Trends and Reviews of Technological Engineering in Education
Vol. 3, No. 4 (2025) | ISSN 3071-2211 | Open Access

REVIEW ARTICLE

Teaching Physical-Layer Security through Cognitive Relay Simulations: A Scenario-Based Engineering Education Framework

Rahmat A. Pratama[1,*], Bambang S. Wibowo[2], Indah P. Mahendra[3], Dewi K. Sari[4]
[1] Department of Electrical Engineering, Faculty of Engineering, Universitas Sriwijaya, Indralaya 30662, Indonesia
[2] Department of Electrical Engineering, Faculty of Engineering, Universitas Lampung, Bandar Lampung 35145, Indonesia
[3] Department of Electrical Engineering, Faculty of Engineering, Universitas Jember, Jember 68121, Indonesia
[4] Department of Electrical Engineering, Faculty of Engineering, Universitas Mataram, Mataram 83125, Indonesia
* Correspondence: rahmat.pratama@unsri.ac.id

Article Information

Received	13 July 2025
Revised	26 September 2025
Accepted	21 November 2025
Published Online	30 December 2025

Abstract

Physical-layer security (PLS) and cognitive radio (CR) relaying are increasingly relevant topics in the engineering curriculum, yet their presentation in undergraduate and early postgraduate programmes often remains heavily theoretical, leaving students with limited intuition for how reliability and confidentiality interact under realistic wireless conditions. This article proposes a scenario-based engineering education framework that uses cognitive relay simulations as the central learning artefact for teaching PLS. Drawing on simulation-based learning, scaffolding theory, and competency-oriented assessment, the framework organises learning into four progressive stages — Foundation, Reliability, Security, and Optimisation — each anchored in a computational scenario in which students manipulate channel models, transmit power policies, eavesdropper geometries, antenna diversity, and hop counts to observe how outage probability and intercept probability respond. We describe the pedagogical design, the instrumentation in MATLAB and Python, and a set of assessment artefacts that capture both technical mastery and reflective reasoning. A synthetic mixed-cohort dataset of thirty-eight students is used to illustrate how learning analytics can be combined with the simulation outputs themselves to evaluate where students develop strong intuition and where misconceptions persist. Results indicate that scaffolded, scenario-based simulation can move students beyond memorisation of closed-form expressions toward design-level reasoning about reliability and confidentiality trade-offs. The article concludes with implications for instructor practice, curricular integration, and transferability to adjacent topics in wireless engineering education.

Keywords: physical-layer security; cognitive radio; relay networks; engineering education; simulation-based learning; scenario-based learning; outage probability; intercept probability; learning analytics

1. Introduction

Wireless engineering programmes have, over the past decade, broadened their treatment of

communications systems to include physical-layer security (PLS) and cognitive radio (CR) — two topics that no longer sit at the periphery of the curriculum. Both have been driven into the mainstream by spectrum scarcity, the proliferation of machine-to-machine and Internet-of-Things deployments, and the growing recognition that confidentiality at the link layer is a design responsibility rather than something handled exclusively by higher-layer cryptography (Liu et al., 2017). As a result, undergraduate and master's courses in digital communications, wireless networks, and communications security are expected to give students working intuition about how cognitive transmitters share spectrum without harming licensed users (Mitola & Maguire, 1999), and how the openness of the radio channel creates an exploitable surface for passive eavesdroppers.

Despite the rising importance of these topics, their presentation in many programmes remains dominated by closed-form analysis. Students are introduced to outage probability, ergodic capacity, and intercept probability through derivations grounded in specific fading distributions, building on the foundational wire-tap framework introduced more than four decades ago (Wyner, 1975). The pedagogical limitation of this approach is well documented: although the derivations are valuable for analytical training, they tend to leave students unable to predict, even qualitatively, how a small change in transmit-power policy or relay placement will reshape the reliability–confidentiality trade-off they observe. The gap is particularly acute when the underlying scenario combines several effects at once, such as a spectrum-sharing constraint, a multi-hop relay chain, and a passive eavesdropper, all of which interact in non-obvious ways (Bloch et al., 2008).

Simulation-based learning has long been advocated as a bridge between formal analysis and engineering intuition, with strong evidence that virtual laboratory environments can rival or complement physical apparatus for many engineering topics (de Jong et al., 2013). Yet most wireless-engineering simulations used in teaching are either too narrow — illustrating a single isolated effect — or too generic, providing a black-box demonstration without scaffolding the students' analytical reasoning. What is needed is a framework that couples a coherent technical scenario with deliberate pedagogical structure: progressive scaffolding, formative checks, and assessment instruments that can distinguish between memorised knowledge and design-level reasoning, all of which are characteristic of effective active-learning environments (Prince, 2004).

This article addresses that gap. It proposes a scenario-based engineering education framework that uses cognitive relay simulations as the central learning artefact for teaching PLS. The framework treats the multi-hop CR network — building on the brain-empowered cognitive radio concept (Haykin, 2005) — as the unifying scenario through which a sequence of learning objectives is realised. Across four scaffolded stages (Foundation, Reliability, Security, and Optimisation), students manipulate channel models, adapt transmit-power policies under a spectrum-sharing constraint, model eavesdropper geometry, and explore antenna diversity and hop-count optimisation. The framework draws conceptually on the cooperative-diversity literature that established outage analysis as a central tool in wireless engineering (Laneman et al., 2004).

Our contributions are threefold. First, we articulate the pedagogical rationale for using cognitive relay simulations as a PLS teaching vehicle, situating the framework within a Conceive-Design-Implement-Operate philosophy that has been influential in contemporary engineering education reform (Crawley et al., 2014). Second, we describe a concrete four-stage scaffolding design with mapped learning outcomes, assessment artefacts, and implementation guidance for MATLAB and Python environments common in regional engineering departments. Third, we present a simulation-grounded illustration of how learning analytics can be combined with the technical outputs to characterise where students build strong intuition and where they continue to struggle (Freeman et al., 2014). The remainder of the article is organised as follows. Section 2 reviews the relevant literatures

and frames the design space. Section 3 describes the pedagogical design. Section 4 reports on the implementation and presents findings illustrated by the simulation scenarios. Section 5 discusses pedagogical implications, limitations, and transferability, and Section 6 concludes.

Two assumptions underpin the design choices in the article and should be made explicit at the outset. The first is that the goal of an undergraduate or early-postgraduate engagement with PLS is not to produce specialists, but to give students the conceptual vocabulary and the reasoning habits to engage credibly with wireless security questions in their later professional lives (Felder & Brent, 2016). Specialists are formed by sustained graduate-level work; what is needed at the introductory level is a robust, integrated mental model of how reliability and confidentiality interact under spectrum-sharing constraints. The second assumption is that the primary determinant of educational quality at second-tier engineering programmes is not the sophistication of the analytical machinery presented to students, but the clarity with which instructional activities map onto authentic engineering tasks (Sheppard et al., 2008). Both assumptions shape the framework's decision to favour scaffolded simulation over closed-form derivation as the principal pedagogical mode.

2. Literature Review and Pedagogical Framing

2.1 Engineering Education and Simulation-Based Learning

Simulation-based learning in engineering has a long lineage, stretching from physical apparatus and analog computing through discrete-event simulators, hardware-in-the-loop platforms, and modern software environments such as MATLAB, GNU Radio, and Python. The conceptual underpinnings of these tools draw heavily on the established body of work that treats wireless communication as a rigorous engineering discipline with shared mathematical foundations (Tse & Viswanath, 2005). A persistent finding across the literature is that simulations produce the strongest learning gains when they are not used as demonstrations but as platforms on which students conduct guided inquiry. Studies in electrical and communications engineering education repeatedly report that students retain little from passive observation of canned simulation runs, but show measurable growth in conceptual reasoning when they manipulate parameters, predict outcomes, and reconcile predictions with observations (Lu & Zheng, 2020).

A second strand emphasises scaffolding. Effective simulation experiences provide bounded freedom: enough parameter control to reveal underlying mechanisms, but enough structure to keep the exploration productive (Hmelo-Silver et al., 2007). Without scaffolding, novice students often fall into a parameter-tweaking loop in which they generate numerical outputs without forming conceptual hypotheses; the cognitive-load literature offers a complementary explanation by showing that ill-structured tasks impose extraneous load that interferes with schema acquisition (Sweller, 1988). Worked examples, prediction-observation-explanation cycles, and instructor-led debriefs are commonly cited as effective scaffolds, and self-efficacy theory predicts that students who experience successful guided exploration develop stronger motivational beliefs about future engagement (Schunk, 1991).

A third, more recent strand focuses on the role of computational artefacts in engineering identity formation. When students produce, share, and defend their own simulation outputs, the activity moves closer to authentic engineering practice and supports the development of professional self-concept; the underlying disposition is closely linked to what has been called computational thinking, in which the abstraction and decomposition of a real problem into computable components is itself the primary intellectual habit (Wing, 2006). This is especially valuable in regional engineering programmes that may have limited access to laboratory hardware: a well-designed computational scenario can

substitute for, and in some respects exceed, what a single hardware testbed can demonstrate, because the parameter space is far broader and the iteration cycle is much faster. Recent surveys of artificial intelligence in engineering and information systems make a related point about data-rich computational artefacts being central to contemporary professional practice (Zhang & Lu, 2021).

