

SPATIAL LOCALISATION OF WI-FI THREAT SOURCES IN CRITICAL INFRASTRUCTURE VIA RADIO-SOC EVENT CORRELATION

Dmytro I. Prokopovych-Tkachenko(1), Oleksandr Galushchenko(2), Yuliia Kovalenko(4),
Mykola Mormul(1), Volodymyr I. Sarychev(3), Anton Herasymenko(4)*

- (1) Department of Cybersecurity and Information Technologies, University of Customs and Finance, Dnipro; (2) Vinnytsia National Technical University, Vinnytsia;
(3) Department of Economics and Economic Security, University of Customs and Finance, Dnipro; (4) State University of Information and Communication Technologies, Kyiv
Ukraine

* Corresponding Author, e-mail: omega2417@gmail.com

Abstract: Critical-infrastructure facilities increasingly rely on dense Wi-Fi deployments, which creates exposure to rogue access points, evil-twin impersonation, deauthentication attacks and hidden clients. The paper proposes Correlated Radio-SOC Localisation (CRSL), a framework that fuses distributed RF-sensor observations, wireless-activity features, indicators of compromise and SIEM/SOAR events. The method combines localisation based on multi-sensor measurements with temporal, identity and behavioural correlation of SOC events. The framework produces classified threat findings with an estimated uncertainty region and confidence score. The proposed architecture and evaluation protocol show how radio-event fusion can improve incident attribution and accelerate operational response in protected wireless environments.

Key words: wi-fi security, rogue access point, rf localisation, soc correlation, critical infrastructure.

1. INTRODUCTION

Wireless local-area networks have become an integral communication layer in modern critical infrastructure (CI), including energy distribution, transport, water management and industrial control environments. The convenience and flexibility of Wi-Fi, however, introduce a broad and continuously evolving attack surface. Adversaries can deploy rogue access points (APs), impersonate legitimate networks through evil-twin attacks, disrupt connectivity with deauthentication and disassociation frames, and operate hidden clients that probe or attack the environment without ever associating with a monitored AP. In CI settings, where a loss of availability or integrity may propagate into physical processes, the timely detection and physical attribution of such threats is operationally significant.

Two families of defensive technology address parts of this problem but rarely cooperate. The first family consists of RF-monitoring and wireless intrusion-detection systems (WIDS/WIPS), which observe the radio spectrum, measure signal characteristics and can

estimate the position of an emitter through received-signal-strength indication (RSSI), time-based ranging or fingerprinting. These tools are strong at identifying where a signal originates but weak at relating that signal to a broader security incident. The second family consists of SOC tooling - security information and event management (SIEM) platforms and security orchestration, automation and response (SOAR) systems - which correlate authentication logs, host telemetry, network flows and threat intelligence. These tools are strong at identifying what is happening across the enterprise but typically have no notion of the geographic source of a wireless event.

This separation creates a practical blind spot: an analyst may receive a SIEM alert indicating credential abuse or anomalous association behaviour yet be unable to determine whether the responsible device is a permanent rogue installation inside a restricted zone, a transient attacker in a car park, or a misconfigured legitimate device. Conversely, an RF sensor may flag an anomalous beacon without sufficient context to decide whether it warrants an immediate, costly response.

To close this gap, this paper makes the following contributions:

- It proposes the Correlated Radio-SOC Localisation (CRSL) framework, a layered architecture that fuses distributed RF-sensor observations, derived wireless-activity features, IoCs and SIEM/SOAR events into a unified detection, correlation and spatial-localisation pipeline tailored to critical infrastructure.
- It defines a correlation model that links radio-plane evidence (signal signatures, frame anomalies and position estimates) with security-plane evidence (authentication events, host IoCs and threat-intelligence matches), so that each confirmed threat is both classified and spatially attributed with an associated confidence.
- It specifies an evaluation protocol through which the contribution of radio-event fusion can be measured against RF-only and SOC-only approaches and identifies the operational benefit in terms of reduced mean time to respond (MTTR).

The remainder of this paper is organised as follows. Section 2 reviews related work on RF-based localisation, Wi-Fi threat detection and SOC-side event correlation. Section 3 presents the proposed CRSL framework and its data flow. Section 4 describes the implementation considerations and evaluation protocol. Section 5 discusses the significance, limitations and a threat-to-defence mapping. Section 6 concludes the paper and outlines future work.

