EAI Endorsed Transactions
on Industrial Networks and Intelligent Systems
Research Article EAI.EU

Functional Security and Trust in Ultra-Connected 6G Ecosystem

Vishal Sharma*

School of Electronics, Electrical Engineering and Computer Science (EEECS), Queen's University Belfast, NI, UK, BT7 1NN.

Abstract

Security and trust are the entangled role players in the future generation of wireless networks. Security in 5G networks is currently supported using several functions. Given the advantages of such a system, this article explores the functional security and trust for the 6G ecosystem with ultra-connectivity. Several associated challenges, application-specific domains, and consumer issues related to 6G security are discussed. The article highlights the network security-by-design and trust-by-design principles and performance expectations from the security protocols in supporting handover in an ultra-connected scenario. Finally, potential research directions are presented for a road towards the 6G ecosystem.

Received on 07 November 2022; accepted on 22 November 2022; published on 20 December 2022

Keywords: Security Functions, Network Security, 6G, Trust, Adversaries

doi:10.4108/eetinis.v9i4.2846

1. Introduction to 6G and Zero-Touch Networks

Next-generation wireless networks have evolved to ultra-reliable, ultra-low latency networks with support of ultra-dense communication, where several devices operate in the periphery of each other. This situation often leads to network entities competing for resources, interference-free transmissions, capacity enhancement, and improved coverage at a lower OPEX/COPEX. At present, 5G networks are being deployed with improved mobile internet communications, more functionalities, and a broad scope of service accessibility. Device to device communication, better fronthaul and ultra-reliable backhaul are considered as core factors supporting services in 5G, which are expected to be improved further as the operators look towards beyond 5G deployments. Moving to 5G saw new radio technologies as it is known from the earlier generation of the networks. This means that the security and trust will be the centric concerns for having deployments ready while focusing on ultra-connected networks with better resources and services of 6G [1][2].

Because of the excessive virtualization leading to zero-touch networks, further extensions are desired for security and trust functions. Zero-touch networks are all about having extensive dependence on AI for most of the operations following 'self' as a driving factor that may include recovery, configurations, authentication, assurance and diagnosis. Zero-touch networks can help improve the management of security across the ultra-connected ecosystem. However, with excessive dependence on automation and virtualization, controlling AI-assisted components from self-initiating authentication will be a considerable challenge.

The concept behind understanding the security and trust of any network is to observe its architecture and identify crucial entities compromising which the network may fail and be dominated by adversaries. 5G services are more dominated towards virtualized operations attainable through Service-Defined Networks and Network Function Virtualization features. The 6G network will be more overwhelmed by the service requests to support the virtual world applications ranging from healthcare and Industry 5.0 to Digital Twins [3]. However, current settings may not be sufficient to handle the ultra-low latency needs of applications deployed by organizations aiming at metaverse, let alone the ultra-high demand of authentication and encryption of messages, which are responsible for slowing down the network. An exemplary illustration of network entities