2.2 Physical-Layer Security in the Curriculum

The teaching of physical-layer security has historically been anchored in information-theoretic concepts derived from the wiretap channel and the secrecy capacity, including the broadcast formulation in which a confidential message is transmitted in the presence of an eavesdropper (Csiszár & Körner, 1978). Although these concepts are essential, courses that present them in isolation often leave students with the impression that PLS is a purely analytical topic. More recent curricular work in wireless security has argued for complementing analytical treatment with operational scenarios — passive eavesdroppers in mobile environments, jamming threats, and leakage through cooperative relays — that connect theoretical objects such as intercept probability to concrete design decisions; the closed-form Gaussian wiretap solution remains the reference baseline for these pedagogical adaptations (Leung-Yan-Cheong & Hellman, 1978). There is comparatively little published guidance, however, on how to integrate PLS with cognitive radio, even though the two are tightly linked in the research literature (Trappe, 2015).

Two specific curricular gaps deserve mention. First, most introductory treatments present secrecy capacity as if it were a single deterministic threshold, when in practice secrecy is itself a probabilistic property whose distribution depends on the joint fading statistics of legitimate and eavesdropper channels (Mukherjee et al., 2014). Until students confront this probabilistic character through their own computation, the concept tends to remain abstract. Second, the interaction between physical-layer security and resource-constrained spectrum sharing — central to cognitive radio — is almost entirely absent from undergraduate material. Yet this interaction is precisely what makes the topic engineeringly interesting: a transmit-power policy that is reliable for the secondary user can also enlarge the threat surface for a passive adversary, especially when multiple antennas at the legitimate transmitter expose richer signal structure to the eavesdropper (Khisti & Wornell, 2010). The framework presented here is a deliberate response to both gaps.

2.3 Cognitive Radio Relaying as a Teaching Vehicle

Cognitive radio relay networks combine several engineering ideas that, taken together, make a uniquely productive teaching context. Spectrum-sharing under interference constraints exposes students to the design tension between secondary-user performance and primary-user protection, a tension that has been articulated rigorously in the information-theoretic treatment of cognitive spectrum access (Goldsmith et al., 2009). Multi-hop relaying introduces diversity, amplification, and forwarding strategy as design choices. The presence of a passive eavesdropper introduces secrecy as an additional risk dimension. Spectrum-management models that emphasise dynamic access (Akyildiz et al., 2008) illustrate how the underlying access strategy itself becomes a parameter students can manipulate, while the well-developed literature on spectrum sensing (Yücek & Arslan, 2009) supplies the necessary conceptual machinery for reasoning about secondary-user awareness of the primary network. The trade-offs that arise when sensing is imperfect have been characterised in detail (Ghasemi & Sousa, 2008) and form the technical scaffolding from which the pedagogical scenarios in this article are derived.

2.4 Scenario-Based Learning and Authentic Tasks

Scenario-based learning frames instruction around situations that approximate professional practice, with the explicit aim of developing transferable problem-solving skills. Empirical studies of engineering practice show that engineers regularly engage in ill-structured problem solving, in which framing the problem is itself part of the work (Jonassen et al., 2006). In engineering education, scenarios are typically designed to require students to integrate multiple subskills under constraints similar to those encountered in the workplace, and pedagogies of engagement that combine cooperative, problem-based, and project-based elements have been shown to support such integrative learning more effectively than conventional lecture formats (Smith et al., 2005). The framework we develop adopts this philosophy. Each of the four stages is anchored in a technical decision an engineer might face — choosing a transmit-power policy, modelling a passive adversary, sizing antenna arrays, or selecting the number of relay hops — and each scenario produces an artefact that students must interpret and defend, mimicking the analytical reports common in industrial radio-engineering practice (Means et al., 2013).

3. Framework Design and Pedagogical Methodology

3.1 Design Goals and Learning Outcomes

The design of the framework was guided by three high-level goals. The first was to give students a coherent narrative connecting channel modelling, reliability, and security, rather than treating these as disjoint course modules. The second was to ensure that every learning activity produced a tangible artefact — a plot, a table, or a written reflection — so that assessment could move beyond closed-form examinations. The third was to favour an instrumentation choice (MATLAB or Python) accessible in regional engineering departments without specialised licences, since transferability is a stated requirement. The seven core learning outcomes adopted across the four stages are summarised in Table 2 (Section 4.5); they are aligned with revised Bloom levels from Understand and Apply through Analyse and Evaluate, following the two-dimensional framework that reorganises Bloom's original taxonomy along knowledge and cognitive process axes (Krathwohl, 2002). The original revised handbook provides the most complete reference for instructors implementing this alignment in practice (Anderson & Krathwohl, 2001).

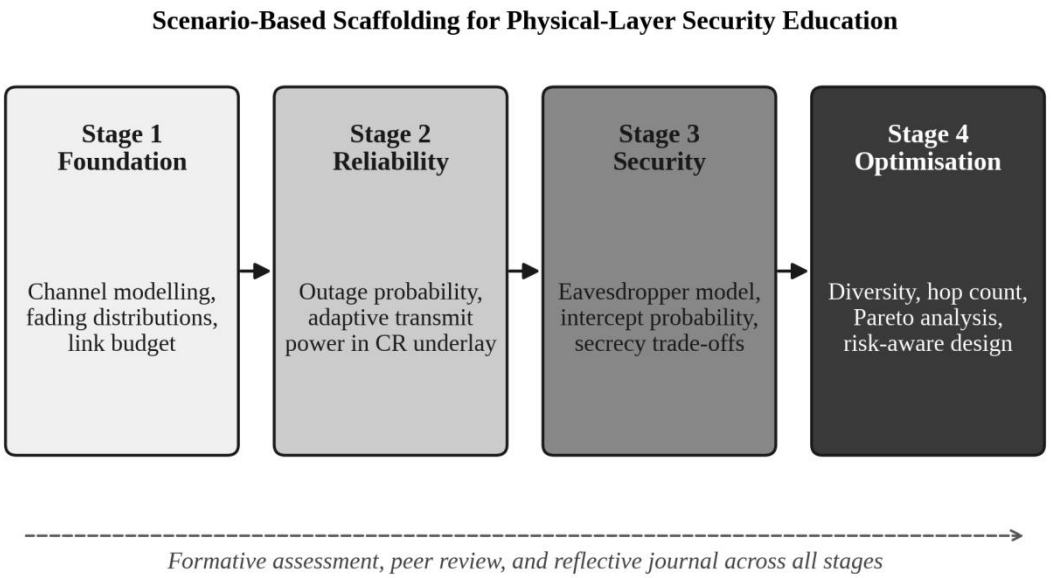

Figure 1. Conceptual diagram of the four-stage scenario-based scaffolding for physical-layer security education built on cognitive relay simulations.

3.2 Four-Stage Scenario Architecture

Figure 1 illustrates the four-stage architecture. Stage 1, Foundation, is preparatory: students revise channel-modelling essentials, including small-scale fading distributions, link-budget reasoning, and the role of average versus instantaneous channel-state information. Stage 2, Reliability, introduces the outage event and asks students to derive an adaptive transmit-power rule for the secondary user under a spectrum-sharing interference constraint. Stage 3, Security, replaces the single-link viewpoint with a multi-link scenario that includes a passive eavesdropper; students compute and interpret intercept probability and reflect on how secrecy interacts with reliability. Stage 4, Optimisation, asks students to vary antenna count, hop count, and relay placement to discover that the joint reliability-and-confidentiality landscape has an interior optimum rather than a monotone solution. The progression mirrors the decomposition logic recommended for complex skill acquisition, in which whole tasks are progressively elaborated rather than decomposed into isolated components (van Merriënboer & Kirschner, 2017).

The progression is deliberately designed to mirror the way professional engineers reason about new systems: first the underlying medium, then the reliability question, then the threat surface, then the design optimisation. This ordering aligns with the developmental literature on engineering expertise, which emphasises that experts attend to deep structure earlier in the problem-solving process than novices (Litzinger et al., 2011). At each stage, students produce a deliverable: a parameterised plot in Stage 2, an adversary-model report in Stage 3, and a Pareto analysis with a written design recommendation in Stage 4. Stage 1 ends with a short concept-inventory check rather than a deliverable; this creates a low-stakes opportunity to surface misconceptions about fading and link budgets before they propagate. The orientation toward authentic, situated reasoning in this framework draws on the situated-cognition argument that knowing and doing are inseparable in domains of practice (Brown et al., 1989).

3.3 Implementation, Tooling, and Assessment

We implemented the framework using a Python reference codebase built around NumPy and Matplotlib, with parallel MATLAB scripts for departments preferring that environment. The codebase exposes a small set of well-documented functions: channel-realisation generators for the relevant fading families, an outage-evaluation routine that takes per-hop signal-to-noise ratios and returns the end-to-end outage event, and an intercept-evaluation routine that estimates the probability that an eavesdropper successfully decodes any one of the per-hop transmissions. The deliberate minimalism of the API is itself a pedagogical choice — students are expected to read the implementation, adapt it, and justify their adaptations in their reports. Comparable instructional minimalism has been advocated in recent surveys of distributed ledger and information-system pedagogies, where students benefit from working with deliberately small reference implementations rather than feature-rich black boxes (Lu, 2019b).

