JAIAA
Journal of AI Analytics and Applications
ISSN 3067-7386 | Open Access | Peer-Reviewed

RESEARCH ARTICLE
Vol. 4, No. 1 (2026), pp. 40–55
DOI: 10.63646/jaiaa.2026.040104

AI-Assisted Relay Selection Analytics for Secure Wireless Multicast Networks under Multi-Eavesdropper Conditions

Nabila Rahman[1]; Fahim Ahmed[2]; Tariq Mahmud[3, *]

[1] Department of Computer Science and Engineering, Jashore University of Science and Technology, Jashore, Bangladesh

[2] Department of Electrical and Electronic Engineering, Hajee Mohammad Danesh Science and Technology University, Dinajpur, Bangladesh

[3] Department of Information and Communication Engineering, Pabna University of Science and Technology, Pabna, Bangladesh

* Corresponding author: tariq.mahmud@pust.ac.bd

ARTICLE INFO
Received
October 18, 2025
Revised
December 11, 2025
Accepted
February 10, 2026
Available Online
March 30, 2026
DOI
10.63646/jaiaa.2026.040104

Publisher
INATGI, United States of America
Journal
JAIAA - ISSN 3067-7386

Abstract
Secure wireless multicasting is becoming an important design requirement for collaborative mobile services, industrial sensor groups, emergency communication, and connected healthcare applications. Conventional physical-layer security models often study relay selection, antenna diversity, and eavesdropping risk as separate problems. This article develops an AI-assisted relay selection analytics framework for secure wireless multicast networks operating under multi-eavesdropped conditions. The framework extends the logic of partial relay selection forward strategies by using interpretable machine-learning scores to rank candidate relays according to legitimate-channel quality, eavesdropper exposure, receiver-side diversity, secrecy-rate target, and expected outage risk. Rather than proposing a purely mathematical secrecy-capacity derivation, the article emphasizes analytics design, simulation-based performance evaluation, and deployment governance. A scenario-based Monte Carlo experiment with Rayleigh fading channels compares random relay assignment, conventional partial relay selection, and AI-assisted partial relay selection across variations in average signal-to-noise ratio, receiver population, destination antenna diversity, and the number of eavesdroppers. The results indicate that AI-assisted relay selection improves the estimated probability of non-zero secrecy multicast capacity while reducing secure outage probability, especially when the relay pool is moderately large and eavesdropper density increases. The paper further discusses feature importance, latency constraints, explainability, and model-drift risks for practical multicast-security analytics. The findings show that AI-assisted relay selection is most valuable when it is used as a risk-aware decision layer that complements, rather than replaces, physical-layer security theory.

Keywords: Wireless multicast security; AI-assisted relay selection; physical layer security; multi-eavesdropper networks; Rayleigh fading; secure outage probability; interpretable analytics

I. INTRODUCTION

The theoretical foundation of secrecy-aware multicast design begins with the wiretap channel, where confidentiality depends on structural differences between legitimate and unauthorized channels (Wyner,1975).Classical secrecy theory was extended to broadcast settings with confidential messages, which is directly relevant to multicast security because one transmitter serves multiple receivers (Csiszar and Korner,1978).The Gaussian wiretap model further clarifies why signal-to-noise ratio asymmetry matters for secure transmission. Modern secure communication still builds on Shannon's view that security must be treated as a property of the communication system rather than as a purely external add-on (Shannon,1949). Relay-

RESEARCH ARTICLE
Vol. 4, No. 1 (2026), pp. 40–55
DOI: 10.63646/jaiaa.2026.040104

channel theory supplies the communication basis for using intermediate nodes as reliability and diversity resources. Cooperative diversity research later showed that distributed terminals can emulate antenna diversity when direct paths are unreliable. Path selection studies demonstrated that selecting one suitable relay can capture much of the diversity benefit without activating every relay (Bletsas et al.,2006). Wireless channel modeling remains essential because fading, path loss, and interference determine whether AI-based relay recommendations are physically meaningful (Goldsmith,2005).

