Model and methodology for the formation of adaptive security profiles for the protection of wireless networks in the face of dynamic cyber threats*

Pavlo Skladannyi[1,2,*,†], Yuliia Kostiuk[1,†], Karyna Khorolska[1,†], Bohdan Bebeshko[1,†] and Volodymyr Sokolov[1,†]

[1] *Borys Grinchenko Kyiv Metropolitan University, 18/2 Bulvarno-Kudriavska str., 04053 Kyiv, Ukraine*

[2] *Institute of Mathematical Machines and Systems Problems of the National Academy of Sciences of Ukraine, 42 Ac. Glushkov ave., 03680 Kyiv, Ukraine*

Abstract

The paper introduces a comprehensive model and accompanying methodology for constructing adaptive security profiles aimed at protecting wireless networks under dynamic cyber-threat conditions. The significance of the study stems from the ever-escalating complexity of attacks targeting wireless infrastructures, the widespread emergence of hybrid threat scenarios, the continual expansion of client-device diversity (including IoT endpoints), and the increasingly rapidly evolving risk landscape. The investigation was conducted with explicit reference to contemporary international cybersecurity standards—IEEE 802.11ax/802.11be, ISO/IEC 27033, ISO/IEC 15408, and NIST SP 800-53—and was guided by the principles of Zero-Trust architecture, which advocates a context-sensitive approach to designing access-control, authentication, encryption, and monitoring policies. The proposed model facilitates the creation of a family of security profiles that can be dynamically updated in accordance with the prevailing threat level, interaction modality, trust degree assigned to participating nodes, and detected behavioral anomalies within network traffic. The developed methodology incorporates a multifactorial risk assessment that considers the technological characteristics of the transmission medium, observed attack activity, interference levels, and the specific access context. Consequently, the model can underpin automated solutions that enhance cyber-resilience, certify the security posture of wireless networks, and enable dynamic, real-time audit mechanisms.

Keywords

adaptive security, security profiles, wireless network, Zero Trust, IEEE 802.11, dynamic threats, risk assessment, access policy, audit, international standards

1. Introduction

In the current era of digital transformation and the rapid deployment of wireless data-transmission technologies, the demand for reliable, adaptive, and resilient protection of network infrastructure is steadily increasing. Wireless networks that adhere to the IEEE 802.11ax and 802.11be standards are now pervasive across corporate, industrial, governmental, and public domains, yet they remain among the most vulnerable components of the contemporary information-and-communication ecosystem. The open radio spectrum, highly dynamic connection topology, and elevated mobility of client devices—including numerous IoT endpoints—create favorable conditions for sophisticated, multi-stage attack campaigns, thereby necessitating a fundamental re-evaluation of existing security mechanisms.

Concurrently, regulatory bodies are intensifying their demands for the formal certification of wireless-system security, stipulating that audits must evaluate not only architectural and technical parameters but also each system's capacity to react rapidly to shifting risk levels, detect anomalous behaviour, and adapt access-control policies to the prevailing threat context. Conventional, rule-

* *CSDP'2025: Cyber Security and Data Protection, July 31, 2025, Lviv, Ukraine*

* Corresponding author.

† These authors contributed equally.

p.skladannyi@kubg.edu.ua (P. Skladannyi); y.kostiuk@kubg.edu.ua (Y. Kostyuk); k.khorolska@kubg.edu.ua (K. Khorolska); b.bebeshko@kubg.edu.ua (B. Bebeshko); v.sokolov@kubg.edu.ua (V. Sokolov)

0000-0002-7775-6039 (P. Skladannyi); 0000-0001-5423-0985 (Y. Kostyuk); 0000-0003-3270-4494 (K. Khorolska); 0000-0001-6599-0808 (B. Bebeshko); 0000-0002-9349-7946 (V. Sokolov)

based solutions—anchored in static configurations—frequently fail to satisfy the flexibility and scalability imperatives of today's cyber landscape. The emergence of the Zero-Trust Architecture (ZTA) paradigm, which mandates the verification of every request irrespective of origin or network location, further accentuates the urgency for novel, dynamically adaptive security mechanisms.

The study advances an approach that constructs a formalised model for adaptive security-profile management in wireless networks, thereby enabling not only the automated generation and continual updating of security profiles, but also the dynamic adjustment of individual security parameters with respect to the actual network state, observed behavioural deviations, device-specific trust levels, traffic intensity, and the activity of prospective threats. Moreover, the integration of the proposed solution with comprehensive security-monitoring platforms—such as security information and event management (SIEM) systems—significantly augments context-aware response capabilities and sustains fine-grained, real-time access-control policies.

The proposed mechanisms are grounded in contemporary international standards and guidelines (NIST SP 800-53, ISO/IEC 27033, ISO/IEC 15408) and exhibit heightened effectiveness in operational contexts that demand not only strict regulatory compliance but also rapid adaptation to environmental fluctuations. Their deployment significantly increases the transparency of audit procedures throughout the entire security-lifecycle, optimises both direct and indirect certification expenditures, and formalises end-to-end security-assessment workflows through a rigorously risk-oriented logic. Accordingly, the adaptive security-profile model constitutes a robust foundation for holistic, multilayered protection mechanisms in wireless networks, seamlessly integrating granular automation, context-driven awareness, and continuously updated, dynamic risk evaluation. Its utilisation not only equips organisations of varying scale to address an array of contemporary cybersecurity challenges, but also facilitates the practical realisation of flexible, efficient, and standardised approaches to safeguarding critical information-and-communication infrastructures.

2. Literature review

A review of contemporary scientific literature affirms the increasing scholarly interest in developing adaptive security profiles for wireless networks, particularly under conditions of dynamic cyber threats. Khan et al. [1] investigate the feasibility of deploying lightweight authentication protocols within nascent 6G architectures, with specific attention to safeguarding unmanned-aerial-vehicle communications. The authors survey state-of-the-art lightweight authentication schemes and underscore the imperative to calibrate these mechanisms to environmental volatility and the constrained computational resources of client devices—a position that coheres with the broader objective of constructing adaptive security profiles for IoT-enabled and conventional wireless infrastructures.

Abie and Pirbhulal [2] have proposed an autonomous, adaptive security system for IoT environments operating within 5 G networks. Their work introduces a dynamic risk-management paradigm based on closed-loop feedback models, enabling the system to modify its security policies in real time without human intervention. This methodology is highly relevant to the development of adaptive security profiles that prioritise continuous monitoring and self-adjustment.

Ahmadi's investigation [3] occupies a particularly prominent position in the discourse on adaptability, providing a detailed analysis of Zero-Trust Architecture deployment within cloud-network environments. The study delineates both the key challenges and the prospective benefits of applying machine-learning techniques to implement dynamic access-control and authentication mechanisms, thereby empowering systems to adjust swiftly to emergent threat types and evolving multi-stage attack scenarios.

Within the domain of anomaly- and mixed-threat detection, Abdulkareem et al. [4] performed a large-scale comparative analysis of intrusion-detection mechanisms for both IoT and non-IoT environments. Their study investigates the specific requirements for dynamic responses to evolving traffic patterns and the nuanced challenges of engineering adaptive defence mechanisms—considerations that are essential when constructing robust security profiles for wireless networks.

Particular attention should be directed to the study by Kamble and Jog [5], which introduces an efficient key-management methodology for dynamic wireless-sensor networks. Their model incorporates periodic key rotation and seamless adaptation to topological changes, thereby supplying the degree of flexibility and scalability that contemporary wireless infrastructures demand. Collectively, the reviewed literature confirms that the research community is vigorously advancing toward the development of adaptive, self-configuring security frameworks that fully accommodate risk dynamics, environmental context, device heterogeneity, and user behaviour. This momentum establishes a solid scientific foundation for formulating a rigorous methodology to generate adaptive security profiles as a pivotal component of wireless-network protection. Recent studies by Shevchuk et al. [6] highlight the critical role of designing secured services for authentication, authorization, and accounting within dynamic network environments. Their work underlines the importance of integrating adaptive security mechanisms that ensure reliable identity management and access control, which are fundamental components in forming resilient security profiles for wireless networks facing evolving cyber threats.

3. Research methods

Techniques drawn from discrete mathematics, graph-analytic modelling, set theory, and fuzzy logic were employed to implement the adaptive security-profile model. Behavioural analysis combined with fuzzy-membership functions underpinned the construction of the trust model. Principles of mathematical induction were applied to formally prove the correctness of the profile-update mechanisms. Machine-learning algorithms, complemented by statistical analyses of risk dynamics, facilitated robust anomaly detection. The overarching system architecture and operative workflows were visualised by means of data-flow diagrams (DFDs) and associated graph structures.