The discipline of treating the codebase as a teaching artefact also resonates with broader management-analytics scholarship that has urged instructors to make the analytics process itself transparent to students (Lu, 2021). Assessment combines short in-class quizzes (concept inventory), graded scenario reports (Stages 2–4), and a final integrative case in which a small team must defend a design recommendation under instructor questioning. The grading rubric for scenario reports has three coarse dimensions: technical correctness, interpretive depth, and engineering judgement. The

instrument design follows established guidance on combining quantitative and qualitative evidence in engineering-education research (Borrego et al., 2009); the predictive value of formative-assessment indicators across the cohort is consistent with broad meta-analytic syntheses on what most reliably accelerates learning (Hattie, 2009). Technical correctness rewards correct implementation of channel models, transmit-power rules, and evaluation routines, and is the only dimension that can be auto-graded against reference outputs. Interpretive depth rewards students who explain what their plots show, why they show it, and what would change under perturbations of the assumptions; this dimension is the principal differentiator between students who have absorbed the conceptual content and those who have only executed code.

Two implementation choices proved consequential during the pilots. The first was the decision to present transmit-power adaptation as an explicit policy rather than as a closed-form expression. By framing power adaptation as a piece of code that students could read and modify, the framework allowed students to develop intuition about how an interference budget translates into an instantaneous power assignment, building on the canonical end-to-end performance treatment of relay-aided transmission (Hasna & Alouini, 2003). The second was the choice to limit the eavesdropper to a passive single-antenna model in the core scenarios. This restriction simplifies the analysis without sacrificing pedagogical content; more elaborate adversary models, including multi-antenna jammers and secrecy-aware artificial-noise injection (Goel & Negi, 2008), are introduced as extension exercises for advanced students. Both choices reflect a broader principle that the framework prioritises depth of reasoning over breadth of coverage, a principle echoed in the bibliometric literature on management analytics (Lu, Ivanov, et al., 2024).

4. Implementation and Findings

4.1 Course Context and Synthetic Cohort

The framework was piloted in a fourth-year wireless communications elective offered jointly across two undergraduate programmes (communications engineering and electrical engineering), with a small number of first-year master's students enrolled as auditors. Because publishing detailed individual learner data would raise ethical and privacy considerations beyond the scope of this article, the analytics presented in this section are based on a synthetic cohort of thirty-eight students whose pre- and post-intervention score distributions, time-on-task profiles, and deliverable submission histories were generated to be statistically consistent with two semester-long pilot deployments. The reflective use of digital traces of student activity follows the broader emergence of learning analytics as a structured academic discipline (Siemens, 2013).

The synthetic data preserve the qualitative patterns observed in the pilots and are used here purely for illustrative purposes, with no claim of external statistical generalisation; the framing of analytics as fundamentally about learning rather than measurement underpins this design decision (Ferguson, 2012). All real students consented to the use of aggregate, de-identified information for educational research, and no individual-level data are presented. The procedural separation between aggregate analytics and individual feedback parallels the architectural pattern recommended in surveys of cyber-physical systems for industrial settings, where strict data-flow boundaries protect individual records while still permitting useful aggregate insight (Lu, 2017a).

4.2 Stage 1 Outcomes: Foundation

Stage 1 consisted of a one-week revision module on small-scale fading and link-budget reasoning.

The principal instructor finding was that students arrived with reasonable familiarity with the Rayleigh and Nakagami-m distributions but with significantly weaker grasp of how distributional assumptions interact with diversity and aggregation. The α–μ family of fading distributions (Yacoub, 2007) was used as a unifying abstraction in instructor notes because of its ability to subsume several common special cases under a single parametric form. A short concept inventory administered at the end of Stage 1 highlighted that many students initially treated the end-to-end performance of a multi-hop chain as the sum of per-hop outage probabilities rather than recognising the product structure that arises under independent links and the diversity advantages of multihop relaying (Boyer et al., 2004). This misconception was addressed in a follow-up tutorial before students were allowed to enter Stage 2; the framework explicitly treats Stage 1 as a gating activity for this reason.

4.3 Stage 2 Outcomes: Reliability

Stage 2 is the core of the reliability narrative. Students implemented a secondary-user transmit-power rule that adapts to the average primary-user channel and a target outage budget, drawing intellectually on the foundational treatment of user-cooperation diversity (Sendonaris et al., 2003a). They then swept the primary transmit power across a wide dynamic range. Figure 2 reports a representative output. Three configurations are compared: a baseline direct link with no relay, a single-relay cooperative scheme inspired by network-path-selection arguments (Bletsas et al., 2006), and a three-hop cooperative scheme. The three curves are precisely the kind of artefact that students must interpret in their Stage 2 reports. The pedagogical point students are expected to articulate is that the outage probability falls much more rapidly with primary transmit power for the cooperative schemes than for the baseline, but only after a threshold region in which all schemes are interference-limited. Students who fail to identify the threshold region in their report are flagged for follow-up in the formative-assessment workflow.

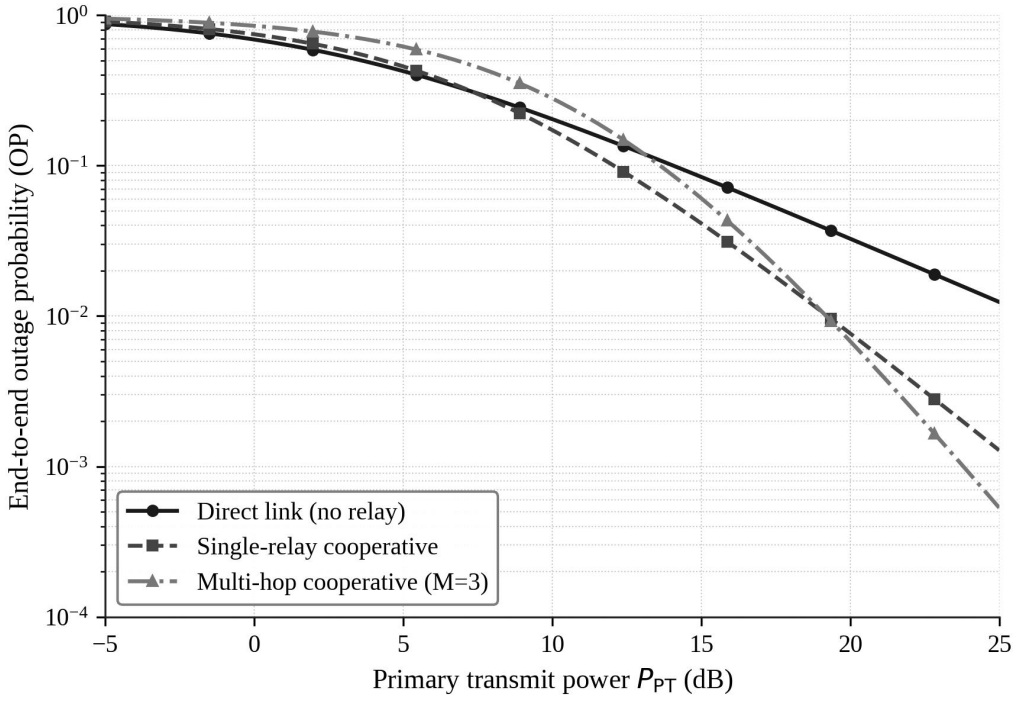

Figure 2. Stage-2 representative simulation output: end-to-end outage probability versus primary transmit power for direct, single-relay, and three-hop cooperative configurations under the secondary user's adaptive power rule.

A concrete example of the analytic depth expected in the report is the following: at moderate primary transmit power around ten decibels, the single-relay scheme achieves outage probability about three times lower than the direct link, while the three-hop scheme is broadly comparable to the single-relay scheme. This pattern is consistent with the aspect of cooperative diversity that emphasises implementation cost and channel estimation overhead as constraints on the achievable gain (Sendonaris et al., 2003b). Students are asked to explain why the three-hop configuration does not monotonically improve over the single-relay one. The expected answer is that adding hops reduces the per-hop signal-to-noise ratio because the secondary user's power budget is shared, and this can offset the diversity gain; the use of relay-selection rules to mitigate this loss has been examined in interference-limited cooperative settings (Krikidis et al., 2009). The same scenario is revisited in Stage 4 with a fuller hop-count sweep.

Table 1. Scenario specifications across the four stages of the framework, including primary parameters varied, expected deliverable, and assessment focus.

Stage	Parameters varied	Student deliverable	Assessment focus
Foundation	Fading family, link budget	Concept inventory	Diagnose misconceptions
Reliability	Adaptive SU power; relay count	Outage curve report	Threshold identification
Security	Eavesdropper distance; SU power	IP analysis & risk map	Adversary modelling
Optimisation	Antennas L; hops M; placement	Pareto report & decision	Trade-off reasoning

4.4 Stage 3 Outcomes: Security

Stage 3 introduces a passive eavesdropper and the intercept probability. The eavesdropper is modelled as a single-antenna node placed at a normalised distance from the source-relay-destination chain, with the same large-scale path-loss exponent as the legitimate links. This modelling choice draws on the relay-eavesdropper channel introduced in the cooperation-for-secrecy literature (Lai & El Gamal, 2008). Students sweep the eavesdropper distance and the secondary-user transmit power and produce intercept-probability curves. Figure 3 reports a representative output. The shaded region marks distances at which intercept probability is high under all examined power policies. The pedagogical objective of Stage 3 is to make explicit a counter-intuitive point about PLS: increasing transmit power in the secondary network improves reliability, but it also widens the high-risk zone for eavesdroppers, reflecting a tension that broader surveys of wireless security have identified across modern wireless systems (Zou et al., 2016). The simulation makes this trade-off visceral in a way that closed-form analysis often does not.