*Corresponding author. Email: v.sharma@qub.ac.uk

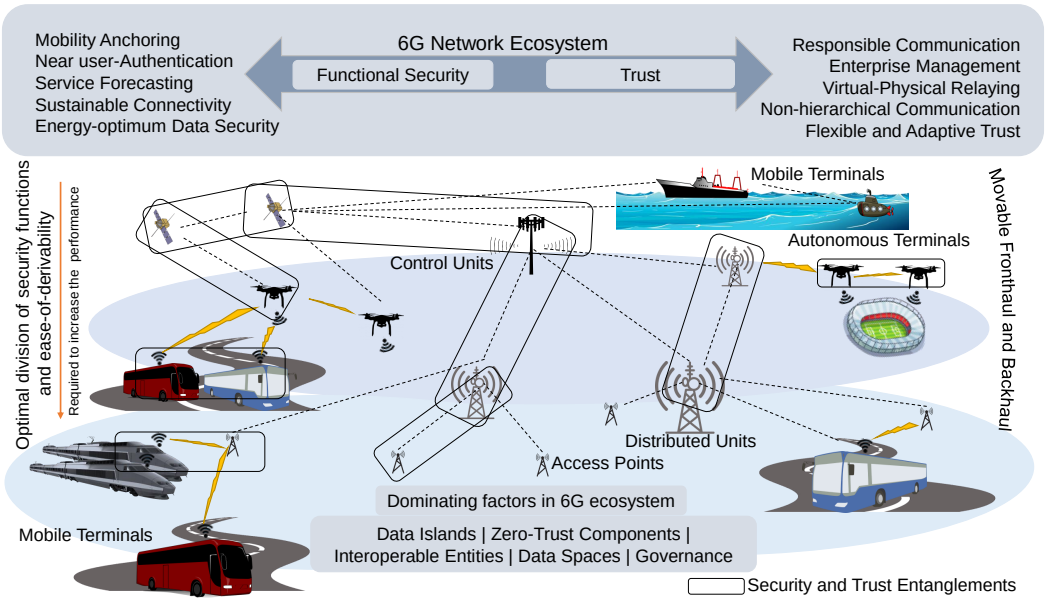

Figure 1. An exemplary illustration of the functional requirements of security and trust for 6G network ecosystem.

with functional requirements of security and trust is shown in Figure 1.

Services in 6G and zero-touch networks are expected to offer a virtual assessment of the actual physical environment for the prime purpose of evaluating the real-time operations of the system. More significantly, deploying 6G networks with open settings having far better interoperability between the operators to understand better the network needs a better mechanism to manage the access and assign roles to the users. And, service migrations from the 5G to the 6G ecosystem need additional 'management' layers in the traditional network setup.

The contributions in this paper are summarized as follows:

- Functional security and trust of 6G ultra-connected ecosystem are discussed, enhancing our understanding and requirements on top of the current security settings applicable to 5G and beyond, requiring re-investigation by the research community.
- Innovative domains, such as quantum, satellite-to-autonomous vehicle constellations, Digital Twins and their associated security are discussed, followed by consumer issues related to 6G security.
- A numerical case study is presented, which overviews the potential impact of the passes in a protocol, channel and network latency when securing the handovers in ultra-connected networks.
- Security-by-design and trust-by-design principles are explored along with potential future directions that directly impact the security and trust of the 6G ecosystem.

The rest of the paper is organized as follows. Section 2 discusses detailed aspects of functional security and trust in 6G ultra-connected networks, Section 3 focuses on quantum supremacy, which is expected to be one of the core motivators for 6G. Security of satellite constellations is discussed in Section 4 followed by the discussions on securing Digital Twins in Section 5. Consumer issues related to 6G security are discussed in Section 6. Section 7 expresses design principles related to security and trust and operational impact on securing handovers. Road map and future research directions are highlighted in Section 8. Finally, Section 9 concludes the paper.

2. Functional Security and Trust in 6G Ecosystem and Ultra-Connected Networks

6G virtualization will be an ecosystem of many processes operating to help analyze the network's workflow, offering better connectivity, access management and supporting a large domain of applications that otherwise are not practical through current deployment, as illustrated in Figure 2. However, a compromised network will ruin the workflow by generating faulty output or making incorrect inputs to the entities, which results in incorrect settings for the actual physical world. These will further depend on several security functions [4], which, if not configured properly, can generate a wrong sequence of access control and authorization and can be

enormous enablers of zero-day attacks on the networks. Thus, security and trust of the 6G ecosystem are of immense importance. Below are listed some of the essential aspects, which require *re-investigation* by the research community:

- **Data theft:** 6G networks will rely on fine twinning of real-world and virtual-world components and making precise and accurate connections to improve performance and security. However, with increased interaction and astronomically high virtualization, excessive data exposure can lead to future attacks on the network. The density of devices will be ultra-high, and it would not be easy to contain the data. Exposing data can give details on the network's algorithms and security functions that adversaries can aim to harm the actual devices responsible for carrying out the activities of security functions and trust management activities. Furthermore, data collection, processing and visualization pose additional security and trust hazards, as the adversaries can use the data to test their attacks before attacking the networks.

- **Authentication:** In the 6G ecosystem, several devices will rely on digital clients to obtain information for different associated services. Having a client not authenticated before granting access to the network can be a window for the attackers. A multi-factor authentication system based on privileges allows users to have customized security access to their devices and set conditions for trusting the associated services. For network-assisted virtualization, authentication must be similar to enterprise-level security. The software can be secured using third party SDKs or a local Authentication Server. It is still an open area of research to understand what type of functional architecture can be used for ultra-low latency in authentication of a billion industrial or IoT devices. Another aspect is to address the network's performance and authentication of components collectively. A weaker authentication can result in access issues, and more robust authentication with slow performance can generate overheads.