2. RELATED WORKS

The literature relevant to spatial localisation of Wi-Fi threats can be grouped into three streams that have largely developed in parallel.

RF-based localisation of wireless emitters. A substantial body of work addresses the estimation of an emitter's position from radio measurements. Fingerprinting approaches build a reference map of signal characteristics across a site and match live observations against it; the seminal RADAR system established RSSI fingerprinting as a practical indoor-localisation technique [1]. Subsequent surveys and studies extended this direction with probabilistic models, machine-learning regressors and multi-sensor trilateration based on RSSI or time-of-arrival measurements [2-7], while sensor-fusion approaches combine Wi-Fi RSSI with complementary signals to improve robustness [8]. These methods can achieve useful spatial resolution, but they are generally designed for cooperative localisation of known devices rather than for adversarial sources, and they treat localisation as an end in itself rather than as evidence within a security workflow.

Detection of Wi-Fi threats. A second stream focuses on detecting specific wireless attacks. Rogue-AP detection has been approached through MAC and SSID heuristics together with beacon-timing and clock-skew analysis [9, 10]. Evil-twin detection compares frame-arrival-time, round-trip-time or traffic characteristics between the suspected access point and the legitimate gateway [11-13]. Deauthentication and disassociation attacks exploit unprotected management frames; mitigations include the protected-management-frame mechanism standardised in IEEE 802.11 [14], although residual weaknesses persist even under WPA2 and WPA3 [15]. Hidden or non-associated clients - devices that probe, inject or jam without associating - remain comparatively under-served by access-point-centric monitoring and motivate dedicated spectrum sensing. WIDS/WIPS platforms integrate several of these detectors, but their alerts are seldom enriched with incident context drawn from the wider security environment.

SOC-side correlation and response. A third stream concerns the correlation of security events. SIEM platforms aggregate heterogeneous logs and apply rule-based or analytics-driven correlation to surface incidents, and their role in critical infrastructure has been examined in detail [16], while SOAR systems automate triage and response playbooks, increasingly augmented by AI/ML techniques [17]. Within IJITS, related monitoring-and-correlation architectures have been investigated: a DNS-monitoring module integrated into a cybersecurity architecture to counter spoofing and phishing [18]; a real-time framework for malware detection and monitoring in production [19]; and the organisation of program-monitored virtual networks [20]. These works demonstrate the value of architectural monitoring and correlation, yet they operate predominantly on host and network telemetry and do not incorporate the radio plane or physical-source attribution.

Research gap. Across the three streams, a consistent gap emerges. RF-localisation research locates emitters but does not place them in an incident context; Wi-Fi-detection research identifies attacks but rarely attributes them spatially with quantified confidence; and SOC-correlation research reasons over enterprise events while remaining blind to wireless geography. No widely adopted framework jointly correlates RF observations, wireless-activity features, IoCs and SIEM/SOAR events to deliver context-aware spatial attribution of Wi-Fi threats in critical infrastructure. The CRSL framework proposed in this paper is motivated directly by this gap.

3. PROPOSED SOLUTION

This section presents the design and operational logic of the Correlated Radio-SOC Localisation (CRSL) framework. The central idea is that radio-plane evidence and security-plane evidence are individually incomplete but jointly sufficient to both confirm and localise a wireless threat. CRSL therefore treats localisation not as a stand-alone service but as a correlated output of a security pipeline.

3.1. Framework overview

As shown in Figure 1, CRSL is organised as five interacting layers that transform raw radio measurements and security telemetry into localised, context-rich threat findings.

- **RF sensing layer.** A set of distributed, time-synchronised RF sensors monitors the Wi-Fi spectrum across the protected site. Each sensor captures management and control frames, per-frame metadata (source and destination addresses, SSID, channel and sequence numbers) and physical-layer measurements such as RSSI and, where available, time-of-arrival. Sensor

placement is chosen to provide overlapping coverage so that a single emitter is observed by multiple sensors.