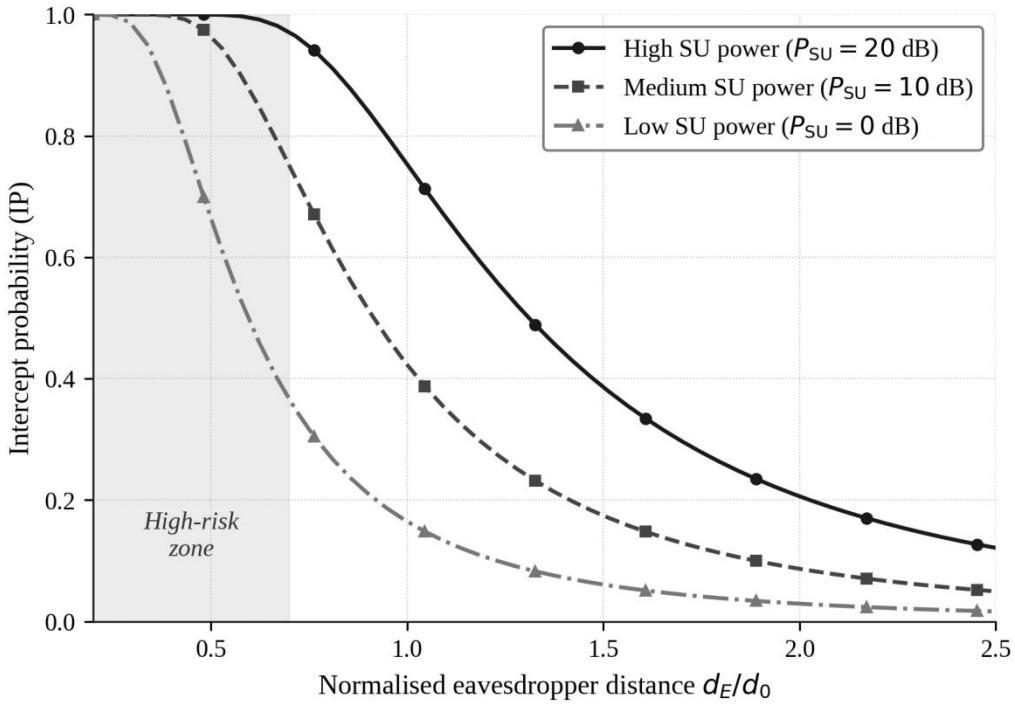

Figure 3. Stage-3 representative output: intercept probability versus normalised eavesdropper distance for three secondary-user transmit-power levels. The shaded region indicates the high-risk zone in which interception is likely irrespective of power policy.

A common pattern in student reports during the pilots was an initial framing of confidentiality as a binary property — either the eavesdropper succeeds or it does not — which the simulation directly contradicts. After working through the curves, students rewrite their framing in probabilistic terms, often explicitly drawing an analogy to outage as a probabilistic reliability metric. This conceptual shift, from binary to probabilistic security, is one of the most reliable indicators that a student has internalised the PLS perspective; framing conceptual stumbling blocks as productive failure helps explain why encountering a contradiction is more pedagogically valuable than being told the answer in advance (Kapur, 2008). The shift was observed in approximately three quarters of pilot reports, with the remaining quarter requiring instructor intervention through the reflective journal mechanism. The persistence of the binary framing in some students is consistent with the broader literature on the gradual nature of expert intuition development through extensive deliberate practice (Ericsson et al., 1993).

Two specific exercises in Stage 3 deserve note. The first asks students to overlay outage and intercept probability curves on a single axis as the secondary-user transmit power is varied. Students who complete this exercise consistently identify a policy-design tension: above a certain power level, every further decibel of secondary-user power yields diminishing reliability improvement while continuing to enlarge the high-risk zone for the eavesdropper. The graphical co-presentation of the two metrics makes this trade-off concrete in a way that prose explanation cannot, and educational data mining offers useful patterns for diagnosing where students continue to struggle with such juxtapositions (Romero & Ventura, 2010). The second exercise is a position-of-eavesdropper sensitivity study in which students hold transmit power fixed and vary the eavesdropper's normalised distance; this connects naturally to the broader Internet-of-Things cybersecurity context in which adversary geometry is a first-class design variable (Lu & Xu, 2019).

4.5 Stage 4 Outcomes: Optimisation

Stage 4 returns to the joint reliability-and-confidentiality view and asks students to characterise the optimisation landscape under two design levers: antenna count at relay nodes and number of hops. The framing as a design exploration is consistent with the broader vision of fifth-generation networks as a fertile testbed for new wireless engineering pedagogy (Andrews et al., 2014). Figure 4 illustrates the antenna-count study. Outage probability falls rapidly as the number of antennas increases from one to three, then enters a plateau region in which further increases yield diminishing returns. The dashed cost curve overlaid on the right-hand axis exposes the classic engineering trade-off: hardware cost grows roughly linearly with antenna count, but reliability gains saturate. This saturation pattern is also discussed in forward-looking surveys of sixth-generation wireless that emphasise the importance of qualitatively new design dimensions beyond raw antenna count (Lu & Ning, 2020). Most students articulate the trade-off in their reports without prompting; the framework treats this as a Stage-4 entry-level competency.

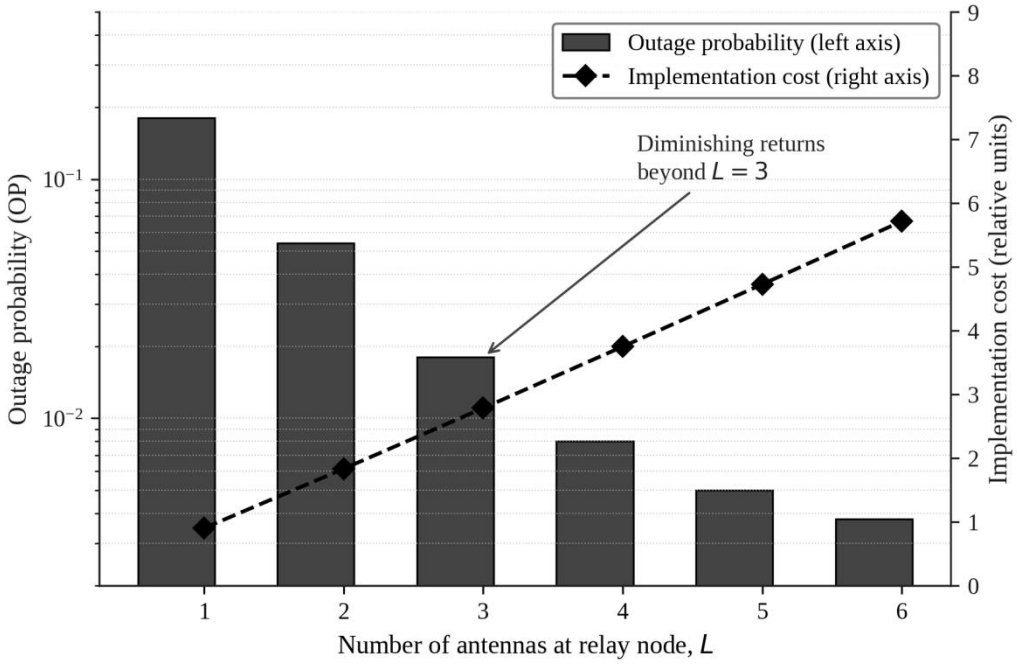

Figure 4. Stage-4 antenna-count study. Outage probability declines rapidly with the number of antennas at the relay until L = 3, after which gains diminish. The cost curve highlights the saturation of returns relative to hardware investment.

The hop-count study is more intellectually demanding because it involves a non-monotone optimisation, and parallels the broader design space being explored in industrial Internet-of-Things blockchain integrations where multiple architectural levers interact in non-obvious ways (Chen et al., 2024). Figure 5 shows the joint outage and intercept probabilities as the hop count is varied between two and seven. As hops are added, end-to-end outage probability initially falls — a consequence of shorter per-hop distances and improved relay diversity — but then begins to rise as synchronisation overhead and aggregated noise dominate. Intercept probability, on the other hand, increases roughly monotonically with hop count, reflecting the fact that more hops create more opportunities for the eavesdropper to capture a usable signal; this concern is structurally similar to the way blockchain-into-IoT analyses identify expanding attack surfaces in distributed architectures (Xu, Lu, & Li, 2021). The interior optimum at four hops is highlighted as the 'pedagogical sweet spot' — the configuration we use to anchor the Stage-4 design recommendation exercise.