- **Credential management:** Authenticating devices over the network or via direct input from security requires efficient and secure credential management. Credential theft has been a primary concern for many real-world applications, especially for the services that rely on remote servers to authenticate the devices. It requires transmission and storing information across the network leading to several security breaches observed even in the current setup, where *Kaspersky* [5] has reported 1.5 billion breaches of IoT devices in the first half of 2021, and *Security Boulevard* [6] reported 64% attacks on credential thefts. Relying on cloud services or network operators can be a good solution if these are ensured to follow a straightforward security process through novel security functions and new trust management policies. However, attacks like Man-in-the-middle, session-hijacking, or physical attacks on the host can be additional challenges to address for credential management.

- **Network software security and cloning:** Controlling the amount of information amongst ultra-connected users is an essential factor to consider. It deals with the software level security and privacy of content. Services operating in the public domain must adhere to the principles of data sharing and privacy policies, ensuring that any theft and software vulnerability must not expose the private information from the network [7]. Having thefts on the data, operations and forecast models used by the user software, adversaries aim to clone the network, which can take advantage of either instantly or with time. Adversaries may consider the advantage model and evaluate the best time to attack the system. The adversaries can even expose the network-functions or sell data to rival systems, which may leave the network unpatched, resulting in many attacks.

- **Buffer control:** Segmentation faults and buffer overflow are major issues behind security attacks on digitized networks. An attacker can operate on kernel level, and launching several kernels can lead to segmentation faults and buffer overflow where the digital systems cannot compile on some process and fail to ensure transmission. Such situations must not arise, and the network infrastructure must be accurately designed and coded before being deployed by the industry.

- **Access management:** 6G ecosystem will be a system of a system. Thus, different components may need to have additional access. Therefore, ensuring access to desired features is necessary to ensure that information or the resulting performance is not in the wrong hands and can mistreat the networks' knowledge. Access management will vary depending on the remote or direct interaction between the entities. With modern technologies requiring networks for the complex and devolved system, remote access management is another direction to look into and ensure that the security is not compromised. Access management through security keys must

be free from replay attacks, ensure perfect forward secrecy, and adhere to the principles of credential management [8].

- **Zero-click processes:** Adversaries can use the network workflow to understand security features executed without requiring human intervention to respond. Such techniques can have several layers of code executions that can often lead to zero-click issues. It is of utmost importance to ensure that the security functions and their generators, bound with the real-world system, must not have zero-click processes that can be an entry point for attackers.

- **Design accessibility:** Although accessibility is related to access control and authentication, it specifically relates to the underlying technological code used to build the virtual network comprising many third-party systems. It needs to understand the software-firmware bindings, which explicitly raises the security issues associated with the design accessibility and how the network gets deployed. Since the 6G ecosystem will be more about accessibility and better usage, involving third parties in its design may have other implications related to access control and authentication, which must be dealt with carefully.

3. Quantum-leap in 6G

As per the recent interests of the organizations aiming towards quantum supremacy, speculations have been made that the 6G ecosystem will have quantum computing as a significant role player [2]. Literature has already presented the concept of quantum Internet and how quantum communication can help bridge the actual deployment and use-cases. Here, an essential factor that needs further understanding is the perceiving of the quantum technology to the user. What significant difference a user will feel and if an entire shift of security has to be done towards the quantum and failures of classical algorithms could be huge. How the transitions will be made towards the quantum Internet and what will happen to Mobile Internet Security, which is the dominating aspect of modern Internet Security.

There are several factors to be considered, such as what type of security functions would be required? How are the entanglements between the classical devices and quantum devices handled? Will quantum-era mean a harsh operational environment for the classical devices as security requirements would be tougher? What will be the roll-out process of the technology? Will the circuits be customized for every application, or will they be only used as a backbone? What type of architecture are we looking at as a part of security functions and trust establishment? How will the factors of scalability and inclusion of devices consider the impact of security and trust? Will 5G and beyond allow glimpses into possible settings of quantum communications in 6G? And, in terms of usability, who will own the bands and be responsible for handling the resources? And what types of encryption and decryption mechanisms will come into play? What implications do 6G quantum security functions have on the way users interact and use several on-demand services? Furthermore, the role of government bodies, stakeholders and organizations need to be clear when possibilities of the 6G ecosystem are rolled out.