4. Main material

During the development of an adaptive wireless-network protection model, the evolution of the IEEE 802.11 family of standards (802.11a/b/g/n/ac/ax/be)—which collectively define the architectural foundations and information-security mechanisms of the wireless medium—was thoroughly analysed. As the physical and data-link layers advanced, increasing emphasis was placed on authentication controls, a consideration that is particularly critical given the contemporary dynamics of cyber-threat landscapes. Early schemes (open authentication and shared-key authentication) proved susceptible to numerous attacks; consequently, modern implementations rely on Extensible Authentication Protocol (EAP) methods—specifically EAP-TLS, PEAP, EAP-TTLS, EAP-FAST, and EAP-PWD [1, 2, 7]—which enable multifactor authentication, X.509 digital certificates, dynamic session-key exchange, and context-aware configuration of access profiles. In the cryptographic domain, the longstanding transition from the obsolete WEP algorithm to current solutions embodied in WPA2 and WPA3 has been completed; these frameworks employ AES-CCMP, AES-GCM, Simultaneous Authentication of Equals (SAE), Protected Management Frames (PMF), and forward-secrecy techniques. The Advanced Encryption Standard (AES) thereby continues to ensure data confidentiality and integrity within the inherently open radio channel, serving as the fundamental means of protection.

Threats can be categorised by their level of impact into signal-level attacks—such as jamming, radio-frequency interference, and rogue access-point spoofing—and information-level attacks, including traffic interception, man-in-the-middle insertion, and unauthorised resource access. Hybrid assaults that blend physical-layer and logical-layer vectors demand highly flexible mitigation capabilities. Consequently, the construction of adaptive security profiles enables the dynamic selection of cryptographic primitives, granular access-control policies, and authentication modalities on the basis of continuous risk evaluation, environmental context, and observed user behaviour.

The proposed approach enhances the overall cybersecurity posture of the system and facilitates seamless integration with dynamic auditing, continuous-monitoring, and formal certification instruments that align with leading international standards—namely NIST SP 800-53, ISO/IEC 27033, and ISO/IEC 15408 [3]. Consequently, the adaptive security-profile model is positioned as a pivotal component within the wireless-network security architecture, furnishing granular contextual awareness, real-time adaptability, and sustained assurance of confidentiality, integrity, and availability of information assets for organisations of diverse scale amid rapidly evolving cyber-threat landscapes.

Figure 1 presents a spatial architectural model for establishing adaptive wireless-network protection, organised around a three-tier "input—processing—output" paradigm. The input tier integrates the IEEE 802.11 standards suite, user context (trust levels and behavioural attributes), and the principal threat vectors—namely, signal-level and information-level attacks. The processing tier incorporates authentication modules (EAP-TLS, PEAP), cryptographic mechanisms (AES, SAE), risk-assessment engines, and an adaptive-profile manager that synthesises policies commensurate with the prevailing threat landscape. The output tier displays the resultant artefacts: generated access-control policies, cryptographic requirements, audit logs, and compliance reports that align with NIST and ISO/IEC specifications. Dashed connectors illustrate the logical interactions among subsystems without obscuring the diagram's elements. Collectively, the model highlights the consolidation of standards, contextual data, and risk-driven management into a unified security architecture.

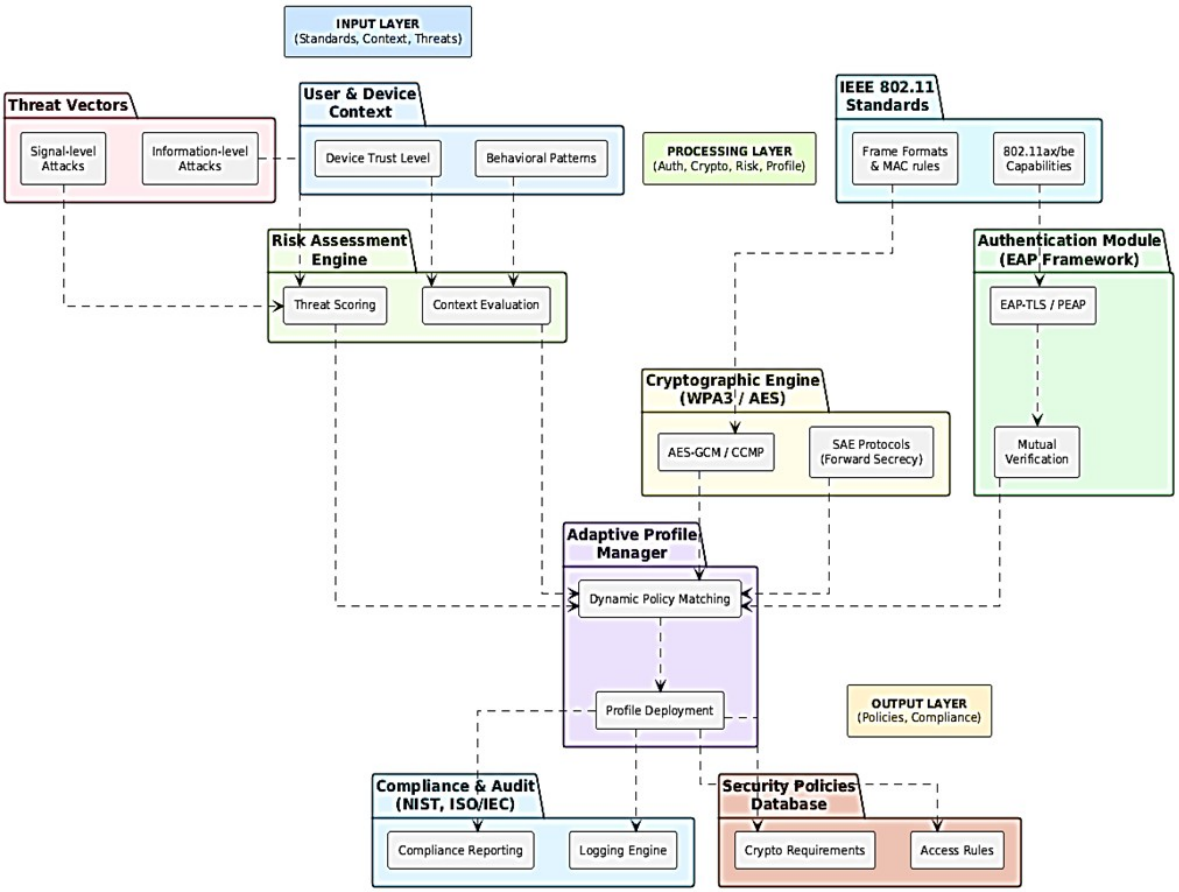

Figure 1: Spatial architectural model for the formation of adaptive protection of wireless networks

The study proposes a comprehensive methodology for assembling an adaptive family of security profiles intended to safeguard wireless networks, explicitly accounting for the taxonomy of critical information-security components that operate within an open radio environment. The methodological foundation rests on rigorous mathematical modelling of profile structures

consistent with the requirements of the IEEE 802.11ax and 802.11be standards [8], complemented by the design of a multi-layer security-assessment framework that simultaneously evaluates architectural, cryptographic, contextual, and behavioural parameters.

The construction of an adaptive security profile is performed with careful consideration of network architecture, connection dynamics, traffic composition, and specific threat vectors. The peculiarities of an open radio environment demand rigorous oversight of authentication, encryption, access governance, and strict adherence to security policies. Essential profile components include: zone-isolation mechanisms (VLANs, DMZs); state-of-the-art cryptographic protocols (AES-GCM, WPA3, SAE) [9]; authentication frameworks (EAP, TLS, RADIUS); and controls that limit the dissemination of sensitive information in accordance with its classification and the corresponding trust level. The methodology explicitly incorporates the provisions of national and international standards (ISO/IEC, NIST, ETSI) [3, 10] that regulate cryptographic protection measures and personal-data processing. Requirements are likewise defined for the physical infrastructure—covering access points, controllers, client devices, intrusion-detection sensors, and event-monitoring tools. All components must be integrated into a continuous-monitoring system underpinned by a clearly delineated distribution of responsibilities.

Given the constant mobility of users and the prevalence of hybrid-access scenarios, network nodes are treated as constituents of a remote infrastructure that remains susceptible to a spectrum of attacks, including traffic interception, man-in-the-middle intrusions, authentication spoofing, and forcible de-authentication. Accordingly, adaptive security profiles must enable the dynamic, real-time adjustment of policies in direct response to the prevailing threat context. The proposed model establishes a holistic security architecture that continuously aligns with risk fluctuations, automates the selection of counter-measures, guarantees conformity with international standards (ISO/IEC 27033, ISO/IEC 15408, NIST SP 800-53 [3, 10]), and ultimately augments the cyber-resilience of wireless infrastructure amid ongoing digital transformation.

The analytical model for constructing an adaptive family of security profiles under dynamic cyber-threat conditions relies on a graph-analytic framework that formalises the structure and interrelationships among profiles of distinct tiers. A multi-level hierarchy is prescribed, wherein each profile functions as a discrete structural entity governed by harmonised requirements for access control, cryptographic provisions, and compliance monitoring. This arrangement enables adaptive governance of protection levels in accordance with prevailing threats, user roles, network topology, and resource categories.