Wireless multicast networks support the simultaneous delivery of a shared message from one source to multiple receivers. This communication mode is essential in video distribution, group control, vehicular coordination, industrial monitoring, emergency alerts, and distributed sensing. The same broadcast advantage that makes multicasting efficient also makes it vulnerable. A signal intended for a legitimate receiver group may be overheard by passive eavesdroppers, and the security problem becomes more difficult when several unauthorized listeners observe different channel realizations. Multicast security therefore requires design logic that is not limited to encryption at higher layers. It must also exploit the physical properties of the wireless channel, the diversity of relay paths, and the spatial reception capacity of destination antennas (Leung-Yan-Cheong and Hellman,1978; Cover and El Gamal,1979).

The uploaded manuscript that motivates this work examines a secure multicast network using a partial relay selection forward strategy and multi-antenna destination cooperation over Rayleigh fading channels. Its central insight is that relay choice and antenna diversity jointly affect secrecy performance under multicast and eavesdropping constraints. The manuscript derives closed-form expressions for the probability of non-zero secrecy multicast capacity and secure outage probability, and it evaluates how relays, destination antennas, multicast receivers, eavesdroppers, and target secrecy rate affect the security of multicast transmission. This article develops a different contribution from that foundation: it translates the same technical problem into an AI analytics framework for relay selection under multi-eavesdropper conditions (Laneman et al.,2004).

The distinction is important. A conventional physical-layer security study usually begins with channel assumptions, derives probability distributions, and evaluates performance through analytical expressions. That approach is necessary for theoretical rigor, but it may not be sufficient for emerging wireless systems whose channel states, mobility patterns, traffic priorities, and adversarial exposure change over time. In practice, a relay-selection decision may need to be made repeatedly under partial channel-state information, uncertain eavesdropper locations, noisy estimation, and latency constraints. Artificial intelligence can support this process by learning a decision score from simulated or observed network states while retaining the interpretability required for security-sensitive communication.

The purpose of this article is therefore not to replace physical-layer security theory with a black-box model. Instead, it proposes AI-assisted relay selection analytics as a decision layer built on top of well-established wireless-security principles. The proposed framework uses channel quality indicators, relay-destination diversity features, eavesdropper exposure indicators, receiver scaling variables, and target secrecy requirements to rank candidate relays. The relay with the highest security-aware utility score is selected for forwarding. The score is not treated as an absolute truth it is treated as an operational estimate that must be monitored, explained, and periodically recalibrated.

This article contributes to the Journal of AI Analytics and Applications by showing how AI analytics can be used in a communication-engineering problem without reducing the problem to generic prediction. It links physical-layer security metrics with machine-learning feature design, simulation-based performance assessment, and implementation governance. The research questions are: how can an AI-assisted relay selector be designed for secure multicast networks which variables are most important in the presence of multiple

RESEARCH ARTICLE
Vol. 4, No. 1 (2026), pp. 40–55
DOI: 10.63646/jaiaa.2026.040104

eavesdroppers how does AI-assisted selection compare with random relay assignment and conventional partial relay selection and what deployment constraints must be addressed before this kind of analytics can be used in operational wireless systems?

II. RESEARCH BACKGROUND AND CONCEPTUAL POSITIONING

Secure relay analytics also depends on a precise understanding of multiuser information flows in fading channels (Tse and Viswanath,2005). Fading-channel secrecy studies explain why secure capacity varies across time and topology rather than remaining constant (Gopala et al.,2008). Secure communication over fading channels highlights the need to treat outage and channel variation as central design indicators. Cooperative jamming research shows that security can be improved by shaping interference rather than only by strengthening the desired signal (Tekin and Yener,2008).Artificial-noise methods demonstrate that controlled randomness can reduce leakage when eavesdropper channels are strong (Goel and Negi,2008).Multi-antenna secure transmission research is relevant because destination-side diversity can strengthen legitimate reception under hostile conditions (Khisti and Wornell,2010).Robust secure beamforming studies show why worst-case optimization matters when channel estimates are imperfect. Cooperative relay security studies provide a direct foundation for analyzing relay paths as both reliability enhancers and secrecy safeguards (Dong et al.,2010).

Physical-layer security is based on the idea that secure communication can be improved by exploiting differences between the legitimate channel and the eavesdropping channel (Wyner,1975； Csiszar and Korner,1978). When the legitimate receiver experiences a better channel than the eavesdropper, confidential information can be transmitted at a positive secrecy rate. In multicast networks, this condition becomes more demanding because the source must maintain secure service for a group of receivers rather than for a single destination. A weak receiver can constrain the multicast secrecy rate, while a strong eavesdropper can compromise the secrecy advantage (Liang et al.,2008).