4. Securing satellite-to-autonomous vehicles constellations in 6G

Innovative topology in 6G and zero-touch networks would largely depend on autonomous vehicles and the satellite. Here, free-space optical transmissions would be interesting to explore to exploit satellite-assisted wireless communications' full capabilities. The number of applications depending on the fine-tuning of autonomous vehicles and the satellite will increase astronomically. In the case of satellites, the constellations are pre-validated. In contrast, with the involvement of autonomous vehicles (be it in the air, ground or sea), the topology gets severely affected, and trust becomes an essential factor on top of the security of communication when handovers are involved [9] [10]. These trust issues go beyond the topology and involve several data spaces where the trust needs to be maintained between the satellites and the autonomous vehicles to ensure accurate delivery of services. Several use-cases need to have an additional layer of security and trust. The security functions should be further derivable to support the customized application, such as relying on unmanned aerial vehicles and satellite communication to support public safety communications. Another interesting point of security functions would be supporting deep-space communication via 6G bands where several individual organizations may compete for information and can often lead to conflict over resources, which also exposes the network to attack from cyber-manipulators.

5. Securing Digital Twins in 6G

A digital twin must provide a complete physical to virtual mapping, which will support the vision of 6G's efforts towards service-centring and virtual applications [11]. Alongside accurate mapping, it is of utmost importance that the models built for replicating the physical networks are precise, trust-full, secure and efficient. The digital twin relies on sensory input and output in specific scenarios to build the model. In those setups, data security becomes critical as adversaries

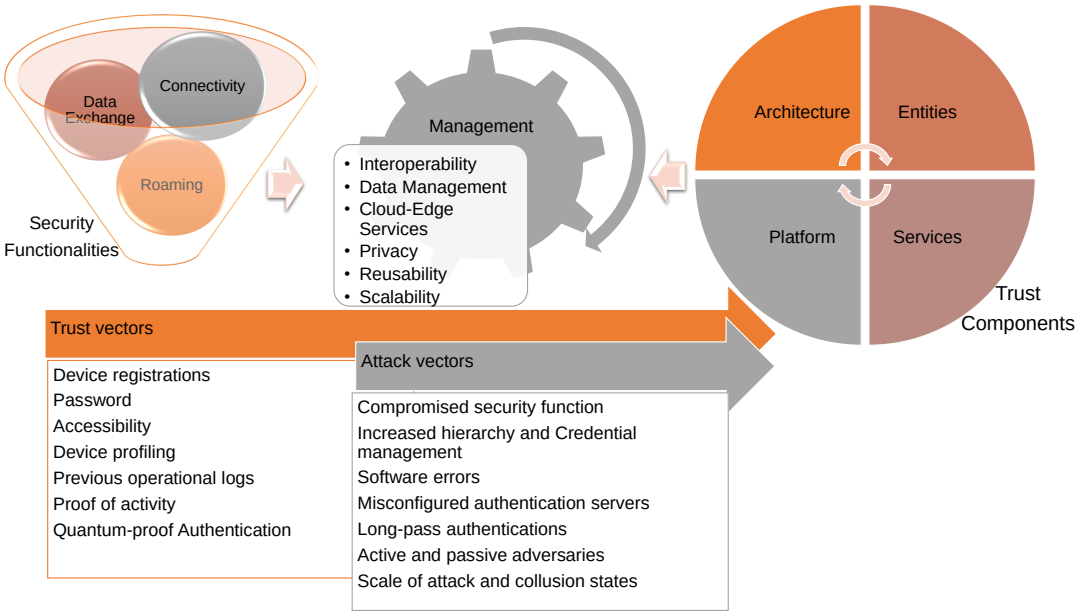

Figure 2. Functional security management with trust and attack vectors.

can ploy attacks against the network by compromising the modules of the digital twin. For applications in 6G networks, the digital twins must produce accurate simulations. Identifying security concerns and faults should be amongst the key motives of using the digital twins. In cases where the digital twin is a replica of the network's software processes, data thefts can expose the software model, information life cycle, and associated functions, and the following challenges become prominent:

- **Accurate testing environment:** Models for checking the accuracy of digital twins must be carefully developed. Models must be able to identify loopholes related to the integrity and confidentiality of the digital twins. The advantage of a digital twin is to use data and forecast outputs to improve the reliability and performance of the system. However, the question here arises- how to ensure that the forecast from the digital twin is accurate? Thus, testing environments must be built that can evaluate the working of the digital twin for correct observations.
- **Software-firmware binding:** For accurate forecast on the performance, digital twins are often given access to the system's operability, where it interacts with the firmware to gather information for building the prediction charts. However, this binding of the digital twin resulting from the software and firmware interaction must not compromise the system's security.
- **Handling misconfigurations:** An attacker having access to the digital twin can manipulate the algorithms to produce faulty outputs for the network entities. Misconfigurations are challenging to identify. In cases where third parties manage the digital twins and have bindings with the underlying sensors, the misconfigurations can be devastating. The result may vary from small error to a catastrophe.

