ICT Security and Privacy in Future Wireless Networks (5G, UDN)

Ph.D. research activity in Energetic, System, Computer and Telecommunications Engineering – XXXI cycle

Emanuele Catania, Ph.D. student - Prof. Aurelio La Corte, Supervisor - Prof. Paolo Arena, Coordinator
DIEEI, Univ. of Catania, Italy

Introduction

Wireless network is coping with an even higher data demand due to increasing number of entities accessing to data communication services and to novel, resource-consuming applications (e.g. 4k ultra-HD video streaming, virtual and augmented reality). As to provide more flexibility to the network and seamless network connectivity to users, ultra-dense network (UDN) approach will represent one of the most interesting paradigm shift toward future 5G networks. In this context, the scientific community has raised some concerns about UDNs security [1] [2] [3]. Indeed, UDNs should not only provide reliable connectivity to users, but also cope with issues related to information hiding, accounting, authentication, and authorization, thus requiring novel, light-weight cryptographic protocols and algorithms that best suit the ultra-dense scenario [4]. Since in UDN deployments each cell can serve only a small number of users in a very limited area, their preservation stresses the need to draw up new protection techniques against location privacy threats. In addition, limited capabilities of the million interconnected both wireless and wired devices of which the IoT is composed, and the lack of or incompatibility among communication standards makes hard addressing the security challenges in the IoT [5]. Among all, leakage of sensitive information is one of the most serious threat to the privacy. Thus, tools for identifying privacy weaknesses affecting the evolving and heterogeneous IoT ecosystem would be desirable.

Privacy issues in 5G networks

- The higher the density of communicating entities, the higher is the risk of information eavesdropping [6].
- By combining eavesdropped information about the absence of a user in a specific area with additional knowledge (e.g., a map data), the adversary could infer the sensitive information [7].
- The most spread devices in the IoT cannot implement strong security and cryptographic functions [8].
- UDNs adapt to the spatial distribution of mobile nodes and to data load, thereby essentially providing new, updated and valuable information about mobile nodes' location to malicious entities.

Results

Location Privacy in Virtual-Cell Equipped UDNs

Many factors limit wireless network densification, such as drastic interferences, energy constraints, and backhaul bottlenecks. It has been studied the effect of mobile node densification, access node densification, and their aggregation into virtual entities, referred to as virtual cells, on location privacy. Because of the short-range characteristic of UDNs, mobile users might experience frequent handovers and authentications. This make them exposed to many security threats, such as man-in-the-middle, denial of service, eavesdropping, impersonation, identity matching (and so forth). Through simulation, it has been observed that location privacy in ultra-dense networks is directly related to users density and that it can be strengthened by implementing virtual cells.

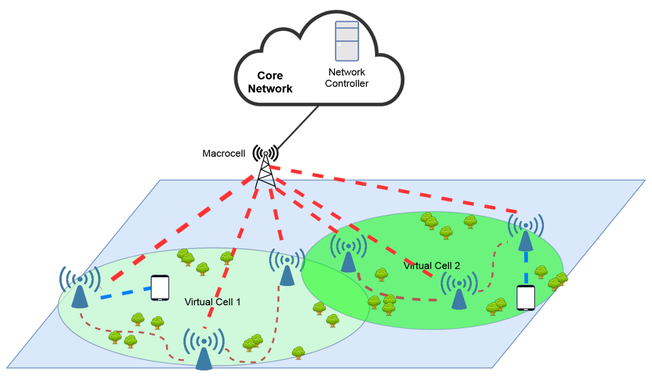


Fig. 1. Illustration of a heterogeneous network enhanced with virtual cell functionality. Control plane/data plane are split to provide both always-on, high data rate connectivity.

Fig. 2. Implementing virtual cells can determine a reduction in term of frequent key patterns identification

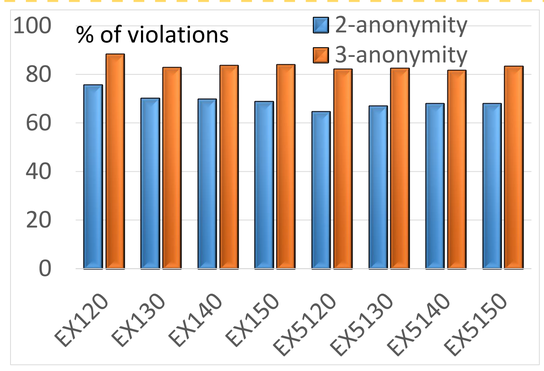
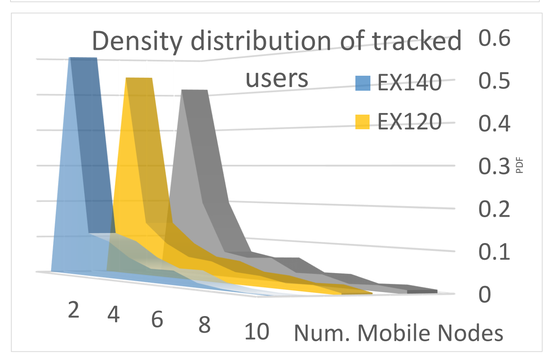


Fig. 3. By exploiting virtual cells further reduces the probability of mobile nodes tracking



IoT Privacy in 5G Networks

It has been defined a framework for exploration of privacy issues in the IoT. It introduces a methodology of analysis for disclosing privacy weaknesses that might affect the IoT eco-system from different viewpoints. In particular, it is inspired by the popular Zachman framework [9] and the LINDDUN [10] framework. Among all the abstractions (see Fig. 4), the "Network" and the "Time" enrich the sets of observable information as respect to the LINDDUN framework.