The hierarchical profile system is predicated on the principle of inheritance, wherein each successive tier extends the functionality of its predecessor. The foundational—or base—profile is devised with an enterprise-wide perspective, encompassing access points, routers, gateways, and the associated authentication and monitoring subsystems. Its functional requirements span authentication (EAP, TLS, the public-key infrastructure, and multifactor authentication) [5, 8]; encryption (AES, SAE, and Protected Management Frames); dynamic access control; and strict data-isolation measures. The overall framework adheres to the regulatory directives of ISO/IEC 15408, ISO/IEC 27033, and NIST SP 800-53 [10]. Structurally, the profiles form an explicit inheritance tree in which each tier maps to either a distinct threat class or a specific operational role. For instance, guest connections are restricted to baseline privileges, whereas mission-critical nodes are assigned profiles that incorporate fortified cryptographic safeguards, compulsory multifactor authentication, channel isolation, and enhanced monitoring. In aggregate, the model delivers a fully context-aware security posture, inherent scalability, seamless SIEM integration, and robust certification alignment—factors that collectively elevate the cyber-resilience of the wireless infrastructure.

To ensure robust protection of wireless networks under conditions of dynamic cyber threats, it is essential to create flexible, adaptive security profiles grounded in a comprehensive analysis of network characteristics, device-trust levels, and the prevailing threat landscape. To illustrate the overarching architecture for constructing such an adaptive security profile, a corresponding structural-and-functional model has been devised. The accompanying diagram (Figure 2) depicts

the architecture for forming an adaptive security profile for wireless networks confronted with dynamic cyber threats. The construction proceeds in sequential stages: first, the network topology and device-trust levels are examined; next, threats are assessed at both the physical and information layers, followed by risk modelling. Using these data, functional security requirement — encompassing authentication, encryption, and access control—are derived. Subsequent steps involve aggregating these requirements into a foundational functional package, establishing a hierarchy of profiles by access tier (guest, standard, critical), and enabling real-time policy adaptation. The final output is a formalised security profile that responds dynamically to shifts in the threat environment while maintaining strict conformity with contemporary information-security standards.

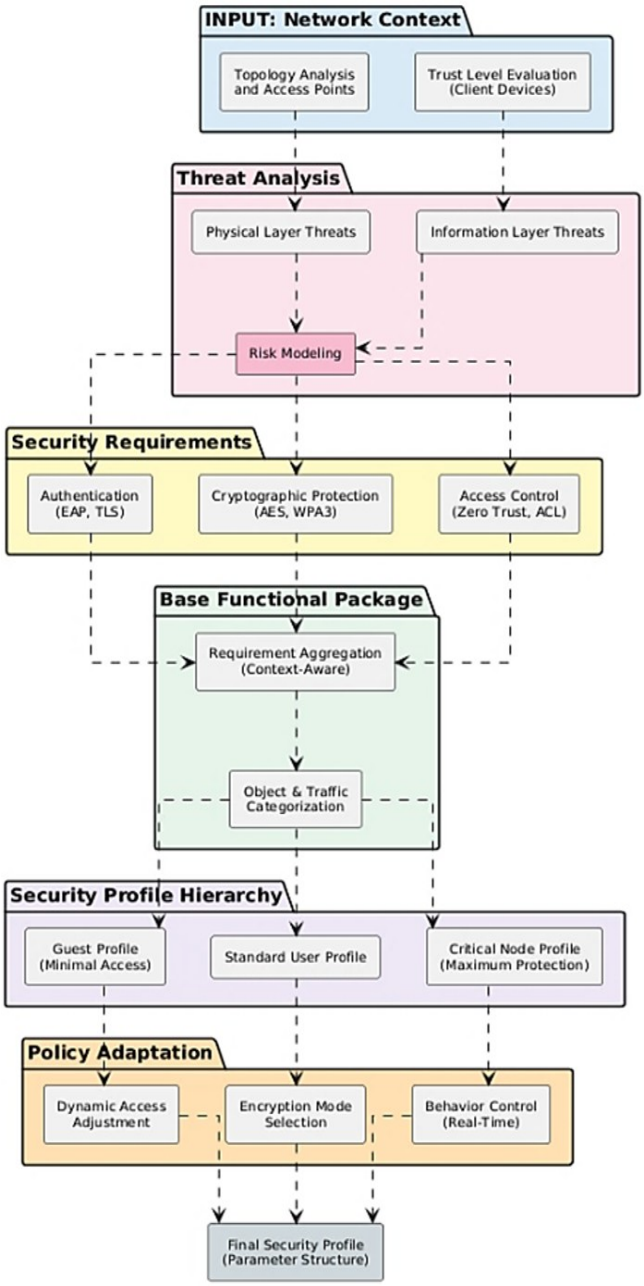

Figure 2: Scheme of forming an adaptive security profile for wireless networks

The generalised model that defines the adaptive family of security profiles [2, 11] is anchored in a canonical—or "typical"—profile and employs formalised methodologies grounded in set theory, graph-analytic constructs, and risk-oriented modelling. It explicitly captures the dependencies

among security tiers, functional requirements, and interaction context, thereby guaranteeing seamless adaptability to evolving cyber-threat conditions. The design adheres to a principle of hierarchical inheritance: every successive profile augments its predecessor in both functional breadth and protective depth. At the foundational tier, only minimal policies are enforced—such as guest access safeguarded by baseline encryption [5, 8, 12]—whereas higher tiers introduce advanced authentication schemes, behavioural-anomaly monitoring, adaptive encryption mechanisms, and robust network segmentation.

The proposed model facilitates the creation of adaptive security profiles that are calibrated to the network's prevailing risk posture, device typology, client-trust level, data-sensitivity category, and applicable regulatory obligations. It thus furnishes a structured framework for the automated generation, continual updating, and systematic auditing of profiles within wireless environments—an essential capability given the dynamic, targeted cyber-attacks that typify contemporary wireless infrastructures [12]. Figure 3 illustrates the spatial architecture underlying the structural model of an adaptive family of security profiles. Leveraging device type, trust level, data sensitivity, and the outputs of threat and behavioural analyses, the methodology derives functional security requirements encompassing authentication, encryption, and access-control mechanisms [13]. These requirements, in turn, inform the construction of a hierarchical set of profiles—categorised as basic, intermediate, and high-security tiers. The final phase entails generating an adaptive profile that integrates contextual factors and aligns with international standards, thereby delivering dynamic, standards-compliant protection for wireless infrastructures.

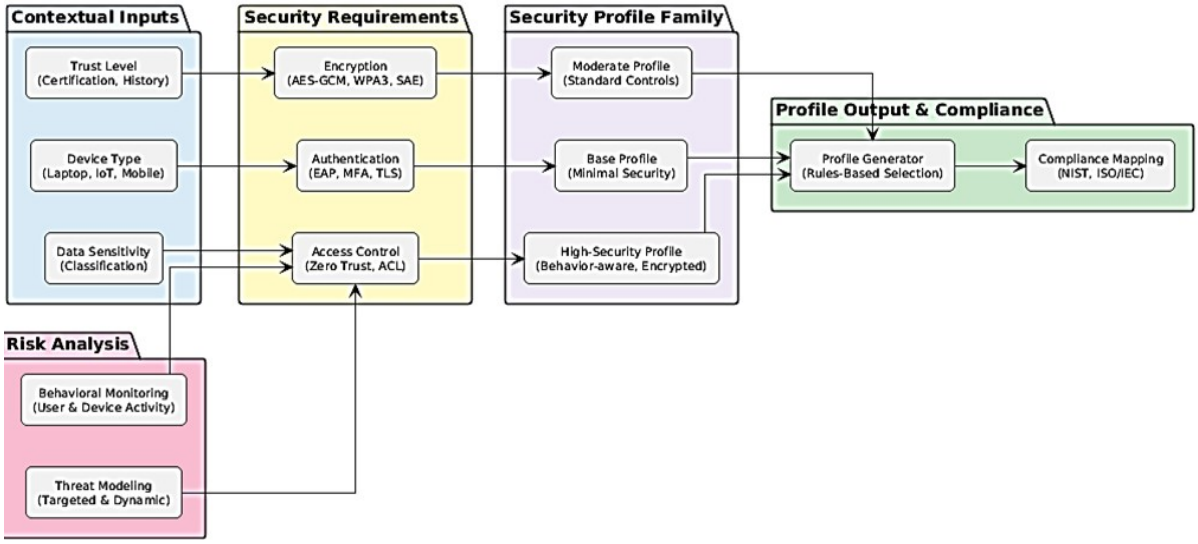

Figure 3: Structure model of an adaptive family of security profiles for wireless networks

To systematise and facilitate comprehension of the proposed mathematical model for an adaptive security profile, all formalised dependencies (Formulae 1–30) are grouped into four functional layers, each aligned with its role within the overall protection structure. Layer 1 (Basic) embraces the fundamental components that establish the system's initial security-and-trust framework: W_0(baseline functional package), PZ (adaptive security profile), Trust (device-trust model). Layer 2 (Risk Adaptation) incorporates dynamic mechanisms that react to changes in threat level and interaction context—captured by Formula $R(t)$, $Impact(t)$, ΔPZ enabling the model to adjust security policies in real time [3, 14]. Layer 3 (Performance Metrics) contains the formulas used to assess the effectiveness of implemented security profiles, including integral criteria, adaptation indices, and standards-compliance indicators E_{int}, A_{index}, $Conf_{\text{ISO}}$, $U(PZ)$. Layer 4 (Specialised Models) reflects the model's extended capabilities: responding to zero-day attacks, supporting Markov transitions between profiles, and operating under uncertainty through fuzzy-logic constructs (Z_{day}, Markov, Fuzzy) [13].