6. Consumer Issues to 6G Security

Security practitioners always face a concern when it has to pick between the ease of use (or deployment) and the level of protection provided to equipment, process, and applications, which will presumably grow for the 6G ecosystem leading to the formation of zero-touch networks. Considering that the number of devices for each user will increase to many folds, the consumer issues will prevail as following aspects:

- **Intelligent and Flexible Security:** The most exciting aspect of security and trust in the 6G ecosystem will be understanding the requirements of a device and its role in the system. Safety and trust should be flexible based on the type of applications. In applications with minor priorities, the number of security operations could be reduced without compromising the crucial equipment in the network. It also requires investigating the type of encryption/decryption that may be usable on the transceivers. Here, the concern is who decides on the flexible security and trust establishment. The networks need to have sufficient intelligence to decide on these flexible security requirements

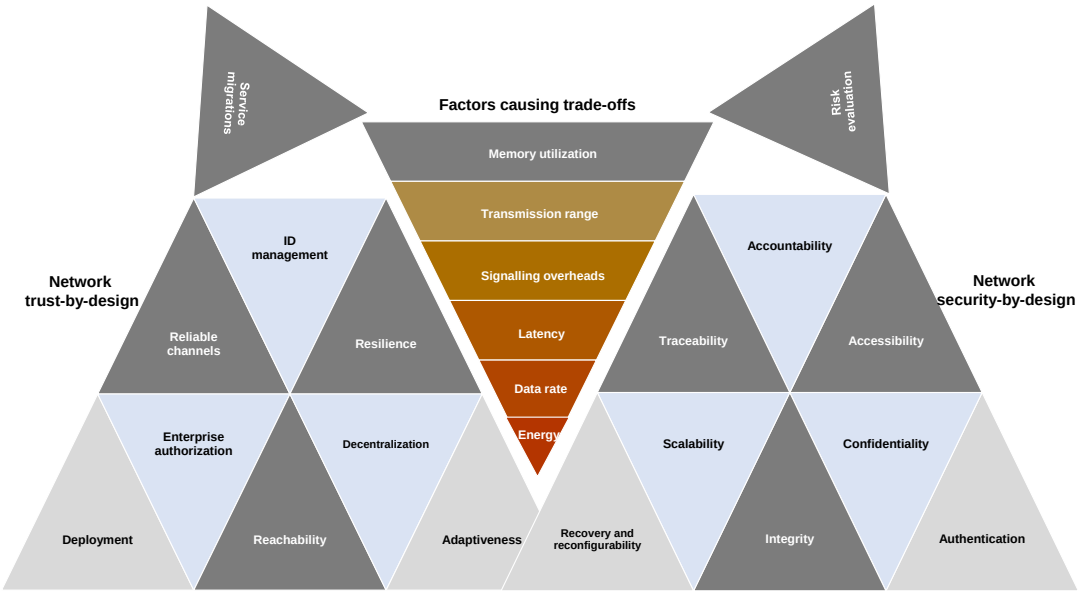

Figure 3. Principles of security-by-design and trust-by-design with associated performance trade-offs for 6G ecosystem.

here, so they must pick the security functions or equipment that can help attain this requirement.

- **Devolved Security:** In the 6G ecosystem, operational security will be crucial to ensure that trust between the devices is always maintained. To attain exceptional performance across the network at ultra-low latency with high connectivity is possible when the number of security passes between the users and the core is reduced to a certain extent. This reduction is possible if the security functions move near the users and do not require periodic exchanges with the core. Similar issues are observed in the 5G ecosystem. However, the extent of deploying those functions is still unclear, and research is expected to understand the impact of having more security functions near the users.

- **Managing Multi-Factor Authentication (MFA):** One of the important concerns when the number of devices is high for each user, management of MFA becomes crucial as well as challenging. With several critical devices connected through an edge-gateway, security in 6G will be crucial. In general, devices with multiple devices sharing similar authentication methods make the entire system vulnerable if one of the devices gets compromised by a cyber threat. It is desirable to explore approaches to prevent using similar authentications for all devices without increasing interaction between the user and the machines. Multiple authentication methods can be embedded in the user controller, whereby the devices will use different authentication mechanisms to establish a session.