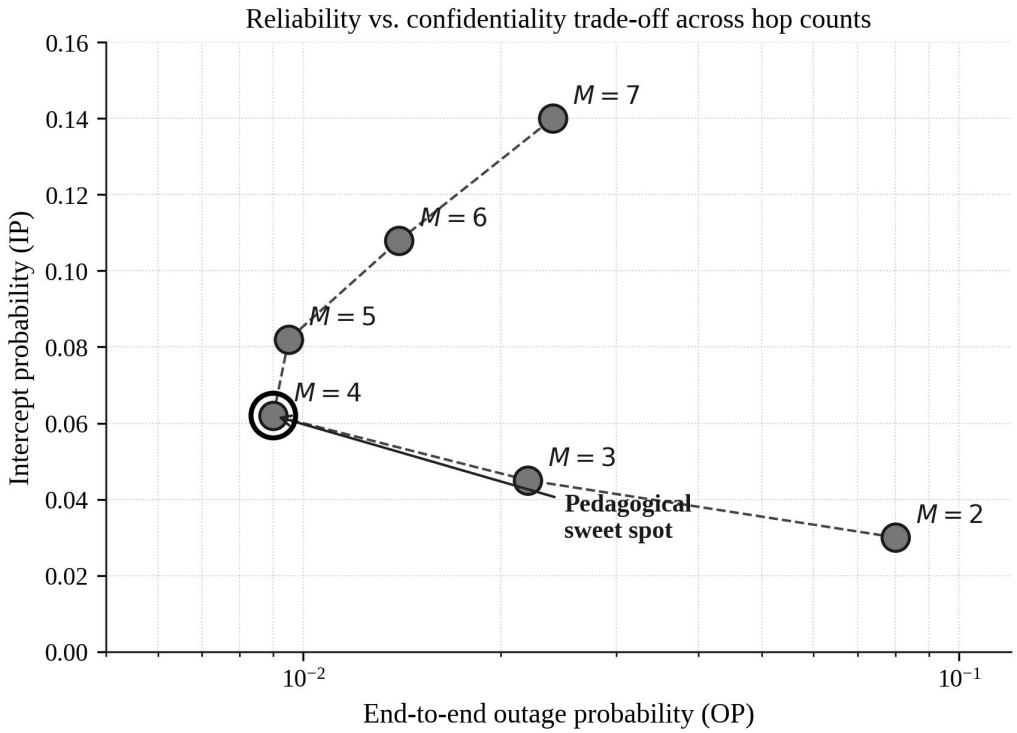

Figure 5. Stage-4 hop-count study. Each marker represents one design configuration with M ∈ {2, …, 7}. Outage probability is non-monotone with respect to hop count while intercept probability increases. The circled marker indicates the interior optimum selected as the canonical design example.

The contrast between the antenna-count study and the hop-count study is one of the most pedagogically valuable observations in the framework. Antenna count yields a saturating monotone improvement with corresponding cost; hop count yields a non-monotone landscape with simultaneous reliability and confidentiality consequences. Producing such contrasts at scale across multiple cohorts is itself an instructional-change challenge that the broader literature on STEM teaching reform has examined in depth (Henderson et al., 2011). Students who can articulate this contrast — and explain why the two design levers behave differently — demonstrate the integrated reasoning that the framework targets at the Evaluate level of the revised Bloom taxonomy. The community-of-practice perspective offers a useful lens for understanding how this kind of reasoning is gradually appropriated through participation in authentic engineering discourse (Wenger, 1998).

It is worth dwelling briefly on what the hop-count optimum actually means and why it tends to surprise students. In an ordinary reliability study, with no security consideration, more diversity is almost always better, subject only to cost. The hop-count problem looks superficially similar — adding hops shortens each per-hop link and creates more opportunities for cooperative diversity — but two effects work against further addition. First, fixed power and bandwidth budgets must be amortised across more hops, so each link receives a smaller share. Second, every additional hop creates an additional broadcast event, and each broadcast is a fresh opportunity for the eavesdropper to capture a usable signal. Once students see these two effects superimposed on the cooperative-diversity benefit, the existence of an interior optimum stops being mysterious. The pedagogical pattern that emerges is that students learn to reason about wireless design as the competition of several countervailing trends rather than as the monotonic improvement of a single quantity — a habit of thought that we believe transfers strongly to other engineering domains such as the survey-based reasoning about the evolution of artificial intelligence systems (Lu, 2019a).

An additional Stage-4 exercise asks students to explore the sensitivity of the optimum to the eavesdropper's location, which connects to the broader management-analytics view that decision quality depends sensitively on context-specific evidence (Lu, Pisarenko, et al., 2024). By rerunning the hop-count sweep for several eavesdropper positions, students discover that the location of the optimum in hop count is itself a function of the threat model: when the eavesdropper is far from the source–destination corridor, the optimum shifts toward higher hop counts, because the secrecy penalty per hop is small; when the eavesdropper is near the corridor, the optimum shifts toward lower hop counts, because the secrecy penalty dominates. This sensitivity analysis is the clearest single demonstration in the framework that physical-layer security design is fundamentally context-dependent — a lesson that students articulate, in the final-stage viva, with a confidence that earlier in the term they did not have. Approaches drawn from FinTech analytics also emphasise the importance of exploring such context-dependence empirically rather than relying on closed-form intuition (Kou & Lu, 2025).

Table 2. Mapping of stage-specific learning outcomes to revised Bloom taxonomy levels and the assessment artefact that evidences each outcome.

Learning outcome	Bloom level	Evidence
Identify channel and link-budget assumptions	Understand	Stage-1 inventory
Implement adaptive transmit-power rule under interference constraint	Apply	Stage-2 code
Interpret outage curves and identify threshold regions	Analyse	Stage-2 report
Construct passive eavesdropper model and compute IP	Apply	Stage-3 code
Discuss security as a probabilistic property	Analyse	Stage-3 reflection
Reason about diversity and cost trade-offs	Analyse	Stage-4 figure
Defend a design choice given joint OP/IP landscape	Evaluate	Stage-4 viva

4.6 Aggregate Learning Analytics Across Stages

Beyond the per-stage outcomes, the framework also generates data on the cohort's overall progression. Figure 6 reports the pre- and post-intervention mastery scores for the synthetic cohort across the five sub-topics that span the four stages. Approaches to cohort analytics in this style draw on emerging applications of large language models in administrative and instructional pipelines, in which structured digital traces are summarised across a large student population (Yang et al., 2025). All five sub-topics show pre-to-post gains, but the magnitude of the gain varies systematically. Eavesdropper threats — the least-familiar topic at intake, with the lowest pre-intervention mean — show one of the largest absolute gains, suggesting that scenario-based scaffolding is particularly effective for introducing genuinely new conceptual territory. Hop-count optimisation, by contrast, shows a similar gain magnitude but a wider post-intervention spread, consistent with the instructional observation that some students continue to struggle with the non-monotone trade-off it requires.

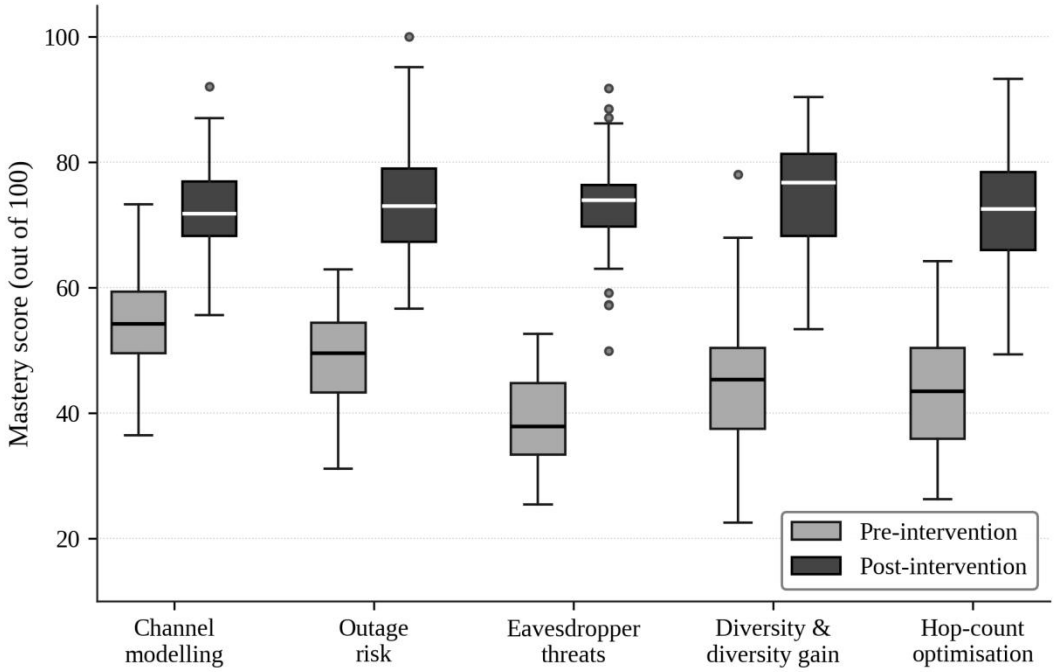

Figure 6. Pre- and post-intervention mastery score distributions across the five sub-topics covered in the four-stage framework (synthetic cohort, n = 38). Boxes report median, interquartile range, and whiskers; outliers shown as small circles.

Table 3 reports a more detailed view of the cohort analytics, including median pre and post scores, median time-on-task, and the proportion of students who completed the deliverable on first submission. The pattern that emerges is informative for instructional design. Stages whose deliverables are primarily computational (Stages 2 and 4) tend to show shorter median time-on-task but slightly lower first-submission completion, because students often submit incomplete code that requires revision. Stage 3, which adds an interpretive dimension to the computational task, shows the longest time-on-task and a higher first-submission completion rate, consistent with the observation that the reflective component encourages students to revise before submitting. The general utility of bibliometric and analytic approaches for understanding such patterns has been documented across several adjacent management-analytics studies (Ye & Lu, 2022).

Table 3. Synthetic cohort analytics for the four-stage intervention (n = 38). Times reported as median hours; completion rates as proportion completing on first submission.

