Influence of the Human Factor on Radio Network Security and Signal Propagation

Mavula Kikwe Alexis[1]

[1]National Pedagogical University (UPN/ETS), Kinshasa, DR Congo.

Publication Date : 2026/02/04

Abstract: Radio network security traditionally relies on technical mechanisms such as cryptography, authentication, and reliable communication protocols. However, the human factor remains a critical source of vulnerability, frequently exploited through social engineering attacks. This paper investigates the influence of human behavior on radio network security and its indirect impact on signal propagation. Through a systematic review of recent scientific literature, the study identifies major social engineering attack vectors, analyzes their effects on radio equipment configuration, transmission quality, and data confidentiality, and proposes integrated mitigation strategies combining user training, technical controls, and organizational policies. The findings highlight that addressing human-related vulnerabilities is essential to improving the resilience and reliability of modern radio networks.

Keywords: *Human Factor, Network Security, Radio Networks, Signal Propagation, Social Engineering.*

How to Cite : Mavula Kikwe Alexis (2026) Influence of the Human Factor on Radio Network Security and Signal Propagation. *International Journal of Innovative Science and Research Technology*, 11(1), 2701-2703. https://doi.org/10.38124/ijisrt/26jan1313

I. INTRODUCTION

Radio networks, including cellular networks, wi-fi, and Internet of Things (IoT) systems, represent critical infrastructures for modern communications. Their security traditionally relies on technical mechanisms such as cryptography, authentication, and reliable communication protocols. Nevertheless, these protections can be bypassed by attacks that exploit human behavior rather than technical weaknesses, particularly through social engineering techniques, as highlighted in recent studies on human factors and cybersecurity risks (Eylem Thron et al., 2024).

Network operators and users may unintentionally disclose sensitive information, misconfigure equipment, or grant unauthorized access. Such human-related actions can compromise radio network security and negatively affect signal propagation an issue that has been observed in various wireless environments where human presence and activity affect radio channels (Ben Graham et al., 2011; sylvain collonge et al., 2004).

This study aims to analyze the role of the human factor in radio network security, identify relevant social engineering attack vectors, and propose defense strategies suitable for modern telecommunications environments.

II. THEORETICAL BACKGROUND

➢ *Social Engineering and Human Vulnerabilities*

Social engineering refers to a set of techniques designed to manipulate individuals into revealing confidential information or granting unauthorized access without directly attacking technical systems. These attacks exploit cognitive biases such as trust, authority, urgency, and curiosity. Consequently, the human factor is widely recognized as one of the weakest links in cybersecurity, requiring integrated frameworks that combine behavioral, psychological, and technological considerations, as discussed in human-centric cybersecurity analyses (Eylem Thron et al., 2024).

➢ *Impact on Radio Networks*

In radio networks, human errors related to configuration, maintenance, and operation of equipment can create significant security gaps and disrupt signal propagation. Previous experimental and analytical studies have demonstrated that human presence and movement can significantly influence radio channel characteristics, leading to signal attenuation, multipath variation, and interference (Sylvain Collonge et al., 2004; Richa Bharadwaj and Shiban K. Koul, 2021).

These socio-technical vulnerabilities increase the risk of unauthorized access, radio interference, and signal degradation. Therefore, effective security requires a combination of technical safeguards and continuous personnel training.

III. METHODOLOGY

This study is based on a systematic review of scientific literature and technical reports published between 2018 and 2023.

The analyzed sources include peer-reviewed articles from recognized databases such as IEEE Xplore, Sensors, and the Journal of Applied Informatics institutional reports related to telecommunications security, including the Zero Trust model proposed by the National Institute of Standards and Technology.

➢ *The Methodological Approach Consists of:*

- Identifying social engineering attack vectors targeting radio networks based on recent cybersecurity and human-factor studies (Eylem Thron et al., 2024)
- Analyzing the impact of human errors and presence on signal propagation using experimental and modeling studies in wireless and sensor networks (Ben Graham et al., 2011; Firdaus Firdaus et al., 2019)
- Proposing mitigation strategies integrating human, technical, and organizational factors in line with modern radio and IoT security research (Jianwei Liu et al., 2022)

IV. RESULTS

➢ *Identified Social Engineering Attack Vectors*

The literature review reveals several common social engineering attack vectors affecting radio networks:

- Phishing and spear phishing: targeting access credentials, commonly reported in critical infrastructure environments (Eylem Thron et al., 2024)
- Whaling attacks directed at network administrators and decision-makers
- Baiting through the introduction of infected storage devices into radio facilities
- SMiShing and vishing, enabling information harvesting via SMS messages or phone calls
- Pretexting and quid pro quo techniques relying on psychological manipulation
- Physical intrusions (tailgating), enabling unauthorized entry into critical network facilities

These vectors demonstrate that attackers frequently exploit trust and procedural weaknesses rather than radio-frequency vulnerabilities alone.