In the proposed adaptive-protection model for wireless networks, the cluster of output states is treated as a graph vertex corresponding to the baseline functional package of the security profile. This package encompasses a set of fundamental security-functional requirements that specifies the minimally sufficient suite of counter-measures necessary to safeguard the information environment. Formalisation of the baseline functional package:

$$W_0=\left\{(u_i,c_j)\vee(u_i\in U_0,c_j\in C_0,c_j\vDash u_i\right\}, \quad (1)$$

where U_0 denotes the set of baseline threats (e.g., interception, spoofing, de-authentication), C_0 represents the set of baseline counter-measures (e.g., AES-GCM, WPA3, PMF) [5], and the symbol $\vDash$ signifies logical correspondence or effective mitigation—that is, counter-measure c_j removes or markedly diminishes the risk of threat u_i. Formalising the baseline functional package of the security profile in this way makes it possible to specify the minimally required mapping between canonical threats and the counter-measures that furnish the foundational level of protection for a wireless network. The relation $c_j\vDash u_i$ in Formula (1) indicates that a particular security mechanism effectively neutralises a specific threat. This structured approach establishes a stable basis for the subsequent construction of adaptive profiles, wherein W_0 remains an invariant baseline while additional requirements are incrementally layered according to the evolving threat and risk context.

Adaptive security profile for a specific class:

$$PZ_i=W_0\cup W_d=\left\{(u_k,c_l)\vee(u_k\in U,c_l\in C,p(u_k,c_l)\geq\delta\right\}, \quad (2)$$

where $W_d=\{(u,c)\}$denotes the set of additional security-functional requirements generated in response to the external operating environment; $p(u_k,c_l)$—is the concordance function that maps a counter-measure to a threat (i.e., its effectiveness coefficient) and δ represents the concordance threshold—the minimally acceptable protection level. An adaptive security profile for a given class is thus formalised as the union of baseline and additional security-functional requirements, each selected to match the prevailing threat landscape. Equation (2) describes the set of "threat–counter-measure" pairs for which the concordance function $p(u_k,c_l)$ exceeds the threshold δ, thereby defining the minimally admissible level of defensive efficacy. Consequently, the profile adapts to its environment by incorporating only those mechanisms that provide a sufficient degree of resistance to current threats [15, 16]. This approach supports the flexible tuning of security policies in accordance with the contextual factors and risk dynamics inherent in network interactions.

Graph-structural model of the profile:

$$M=\left\{G_x=\left(S_x,E_x,w_x\right)\vee x\in\{A,C,I.D\}\right\}, \quad (3)$$

where S_x denotes the set of graph vertices (security agents grouped by category), E_x the set of edges (interaction channels or dependencies among agents), and $w_x: E_x\rightarrow[0,1]$ the weight function that quantifies the trust level or criticality of each connection. The graph-structural model of the security profile formalises the web of relationships linking the system's security agents. According to Formula (3), the model M is expressed as a collection of graphs G_x, with each graph corresponding to a distinct security-service category: authentication (*A*), confidentiality (*C*), integrity (*I*) or access control (*D*). Vertices S_x represent individual security agents, whereas edges E_x depict the logical or physical channels through which those agents interact. The weighting function w_x enables assessment of the trustworthiness or criticality associated with every connection, thereby supporting analysis of the profile's resilience to threats and identification of high-priority zones for security reinforcement [2, 14, 17, 18]. This methodology structures the protection system and facilitates its adaptive reconfiguration in response to the evolving operational conditions of the wireless network.

Functional target model for profile evaluation:

$$score(PZ) = \sum_{x \in \{A,C,I.D\}} \int_{t_0}^{t_1} (\alpha_x \cdot \varphi_x(S_x(t), R(t)) - \beta_x \cdot C_x(t))\, dt, \tag{4}$$

where $\varphi_x(S_x(t), R(t))$is the response function of security service x to the risk profile $R(t)$, $C_x(t)$ denotes the dynamic cost of maintaining that service at time t and α_x, β_x are weighting coefficients that express the relative importance of the service's effectiveness and cost. The functional target model for security-profile evaluation quantitatively determines the effectiveness of adaptive protection over a given time interval. Formula (4) incorporates the integral performance assessment of each security service—authentication, confidentiality, integrity, and access control—during the period from t_0 to t_1. The function $\varphi_x(S_x(t), R(t))$ characterises how service x reacts to the risk profile $R(t)$, whereas $C_x(t)$ captures the variable expenditures required to sustain that service. The coefficients α_x, β_x enable a weighted consideration of both efficacy and cost for each category [3, 15, 19]. This approach allows practitioners to dynamically evaluate the suitability of a selected protection profile in the face of a changing threat landscape.

Dynamic client-trust model:

$$Trust(a_j, t) = \frac{1}{Z_j} \sum_{i=1}^{N} \theta_{ij} \cdot e^{-\lambda \cdot |b_i(t) - \underline{b}_i|}, \tag{5}$$

where $b_i(t)$ denotes the behavioural profile of a device / user at time t, $\underline{b}_j$ represents the reference (benchmark) behavioural model; θ_{ij} are the weighting coefficients that quantify the influence of individual behavioural factors on the overall trust level and λ is the anomaly-sensitivity coefficient. The dynamic client-trust model provides a formal mechanism for evaluating, in real time, the reliability of a device or user on the basis of its behavioural characteristics. The quantity $Trust(a_j, t)$ specifies the trust level assigned to agent a_j at time t i and is computed as a weighted mean deviation of its current behaviour $b_i(t)$ from the reference model $\underline{b}_j$. The coefficient θ_{ij} captures the contribution of each behavioural indicator to the aggregate evaluation, while the exponential function governed by λ models sensitivity to deviations by reducing the trust value in the presence of significant anomalies. The normalisation factor Z_j rescales the resulting metric to the interval 0 to 1 [2, 14]. This model is critically important for adaptive security systems, as it enables the dynamic adjustment of access-control policies in response to shifts in client behaviour within a wireless-network environment.

The spatial model of the adaptive security profile, PZ_{3D} is conceived as a three-tier structure that formalises the dynamic interaction among the contextual, computational, and control components of the security system. The model is defined as a tuple comprising three layers:

$$PZ_{3D} = (L_{\text{Context}}, L_{\text{Processing}}, L_{\text{Control}}), \tag{6}$$

where each tier constitutes a set of operators acting upon the profile:

$$L_{Context} = \{f_k : IoT, Trust, Risk\}, \tag{7}$$

$$L_{Processing} = \{g_k : EAP, AES, SIEM\}, \tag{8}$$

$$L_{Control} = \{h_k : ACL, PolicyUpdate, ComplianceCheck\}, \tag{9}$$

The Context layer (L_{Context}) comprises the set of operators f_k, that ingest external-context sources—such as IoT-device states, client-trust levels, and risk assessments. Serving as the input tier, this layer generates the initial evaluation of the security profile in accordance with the

surrounding environment. The Processing layer ($L_{\text{Processing}}$) contains the operators g_k that execute authentication mechanisms (EAP), cryptographic safeguards (AES), and event-telemetry collection for SIEM platforms [3]. It is responsible for performing the protective functions dictated by the predefined policies. The Control layer (L_{Control}) is represented by the operator set $h_k$which enforces access control (ACL), updates policies (PolicyUpdate) and verifies compliance with security requirements (ComplianceCheck). This tier undertakes decision-making and dynamically tunes the profile in response to evolving conditions. Consequently, the PZ_{3D} model embodies the principle of a modular hierarchy, wherein each layer fulfils a distinct role in the formation and adaptation of the security profile, thereby guaranteeing integrity, scalability, and sensitivity to context.

Any modification to the parameters within the set of functional requirements triggers an update of the security profile, whereas its foundation—the baseline functional package—remains immutable. This design adheres to the principle of modularity, whereby core mechanisms are fixed and only the supplementary components evolve in accordance with the network's current state. The protective profile is therefore represented as the union of security-requirement sets that encompass both baseline and dynamic elements across four key functions—authentication (A), confidentiality (C), integrity (I), and access control (D) is each modelled as a corresponding subgraph of agents [12, 15]. Baseline agents G_x^{base} provide continuous support for the minimal protection level, while dynamic agents G_x^{dyn} are activated whenever the threat level rises or the context shifts. Formally, this relationship can be expressed as:

$$PZ = \sum_{x \in \{A,C,I,D\}} (G_x^{\text{base}} + G_x^{\text{dyn}}), \tag{10}$$

where G_x^{base} denotes the baseline agents of service x, while G_x^{base} represents the dynamic (adaptive) agents that are activated when the threat level rises. This approach preserves the stability of the protective environment through the immutable core components and, at the same time, provides flexibility and adaptability by dynamically expanding the profile in response to current threats [14]. Such a design maintains an essential balance among effectiveness, performance, and security—an equilibrium that is critically important amid dynamic cyber-threat conditions.