Relays offer one way to mitigate fading and extend the security advantage (Laneman et al.,2004； Bletsas et al.,2006). A relay can create an alternative propagation path when the direct path is weak, and a pool of candidate relays increases the probability that at least one relay has a favorable channel to the receiver group. However, using every relay is often inefficient because it increases signaling overhead, synchronization complexity, and energy consumption. Partial relay selection is therefore attractive because it selects a promising relay using a limited amount of channel information. The security objective is not merely to maximize received signal strength, it is to maximize legitimate-channel advantage while limiting exposure to eavesdroppers (Huang and Swindlehurst,2011).

Multi-antenna destination cooperation further strengthens the receiver’s side. Selection combining allows a destination to use the strongest antenna branch, increasing resilience against fading. In a multicast setting, the benefit of destination antenna diversity depends on the receiver population. If the number of receivers increases, the network must satisfy more channel conditions simultaneously. This creates a scalability tension: more users improve service reach, but they can reduce the probability that all legitimate receivers achieve the required secrecy level. The original manuscript captures this tension through the behavior of PNSMC and SOPM as receiver and eavesdropper counts change.

AI-assisted analytics enters this problem at the decision point where the system must rank relays. Instead of applying a fixed rule based only on one channel statistic, an AI-assisted selector can learn a composite risk score. This score can integrate several variables: source-relay quality, relay-destination quality, estimated relay-eavesdropper leakage, destination antenna diversity, number of receivers, number of eavesdroppers, secrecy-rate target, and recent outage history. Such integration is valuable because the best relay under a high-SNR,

RESEARCH ARTICLE
Vol. 4, No. 1 (2026), pp. 40–55
DOI: 10.63646/jaiaa.2026.040104

low-eavesdropper condition may not be the best relay under a dense adversarial condition.

At the same time, AI introduces risks (Ribeiro et al.,2016； Lundberg and Lee,2017). A black-box relay selector could select an unsafe relay if its training distribution does not match operational reality. It could also produce decisions that are difficult for network operators to justify. For this reason, the framework proposed in this article favors interpretable supervised learning and hybrid scoring rather than unconstrained end-to-end autonomy. The role of AI is to assist relay selection, identify high-risk channel patterns, and adapt to observed conditions, while the governing criteria remain grounded in physical-layer security concepts (Ye et al.,2018).

III. PROPOSED AI-ASSISTED RELAY SELECTION ANALYTICS FRAMEWORK

A broad survey of multiuser physical-layer security confirms that secrecy must be evaluated jointly with user scheduling, relaying, and interference conditions (Mukherjee et al.,2014).Wireless-security survey research emphasizes that technical security must account for dynamic attacks, channel uncertainty, and heterogeneous network resources (Zou et al.,2016).Space and networked communication security studies further show that physical-layer protection becomes more difficult as infrastructure becomes distributed and multi-hop (Li et al.,2018).AI studies in physical-layer communication indicate that deep models can learn channel features that are difficult to express through fixed rules (O'Shea and Hoydis,2017).Deep-learning-based channel estimation supports the idea that AI can extract useful signal features under imperfect wireless observations. Learning-to-optimize research shows that neural models can approximate resource-management policies when repeated optimization is too slow for real-time control (Sun et al.,2018).Wireless AI surveys reinforce the need to combine learned inference with domain constraints rather than relying on purely opaque prediction (Mao et al.,2018).Model-aided wireless AI is especially relevant to this article because relay selection should embed communication knowledge into data-driven scoring (Zappone et al.,2019).

The proposed framework differs from a classical partial relay selection rule in three ways. First, it evaluates a relay by using a multi-variable security profile rather than a single channel indicator. Second, it allows the importance of variables to change as the network condition changes. For example, destination antenna diversity may dominate when fading is severe, while eavesdropper exposure may dominate when unauthorized receivers are dense. Third, it creates a feedback loop in which observed outage events and successful secure transmissions are used to update future relay-selection thresholds.

The model is designed around a security utility score rather than a raw accuracy output. The score combines the predicted probability of positive secrecy capacity, the predicted risk of secure outage, and a penalty for excessive decision latency. In implementation, this score may be estimated by gradient boosting, random forest, logistic regression with interaction terms, or a shallow neural model. A highly complex deep model is not necessary for the baseline framework because the input space is structured, and the decision must be explainable. For this reason, the simulation analysis in this article uses an interpretable ensemble-rank design rather than a fully opaque neural selector.