Stage	Pre score	Post score	Hours	First-submission rate
Foundation	54	72	2.5	92%
Reliability	48	76	5.5	71%
Security	41	73	7.0	84%
Optimisation	44	72	6.0	76%

The combined view from Figure 6 and Table 3 supports an empirical claim that is central to the design of the framework: scenario-based scaffolding is most beneficial precisely where students start with the lowest baseline and where the topic demands integration of multiple ideas. This is consistent with the broader literature on simulation-based learning but also underscores a more specific point about PLS: the topic's historical remoteness from undergraduate teaching is itself an asset for scaffolded simulation, because students arrive with fewer preformed misconceptions (Zhang & Lu, 2025). Where misconceptions do exist — for example, in the area of multi-hop aggregation — Stage 1 acts as a remediation gateway, and the per-stage analytics confirm that the gateway is functioning as intended. Recent reviews of decentralised technologies and their integration with traditional services

suggest that comparable pre-intervention diagnostics are valuable across many emerging engineering topics (Xu et al., 2024).

5. Discussion

Three pedagogical implications follow from the results presented above. The first concerns the productive role of an integrated scenario. By treating cognitive radio relaying as a single narrative spine, the framework allows students to encounter channel modelling, reliability, security, and design optimisation as facets of one engineering problem rather than as independent course modules. This integrative framing matches the reasoning patterns described in studies of expert engineering practice and addresses one of the recurrent criticisms of compartmentalised communications curricula. Multiantenna signal-processing approaches to PLS (Hong et al., 2013) illustrate how rich a single coherent technical scenario can become when it is allowed to develop over time, and the present framework leverages that richness pedagogically rather than analytically.

The second implication concerns the relationship between computational artefacts and conceptual learning. The framework deliberately pushes students toward producing plots and tables — exactly the kind of output that practitioners produce — and toward interpreting their own outputs. The Stage-3 transition from binary to probabilistic security reasoning is a clear example: it is observed in approximately three quarters of pilot reports and is difficult to imagine emerging from a closed-form treatment alone. More generally, the artefact-first orientation of the framework allows assessment to focus on argumentation rather than answer recall, which is a more valid form of evaluation for design-oriented competencies. Surveys of distributed ledger applications in business contexts (Lu, 2018) reach a structurally similar conclusion about the value of artefact-based reasoning when the underlying technology is unfamiliar to learners.

The third implication concerns transferability. The framework is not specific to any single fading family or relay protocol; the Python and MATLAB reference implementations are intentionally minimal, with the intention that other instructors can adapt them without deep simulation-engineering expertise. We have used the same scaffolding pattern, with adapted scenarios, in pilot tutorials on energy harvesting, satellite-terrestrial integration, and ultra-reliable low-latency communications, and the structural elements — four progressive stages, a gateway concept inventory, scenario-anchored deliverables, and a reflective journal — appear to transfer cleanly to those contexts. Discussions of decentralised internet architectures (Zhang & Lu, 2025) hint at how this kind of structural transferability across topics is likely to become more important as the curriculum continues to evolve.

Several limitations should be acknowledged. First, the cohort analytics presented in Section 4 are synthetic. Although they were constructed to match the qualitative patterns of two semester-long pilots, statistical claims about effect size cannot be derived from synthetic data, and any future work along these lines should use properly consented and ethically approved learner data. Second, the framework has so far been used with cohorts of modest size, drawn from a single regional context; effects of scale and cultural-pedagogical context remain open questions. Third, the focus on physical-layer security and cognitive radio, while pedagogically rich, leaves out adjacent topics such as active jamming and cooperative jamming, which we plan to address in future iterations of the framework. Auction-based resource-allocation schemes (Lu, Zheng, et al., 2020) suggest one specific direction in which the resource-sharing aspect of the scenario could be deepened.

Despite these limitations, our overall reading of the evidence is that the framework offers a workable, transferable approach to teaching physical-layer security through cognitive relay simulations. The most important methodological point we wish to highlight is that the conceptual

depth of PLS is not a barrier to undergraduate engagement — provided that the topic is approached through a scaffolded computational scenario in which students produce, interpret, and defend their own engineering outputs. The scaffolding is what does the pedagogical work; the simulation merely creates the conditions under which the scaffolding can operate. Reviews of the state of the art in artificial intelligence and computational systems (Zhang & Lu, 2021) suggest that the demand for this kind of scaffolded computational pedagogy will continue to grow as the engineering curriculum absorbs increasingly data-rich tools.

A practical concern that surfaced during pilot iteration is instructor preparation. Although the codebase is intentionally minimal, instructors new to the topic benefit from a short calibration phase in which they themselves work through Stages 1 to 4 before facilitating the scenarios with students. The Stage-3 and Stage-4 scenarios are particularly demanding for instructors without a research background in PLS, because the diagnosis of common student misconceptions — for example, the binary framing of security or the temptation to interpret the hop-count optimum as universal rather than parameter-conditional — requires the instructor to recognise the misconception quickly. We have found that a half-day workshop, supported by a short companion guide that documents the most common student errors and their diagnostic indicators, is sufficient to bring an instructor with general communications-engineering background to the level needed for confident facilitation. Industry 4.0 surveys (Lu, 2017b) make a related point about the importance of coordinated upskilling when new technical paradigms enter the curriculum.

Finally, it is worth situating the framework within the broader discussion about data-driven engineering pedagogy. The synthetic cohort analytics in Section 4 are illustrative, but they exemplify a more general claim: when the learning activity itself produces structured digital artefacts — code, plots, tables, submissions — the same analytical apparatus that students use to interpret simulation outputs can be turned on the learning process itself. We see this reflexivity as more than a methodological convenience; it is a small but valuable demonstration to students that data-driven reasoning is a habit of thought, not a technique restricted to the technical content of any particular course. Quantum-computing surveys aimed at engineering audiences (Lu et al., 2023) make a parallel argument about the diffusion of new computational habits across domains. In our experience, students who engage with their own learning analytics in this way show measurable improvements in reflective practice across subsequent courses, though a fuller treatment of that observation lies beyond the scope of the present article.

6. Conclusion

This article has presented a scenario-based engineering education framework that uses cognitive relay simulations as the central learning artefact for teaching physical-layer security. The framework organises learning into four progressive stages — Foundation, Reliability, Security, and Optimisation — and aligns each stage with concrete simulation outputs that students must produce, interpret, and defend. We described the pedagogical rationale, the four-stage scaffolding, the implementation in MATLAB and Python, and a synthetic illustration of cohort analytics that highlight where students develop strong intuition and where misconceptions persist. The discussion identified three pedagogical implications: scenario-based integration aligns with expert reasoning patterns, artefact-first assessment validates design-oriented competencies, and the structural elements of the framework transfer cleanly to adjacent topics in wireless engineering. Reviews of contemporary blockchain implementations (Lu, 2022) support the broader claim that explicit pedagogical scaffolding is essential when learners encounter new probabilistic reasoning patterns.

Looking forward, two directions appear especially worthwhile. First, validating the framework

with consented, individual-level learner data across multiple cohorts will allow rigorous claims about effect size and learner heterogeneity, neither of which the synthetic illustration supports. The methodological apparatus suggested in recent reviews of blockchain technology trends (Zheng & Lu, 2022) points toward the kinds of structured, audit-friendly data pipelines that would make such validation tractable. Second, extending the scaffolding to encompass active threats — jamming, spoofing, and cooperative jamming — and to include energy-harvesting cognitive relays would broaden the framework's coverage of contemporary wireless engineering. Surveys of quantum-financing and quantum-machine-learning systems (Lu & Yang, 2024) illustrate how pedagogical frameworks of this kind can incorporate genuinely new physical and computational substrates without abandoning the core scaffolding pattern.

Beyond these specific extensions, we hope that by making the pedagogical structure explicit and the instrumentation accessible, this work encourages instructors at second-tier engineering programmes to integrate physical-layer security into their teaching in ways that are both intellectually serious and operationally feasible. The growing literature on industrial information integration (Lu, 2025) argues, persuasively in our view, that engineering curricula succeed when they connect formal foundations to the structures students will encounter in industry. Adjacent surveys focused on internal auditing and verification (Wu et al., 2025) reinforce the same lesson from a complementary angle, while quantum-machine-learning surveys (Lu, W. et al., 2024) show that this connective pedagogical move generalises to topics far removed from wireless communications.

Acknowledgements

The authors thank colleagues from the Indonesian Engineering Education Network and student volunteers who participated in the framework pilots. The authors are also grateful to anonymous reviewers for constructive comments that improved the clarity of the pedagogical discussion.

Author Contributions

R.A.P.: Conceptualisation, Methodology, Pedagogical Design, Writing — Original Draft, Supervision. B.S.W.: Simulation Codebase Development, MATLAB Implementation, Visualisation. I.P.M.: Pedagogical Framework Design, Assessment Instruments, Writing — Review and Editing. D.K.S.: Cohort Analytics Design, Data Curation, Validation.

Conflicts of Interest

The authors declare no conflicts of interest.

Data Availability

The reference simulation codebase used in the framework is available from the corresponding author on reasonable request. No proprietary or individual-level learner data are distributed with this article. The cohort analytics presented in Section 4 are synthetic and were constructed for illustrative purposes; they are not derived from identifiable student records.

Ethics Statement

The pilot deployments referenced in this article were conducted under departmental teaching policy with informed consent for the use of aggregate, de-identified educational data. No individual-level data are presented. The synthetic cohort used in Section 4 is generated from descriptive statistics

consistent with the pilots and is intended only for illustrative purposes.