7. Design principles and impact of security functions on handovers

In the 6G ecosystem, security-by-design [14] and trust-by-design [15] principles, shown in Figure 3, must be considered when deploying the network and ensuring connectivity to an astronomically large number of devices. Network security-by-design principles ensure that the expected devolved functional security follows better recovery and reconfigurability and enables better risk evaluation strategies. It will help adapt and provide better service migrations supporting the principles of network trust-by-design. Here, another concern involves handling the factors causing trade-offs with the security-by-design and trust-by-design principles where the energy is a dominating issue given the dominance of green computing, which also invokes trade-offs amongst the performance factors. However, balancing these performance factors and preventing violations of these principles will be a complex task because of the heterogeneity of operations and types of devices.

To further understand the expectations from the security functions, numerical observations are presented following modelling in [16], which with a reverse fitting of the model allows understanding the requirements of operational latency as well as the number of passes under strict conditions of handover latency (including authentication) in 6G ecosystem,

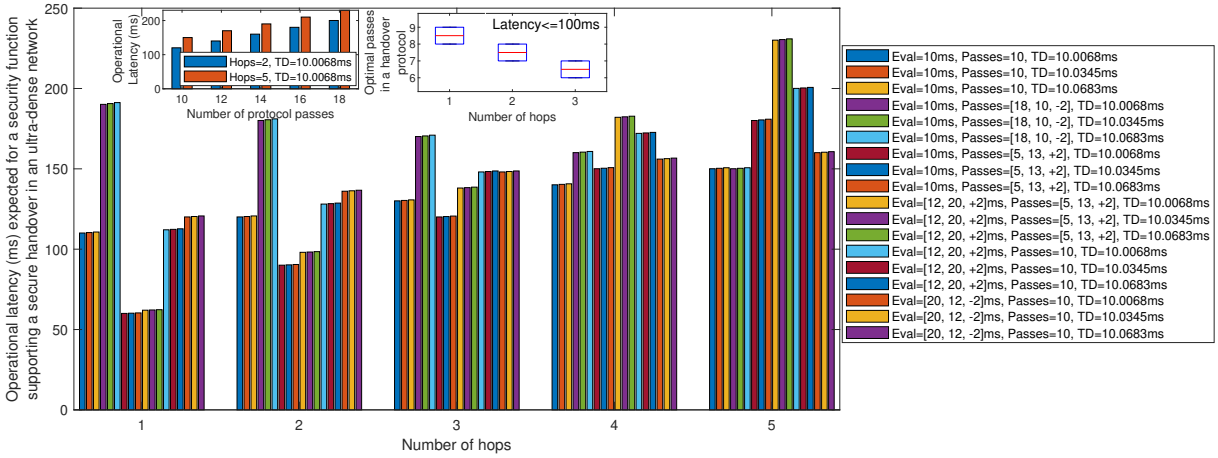

Figure 4. Understanding the expected impact on secure handover latency in terms of operational activity of a security function for 6G networks with variation in the number of hops, evaluation time (Eval), number of protocol passes (Passes), and one-way packet transportation delay (TD).

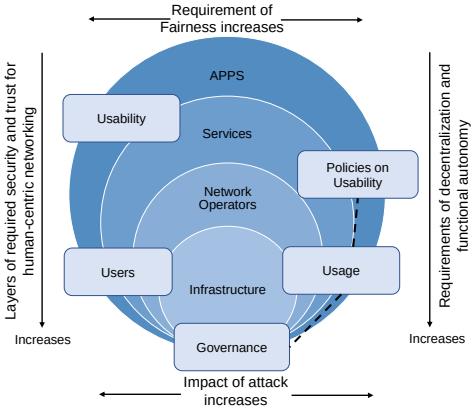

Figure 5. An illustration of human-centric security pillars for networks [12] [13].

as shown in Figure 4. With an expectation of 10-100μs channel latency [17], one-way packet transportation delay will approximately be around 10.0068ms to 10.0683ms, if the re-transmission trial is one, inter-frame time is 10ms, the ratio of packets to frame is two to one, and probability of zero error frame between 0.1 and 0.9. These values further help to get the operational latency for a security function with a specific observation that the number of passes in the protocol and the time of evaluation at a hop has far more considerable impact than the number of hops used in the handover process as channel latency will be extremely low in 6G setup. Another observation is if the network needs to attain an operational complexity of ≤100ms, the security protocol requires to complete all handover operations with the number of passes in the range [8,9], [7,8], and [6,7] for 1, 2 and 3 number of hops, respectively at a constant decision time of 10ms for each pass. Though these results do not give conclusive evidence as each pass may involve an operation with a different decision time, these results can provide an expected range for the number of passes in a protocol, which can be used by the researchers when designing secure handover techniques for 6G ecosystem.