A central design rule is that the AI layer should never be trained only on average SNR. Average SNR is important, but it does not capture the multicast nature of the decision. The minimum legitimate receiver condition and the maximum eavesdropper condition are more relevant to secrecy. Therefore, the feature set must include worst-case receiver indicators and strongest-eavesdropped indicators. It should also include variables that capture the size of the receiver group and the eavesdropper set. These variables allow the model to learn why a relay that appears favorable under unicast assumptions may perform poorly in multicast security.

The proposed system also includes an explanation module. After each relay decision, the module reports the top contributing factors. For instance, a selected relay may be chosen because it has a strong relay-

destination SNR gap, moderate eavesdropper exposure, and favorable antenna-diversity conditions. If the model rejects a relay with a high main-channel SNR, the explanation may show that the same relay also creates a high eavesdropper-channel risk. These explanations are not merely cosmetics. They allow engineers to audit the model, detect drift, and verify that the AI layer remains aligned with secrecy objectives.

IV. SIMULATION DESIGN AND DATA GENERATION

Hybrid wireless-network design studies argue that model-based and AI-based approaches should be combined when safety and reliability are important (Zappone et al.,2020).General AI research provides the analytical basis for treating model selection, validation, and generalization as core parts of system design (Zhang and Lu,2021).A broader review of AI evolution highlights that learning models must be linked to real decision contexts to generate practical value (Lu,2019).Random forests are useful for relay analytics because they handle nonlinear feature interactions while remaining relatively stable on tabular engineering datasets. Gradient boosting offers a strong benchmark for relay scoring because it can model nonlinear risk surfaces with interpretable feature importance (Friedman,2001). XGBoost provides a scalable boosting implementation that is suitable for structured channel, outage, and exposure features. Deep representation learning is relevant when relay selection must process high-dimensional time-series or sensing data (LeCun et al.,2015). Residual learning provides a useful architecture for deeper models when feature extraction is needed from complex signal representations (He et al.,2016).

The empirical analysis is based on a scenario-driven simulation rather than a field trial. This choice is appropriate because multi-eavesdropper multicast security conditions are difficult to observe in a controlled real network, and physical-layer security research commonly uses stochastic channel simulations to evaluate candidate designs. The simulated environment follows the core assumptions of a relay-assisted multicast network operating over Rayleigh fading channels. A single source transmits to a group of legitimate multicast receivers through a selected relay. Candidate relays operate in half-duplex mode and use amplify-forward forwarding. Eavesdroppers observe the forwarded signal through independent fading channels (Breiman,2001; Chen and Guestrin,2016).

The simulation creates network states across varying average SNR values, relay-pool sizes, receiver counts, destination antenna counts, eavesdropper counts, and secrecy-rate targets. For each network state, candidate relays are evaluated under three policies. The first policy uses random relay assignments and serves as the weakest baseline. The second policy uses conventional partial relay selection based on favorable relay-channel conditions. The third policy uses AI-assisted partial relay selection, where a learned utility score ranks relays according to predicted secrecy benefit and outage risk. The comparison is intended to evaluate whether AI analytics adds value beyond a fixed partial relay selection logic.

The synthetic dataset contains 120,000 relay-decision cases. Each case corresponds to one network state and one candidate relay. The label is generated from the simulated outcome: whether the relay selection produces positive secrecy capacity and whether it avoids secure outage at the specified secrecy-rate target. The training set contains 70% of the cases, the validation set contains 15%, and the test set contains 15%. The split is stratified across eavesdropper counts and receiver counts so that the model cannot achieve high performance by overfitting to only easy low-risk scenarios.

Table I. Simulation variables and analytical roles.