- **Feature and IoC layer.** Raw captures are reduced to wireless-activity features, including beacon-interval regularity, management-frame rate, probe patterns, SSID/BSSID inconsistencies and clock-skew estimates, and are matched against an IoC repository of known malicious BSSIDs, suspicious vendor OUIs, blacklisted SSIDs and threat-intelligence indicators.

- **Localisation engine.** Multi-sensor RSSI/time measurements for a candidate emitter are combined via fingerprint matching and/or trilateration into a spatial estimate with an associated uncertainty region, rather than a single point.

- **Correlation layer.** This layer is the core contribution. It associates radio-plane evidence with security-plane evidence received from the SOC, including authentication failures, host IoCs, network-flow anomalies and SIEM alerts, aligning them in time and identity space to produce confirmed, classified and spatially attributed threat findings.

- **SOC and response layer.** Correlated findings are delivered to the SIEM/SOAR environment, where they enrich existing incidents, drive automated playbooks and are presented to analysts on a situational map.

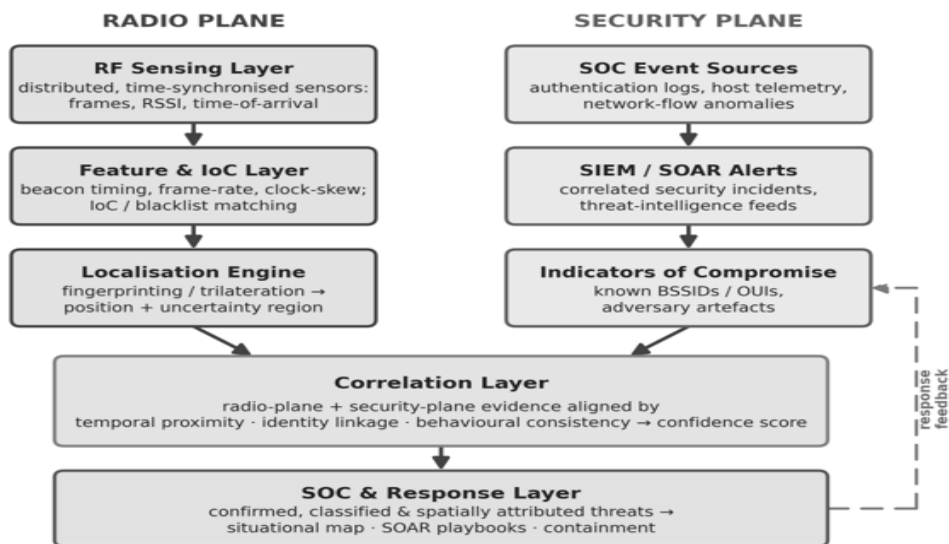


Figure 1. Layered architecture of the CRSL framework, showing the RF sensing, feature/IoC, localisation, correlation and SOC/response layers and the data flows between the radio and security planes.

3.2. Data flow and correlation logic

The end-to-end processing sequence is illustrated in Figure 2. Sensors continuously stream frame metadata and physical measurements to the feature and IoC layer. When a candidate threat signature is raised - for example an SSID that duplicates a legitimate network but advertises a different BSSID, or a burst of deauthentication frames - the localisation engine gathers the corresponding multi-sensor measurements and computes a position estimate with uncertainty.

In parallel, the correlation layer subscribes to SOC events. Each radio-plane candidate is correlated with security-plane evidence using three association keys: temporal proximity (events within a configurable window), identity linkage (shared MAC/BSSID, client identifiers or affected user accounts) and behavioural consistency (an RF anomaly accompanied by a matching host or network IoC). A weighted scoring function combines these signals into an overall confidence; only findings exceeding a configurable threshold are promoted to confirmed, localised incidents. This design ensures that an isolated radio anomaly with no security corroboration, or a SIEM alert with no radio evidence, is treated more cautiously than a finding supported by both planes.