By integrating temporal variations in protection parameters, the adaptive security-profile model can be expressed as a time-dependent function $PZ(t)$ that reflects the dynamic activity of each security service and its current significance [2, 3, 14]. The corresponding formalisation is as follows:

$$PZ(t) = \sum_x \int_O^T \omega_x(t) \cdot S_x(t)\, dt, \tag{11}$$

where $S_x(t)$ represents the operational intensity of security service x at time t, $\omega_x(t)$ is the weighting function that captures that service's relative significance; and T denotes the integration horizon (i.e., the observation period). This time-dependent formulation permits a quantitative assessment of both the effectiveness and the contextual relevance of the protection profile under dynamic conditions [14]. By integrating over time, the system can track fluctuations in service loading and adjust security policies in accordance with prevailing threat levels, thereby upholding the necessary flexibility and sensitivity to changes within the network environment.

Given that the baseline set of security-functional requirements W_0 and the additional set W_d are generated independently, they share no intersection. Consequently, no element of one set is duplicated in the other, and the total number of all pertinent security-profile requirements can be expressed as the simple sum of their cardinalities [12]:

$$|W_{\text{total}}| = |W_0| + |W_d| = n + m, \tag{12}$$

where $|W_0| = n$ denotes the number of baseline security-functional requirements; $|W_d| = m$ represents the number of additional requirements generated in response to external influences or shifts in the threat landscape; and $|W_{\text{total}}|$ is the aggregate set of requirements that define the parameters of the adaptive security profile. This formalism permits an exact appraisal of the total security measures that must be implemented within the adaptive profile and provides for the flexible scaling of protection policies commensurate with any increase in the complexity or density of attacks.

Each adaptive security profile can be formalised as a set of functional requirements that are mapped onto the corresponding security services [2, 16, 17]. This approach permits a granular evaluation of the profile in four domains: authentication (*A*), confidentiality (*C*), integrity (*I*), and access control (*D*). Formally, the representation is:

$$PZ = \bigcup_{x \in \{A,C,I,D\}} \left(\bigcup_{g \in G_x} FT\,R_g \right), \tag{13}$$

where FTR_g designates the set of Functional Technical Requirements associated with agent g and G_x represents the set of security agents assigned to functional service x. This projection renders the adaptive profile in a structured form that explicitly reflects the roles and functional purposes of every component within the protection system. Such formalisation significantly enhances the transparency of security-management processes and facilitates seamless integration with auditing, certification, and regulatory-compliance systems.

To evaluate the protection level of a wireless network and to analyse the subsequent effectiveness of its security profile, a multilevel system of criteria has been proposed that encompasses the principal facets of information security. One of the key layers focuses on cryptographic criteria, which characterise the strength and resilience of the employed encryption algorithms [12, 16, 20]. These criteria are formalised as an integral metric:

$$K_{\text{sec}} = \alpha_1 \cdot l_k + \alpha_2 \cdot R_k + \alpha_3 \cdot f_{\text{IV}}, \tag{14}$$

where l_k denotes the key length (e.g., 128, 192, or 256 bits); R_k specifies the key-rotation algorithm type (the presence of periodic renewal markedly enhances protection); f_{IV} expresses the effectiveness of initialization-vector utilisation (for example, preventing IV reuse in AES-GCM) [20]; and $\alpha_1, \alpha_2, \alpha_3$ are weighting coefficients that capture the relative significance of each parameter in the composite security score. The resulting formula provides a rigorous, quantitative means of evaluating the cryptographic resilience of a given security profile, facilitates comparative analysis among alternative configurations, and supports evidence-based algorithm selection in light of prevailing threat conditions [14, 21, 22]. Moreover, it serves as a foundational element within the integrated model for assessing the security of wireless networks.

The authentication criteria in the adaptive security-profile model play a pivotal role in establishing trust in connected devices and users [23]. To facilitate a quantitative assessment of authenticity, an integral metric has been devised:

$$A_{\text{score}} = \delta_1 \cdot M_{\text{EAP}} + \delta_2 \cdot Cert_{\text{use}} + \delta_3 \cdot MFA, \tag{15}$$

where M_{EAP} denotes the degree of support for contemporary EAP-based authentication methods (e.g., EAP-TLS, PEAP, EAP-TTLS) [11]; $Cert_{\text{use}}$ represents the presence and implementation quality of public-key digital certificates (PKI); *MFA* indicates the availability of multi-factor authentication (for instance, password plus hardware token or biometrics); and $\delta_1, \delta_2, \delta_3$ are the weighting coefficients that express the relative importance of each component in the consolidated assessment [15, 20]. This criterion makes it possible to align the deployed authentication mechanisms with the requirements of current standards—particularly ISO/IEC 27001 and NIST SP 800-63—and to compare the effectiveness of different security implementations

when constructing an adaptive profile [24, 25]. The resulting value A_{score} indicates how closely the present authentication implementation satisfies the target trust level and may be used to trigger dynamic updates of access-control policies.

Assessing device trust is a critical element in forming an adaptive security profile, because it considers the behavioural characteristics of the node and the current risk level associated with its activity [26]. This is formalised by the following integral model:

$$T(u)=\int_{O}^{T} \mu_{\text{beh}}(u,t)\cdot\theta_{\text{risk}}(t)\,dt, \tag{16}$$

where $T(u)$ denotes the integral trust score for device uuu over the interval [0,T], $\mu_{\text{beh}}(u,t)$ is the behavioural function that gauges the conformity of the device's actions to its reference profile at moment t, $\theta_{\text{risk}}(t)$ is the time-varying risk coefficient that reflects the prevailing threat conditions in the network environment [4, 27]. This model enables the system to determine—on the basis of accumulated behavioural statistics and the current threat landscape—whether the access rights of a given device should be maintained, escalated, or revoked [15, 17]. It is an indispensable element of a Zero-Trust architecture, wherein trust is continuously verified rather than presumed.

The system-level risk quantifies the aggregate danger facing the wireless network at a specific instant, accounting for both the probability of individual threats materialising and the potential impact of each [10, 12, 14, 16, 28, 29]. Formally, the risk level is expressed as a weighted sum:

$$R(t)=\sum_{i=1}^{n} p_i(t)\cdot S_i, \tag{17}$$

where $R(t)$ represents the overall system-risk level at time t, $p_i(t)$ is the probability of occurrence of threat i, S_i denotes the magnitude of damage or impact that the system would incur should threat $i$materialise and n is the total number of identified threats. This model makes it possible to assess risk dynamics in real time and serves as a basis for adapting security profiles to the prevailing threat climate [12]. The computed value of $R(t)$ can directly trigger changes in access-control policies, the activation of additional counter-measures, or adjustments to device-trust levels [14]. It is likewise integrated into the global function for reactive profile updating, which is a key element in the construction of context-aware security systems.

The profile-adaptation index reflects the sensitivity of the security profile to variations in the system's risk level, indicating how rapidly and flexibly protection parameters are modified in response to changes in the threat environment. Formally, it is defined as:

$$A_{\text{index}}=\frac{\partial PZ(t)}{\partial R(t)}=\frac{\partial PZ}{\partial R}, \tag{18}$$

where A_{index} denotes the profile-adaptation index; $PZ(t)$ is the adaptive security profile at moment t, $R(t)$ represents the risk level at the same moment; and $\frac{\partial PZ}{\partial R}$ is the derivative of the security profile with respect to the risk level, capturing the system's instantaneous response to changing threats. The index is a critical indicator of the effectiveness of the adaptive-security management system because it quantifies the capability of the system to reconfigure itself promptly—for example, to tighten authentication policies, modify cryptographic parameters, or activate additional counter-measures—when risk increases [14, 22]. A high A_{index} value signifies a highly flexible system, an attribute that is vitally important for wireless networks operating under dynamic cyber-threat conditions.

The integral effectiveness of the profile is a generalised metric that expresses the extent to which the functional capabilities of the adaptive security profile are realised over the time interval

[0, T] relative to the maximum attainable level of effectiveness. Formally, this metric is defined by the following equation [14, 26]:

$$E_{\text{int}} = \frac{\int_{O}^{T} S_{\text{real}}(t)\,dt}{\int_{O}^{T} S_{\max}(t)\,dt}, \tag{19}$$

The formula enables a quantitative appraisal of how effectively the security profile performs its functions throughout the entire operational period. E_{int} values approaching 1 indicate a high degree of conformity between the implemented measures and the prescribed policies and requirements. Conversely, values that fall markedly below 1 signal that the desired security level has not been achieved and that the profile—or the mechanisms through which it is enforced—must be re-evaluated [14].

The standards-compliance assessment is a pivotal indicator in the certification and audit of security solutions, particularly in the context of adaptive protection profiles for wireless networks. This metric determines the extent to which the implemented security profile fulfils the requirements of international standards such as ISO/IEC 27033 or NIST SP 800-53 [12, 15]:

$$Conf_{\text{ISO}} = \frac{\#(PZ \cap S)}{\#S}, \tag{20}$$

where S is the set of security requirements specified by the relevant standard (e.g., ISO/IEC 27033, NIST SP 800-53); PZ is the set of functional security requirements implemented in the profile; $\#(PZ \cap S)$denotes the number of requirements that are both implemented in the profile and mandated by the standard; and $\#S$ is the total number of requirements contained in that standard. The resulting metric, which ranges from 0 to 1, quantifies the degree to which the security system conforms to regulatory and technical specifications. A high $Conf_{ISO}$value signifies that the system is prepared for formal certification and that its security policies are transparent.