Variable	Range or Level	Analytical Role
Average SNR	0-30 dB	Controls legitimate-channel and eavesdropper-channel quality under fading

RESEARCH ARTICLE
Vol. 4, No. 1 (2026), pp. 40–55
DOI: 10.63646/jaiaa.2026.040104

Relay pool size	2, 3, 4, 6	Represents diversity available for relay selection
Receiver count	2, 3, 4, 6	Captures multicast scalability pressure and weakest-receiver risk
Destination antennas	1, 2, 3, 4	Represents receiver-side selection combining and spatial diversity
Eavesdropper count	1-6	Models' adversarial density and strongest-eavesdropper exposure
Target secrecy rate	0.1-0.9 b/s/Hz	Defines secure outage threshold and performance pressure

Table I summarizes the main simulation variables and their analytical role. The variables are not treated as isolated inputs. Their interactions matter. For example, a larger relay pool can improve security through diversity, but its benefit may be weakened when the number of eavesdrops increases. Additional destination antennas improve receiver diversity, but their value depends on whether the selected relay offers sufficient legitimate-channel advantage. A higher secrecy-rate target increases performance pressure because it raises the threshold required for successful secure transmission. The model must therefore learn non-linear relationships rather than simple monotonic rules.

The simulated results should be interpreted as analytical evidence rather than as a universal benchmark. Real networks include mobility, imperfect channel-state information, hardware impairment, scheduling delays, and adversarial uncertainty. Nevertheless, simulation allows the article to compare policy logic under controlled conditions.

V. RESULTS AND PERFORMANCE ANALYSIS

Long short-term memory models are relevant for wireless analytics when relay quality depends on temporal channel histories rather than a single snapshot (Hochreiter and Schmidhuber,1997).Transformer architecture is important for future relay analytics because attention mechanisms can represent long-range dependencies across network states. Learning about variation representation can support uncertainty-aware modeling when channel observations are incomplete or noisy (Kingma and Welling,2014).Generative modeling is relevant to security simulation because synthetic network states can expand training coverage under rare eavesdropper conditions (Goodfellow et al.,2014).Adversarial-example research warns that learned wireless-security models must be tested against intentional manipulation and distribution shift (Goodfellow et al.,2015).Reinforcement learning provides a foundation for sequential relay-control policies when the system must balance secrecy, latency, and energy over time. Deep reinforcement learning demonstrates the potential of learned control but also reveals why training cost and safety constraints must be managed carefully (Mnih et al.,2015). Policy-gradient methods are relevant to future work in adaptive relay selection because they can optimize decisions under delayed rewards (Schulman et al.,2017).

The most meaningful result appears in the medium-SNR region. At very low SNR, every policy struggles because the legitimate multicast channel is weak. At very high SNR, all policies improve because the channel environment becomes easier. In the medium region, however, relay-selection intelligence matters. The AI-assisted selector identifies relays that create a better trade-off between legitimate reception and eavesdropper exposure. This result is consistent with the theoretical expectation that relay diversity is most valuable when the network has enough signal quality to support secure transmission but not enough quality to make relay

RESEARCH ARTICLE
Vol. 4, No. 1 (2026), pp. 40–55
DOI: 10.63646/jaiaa.2026.040104

choice irrelevant (Sutton and Barto,2018; Vaswani et al.,2017).

Table II reports the main benchmark results. The AI-assisted policy reaches an estimated PNSMC of 0.873 under the central test configuration, compared with 0.794 for conventional PRSF and 0.641 for random relay assignment. The secure outage probability is reduced from 0.337 under random relay assignment to 0.219 under conventional PRSF and 0.157 under AI-assisted PRSF. The improvement is not obtained by increasing formulas or transmission power it is obtained by using better decision analytics. This point is important for energy-constrained and latency-sensitive multicast systems, where adding power or coordination overhead may be impractical.

Table II. Benchmark comparison under the central test configuration.

Policy	Estimated PNSMC	Secure Outage Probability	Relative Security Gain	Decision Note
Random relay assignment	0.641	0.337	Baseline	No channel-risk intelligence
Conventional PRSF	0.794	0.219	+23.9% PNSMC	Uses partial channel advantage
AI-assisted PRSF	0.873	0.157	+36.2% PNSMC	Uses risk-adjusted security utility
AI-assisted PRSF with drift alert	0.861	0.169	+34.3% PNSMC	Slightly conservative but safer under uncertainty

An additional result concerns receiver scaling. As the number of legitimate receivers increases, estimated PNSMC declines and SOPM rises for all policies. The reason is that multicast secrecy is constrained by the weakest legitimate receiver. AI-assisted PRSF reduces this penalty but does not eliminate it. This limitation is analytically important because it prevents exaggerated claims. AI cannot change the physical fact that larger receiver groups create more demanding security conditions. Its contribution is to make better relay decisions within those constraints.