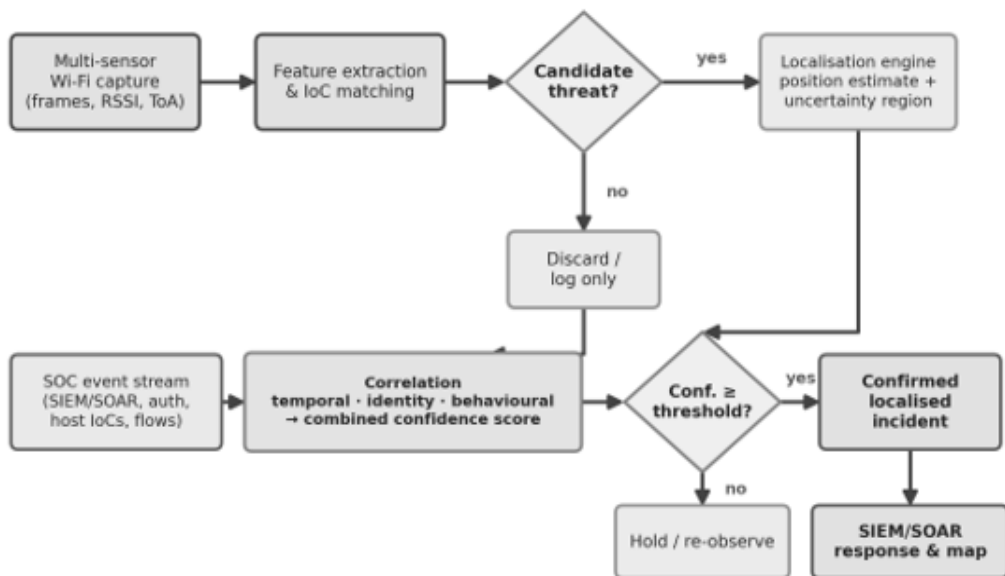


Figure 2. End-to-end dataflow and correlation pipeline of CRSL, from multi-sensor capture through localisation and radio-SOC correlation to SIEM/SOAR enrichment and response.

3.3. Supported threat classes

CRSL is designed to address four representative Wi-Fi threat classes in critical infrastructure: rogue APs (unauthorised infrastructure inside the facility), evil-twin APs (impersonation of a legitimate SSID), deauthentication/disassociation attacks (availability disruption) and hidden clients (non-associated devices that probe, inject or jam). For each class, the framework specifies the radio-plane indicators, expected security-plane corroboration and localisation strategy; these are summarised in the threat-to-defence mapping presented in Section 5.

4. IMPLEMENTATION AND EVALUATION

This section describes the implementation considerations of the CRSL framework and defines the protocol through which its effectiveness can be evaluated. The proposed implementation is designed for a multi-sensor testbed representative of a protected critical-infrastructure wireless environment.

4.1. Implementation considerations

The RF sensing layer can be realised with commodity Wi-Fi adapters operating in monitor mode or with software-defined-radio (SDR) front ends, depending on the required frequency coverage and timing precision. The feature/IoC, localisation and correlation layers are implemented as stream-processing services; correlated findings are exported to the SIEM/SOAR environment through a standard ingestion interface. Time synchronisation across sensors is essential for reliable multi-sensor localisation and time-based correlation.

Table 1 lists the principal configuration parameters of the framework. Concrete values depend on the deployment site, the sensor hardware and the operational risk appetite, and should be calibrated during commissioning.

Table 1. Principal configuration parameters of the CRSL framework.

<i>Parameter</i>	<i>Value</i>	<i>Description</i>
Number of RF sensors	site-dependent	Distributed monitoring nodes providing overlapping coverage
Monitored bands/channels	2.4 / 5 / 6 GHz	Spectral coverage of the sensing layer
Localisation method	fingerprinting / trilateration	Technique for converting multi-sensor measurements to a position estimate
Localisation update interval	calibrated during commissioning	Frequency of position re-estimation for a tracked emitter
Correlation time window	configurable	Temporal proximity threshold for radio-SOC association
Confidence threshold	configurable	Minimum combined score to promote a finding to a confirmed incident
IoC sources	threat intelligence and local blacklists	External and local indicators used for corroboration
SOC integration	SIEM/SOAR	Platform receiving enriched, localised findings

4.2. Evaluation protocol

To assess the framework, controlled threat scenarios are executed for each of the four supported classes (rogue AP, evil twin, deauthentication attack and hidden client) at known physical positions, allowing measured localisation estimates to be compared against ground truth. The evaluation compares CRSL against two baselines: an RF-only configuration (localisation and wireless detection without SOC correlation) and a SOC-only configuration (SIEM/SOAR correlation without radio evidence). The reporting metrics are detection precision and recall, localisation error, false-alarm rate and the reduction in MTTR attributable to spatial context.