➢ *Impact on Signal Propagation*

Human errors in radio equipment configuration and management can result in:

- Radio interference and jamming, leading to reduced transmission quality
- Injection of malicious or covert signals, compromising communication integrity, as explored in cognitive radio and reconfigurable intelligent surface-based systems (Yan Xu et al., 2025)
- Unintentional data exposure, affecting user privacy and network confidentiality, particularly in RF sensing applications (Jianwei Liu et al., 2022)

Additionally, empirical studies confirm that human activity and occupancy significantly affect indoor radio propagation and positioning accuracy (Firdaus Firdaus et al., 2019; Anita Tabassum Biva et al., 2025).

V. DISCUSSION

The finding confirm that the security of modern wireless networks cannot rely solely on technical mechanisms. Human behavior plays a decisive role in network resilience. Training, awareness programs, and well-defined organizational policies significantly reduce human-related vulnerabilities and strengthen overall security posture. This conclusion aligns with previous observations in both wireless communication systems and other critical infrastructures, such as railway signaling networks, where human factors strongly influence cybersecurity outcomes (Eylem Thron et al., 2024).

➢ *Proposed Defense Strategies*

- Training and awareness: continuous education programs, phishing simulations, and practical exercises
- Advanced technical measures: multi-factor authentication, intrusion detection systems, and intelligent filtering
- Organizational policies: multi-channel verification of sensitive requests and strict access control procedures
- Adaptive security approach: post-incident analysis and adoption of the Zero Trust model, particularly relevant for heterogeneous radio and IoT environments

VI. CONCLUSION

Social engineering remains a major threat to radio network security by exploiting human vulnerabilities to bypass technical protections. An effective security strategy must integrate human, technical, and organizational dimensions. By transforming the human factor from a weakness into a resilience enabler, radio networks can achieve improved security, reliability, and signal quality.

REFERENCES

[1]. Reza Shabazian, Irina Trubitsyna (2023), Human Sensing by Using Radio Frequency Signals: A Survey on Occupancy and Activity Detection, IEEE Access, vol. 11, pp. 40878-40904.
[2]. Md Ibrahim, A.S.M. Badrudduza Md Shakhawat Hossen, Milton Kumar Kundu, Imran Shafique Ansari (2021), Enhancing Security of TAS/MRC-Based Mixed RF-UOWC System with Induced Underwater Turbulence Effect, IEEE Systems Journal, vol. 16, no. 4, pp. 5584-5595.
[3]. Ben Graham, Christos Tachtatzis, Fabio Di Franco, Marek Bykowski, David C. Tracey, Nick F. Timmons, Jim Morrison (2011), Analysis of the Effect of Human

Presence on a Wireless Sensor Network, International Journal of Ambient Computing and Intelligence (IJACI), vol. 3, no. 1, pp. 1-13.

[4]. Firdaus Firdaus, Noor Azurati Ahmad, Shamsul Sahibuddin (2019), Accurate Indoor-Positioning Model Based on People Effect and Ray-Tracing Propagation, Sensors, vol. 19, no. 24, article 5546.

[5]. Yan Xu, Jin Qian, Pengcheng Zhu (2025), A Scheme for Covert Communication with a Reconfigurable Intelligent Surface in Cognitive Radio Networks, Sensors, vol. 25, no. 20, article 6490.

[6]. Anika Tabassum Biva, Md Ibrahim, A.S.M. Badrudduza, Imran Shalique Ansari (2025), Enhancing Physical Layer Security in IoT-Based RF-FSO Integrated Networks: Multi-RIS Structures and Their Impact on Secure Communication, arXiv prepint, arXiv:2509.15411.

[7]. Sylvain Collonge, Gheorghe Zaharia, G.E. Zein (2004), Influence of the Human Activity on Wide-Band Characteristics of the 60 GHZ Indoor Radio Channel, IEEE Transactions on Wireless Communications, vol. 3, no. 6, pp. 2396-2406.

[8]. Richa Bharadwaj, Shiban K. Koul (2021), Study of the influence of Human Subject on the Indoor Channel Using Compact UWB Directive/Omni-Directional Antennas for Wireless Sensor Network Applications, Ad Hoc Networks, vol. 118, article 102521.

[9]. Eylem Thron, Shamal Faily, Huseyin Dogan, Martin Freer (2024), Human Factors and Cyber-Security Risks on the Railway – The Critical Role Played by Signalling Operations, Information & Computer Security, vol. 32, no. 2, pp. 236-263.

[10]. Jianwei Liu, Chaowei Xiao, Kaiyan Cui, Jinsong Han, Xian Xu, Kui Ren (2022), Behavior Privacy Preserving in RF Sensing, IEEE Transactions on Dependable and Secure Computing, vol. 20, no. 1, pp. 784-796.