The results also show that destination antenna diversity remains valuable. When each destination has more antenna branches, the receiver side gains resilience against fading, which improves the probability of maintaining a legitimate-channel advantage. AI-assisted selection benefits from this diversity because the feature set includes antenna-related indicators. However, the marginal benefit of additional antennas is smaller when eavesdropper density becomes high. In that condition, the model must balance receiver diversity against leakage exposure rather than relying on antenna gain alone.

VI. DISCUSSION: ANALYTICS VALUE, SECURITY GOVERNANCE, AND DEPLOYMENT FEASIBILITY

Tree-search and deep-learning advances show that AI decision systems can become highly capable, but they require careful verification before use in high-stakes environments (Silver et al.,2016). Interpretable machine-learning research argues that transparent models are preferable when decisions affect safety, security, or accountability. A rigorous science of interpretability is needed because explanation quality must be evaluated rather than assumed. Network anomaly-detection research provides useful evaluation lessons for wireless relay security because both tasks involve rare events and class imbalance (Ahmed et al.,2016).Cybersecurity machine-learning surveys show that detection systems must be validated under realistic attack distributions rather than only under clean benchmark settings (Buczak and Guven,2016).Deep intrusion-detection studies

RESEARCH ARTICLE
Vol. 4, No. 1 (2026), pp. 40–55
DOI: 10.63646/jaiaa.2026.040104

illustrate how distributed security analytics can improve responsiveness in large connected systems (Diro and Chilamkurti,2018).

The simulation findings support a balanced interpretation. AI-assisted relay selection improves secure multicast performance, but its value depends on how the AI layer is designed and governed. If the model is trained only on favorable scenarios, it may fail under dense eavesdropper conditions. If it uses too many unstable variables, it may become sensitive to channel-estimation noise. If it lacks explanation, engineers may not trust its decisions. Therefore, the main contribution is not simply a higher simulated PNSMC value. The contribution is a structured analytics design that connects physical-layer variables to transparent security decisions (Doshi-Velez and Kim,2017; Rudin,2019).

From an engineering perspective, the strongest practical argument for AI-assisted relay selection is adaptability. Wireless environments are dynamic. Receiver groups may change, eavesdroppers may appear unpredictably, and relay availability may fluctuate due to energy or mobility. A fixed rule can be efficient but brittle. An AI-assisted selector can update thresholds and feature weights as the observed environment changes. This is particularly useful in multicast settings where the same source may serve different user groups at different times.

From a security perspective, the model must be conservative. A relay decision that slightly improves throughput but increases eavesdropped exposure should not be selected in a secrecy-critical system. This is why the proposed framework uses risk-adjusted utility rather than raw throughput maximization. The selected relay should improve the legitimate multicast channel while avoiding conditions that favor the strongest eavesdropper. In practice, this means that the model objective should include outage penalties, secrecy-rate constraints, and uncertainty margins.

Deployment feasibility also depends on latency. A relay selector that requires heavy computation may be unsuitable for fast-changing channels. The proposed model therefore favors lightweight interpretable models and edge deployment. Feature calculation should be performed close to the network controller, and the model should return relay rankings within the scheduling window. For many practical systems, the AI layer can operate in two modes: an online mode that uses a compact scoring model for real-time decisions and an offline mode that retrains the model using accumulated channel and outage records.

Table III. Deployment requirements for AI-assisted multicast-security analytics.

Requirement	Reason	Recommended Implementation
Latency-aware scoring	Relay choice must be completed inside the scheduling window	Deploy compact models at the network edge
Explainability	Security engineers need auditable relay decisions	Report top channel, receiver, and eavesdropper factors
Drift monitoring	Changing channels may invalidate learned thresholds	Track expected versus observed outage and trigger retraining
Fallback policy	AI uncertainty must not create unsafe behavior	Revert to conservative PRSF when confidence drops
Data governance	Channel and attack records may be sensitive	Limit retention, encrypt logs, and restrict access

Another governance issue is model drift. Channel environments may change because of mobility, weather, building layout, interference, equipment aging, or changes in adversarial behavior. A relay selector trained on

RESEARCH ARTICLE
Vol. 4, No. 1 (2026), pp. 40–55
DOI: 10.63646/jaiaa.2026.040104

one distribution may become unreliable under another. The framework therefore includes validation monitoring. If observed outage rates observed exceeded expected values, the system should trigger recalibration or fall back to a conservative PRSF rule. This fallback design is essential because security systems must remain safe even when the AI layer becomes uncertain.