Table 2 provides the comparative-results template. The qualitative expectation is that CRSL should outperform RF-only and SOC-only baselines because it combines physical-source evidence with incident context, although final values must be obtained from measured testbed runs.

Table 2. Comparative evaluation of CRSL against RF-only and SOC-only baselines.

Metric	CRSL	RF-only	SOC-only	Meaning
Detection precision	high	moderate	context-dependent	true-threat share
Detection recall	high	moderate-high	moderate	detected-threat share
Localisation error	measured	measured	n/a	distance to ground truth
False-alarm rate	lower	higher	higher	incorrect incidents
MTTR reduction	highest	limited	limited	response-time gain

5. DISCUSSION

The principal argument of this work is that radio-plane and security-plane evidence are complementary, and that their correlation yields capabilities that neither plane provides alone. RF-only monitoring can localise an emitter but cannot establish whether it participates in a broader incident; SOC-only correlation can characterise an incident but cannot point responders to a physical location. By combining both, CRSL is expected to raise detection confidence for ambiguous cases - an anomalous beacon corroborated by an authentication anomaly is far more actionable than either signal in isolation - and to compress response time by directing physical or network containment to a bounded spatial region.

Table 3 summarises how each supported threat class maps from its mechanism and operational impact to the corresponding correlation-and-localisation response in the challenge-impact-defence style suited to a critical-infrastructure context.

Table 3. Wi-Fi threat classes mapped to operational impact and CRSL response.

Threat class	Mechanism and impact	Correlation-and-localisation response
Rogue AP	Unauthorised infrastructure provides covert access; loss of integrity/availability	Detect unauthorised BSSID; localise to facility zone; correlate with asset inventory and access logs
Evil twin	SSID impersonation harvests credentials or relays traffic	Compare BSSID/clock-skew against legitimate AP; localise emitter; correlate with credential-abuse SIEM alerts
Deauthentication / disassociation	Management-frame flood degrades availability	Detect frame-rate anomaly; localise source; correlate with connectivity-loss events; recommend protected management frames
Hidden client	Non-associated device probes, injects or jams	Spectrum-sense and localise; correlate with network-flow or host IoCs to establish intent

5.1. Operational implications

For SOC teams, the practical value of CRSL is not limited to detecting a wireless anomaly. The framework changes the triage object from a disconnected alert into a spatially bounded incident with a probable source region, supporting faster decisions about whether to dispatch physical security, isolate a network segment or continue observation. This is especially relevant in critical infrastructure, where wireless events may be caused by maintenance equipment, contractor devices, misconfigured access points or intentional

adversarial activity. Correlation with authentication logs, host IoCs and network-flow anomalies help distinguish these cases and reduces unnecessary escalation.

For engineering teams, CRSL also provides feedback for improving the sensing architecture itself. Repeated uncertainty regions can reveal weak sensor coverage, poor time synchronisation or zones affected by multipath. In this way, the localisation results become both a response aid and a commissioning instrument for the protected wireless environment. The architecture is therefore suitable not only for incident response but also for continuous improvement of wireless visibility, asset inventory quality and operational resilience.

5.2. Evaluation risks and validity

The evaluation of CRSL should separate detection quality from localisation quality because the two dimensions may fail for different reasons. A detector can correctly identify an evil twin while the localisation engine returns a broad uncertainty region, or a source can be localised accurately while the security-plane evidence is insufficient for incident confirmation. For this reason, the proposed protocol reports precision, recall, localisation error, false-alarm rate and MTTR reduction as separate metrics rather than merging them into a single aggregate score.

The testbed should also include non-malicious wireless activity, including mobile maintenance devices, temporary contractor access points and legitimate bursts of management frames. Such cases are important for estimating false alarms and for demonstrating that correlation improves operational judgement rather than merely increasing the number of alerts. Repeated measurements in different facility zones are necessary to account for multipath, shielding and variable sensor visibility in industrial environments.