8. Road Ahead And Future Research Directions

Based on the current standings of research in the direction of 5G and beyond, it is expected that distribution of entities will have a huge impact on the security of 6G and zero-touch networks, because of which the following directions become more relevant to look into:

- **Secure distributed mobility and learning management:** The number of device interactions increases as the network becomes dense, which means several devices need to be accommodated for their mobility, specifically when the networks are expected to have a mobile fronthaul and a movable backhaul. It is evident from the current research on autonomous networks where drones are explored (or used) as base stations. It is interesting to identify what specific security functions will be needed on top of the current 5G security functions. Will mobility management require passing messages via a control unit or a distributed unit that are motivators of edge-based mobility? Supporting users by having user-security functions is a way forward. On-device security functions can be used as a primary mode of entity management. The users'

secondary devices can rely on authentication and handoffs, causing a lesser burden on the network. Here, another interesting aspect to explore is how devices learn and can the secondary device act as an active attacker to control the primary device for intrusion.

- **Secure device-diversification and green computing:** The energy crisis is enormous, and it certainly has to do a lot with the networks. Improved connectivity directly impacts the number of resources needed by the devices for security evaluations which has to be taken seriously. So far, high-performance algorithms may avoid energy analysis, where it is the right time to make these evaluations mandatory criteria with the space-time observations. Diversity of devices further impacts the initiatives of green computing as similar security algorithms may not apply to all the equipment, and fine-tuning and energy-harvesting may be required before deployment [18].

- **Secure distributed edge computing and service migration:** In the 6G ecosystem, the ultra-connectivity will be supported by a large number of service migrations based on the decision of resources, offloading criteria or support for services. It means the level of service migration will be huge, primarily because of the heterogeneity of the data. Thus, securing the service migration will be essential. More importantly, having lightweight mechanisms that can be deployed with the distributed edge setup has a lot of resource-constrained fronthaul equipment, which is a direction for the researchers. It will be a huge challenge to understand dynamically changing service migrations and their corresponding security features.

- **Secure human-in-the-loop and intelligence representation:** Human-centric computations will be critical in 6G ecosystems. It will involve several human-dependent intelligent operations that may or may not require direct triggering from the user (see Figure 5). However, given the complicacy of human-in-the-loop, securing networks will be a considerable challenge which needs investigation of human-centric infrastructures [19] as well as ethical challenges [20]. If security functions are devolved for the 6G ecosystem to sustain beyond what is currently considered for 5G networks, the distributed operations of the humans and intelligence representation and its security will be game-changer for near user-operations. Exploring the relations of humans with the technologies, specifically the factors related to the establishment of trust, will be a considerable direction to explore.

9. Conclusion

Functional security and trust will be a huge potential area of research for the 6G ecosystem, given that 5G deployments are observing dependence on the security functions to protect the networks. It is desired to explore the associated challenges and motivate the research accordingly. This article expressed several aspects of functional security and trust in the 6G ecosystem. Understanding the design principles of security and trust and expectations from the security protocols in an ultra-connected network are other highlights of this work.

References

[1] U. Gustavsson, P. Frenger, C. Fager, T. Eriksson, H. Zirath, F. Dielacher, C. Studer, A. Pärssinen, R. Correia, J. N. Matos, *et al.*, "Implementation challenges and opportunities in beyond-5G and 6G communication," *IEEE Journal of Microwaves*, vol. 1, no. 1, pp. 86–100, 2021.

[2] Z. Zhang, Y. Xiao, Z. Ma, M. Xiao, Z. Ding, X. Lei, G. K. Karagiannidis, and P. Fan, "6G wireless networks: Vision, requirements, architecture, and key technologies," *IEEE Vehicular Technology Magazine*, vol. 14, no. 3, pp. 28–41, 2019.