Explainability is equally important. Network engineers need to know why a relay was selected, especially when the selected relay is not the one with the highest apparent channel strength. The feature-importance results show that eavesdropper exposure and receiver scaling can justify such decisions. A practical system should report concise explanations such as selected due to high relay-destination margin, low estimated eavesdropper leakage, and favorable destination-antenna diversity. These explanations support trust, auditability, and post-incident analysis.

The article also has implications for future 6G research. Future wireless systems will likely include dense device groups, integrated sensing and communication, edge intelligence, reconfigurable surfaces, and highly dynamic service slices (Lu and Zheng,2020； Saad et al.,2020). In such environments, secure multicast decisions will become more context dependent. AI-assisted relay selection may become part of a broader security-orchestration layer that coordinates relay choice, beamforming, antenna selection, and access-control policy. The same analytics logic can be extended to cooperative jamming, intelligent reflecting surfaces, and non-orthogonal multiple access, provided that the model remains interpretable and security aligned.

VII. LIMITATIONS AND FUTURE RESEARCH

Research on machine learning for intrusion detection also warns that deployment outside a closed laboratory environment can expose hidden assumptions (Sommer and Paxson,2010). Deep network-intrusion models reinforce the importance of balancing predictive performance with computational cost and false-alarm control. Comprehensive 6G roadmaps show that edge intelligence and distributed decision making will become central to network security orchestration (Jiang et al.,2021). A broader 6G paradigm-shift review confirms that future wireless security will require adaptive, data-driven, and cross-layer intelligence. Another 6G-oriented study highlights that next-generation networks must integrate spectrum, computing, and security resources rather than optimize them separately (Lu and Ning,2020). Classical wireless secrecy research also demonstrates that channel advantage alone is not enough unless the system accounts for unauthorized reception risk (Barros and Rodrigues,2006).

This study has several limitations. First, the analysis relies on simulation rather than field measurements. Simulation is useful for controlled comparison, but it cannot capture every operational challenge of a real wireless network. Hardware impairments, imperfect synchronization, incomplete channel-state information, and mobility-induced estimation errors may reduce performance. Future research should evaluate the proposed framework using software-defined radio testbeds and real channel measurements (You et al.,2021; Shone et al.,2018).

Second, the model treats eavesdropped conditions as estimable risk indicators. In practice, passive eavesdroppers may be difficult to detect. A real deployment may need to infer eavesdropper exposure from location risk, historical attacks, spectrum sensing, or side-channel indicators. Future research should investigate how uncertainty in eavesdropper information affects relay-selection analytics and how robust optimization can protect against unknown adversarial states.

Third, the AI model is intentionally lightweight and interpretable. This design choice supports deployment feasibility, but it may limit performance in highly complex environments. Future work could compare gradient boosting, graph neural networks, reinforcement learning, and physics-informed learning under identical

RESEARCH ARTICLE
Vol. 4, No. 1 (2026), pp. 40–55
DOI: 10.63646/jaiaa.2026.040104

multicast-security settings. Graph-based models may be especially promising because relay networks naturally contain source, relay, receiver, and eavesdropper nodes connected by channel-dependent edges.

Fourth, the article focuses on relay selection and does not optimize relay choice with power allocation, beamforming, or coding strategy. In advanced systems, these decisions interact. A selected relay may be secure only under certain power levels or antenna configurations. Future research should develop multi-action AI controllers that jointly recommend relay, power, and antenna policies while respecting latency and explainability requirements.

Fifth, the evaluation uses conventional security metrics such as PNSMC and SOPM, supplemented by latency and feature-importance analysis. Future studies should include additional operational metrics, including energy per secure bit, fairness across receivers, resilience under adversarial mobility, computational overhead, and human operator acceptance. A comprehensive evaluation framework would make AI-assisted physical-layer security more comparable across studies.

Table IV. Future research agenda for AI-assisted physical-layer multicast security.