The reactive-profile-update function is a critical mechanism that enables the system to adapt to changes in the threat landscape and in user behaviour in real time [16]:

$$\Delta PZ = \Psi\left(\frac{\partial R(t)}{\partial t}, \frac{\partial T(u)}{\partial t}\right), \tag{21}$$

where Ψ denotes the decision function that governs policy updates; $\frac{\partial R(t)}{\partial t}$ is the rate of change of the system-level risk over time; and $\frac{\partial T(u)}{\partial t}$ is the rate of change of trust assigned to a user or device. This function enables the system to modify the security-profile configuration automatically in line with risk dynamics and behavioural anomalies—an especially critical capability for safeguarding wireless networks amid highly dynamic cyber-threat conditions [21, 22]. Reactive updates ensure that the protection level remains aligned with the current context and help minimise the probability of a successful attack [14, 23, 18].

The composite-attack resilience assessment formalises the adaptive-protection system's capacity to withstand simultaneous, interacting, or overlapping threat vectors—for example, a combination of a man-in-the-middle attack with forced de-authentication or radio-frequency interference [16, 27, 31].

$$Resilience_{\text{mix}} = \left(\frac{S_{ij}}{p_{ij}}\right), \tag{22}$$

where S_{ij} denotes the counter-measure strength and p_{ij} represents the combined probability of the interacting threats i and j. This indicator makes it possible to evaluate the worst-case scenario under composite attacks and to determine whether the system can maintain a secure operational mode when exposed to highly sophisticated threat combinations. It is employed to identify critical threat pairings that require heightened attention when forming an adaptive profile [14].

Formalising the profile-to-enterprise-policy alignment enables a quantitative appraisal of how well the functional security requirements coincide with the organisation's incumbent information-protection policy [9, 25]. Such an assessment is essential for confirming that the derived adaptive profile satisfies the enterprise's strategic and regulatory mandates. The corresponding formula is expressed as:

$$X_{conf} = \frac{\sum_{i=1}^{k} \delta_i \cdot \text{match}(FTR_i, Policy_i)}{k}, \tag{23}$$

where S_{ij} is the counter-measure strength, $Policy_i$ represents the corresponding security policy defined within the enterprise ICS, $\text{match}(FTR_i, Policy_i)$ is a Boolean or fuzzy compliance function for aligning a functional technical requirement with the policy (e.g., 1 is the full compliance, 0.5 is the partial compliance, 0 is the non-compliance), δ_i is the weighting coefficient that captures the importance of the i-the requirement and k is the total number of functional requirements evaluated [26]. This indicator serves as a metric for the conformity of the adaptive security profile with the organisation's internal regulations. It can be applied during security audits, formal certification processes, or when adjusting security policies to accommodate new technological conditions.

The global adaptive meta-function specifies the overall utility of the constructed adaptive security profile in a dynamic environment, explicitly balancing the effectiveness of each protective service against the costs of sustaining that service:

$$U(PZ) = \sum_{x \in \{A, C, I, D\}} (w_x^+ \cdot E_x - w_x^- \cdot C_x), \tag{24}$$

where $x \in \{A, C, I, D\}$ denotes the service categories—authentication (A), confidentiality (C), integrity (I), and access control (D); E_x is the effectiveness score for service x, C_x represents its operational cost; w_x^+ is the weighting coefficient that captures the importance of the service's effectiveness; and w_x^- is the weighting coefficient that reflects the significance of its cost. This utility function underpins the multi-criteria optimisation of the profile: maximising protective effectiveness while minimising expenditure makes it possible to select the most balanced adaptive-profile configuration for the prevailing conditions and requirements [13, 21].

The Markov-based transition probability to a new profile formalises the mechanism for dynamically updating the adaptive security profile on the basis of changing risk levels, trust assessments, and the cost of switching between profiles. This construct ensures flexible responsiveness of the security system within a volatile cyber environment. The corresponding expression is given by:

$$P\left(PZ_i \rightarrow PZ_j\right) = f(\Delta R, \Delta T, \cos t_{\text{switch}}), \tag{25}$$

The model rests on the principles of Markov processes, whereby the system's next state depends solely on its current state and the observed changes in its environment [14, 17, 29]. This property enables the real-time implementation of intelligent and economically justified security-profile management.

The fuzzy-logic threat-assessment model accommodates uncertainty and incomplete information about the security landscape [16, 27, 32]. It delivers a flexible evaluation of threat

levels in situations where classical techniques are insensitive to weakly formalised data—for example, in behavioural analytics or when detecting novel attack types [8, 11, 18]. The model is formalised by the following expression:

$$\mu_{\text{risk}}(t) = \min\ (\mu_{\text{input}_i}, \mu_{\text{threat}_i}), \tag{26}$$

where $\mu_{\text{risk}}(t)$ denotes the membership function indicating the degree to which conditions at moment t belong to a designated threat class; μ_{input_i} represents the membership grade of the i^{th} input parameter (e.g., traffic volume, type of user action) with respect to a fuzzy concept such as "anomalous" or "risky"; μ_{threat_i} is the membership grade of threat i within the set of known or anticipated hazards; and max and min are the standard Mamdani operators employed to construct the aggregated membership function. This approach enables the dynamic adaptation of protection policies by heightening the system's sensitivity to weak, inconspicuous, or as-yet unclassified threats.

The cumulative-threat impact model for an adaptive profile describes the aggregate effect exerted by multiple threats on the protection system over a specified time interval. Such a model is essential for evaluating the accumulated risk that influences profile adaptation under conditions of the continual presence of dynamic cyber threats. The formal expression is: ‹formula to be inserted›.

$$Impact(t) = \int_0^t \left(\sum_{i=1}^{n} p_i(s) \cdot \rho_i(s) \right) ds, \tag{27}$$

where $Impact(t)$ is a cumulative metric that assesses the total impact of threats on the security system over time$t$, $p_i(s)$ is probability of threat, $\rho_i(s)$ is its impact at a given time s. The indicator allows an adaptive system to assess when the accumulated risk exceeds thresholds and requires a change in the current security profile or an increase in the level of protection, providing proactive security management in the face of prolonged or repeated attack exposure. $Impact(t)$ determines the critical indicator of accumulated risk, which allows assessing the threat impact for the entire time period [0, t] [16, 22, 30]. This value is integrated into the DFD model (Figure 4) as a parameter that is transferred from the Risk and Trust Evaluation Engine (P2) to the Profile Generation (P3) module to decide whether to strengthen the security profile.

The Wireless Infrastructure Segment Criticality Model allows you to determine how important a particular network segment is in terms of security, taking into account the value of assets and associated risks [14]:

$$Crit_{\text{segment}_k} = \gamma_k \cdot \sum_j (Val(a_j) \cdot Risk_j), \tag{28}$$

where γ_k is weighting factor of segment importance k, $Val(a_j)$ is asset value a_j, and $Risk_j$ is the risk associated with this asset.

The profile resilience equation in the risk management system assesses the ability of the security profile to counter threats, taking into account efficiency, risks and degradation factors [14, 29]:

$$\mu_{\text{risk}} = \frac{\sum_x E_x}{\sum_x R_x + D_x}, \tag{29}$$

where E_x is the efficiency of the security service x, R_x is the risk of threats to the service x, and D_x is the degradation factor (for example, due to outdated algorithms or vulnerability exploitation).

The Zero-Day Threat Readiness Index reflects the speed of the adaptive security profile's response to the rapid increase in risk characteristic of unknown attacks [22]:

$$Z_{\text{day}} = \frac{\partial P Z(t)}{\partial t}\Big|_{R(t)\to\infty}, \tag{30}$$

This metric provides a formal gauge of the system's capacity to adjust its security profile to unforeseen threats in real time. The accompanying formulae enable a comprehensive accounting not only of structural and contextual facets of adaptive protection, but also of behavioural dynamics, risk levels, transition logic between profiles, and the influence of pertinent standards. Collectively, they constitute a robust mathematical foundation for an intelligently managed, adaptive protection system safeguarding wireless infrastructure amid an evolving and hostile cyber-threat landscape.

To capture the logic underlying adaptive-profile formation in wireless networks, a general structural-and-functional process model was constructed using the Data-Flow Diagram (DFD) methodology. The model incorporates interactions among external data sources, the system's principal processing modules, and the knowledge bases that guide security-profiling decisions in the face of dynamic cyber threats. This structured approach delineates every stage of adaptive protection—from the collection of primary data to profile deployment and the continual updating of policies in response to shifting risk conditions.

Figure 4 presents a comprehensive Data-Flow Diagram (DFD) that depicts the end-to-end process for forming adaptive security profiles to protect wireless networks under dynamic cyber-threat conditions. The diagram encompasses every functional tier of the system—from the acquisition of raw data through to profile deployment and the continual updating of trust metrics. The external entities comprise the Client Device, Network Administrator, SIEM System, and Threat-Intelligence Provider, which collectively establish the contextual boundary of incoming information streams.