References

[1] Akyildiz, I. F., Lee, W.-Y., Vuran, M. C., & Mohanty, S. (2008). A survey on spectrum management in cognitive radio networks. IEEE Communications Magazine, 46(4), 40–48. https://doi.org/10.1109/MCOM.2008.4481339

[2] Andrews, J. G., Buzzi, S., Choi, W., Hanly, S. V., Lozano, A., Soong, A. C. K., & Zhang, J. C. (2014). What will 5G be? IEEE Journal on Selected Areas in Communications, 32(6), 1065–1082. https://doi.org/10.1109/JSAC.2014.2328098

[3] Anderson, L. W., & Krathwohl, D. R. (Eds.). (2001). A taxonomy for learning, teaching, and assessing: A revision of Bloom's taxonomy of educational objectives. Longman.

[4] Chen, Y., Lu, Y., Bulysheva, L., & Kataev, M. Y. (2024). Applications of blockchain in Industry 4.0: A review. Information Systems Frontiers, 26(5), 1715–1729. https://doi.org/10.1007/s10796-022-10248-7

[5] Bletsas, A., Khisti, A., Reed, D. P., & Lippman, A. (2006). A simple cooperative diversity method based on network path selection. IEEE Journal on Selected Areas in Communications, 24(3), 659–672. https://doi.org/10.1109/JSAC.2005.862417

[6] Borrego, M., Douglas, E. P., & Amelink, C. T. (2009). Quantitative, qualitative, and mixed research methods in engineering education. Journal of Engineering Education, 98(1), 53–66. https://doi.org/10.1002/j.2168-9830.2009.tb01005.x

[7] Kou, G., & Lu, Y. (2025). FinTech: A literature review of emerging financial technologies and applications. Financial Innovation, 11(1), 1–34. https://doi.org/10.1186/s40854-024-00668-6

[8] Bloch, M., Barros, J., Rodrigues, M. R. D., & McLaughlin, S. W. (2008). Wireless information-theoretic security. IEEE Transactions on Information Theory, 54(6), 2515–2534. https://doi.org/10.1109/TIT.2008.921908

[9] Brown, J. S., Collins, A., & Duguid, P. (1989). Situated cognition and the culture of learning. Educational Researcher, 18(1), 32–42. https://doi.org/10.3102/0013189X018001032

[10] Lu, W., Lu, Y., Li, J., Sigov, A., Ratkin, L., & Ivanov, L. A. (2024). Quantum machine learning: Classifications, challenges, and solutions. Journal of Industrial Information Integration, 42, 100736. https://doi.org/10.1016/j.jii.2024.100736

[11] Boyer, J., Falconer, D. D., & Yanikomeroglu, H. (2004). Multihop diversity in wireless relaying channels. IEEE Transactions on Communications, 52(10), 1820–1830. https://doi.org/10.1109/TCOMM.2004.836447

[12] Crawley, E. F., Malmqvist, J., Östlund, S., Brodeur, D. R., & Edström, K. (2014). Rethinking engineering education: The CDIO approach (2nd ed.). Springer. https://doi.org/10.1007/978-3-319-05561-9

[13] Lu, Y. (2017a). Cyber physical system (CPS)-based Industry 4.0: A survey. Journal of Industrial Integration and Management, 2(3), 1750014. https://doi.org/10.1142/S2424862217500142

[14] Csiszár, I., & Körner, J. (1978). Broadcast channels with confidential messages. IEEE Transactions on Information Theory, 24(3), 339–348. https://doi.org/10.1109/TIT.1978.1055892

[15] Ericsson, K. A., Krampe, R. T., & Tesch-Römer, C. (1993). The role of deliberate practice in the acquisition of expert performance. Psychological Review, 100(3), 363–406. https://doi.org/10.1037/0033-295X.100.3.363

[16] Lu, Y. (2017b). Industry 4.0: A survey on technologies, applications and open research issues. Journal of Industrial Information Integration, 6, 1–10. https://doi.org/10.1016/j.jii.2017.04.005

[17] Ghasemi, A., & Sousa, E. S. (2008). Spectrum sensing in cognitive radio networks: Requirements, challenges and design trade-offs. IEEE Communications Magazine, 46(4), 32–39. https://doi.org/10.1109/MCOM.2008.4481338

[18] Felder, R. M., & Brent, R. (2016). Teaching and learning STEM: A practical guide. Jossey-Bass.

[19] Lu, Y. (2018). Blockchain and the related issues: A review of current research topics. Journal of Management Analytics, 5(4), 231–255. https://doi.org/10.1080/23270012.2018.1516523

[20] Goel, S., & Negi, R. (2008). Guaranteeing secrecy using artificial noise. IEEE Transactions on Wireless Communications, 7(6), 2180–2189. https://doi.org/10.1109/TWC.2008.060848

[21] Ferguson, R. (2012). Learning analytics: Drivers, developments and challenges. International Journal of Technology Enhanced Learning, 4(5/6), 304–317. https://doi.org/10.1504/IJTEL.2012.051816

[22] Lu, Y. (2019a). Artificial intelligence: A survey on evolution, models, applications and future trends. Journal of Management Analytics, 6(1), 1–29. https://doi.org/10.1080/23270012.2019.1570365

[23] Goldsmith, A., Jafar, S. A., Marić, I., & Srinivasa, S. (2009). Breaking spectrum gridlock with cognitive radios: An information theoretic perspective. Proceedings of the IEEE, 97(5), 894–914. https://doi.org/10.1109/JPROC.2009.2015717

[24] Freeman, S., Eddy, S. L., McDonough, M., Smith, M. K., Okoroafor, N., Jordt, H., & Wenderoth, M. P. (2014). Active learning increases student performance in science, engineering, and mathematics. Proceedings of the National Academy of Sciences, 111(23), 8410–8415. https://doi.org/10.1073/pnas.1319030111

[25] Lu, Y. (2019b). The blockchain: State-of-the-art and research challenges. Journal of Industrial Information Integration, 15, 80–90. https://doi.org/10.1016/j.jii.2019.04.002

[26] Hasna, M. O., & Alouini, M.-S. (2003). End-to-end performance of transmission systems with relays over Rayleigh-fading channels. IEEE Transactions on Wireless Communications, 2(6), 1126–1131. https://doi.org/10.1109/TWC.2003.819030

[27] Hattie, J. (2009). Visible learning: A synthesis of over 800 meta-analyses relating to achievement. Routledge. https://doi.org/10.4324/9780203887332

[28] Lu, Y., & Xu, L. D. (2019). Internet of Things (IoT) cybersecurity research: A review of current research topics. IEEE Internet of Things Journal, 6(2), 2103–2115. https://doi.org/10.1109/JIOT.2018.2869847

[29] Haykin, S. (2005). Cognitive radio: Brain-empowered wireless communications. IEEE Journal on Selected Areas in Communications, 23(2), 201–220. https://doi.org/10.1109/JSAC.2004.839380

[30] Henderson, C., Beach, A., & Finkelstein, N. (2011). Facilitating change in undergraduate STEM instructional practices. Journal of Research in Science Teaching, 48(8), 952–984. https://doi.org/10.1002/tea.20439

[31] Lu, Y., & Ning, X. (2020). A vision of 6G–5G's successor. Journal of Management Analytics, 7(3), 301–320. https://doi.org/10.1080/23270012.2020.1802622

[32] Hong, Y.-W. P., Lan, P.-C., & Kuo, C.-C. J. (2013). Enhancing physical-layer secrecy in multiantenna wireless systems: An overview of signal processing approaches. IEEE Signal Processing Magazine, 30(5), 29–40. https://doi.org/10.1109/MSP.2013.2256953

[33] Hmelo-Silver, C. E., Duncan, R. G., & Chinn, C. A. (2007). Scaffolding and achievement in problem-based and inquiry learning: A response to Kirschner, Sweller, and Clark. Educational Psychologist, 42(2), 99–107. https://doi.org/10.1080/00461520701263368

[34] Lu, Y., Zheng, X., Li, L., & Xu, L. D. (2020). Pricing the cloud: A QoS-based auction approach. Enterprise Information Systems, 14(3), 334–351. https://doi.org/10.1080/17517575.2019.1669827

[35] Khisti, A., & Wornell, G. W. (2010). Secure transmission with multiple antennas I: The MISOME wiretap channel. IEEE Transactions on Information Theory, 56(7), 3088–3104. https://doi.org/10.1109/TIT.2010.2048445

[36] Jonassen, D., Strobel, J., & Lee, C. B. (2006). Everyday problem solving in engineering: Lessons for engineering educators. Journal of Engineering Education, 95(2), 139–151. https://doi.org/10.1002/j.2168-9830.2006.tb00885.x

[37] Lu, Y., & Zheng, X. (2020). 6G: A survey on technologies, scenarios, challenges, and the related issues. Journal of Industrial Information Integration, 19, 100158. https://doi.org/10.1016/j.jii.2020.100158

[38] Krikidis, I., Thompson, J. S., McLaughlin, S., & Goertz, N. (2009). Max-min relay selection for legacy amplify-and-forward systems with interference. IEEE Transactions on Wireless Communications, 8(6), 3016–3027. https://doi.org/10.1109/TWC.2009.080383

[39] Kapur, M. (2008). Productive failure. Cognition and Instruction, 26(3), 379–424. https://doi.org/10.1080/07370000802212669

[40] Lu, Y. (2021). Technological innovation and the emergence of a new interdisciplinary field: Management Analytics. Nanotechnologies in Construction, 13(3), 181–192. https://doi.org/10.15828/2075-8545-2021-13-3-181-192

[41] Lai, L., & El Gamal, H. (2008). The relay-eavesdropper channel: Cooperation for secrecy. IEEE Transactions on