[3] P. Porambage, G. Gür, D. P. M. Osorio, M. Liyanage, and M. Ylianttila, "6G security challenges and potential solutions," in *Proc. IEEE Joint Eur. Conf. Netw. Commun.(EuCNC) 6G Summit*, pp. 1–6, 2021.

[4] V. Sharma, I. You, and N. Guizani, "Security of 5g-v2x: Technologies, standardization, and research directions," *IEEE Network*, vol. 34, no. 5, pp. 306–314, 2020.

[5] C. Cyrus, "IoT Cyberattacks Escalate in 2021, According to Kaspersky," *IoT World Today*, *https://www.iotworldtoday.com/2021/09/17/iot-cyberattacks-escalate-in-2021-according-to-kaspersky/*, last accessed December 2021.

[6] T. Osofsky, "2021 Mid-Year Phishing Trends Update: More Attacks, with Credential Theft Dominating," *Security Boulevard*, *https://securityboulevard.com/2021/09/2021-mid-year-phishing-trends-update-more-attacks-with-credential-theft-dominating/*, last accessed December 2021.

[7] V. Sharma, I. You, K. Andersson, F. Palmieri, M. H. Rehmani, and J. Lim, "Security, privacy and trust for smart mobile-internet of things (m-iot): A survey," *IEEE access*, vol. 8, pp. 167123–167163, 2020.

[8] J. Zhang, R. Woods, T. Q. Duong, A. Marshall, Y. Ding, Y. Huang, and Q. Xu, "Experimental study on key generation for physical layer security in wireless communications," *IEEE Access*, vol. 4, pp. 4464–4477, 2016.

[9] H. Xie, Y. Zhan, G. Zeng, and X. Pan, "LEO Mega-Constellations for 6G Global Coverage: Challenges and

Opportunities," *IEEE Access*, vol. 9, pp. 164223–164244, 2021.

[10] V. Sharma, I. You, F.-Y. Leu, and M. Atiquzzaman, "Secure and efficient protocol for fast handover in 5g mobile xhaul networks," *Journal of Network and Computer Applications*, vol. 102, pp. 38–57, 2018.

[11] Y. Lu, X. Huang, K. Zhang, S. Maharjan, and Y. Zhang, "Low-latency federated learning and blockchain for edge association in digital twin empowered 6G networks," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 7, pp. 5098–5107, 2020.

[12] M. Grobler, R. Gaire, and S. Nepal, "User, usage and usability: Redefining human centric cyber security," *Frontiers in big Data*, vol. 4, 2021.

[13] G. Ra, T. Kim, and I. Lee, "VAIM: Verifiable Anonymous Identity Management for Human-Centric Security and Privacy in the Internet of Things," *IEEE Access*, vol. 9, pp. 75945–75960, 2021.

[14] K.-Y. Lam, S. Mitra, F. Gondesen, and X. Yi, "ANT-Centric IoT Security Reference Architecture – Security-by-Design for Satellite-Enabled Smart Cities," *IEEE Internet of Things Journal*, pp. 1–1, 2021.

[15] J. Lockl, V. Schlatt, A. Schweizer, N. Urbach, and N. Harth, "Toward trust in Internet of Things ecosystems: Design principles for blockchain-based IoT applications," *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1256–1270, 2020.

[16] J.-H. Lee, J.-M. Bonnin, I. You, and T.-M. Chung, "Comparative handover performance analysis of IPv6 mobility management protocols," *IEEE Transactions on Industrial Electronics*, vol. 60, no. 3, pp. 1077–1088, 2012.

[17] R. Gupta, D. Reebadiya, and S. Tanwar, "6G-enabled Edge Intelligence for Ultra-Reliable Low Latency Applications: Vision and Mission," *Computer Standards & Interfaces*, vol. 77, p. 103521, 2021.

[18] A. A. Nasir, H. D. Tuan, T. Q. Duong, and H. V. Poor, "Secrecy rate beamforming for multicell networks with information and energy harvesting," *IEEE Transactions on Signal Processing*, vol. 65, no. 3, pp. 677–689, 2016.

[19] F. Kammüller, "Human centric security and privacy for the iot using formal techniques," in *International Conference on Applied Human Factors and Ergonomics*, pp. 106–116, Springer, 2017.

[20] F. Kammüller, J. C. Augusto, and S. Jones, "Security and privacy requirements engineering for human centric IoT systems using eFRIEND and Isabelle," in *15th International Conference on Software Engineering Research, Management and Applications (SERA)*, pp. 401–406, IEEE, 2017.