y. & Chtourou, Z., 2017. A Roadmap for Security Challenges in Internet of Things. *Digital Communications and Networks.*

Shaik, A. a. B. R., Asokan, N., Niemi, V. & Seifert, J.-P., 2015. Practical attacks against privacy and availability in 4G/LTE mobile communication systems. *arXiv preprint arXiv:1510.07563.*

Shariatmadari, H. et al., 2015. Machine-type communications: current status and future perspectives toward 5G systems. *IEEE Communications Magazine,* 53(9), pp. 10-17.

Swetina, J. et al., 2014. Toward a standardized common M2M service layer platform: Introduction to oneM2M. *IEEE Wireless Communications,* 21(3), pp. 20-26.

Wuyts, K., 2015. *Privacy Threats in Software Architectures.* s.l.:Ph.D. dissertation, KU Leuven.

Yang, N. et al., 2015. Safeguarding 5G wireless communication networks using physical layer security. *IEEE Communications Magazine,* 53(4), pp. 20-27.

Yaqoob, I. et al., 2017. Internet of Things Architecture: Recent Advances, Taxonomy, Requirements, and Open Challenges. *IEEE Wireless Communications,* 24(3), pp. 10-16.

Zachman, J. A., 1987. A framework for information systems architecture. *IBM systems journal,* 26(3), pp. 276--292.

Zhou, J., Cao, Z., Dong, X. & Vasilakos, A. V., 2017. Security and Privacy for Cloud-Based IoT: Challenges. *IEEE Communications Magazine,* 55(1), pp. 26-33.