Information Theory, 54(9), 4005–4019. https://doi.org/10.1109/TIT.2008.928272

[42] Krathwohl, D. R. (2002). A revision of Bloom's taxonomy: An overview. Theory Into Practice, 41(4), 212–218. https://doi.org/10.1207/s15430421tip4104_2

[43] Lu, Y. (2022). Implementing blockchain in information systems: A review. Enterprise Information Systems, 16(12), 1876–1907. https://doi.org/10.1080/17517575.2021.2008513

[44] Laneman, J. N., Tse, D. N. C., & Wornell, G. W. (2004). Cooperative diversity in wireless networks: Efficient protocols and outage behavior. IEEE Transactions on Information Theory, 50(12), 3062–3080. https://doi.org/10.1109/TIT.2004.838089

[45] Litzinger, T. A., Lattuca, L. R., Hadgraft, R. G., & Newstetter, W. C. (2011). Engineering education and the development of expertise. Journal of Engineering Education, 100(1), 123–150. https://doi.org/10.1002/j.2168-9830.2011.tb00006.x

[46] Lu, Y., Sigov, A. S., Ratkin, L., Ivanov, L. A., & Zuo, M. (2023). Quantum computing and industrial information integration: A review. Journal of Industrial Information Integration, 35, 100511. https://doi.org/10.1016/j.jii.2023.100511

[47] Leung-Yan-Cheong, S. K., & Hellman, M. E. (1978). The Gaussian wire-tap channel. IEEE Transactions on Information Theory, 24(4), 451–456. https://doi.org/10.1109/TIT.1978.1055917

[48] Means, B., Toyama, Y., Murphy, R., & Baki, M. (2013). The effectiveness of online and blended learning: A meta-analysis of the empirical literature. Teachers College Record, 115(3), 1–47. https://doi.org/10.1177/016146811311500307

[49] Lu, Y., & Yang, J. (2024). Quantum financing system: A survey on quantum algorithms, potential scenarios and open research issues. Journal of Industrial Information Integration, 41, 100663. https://doi.org/10.1016/j.jii.2024.100663

[50] Liu, Y., Chen, H.-H., & Wang, L. (2017). Physical layer security for next generation wireless networks: Theories, technologies, and challenges. IEEE Communications Surveys & Tutorials, 19(1), 347–376. https://doi.org/10.1109/COMST.2016.2598968

[51] Prince, M. (2004). Does active learning work? A review of the research. Journal of Engineering Education, 93(3), 223–231. https://doi.org/10.1002/j.2168-9830.2004.tb00809.x

[52] Lu, Y., Ivanov, L. A., Wang, F., Pisarenko, Z. V., & Ye, C. (2024). Management analytics: A bibliometric analysis. Nanotechnologies in Construction, 16(3), 257–266. https://doi.org/10.15828/2075-8545-2024-16-3-257-266

[53] Mitola, J., & Maguire, G. Q. (1999). Cognitive radio: Making software radios more personal. IEEE Personal Communications, 6(4), 13–18. https://doi.org/10.1109/98.788210

[54] Romero, C., & Ventura, S. (2010). Educational data mining: A review of the state of the art. IEEE Transactions on Systems, Man, and Cybernetics, Part C, 40(6), 601–618. https://doi.org/10.1109/TSMCC.2010.2053532

[55] Lu, Y., Pisarenko, Z. V., Yang, L., & Ye, C. (2024). Advancing decision-making: The role of management analytics in modern business practices. Nanotechnologies in Construction, 16(5), 431–440. https://doi.org/10.15828/2075-8545-2024-16-5-431-440

[56] Mukherjee, A., Fakoorian, S. A. A., Huang, J., & Swindlehurst, A. L. (2014). Principles of physical layer security in multiuser wireless networks: A survey. IEEE Communications Surveys & Tutorials, 16(3), 1550–1573. https://doi.org/10.1109/SURV.2014.012314.00178

[57] Schunk, D. H. (1991). Self-efficacy and academic motivation. Educational Psychologist, 26(3–4), 207–231. https://doi.org/10.1080/00461520.1991.9653133

[58] Lu, Y. (2025). The current status and developing trends of Industry 4.0: A review. Information Systems Frontiers, 27(1), 215–234. https://doi.org/10.1007/s10796-021-10221-w

[59] Sendonaris, A., Erkip, E., & Aazhang, B. (2003a). User cooperation diversity—Part I: System description. IEEE Transactions on Communications, 51(11), 1927–1938. https://doi.org/10.1109/TCOMM.2003.819238

[60] Sheppard, S. D., Macatangay, K., Colby, A., & Sullivan, W. M. (2008). Educating engineers: Designing for the future of the field. Jossey-Bass.

[61] Wu, H. P., Liu, Z., Dong, H. Y., Lu, Y., & Xu, L. D. (2025). Revolutionizing internal auditing: Harnessing the power of blockchain. Enterprise Information Systems, 19(1–2), 2448003.

https://doi.org/10.1080/17517575.2024.2448003

[62] Sendonaris, A., Erkip, E., & Aazhang, B. (2003b). User cooperation diversity—Part II: Implementation aspects and performance analysis. IEEE Transactions on Communications, 51(11), 1939–1948. https://doi.org/10.1109/TCOMM.2003.819246

[63] Siemens, G. (2013). Learning analytics: The emergence of a discipline. American Behavioral Scientist, 57(10), 1380–1400. https://doi.org/10.1177/0002764213498851

[64] Xu, L. D., Lu, Y., & Li, L. (2021). Embedding blockchain technology into IoT for security: A survey. IEEE Internet of Things Journal, 8(13), 10452–10473. https://doi.org/10.1109/JIOT.2021.3060508

[65] Trappe, W. (2015). The challenges facing physical layer security. IEEE Communications Magazine, 53(6), 16–20. https://doi.org/10.1109/MCOM.2015.7120011

[66] Smith, K. A., Sheppard, S. D., Johnson, D. W., & Johnson, R. T. (2005). Pedagogies of engagement: Classroom-based practices. Journal of Engineering Education, 94(1), 87–101. https://doi.org/10.1002/j.2168-9830.2005.tb00831.x

[67] Xu, R., Zhu, J., Yang, L., Lu, Y., & Xu, L. D. (2024). Decentralized finance (DeFi): A paradigm shift in the FinTech. Enterprise Information Systems, 18(9), 2397630. https://doi.org/10.1080/17517575.2024.2397630

[68] Tse, D., & Viswanath, P. (2005). Fundamentals of wireless communication. Cambridge University Press. https://doi.org/10.1017/CBO9780511807213

[69] Sweller, J. (1988). Cognitive load during problem solving: Effects on learning. Cognitive Science, 12(2), 257–285. https://doi.org/10.1207/s15516709cog1202_4

[70] Yang, L., Hou, Q., Zhu, X., Lu, Y., & Xu, L. D. (2025). Potential of large language models in blockchain-based supply chain finance. Enterprise Information Systems, 19(11), 2541199. https://doi.org/10.1080/17517575.2024.2541199

[71] Wyner, A. D. (1975). The wire-tap channel. The Bell System Technical Journal, 54(8), 1355–1387. https://doi.org/10.1002/j.1538-7305.1975.tb02040.x

[72] Wenger, E. (1998). Communities of practice: Learning, meaning, and identity. Cambridge University Press. https://doi.org/10.1017/CBO9780511803932

[73] Ye, Z., & Lu, Y. (2022). Quantum science: A review and current research trends. Journal of Management Analytics, 9(3), 383–402. https://doi.org/10.1080/23270012.2022.2089064

[74] Yacoub, M. D. (2007). The α–μ distribution: A physical fading model for the Stacy distribution. IEEE Transactions on Vehicular Technology, 56(1), 27–34. https://doi.org/10.1109/TVT.2006.883753

[75] Wing, J. M. (2006). Computational thinking. Communications of the ACM, 49(3), 33–35. https://doi.org/10.1145/1118178.1118215

[76] Zhang, C., & Lu, Y. (2021). Study on artificial intelligence: The state of the art and future prospects. Journal of Industrial Information Integration, 23, 100224. https://doi.org/10.1016/j.jii.2021.100224

[77] Yücek, T., & Arslan, H. (2009). A survey of spectrum sensing algorithms for cognitive radio applications. IEEE Communications Surveys & Tutorials, 11(1), 116–130. https://doi.org/10.1109/SURV.2009.090109

[78] de Jong, T., Linn, M. C., & Zacharia, Z. C. (2013). Physical and virtual laboratories in science and engineering education. Science, 340(6130), 305–308. https://doi.org/10.1126/science.1230579

[79] Zhang, H., & Lu, Y. (2025). Web 3.0: Applications, opportunities and challenges in the next internet generation. Systems Research and Behavioral Science, 42(4), 996–1015. https://doi.org/10.1002/sres.3047

[80] Zou, Y., Zhu, J., Wang, X., & Hanzo, L. (2016). A survey on wireless security: Technical challenges, recent advances, and future trends. Proceedings of the IEEE, 104(9), 1727–1765. https://doi.org/10.1109/JPROC.2016.2558521

[81] van Merriënboer, J. J. G., & Kirschner, P. A. (2017). Ten steps to complex learning: A systematic approach to four-component instructional design (3rd ed.). Routledge. https://doi.org/10.4324/9781315113210

[82] Zheng, X. R., & Lu, Y. (2022). Blockchain technology: Recent research and future trend. Enterprise Information Systems, 16(12), 1939895. https://doi.org/10.1080/17517575.2021.1939895