The first stage (P1) conducts an environmental and behavioural analysis of devices, capturing telemetry, identification artefacts, and activity characteristics. These data are forwarded to the Risk-and-Trust Assessment module (P2), where the current risk level and device-specific trust score are computed using records housed in the Threat and Trust databases (DB_Threats and DB_Trust).

Subsequently, the Security-Profile Generation stage (P3) constructs a baseline set of requirements (W_0) and appends adaptive components (W_d) in accordance with the prevailing risk context. This procedure references the Standards Repository (DB_Standards) to guarantee compliance with ISO/IEC 27033, NIST SP 800-53, and related frameworks. Profiling modules P3–P4 also ingest the Impact(t) indicator, which aggregates cumulative risk effects and serves as a criterion for adaptively updating security policies in light of long-term threat exposure.

The Decision-Making module (P4) evaluates the generated profile against administrator-defined access policies and selects the most pertinent protection set. The chosen profile is delivered to the Implementation module (P5), which enforces encryption, authentication, access control, and traffic isolation in strict conformity with the profile parameters.

All activities are recorded in the security-event log and processed by the Audit module (P6); the resulting log data are written back to DB_Trust and DB_Profiles to refine behavioural baselines and enhance subsequent adaptive responses.

Collectively, the model realises a holistic, dynamically responsive protection cycle for wireless infrastructures, embodying Zero-Trust principles, automated profile updates, rigorous adherence to international standards, and the orchestration of a multilayered security architecture [33, 34].

The adaptive security-profile model is founded on adherence to ISO/IEC 15408 (Common Criteria for Information Technology Security Evaluation), enabling the systematic structuring of functional requirements for the protection of wireless networks [12, 15, 25]. The principal evaluation domains encompass cryptography, authentication, trust management, and data integrity.

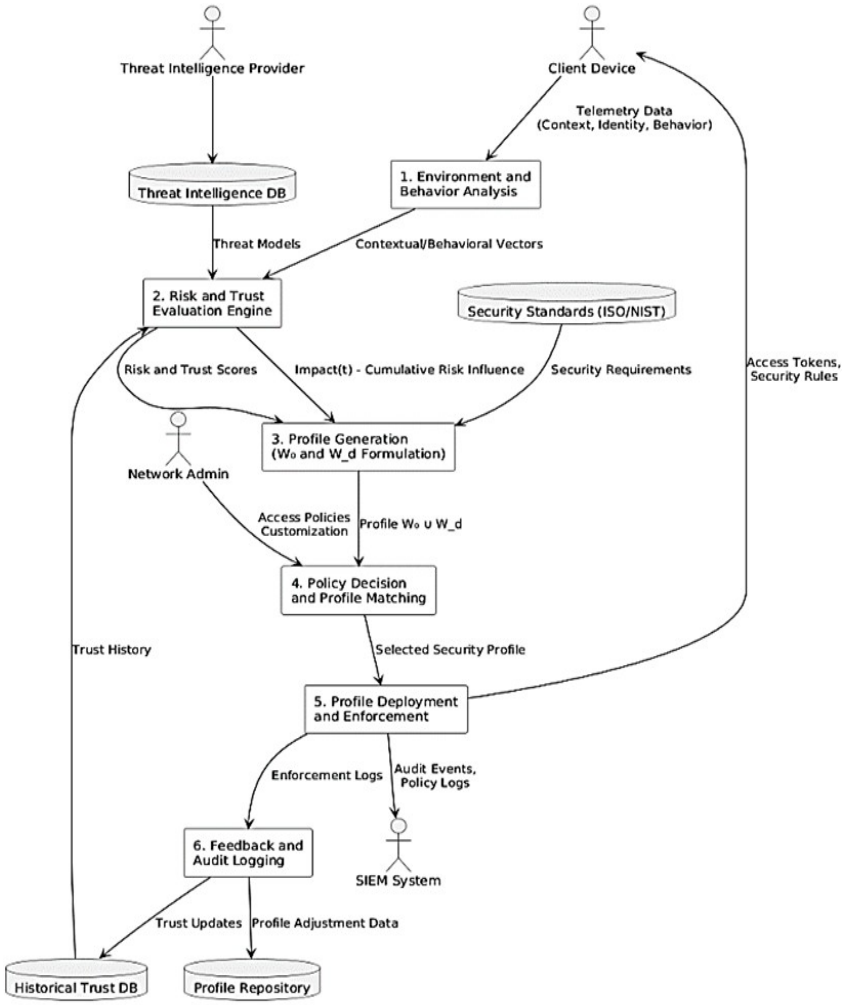

Figure 4: DFD model for creating adaptive security profiles in wireless networks

Cryptographic support corresponds to the FCS (Functional Cryptographic Support) class and covers algorithm selection (FCS_COP.1.1), key-management procedures (FCS_CKM.1.1–2.1), and integrity-verification schemes—such as GCM (Galois/Counter Mode) and CCMP (Counter Mode with CBC-MAC Protocol) [20, 25, 27]. Authentication services are assessed under the FIA (Identification and Authentication) class, with particular emphasis on the Extensible Authentication Protocol (EAP) family—EAP-TLS (TLS-based), PEAP, TTLS, and related variants. The FIA_SOS component governs secret-quality requirements, whereas FPT_SSP.2 specifies mutual-authentication obligations [14, 16, 20].

Trust level (LoT) is categorised into five gradations, ranging from LoT1—minimal safeguards such as WEP-40—to LoT5, which mandates comprehensive protection incorporating EAP-TLS, SIEM (Security Information and Event Management), IDS/IPS (Intrusion Detection/Prevention Systems), and Zero-Day-attack detection [13, 30].

Figure 5 depicts the hierarchical security-profile model, illustrating a five-tier classification by trust level. The tiers span from TL1 (baseline mechanisms, e.g., WEP-40) through TL5 (full-spectrum defence with EAP-TLS, SIEM, IDS/IPS, and Zero-Day analytics). Each successive tier inherits the attributes of its predecessor while augmenting them with enhanced control, encryption, and monitoring capabilities.

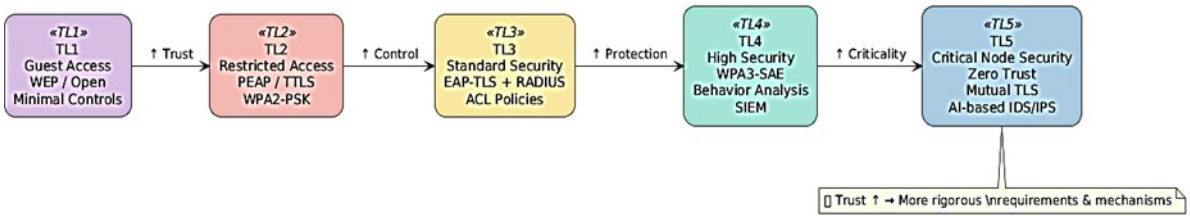

Figure 5: Hierarchy of security profiles by trust levels

The methodology mandates a comprehensive audit of the target system's configuration, encompassing a detailed appraisal of its deployed cryptographic and authentication mechanisms. When these mechanisms satisfy the criteria associated with a higher security tier, the corresponding trust level is elevated, enabling the security profile to self-adapt to the prevailing risk context while maintaining conformity with international standards such as ISO/IEC 27033 (network security), ISO/IEC 15408, and NIST SP 800-53 (information-system security controls). Moreover, the audit findings serve as inputs for constructing a granular risk map, optimising access-control policies, and prioritising protective measures in alignment with the current threat model. This process supports the dynamic updating of security profiles, thereby ensuring continuous compliance with evolving regulatory mandates and contemporary cybersecurity best practices.

Conclusions

The model and methodology developed in this work for forming adaptive security profiles for the protection of wireless networks provide a rigorous foundation for building flexible, scalable, and risk-oriented information-security systems in a dynamic cyber environment. The proposed approach constructs a formalised, multi-level hierarchy of security profiles that can be automatically updated on the basis of behavioural assessments, trust levels, network topology, traffic characteristics, and the prevailing threat landscape.

The study demonstrates that traditional static access policies are inadequate for countering contemporary, multi-vector threats—particularly in open-air wireless channels. By contrast, introducing adaptive profiles that integrate cryptographic controls, authentication mechanisms, behavioural analytics, and contextual risk assessment markedly enhances cyber-resilience.

A key emphasis is the seamless integration with international standards—IEEE 802.11ax/be, ISO/IEC 15408, ISO/IEC 27033, and NIST SP 800-53—and with Zero-Trust architecture, thereby providing a coherent framework for constructing and certifying profiles. The accompanying mathematical models formalise the logic of security-parameter adaptation, performance-evaluation mechanisms, adaptation indices, trust metrics, and transition functions between profiles, enabling precise characterisation of the security system's behaviour across both time and space. Collectively, Models (1)–(30) establish a comprehensive mathematical scaffold for building adaptive, certifiable, and scalable security profiles that operationalise Zero Trust in wireless environments.