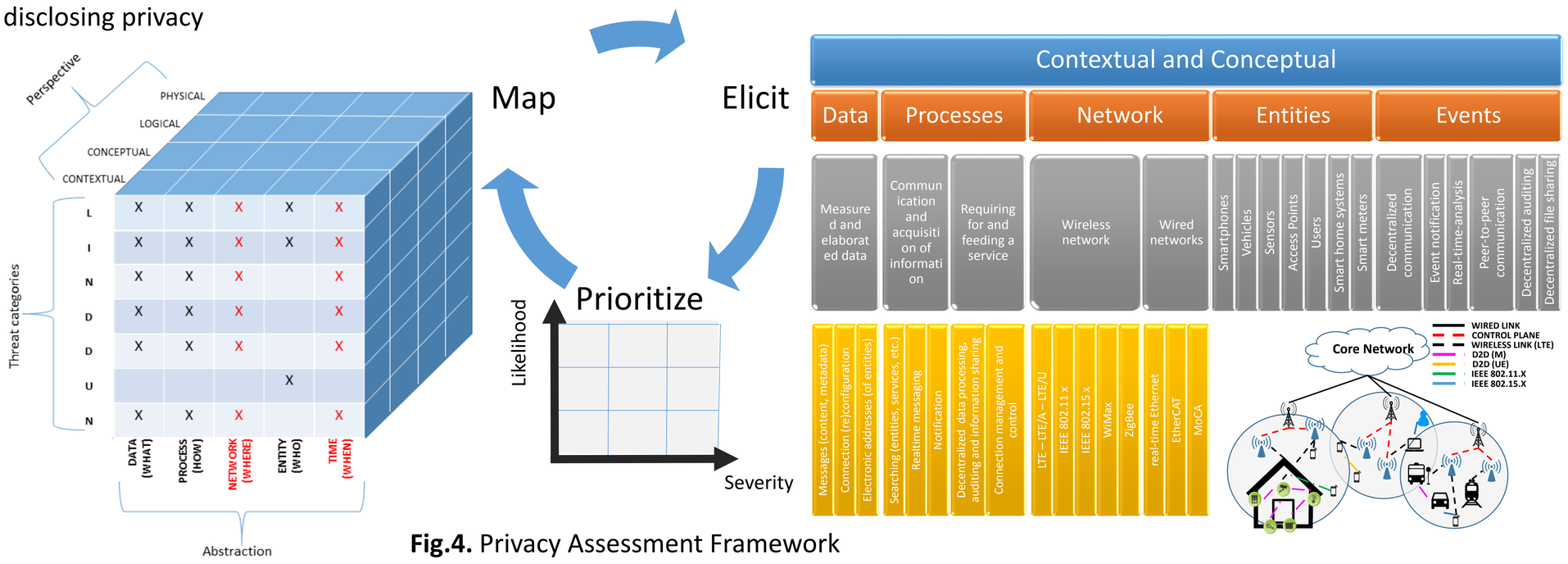


Fig.4. Privacy Assessment Framework

References

1. S. Farhang, Y. Hayel and Q. Zhu, "PHY-layer location privacy-preserving access point selection mechanism in next-generation wireless networks," 2015 IEEE Conference on Communications and Network Security (CNS), pp. 263-271, 2015.
2. X. Duan and X. Wang, "Authentication handover and privacy protection in 5G hetnets using software-defined networking," IEEE Communications Magazine, vol. 53, no. 4, pp. 28-35, 2015.
3. V. Vassilakis, E. Panaousis and H. Mouratidis, "Security challenges of Small Cell as a Service in virtualized mobile edge computing environments," Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 9895 LNCS, pp. 70-84, 2016
4. I. Akyildiz, S. Nie, S.-C. Lin and M. Chandrasekaran, "5G roadmap: 10 key enabling technologies," Computer Networks, vol. 106, pp. 17-48, 2016.
5. Mannilthodi, N., & Kannimoola, J. M. (2017). Secure IoT: An Improbable Reality. IoTBDS. 1, p. 338-343. SciTePress. doi:10.5220/0006352903380343.
6. Yang, N., Wang, L., Geraci, G., Elkashlan, M., Yuan, J., & Renzo, M. D. (2015). Safeguarding 5G wireless communication networks using physical layer security. IEEE Communications Magazine, 53(4), 20-27.
7. G. Ghinita, M. Damiani, C. Silvestri and E. Bertino, "Preventing velocity-based linkage attacks in location-aware applications," GIS: Proceedings of the ACM International Symposium on Advances in Geographic Information Systems, pp. 246-255, 2009.
8. Malina, L., Hajny, J., Fujdiak, R., & Hosek, J. (2016). On perspective of security and privacy-preserving solutions in the internet of things. Computer Networks, 102, 83 - 95.
9. Zachman, J. A. (1987). A framework for information systems architecture. *IBM systems journal, 26*(3), 276--292.
10. Wuyts, K. (2015). *Privacy Threats in Software Architectures.* Ph.D. dissertation, KU Leuven.