Several limitations should be acknowledged. Localisation accuracy depends on sensor density, placement and the radio environment; multipath and obstruction in industrial settings may enlarge the uncertainty region. Correlation quality depends on accurate time synchronisation and on the availability and timeliness of SOC events; gaps in either plane reduce confidence. Adversaries aware of the monitoring may attempt evasion through MAC randomisation, low-duty-cycle operation or transmit-power manipulation, which motivates continued development of robust features.

6. CONCLUSION

This paper introduced the Correlated Radio-SOC Localisation (CRSL) framework, which addresses a gap between RF-localisation tooling and SOC-side event correlation in the protection of critical-infrastructure Wi-Fi environments. By fusing distributed RF-sensor observations, wireless-activity features, IoCs and SIEM/SOAR events within a layered architecture and a defined correlation model, CRSL both classifies and spatially attributes wireless threats - rogue APs, evil twins, deauthentication attacks and hidden clients - with quantified confidence and channels these findings into SOC response.

The main advantage of the proposed approach is the transformation of wireless alerts from isolated technical signals into spatially grounded security incidents. Possible applications include protection of energy, transport, industrial-control and public-service environments where the physical origin of a wireless event is operationally significant. Future work will implement the framework on a multi-sensor testbed, populate the comparative evaluation with measured results, extend the localisation engine with machine-learning models robust under MAC randomisation and variable transmit power, and validate the approach in a representative critical-infrastructure deployment.

REFERENCES

- [1] Bahl, P., Padmanabhan, V.N. RADAR: An in-building RF-based user location and tracking system. *Proceedings of IEEE INFOCOM 2000*, vol. 2, 2000, pp. 775-784. DOI: 10.1109/INFCOM.2000.832252.
- [2] Yang, C., Shao, H.-R. WiFi-based indoor positioning. *IEEE Communications Magazine*, vol. 53, no. 3, 2015, pp. 150-157. DOI: 10.1109/MCOM.2015.7060497.
- [3] Zafari, F., Gkelias, A., Leung, K.K. A survey of indoor localization systems and technologies. *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, 2019, pp. 2568-2599. DOI: 10.1109/COMST.2019.2911558.
- [4] Xiao, J., Zhou, Z., Yi, Y., Ni, L.M. A survey on wireless indoor localization from the device perspective. *ACM Computing Surveys*, vol. 49, no. 2, 2016, Article 25. DOI: 10.1145/2933232.
- [5] Bellavista-Parent, V., Torres-Sospedra, J., Perez-Navarro, A. Comprehensive analysis of applied machine learning in indoor positioning based on Wi-Fi: an extended systematic review. *Sensors*, vol. 22, no. 12, 2022, Article 4622. DOI: 10.3390/s22124622.
- [6] Roy, P., Chowdhury, C., Ghosh, D. A survey on ubiquitous WiFi-based indoor localization system for smartphone users from implementation perspectives. *CCF Transactions on Pervasive Computing and Interaction*, vol. 4, 2022, pp. 298-318. DOI: 10.1007/s42486-021-00089-3.
- [7] Han, Z., Wang, Z., Huang, H., Zhao, L., Su, C. WiFi-based indoor positioning and communication: empirical model and theoretical analysis. *Wireless Communications and Mobile Computing*, vol. 2022, 2022, Article 2364803. DOI: 10.1155/2022/2364803.
- [8] Poulouse, A., Kim, J., Han, D.S. A sensor fusion framework for indoor localization using smartphone sensors and Wi-Fi RSSI measurements. *Applied Sciences*, vol. 9, no. 20, 2019, Article 4379. DOI: 10.3390/app9204379.
- [9] Jana, S., Kasera, S.K. On fast and accurate detection of unauthorized wireless access points using clock skews. *IEEE Transactions on Mobile Computing*, vol. 9, no. 3, 2010, pp. 449-462. DOI: 10.1109/TMC.2009.145.
- [10] Han, H., Sheng, B., Tan, C.C., Li, Q., Lu, S. A timing-based scheme for rogue AP detection. *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 11, 2011, pp. 1912-1925. DOI: 10.1109/TPDS.2011.125.
- [11] Yang, C., Song, Y., Gu, G. Active user-side evil twin access point detection using statistical techniques. *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 5, 2012, pp. 1638-1651. DOI: 10.1109/TIFS.2012.2207383.
- [12] Lu, Q., Qu, H. SLFAT: Client-side evil twin detection approach based on arrival time of special length frames. *Security and Communication Networks*, vol. 2019, 2019, Article 2718741. DOI: 10.1155/2019/2718741.
- [13] Monica, D., Ribeiro, C. WiFiHop - mitigating the evil twin attack through multi-hop detection. *Computer Security - ESORICS 2011, Lecture Notes in Computer Science*, vol. 6879, 2011, pp. 21-39. DOI: 10.1007/978-3-642-23822-2_2.
- [14] IEEE. IEEE Standard for Information Technology - Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks - Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE Std 802.11-2020, 2021, pp. 1-4379. DOI: 10.1109/IEEESTD.2021.9363693.