The proposed model is deployable within corporate Wi-Fi, IoT, and cloud-service security architectures, greatly enhancing its practical value. Specifically, the algorithms can be applied to the design of secure wireless infrastructures, the creation of IoT-oriented profiles, the protection of cloud services and mobile access, and the segmentation of Wi-Fi zones. The methodology is likewise relevant for automated security-audit platforms and expert evaluations of wireless-network compliance with security standards.

In sum, the results of this study address current challenges in information security by elevating the adaptability and dynamic resilience of wireless networks and by establishing a unified methodology to safeguard the confidentiality, integrity, and availability of information resources within heterogeneous digital environments.

Declaration on Generative AI

While preparing this work, the authors used the AI programs Grammarly Pro to correct text grammar and Strike Plagiarism to search for possible plagiarism. After using this tool, the authors reviewed and edited the content as needed and took full responsibility for the publication's content.

References

[1] A. S. Khan, et al., A Survey on 6G Enabled Light Weight Authentication Protocol for UAVs, Security, Open Research Issues and Future Directions, Appl. Sci. 13 (2023). doi:10.3390/app13010277

[2] H. Abie, S. Pirbhulal, Autonomous Adaptive Security Framework for 5G-Enabled IoT, CoRR abs/2406.03186 (2024). doi:10.48550/arXiv.2406.03186

[3] S. Ahmadi, Zero Trust Architecture in Cloud Networks: Application, Challenges and Future Opportunities, J. Eng. Res. Reports 26(2) (2024) 215–228. doi:10.9734/jerr/2024/v26i21083

[4] S. A. Abdulkareem, et al., Network Intrusion Detection: An IoT and Non IoT-Related Survey, in: IEEE Access, 12, 2024, 147167–147191. doi:10.1109/ACCESS.2024.3473289

[5] S. B. Kamble, V. V. Jog, Efficient Key Management for Dynamic Wireless Sensor Network, in: 2017 2nd IEEE Int. Conf. on Recent Trends in Electronics, Information & Communication Technology (RTEICT), 2017, 583–586. doi:10.1109/RTEICT.2017.8256663

[6] D. Shevchuk et al., Designing Secured Services for Authentication, Authorization, and Accounting of Users, in: Cybersecurity Providing in Information and Telecommunication Systems (CPITS-2023-II), 2023, 3550, 217–225.

[7] V. Susukailo, I. Opirsky, O. Yaremko, Methodology of ISMS Establishment Against Modern Cybersecurity Threats, in: Lecture Notes in Electrical Engineering, Springer International Publishing, Cham, 2021, pp. 257–271. doi:10.1007/978-3-030-92435-5_15

[8] A. Bashir, A. H. Mir, An Energy Efficient and Dynamic Security Protocol for Wireless Sensor Network, in: 2013 Int. Conf. on Advanced Electronic Systems (ICAES), 2013, 257–261. doi:10.1109/ICAES.2013.6659404

[9] Y. Kostiuk, et al., Buffer and Priority Optimization for Security Assurance in Bluetooth Networks, Inf. Syst. Technol. Secur. 2(8) (2025) 5–16. doi:10.17721/ISTS.2024.8.5-16

[10] S. Rzaieva, et al., Methods of Modeling Database System Security, in: Cybersecurity Providing in Information and Telecommunication Systems, 3654, 2024, 384–390.

[11] P. Skladannyi, et al., Development of Modular Neural Networks for Detecting Different Classes of Network Attacks, Cybersecur. Educ. Sci. Technol. 3(27) (2025) 534–548. doi:10.28925/2663-4023.2025.27.772

[12] A. S. Ingle, S. U. Nimbhorkar, A Review on Secure Communication Protocol for Wireless Ad Hoc Network, in: 2015 Int. Conf. on Pervasive Computing (ICPC), 2015, 1–4. doi:10.1109/PERVASIVE.2015.7087205

[13] P. Skladannyi, et al., Development of Modular Neural Networks for Detecting Different Classes of Network Attacks, Electron. Sci. J. Cybersecur. Educ. Sci. Technol. 3(27) (2025) 534–548. doi:10.28925/2663-4023.2025.27.772

[14] C.-Y. Lee, et al., A Hardware Validation Framework for a Networked Dynamic Multi-factor Security Protocol, in: 6th Int. Conf. on Advanced Communication Technologies and Networking, 2023, 1–7, doi:10.1109/CommNet60167.2023.10365286

[15] N. F. Syed, et al., Zero Trust Architecture (ZTA): A Comprehensive Survey, in: IEEE Access, 10, 2022, 57143–57179. doi:10.1109/ACCESS.2022.3174679

[16] V. Vaidehi, R. Kayalvizhi, N. C. Sekar, Secure Data Aggregation in Wireless Sensor Networks, in: 2nd Int. Conf. on Computing for Sustainable Global Development (INDIACom), 2015, 2179–2184.

[17] Y. Kostiuk, et al., A System for Assessing the Interdependencies of Information System Agents in Information Security Risk Management using Cognitive Maps, in: Cyber Hygiene & Conflict Management in Global Information Networks 2024, 3925, 2025, 249–264.
[18] Y. Kostiuk et al., Information and Intelligent Forecasting Systems based on the Methods of Neural Network Theory, in: Proc. Smart Information Systems and Technologies (SIST), 2023, 168–173. doi:10.1109/SIST58284.2023.10223499
[19] O. Kryvoruchko, et al., Analysis of Technical Indicators of Efficiency and Quality of Intelligent Systems, J. Theor. Appl. Inf. Technol. 101(24) (2023) 127–139.
[20] H.-Y. Chien, Dynamic Public Key Certificates with Forward Secrecy, Electron. 10(16) (2009). doi:10.3390/electronics10162009
[21] M. Dammak, et al., Decentralized Lightweight Group Key Management for Dynamic Access Control in IoT Environments, in: IEEE Transactions on Network and Service Management, 17, no. 3, 2020, 1742–1757. doi:10.1109/TNSM.2020.3002957
[22] M. Z. Ali, Dynamic Allocation of Data Security in Wireless Sensor Networks, in: IEEE Conference on Dependable, Autonomic and Secure Computing (DASC), 2024, 33–39. doi:10.1109/DASC64200.2024.00011
[23] F. A. Qazi, Study of Zero Trust Architecture for Applications and Network Security, in: IEEE 19th Int. Conf. on Smart Communities: Improving Quality of Life using ICT, IoT and AI (HONET), 2022, 111–116. doi:10.1109/HONET56683.2022.10019186
[24] Y. Kostiuk, et al., Integrated Protection Strategies and Adaptive Resource Distribution for Secure Video Streaming over a Bluetooth Network, in: Cybersecurity Providing in Information and Telecommunication Systems II, 3826, 2024, 129–138.
[25] Y. Kostiuk, et al., Models and Algorithms for Analyzing Information Risks during the Security Audit of Personal Data Information System, in: Cyber Hygiene & Conflict Management in Global Information Networks 2024, 3925, 2025, 155–171.
[26] Y. Kostiuk, et al., Information Protection and Secure Data Exchange in Wireless Mobile Networks with Authentication and Key Exchange Protocols, Cybersecur. Educ. Sci. Technol. 1(25) (2024) 229–252. doi:10.28925/2663-4023.2024.25.229252
[27] A. Bahaa, et al., Monitoring Real Time Security Attacks for IoT Systems using DevSecOps: A Systematic Literature Review, Inform. 12(4) (2021) 154. doi:10.3390/info12040154
[28] C. Hamroun, et al., Intrusion Detection in 5G and Wi-Fi Networks: A Survey of Current Methods, Challenges, and Perspectives, in: IEEE Access, 13, 2025, 40950–40976. doi:10.1109/ACCESS.2025.3546338
[29] Y. Kostiuk, et al., Method for Protecting GRID Environments from Malicious Code During Computational Task Execution, Cybersecur. Educ. Sci. Technol. 3(27) (2025) 22–40. doi:10.28925/2663-4023.2025.27.710
[30] F. Guo, H. Jiao, X. Zhang, Y. Zhou and H. Feng, Information Security Network Intrusion Detection System Based on Machine Learning, in: 2024 Int. Conf.e on Data Science and Network Security, 2024, 01–04. doi:10.1109/ICDSNS62112.2024.10691041
[31] S. S. Abd El Dayem, M. R. M. Rizk, M. A.Mokhtar, Security for Wireless Sensor Network, in: 6th Int. Conf. on Information Communication and Management (ICICM), 2016, 173–177. doi:10.1109/INFOCOMAN.2016.7784237
[32] X. Wang, X. Qiu, A Novel Semi-Supervised Anomaly Detection Method for Network Intrusion Detection, in: 2022 IEEE 22nd Int. Conf. on Communication Technology (ICCT), 2022, 1276–1280. doi:10.1109/ICCT56141.2022.10073098
[33] P. Skladannyi, et al., Improving the Security Policy of the Distance Learning System based on the Zero Trust Concept, in: Cybersecurity Providing in Information and Telecommunication Systems, 3421, 2023, 97–106.
[34] R. Syrotynskyi, et al., Methodology of Network Infrastructure Analysis as Part of Migration to Zero-Trust Architecture, in: Cyber Security and Data Protection, 3800, 2024, 97–105.