- [15] Lounis, K., Zulkernine, M. Cut it: deauthentication attacks on protected management frames in WPA2 and WPA3. *Information Security Practice and Experience, Lecture Notes in Computer Science*, vol. 13107, 2022, pp. 278-295. DOI: 10.1007/978-3-031-08147-7_16.
- [16] Gonzalez-Granadillo, G., Gonzalez-Zarzosa, S., Diaz, R. Security information and event management (SIEM): analysis, trends, and usage in critical infrastructures. *Sensors*, vol. 21, no. 14, 2021, Article 4759. DOI: 10.3390/s21144759.
- [17] Kinyua, J., Awuah, L. AI/ML in security orchestration, automation and response: future research directions. *Intelligent Automation & Soft Computing*, vol. 28, no. 2, 2021, pp. 527-545. DOI: 10.32604/iasc.2021.016240.
- [18] Ivanova, Y. Integrating a DNS monitoring module into a cybersecurity architecture to enhance protection against spoofing and phishing attacks. *International Journal on Information Technologies and Security*, vol. 17, no. 2, 2025, pp. 111-122. DOI: 10.59035/LLQJ9022.
- [19] Baghirov, E. A comprehensive framework for real-time malware detection and monitoring in production. *International Journal on Information Technologies and Security*, vol. 16, no. 4, 2024, pp. 85-94. DOI: 10.59035/GLJY1234.
- [20] Romansky, R. Preliminary organization of virtual network based on program monitoring. *International Journal on Information Technologies and Security*, vol. 16, no. 3, 2024, pp. 111-120. DOI: 10.59035/TQDU5702.

Information about the authors:

Dmytro I. Prokopovych-Tkachenko - PhD in Technical Sciences, Associate Professor, Head of the Department of Cybersecurity and Information Technologies at the University of Customs and Finance, Dnipro, Ukraine. Current research interests: cybersecurity, information technologies, wireless security and digital infrastructure protection. e-mail/ORCID: omega2417@gmail.com; 0000-0002-6590-3898.

Oleksandr Galushchenko - Postgraduate Student at Vinnytsia National Technical University, Vinnytsia, Ukraine. Current research interests: cybersecurity, wireless networks and information security technologies. e-mail/ORCID: ogalus5212@gmail.com; 0009-0002-5597-8818.

Mykola Mormul - PhD in Technical Sciences, Associate Professor at the Department of Cybersecurity and Information Technologies, University of Customs and Finance, Dnipro, Ukraine. Current research interests: mathematical modelling, optimisation methods, statistics, decision theory and optimisation of economic and technical systems. e-mail/ORCID: mormul@umsf.dp.ua; 0000-0002-8036-3236.

Volodymyr I. Sarychev - Doctor of Economic Sciences, Associate Professor, Professor at the Department of Economics and Economic Security, University of Customs and Finance, Dnipro, Ukraine; ORCID: 0000-0002-8544-9901.

Anton Herasymenko - PhD student, State University of Information and Communication Technologies, Kyiv, Ukraine; e-mail/ORCID: anton.hrsmnk@gmail.com; 0009-0008-4475-2040.

Yuliia Kovalenko - Candidate of Pedagogical Sciences, Associate Professor, Department of Artificial Intelligence, State University of Information and Communication Technologies, Kyiv, Ukraine; ORCID/Scopus: 0000-0002-6714-4258; 58193513800.

Manuscript received on 16 June 2026