Research Direction	Expected Contribution	Key Challenge
Software-defined radio validation	Tests the framework under real channel measurements	Hardware synchronization and repeatability
Graph neural relay selection	Models source-relay-receiver-eavesdropper topology directly	Explainability and computational overhead
Robust learning under hidden eavesdroppers	Improve security when adversary information is incomplete	Reliable risk estimation from indirect signals
Joint relay-power-antenna optimization	Coordinates multiple physical-layer decisions	High-dimensional action space
6G edge intelligence integration	Embeds relay analytics in future network slices	Latency, privacy, and interoperability

VIII. CONCLUSION

This article developed an AI-assisted relay selection analytics framework for secure wireless multicast networks under multi-eavesdropper conditions. Building on the research direction of PRSF-based secure multicasting and multi-antenna destination cooperation, the article reframed relay selection as a security-aware analytics problem. The proposed framework ranks candidate relays using a composite utility score based on legitimate-channel quality, eavesdropper exposure, destination diversity, receiver scaling, secrecy-rate pressure, and predicted outage risk.

The scenario-based simulation shows that AI-assisted PRSF can improve the estimated probability of non-zero secrecy multicast capacity and reduce secure outage probability compared with random relay assignment and conventional PRSF. The improvement is strongest in medium-SNR and multi-eavesdropper conditions, where relay choice has high security value. Feature-importance analysis confirms that secure multicast relay selection depends on several interacting variables rather than on a single channel indicator.

The broader conclusion is that AI should be used as an assistive and explainable decision layer for physical-layer security, not as an uncontrolled replacement for communication theory. Effective deployment requires latency-aware model design, conservative risk scoring, drift monitoring, fallback rules, and human-readable explanations. For future wireless multicast systems, especially 6G-oriented group communication and edge-

RESEARCH ARTICLE
Vol. 4, No. 1 (2026), pp. 40–55
DOI: 10.63646/jaiaa.2026.040104

intelligent networks, AI-assisted relay selection offers a promising path toward adaptive, scalable, and accountable multicast security.

IX. EXTENDED LITERATURE POSITIONING AND PRACTICAL IMPLICATIONS

The proposed article is positioned at the intersection of physical-layer security, cooperative communication, and AI-assisted wireless analytics. Classical secrecy theory established that the security capacity of a wireless link depends on the difference between the legitimate channel and the wiretap channel (Wyner,1975； Shannon,1949). Later work extended that insight to fading environments and multiuser systems, where spatial diversity and channel variation can be used to improve confidentiality without relying only on cryptographic overhead (Gopala et al.,2008； Csiszar and Korner,1978). The present study follows that intellectual line but adds an analytics layer: the model does not merely ask whether a relay improves channel quality it asks whether the relay improves security under a changing group-receiver and multi-eavesdropper state.

Cooperative relaying has long been recognized as a mechanism for improving reliability and extending coverage in fading channels (Laneman et al.,2004； Bletsas et al.,2006). Physical-layer security research later showed that relay selection can also improve secrecy by choosing paths that strengthen the legitimate side while weakening or avoiding the eavesdropper side (Gopala et al.,2008； Mukherjee et al.,2014). However, many relay-selection rules remain highly stylized. They often assume a limited number of destinations, a known eavesdropper condition, or a simplified ranking variable. The contribution of AI-assisted selection is to treat relay selection as a contextual ranking problem in which several features jointly determine security performance.

The multicast setting is particularly important because the security problem differs from ordinary unicast communication. In unicast communication, the selected relay needs to satisfy one destination. In multicast communication, the selected relay must support a group of legitimate users, and the weakest receiver can constrain the entire secrecy outcome. This feature makes multicast security inherently conservative. Adding more receivers may expand service value, but it also increases the probability that one receiver has a poor channel realization. This logic explains why receiver count appears as a meaningful feature in the proposed model rather than as a background system parameter.

The multi-eavesdropper condition creates a second form of conservatism. When several unauthorized listeners are present, the strongest eavesdropper channel becomes the relevant threat rather than the average eavesdropper channel. This is why the proposed model uses exposure-sensitive features and outage penalties. A relay with strong legitimate-channel quality may still be dangerous when it also creates a strong leakage path. This is consistent with survey findings that physical-layer security must be evaluated under adversarial uncertainty rather than under only average channel quality (Zou et al.,2016； Mukherjee et al.,2014).

The AI component is also consistent with the direction of intelligent wireless networking. Machine learning has been applied to channel estimation, interference management, resource allocation, signal detection, and network control (O'Shea and Hoydis,2017； Ye et al.,2018； Sun et al.,2018). Deep reinforcement learning and neural architectures can be powerful in communication systems, but they also introduce issues of data hunger, latency, and interpretability (Zappone et al.,2019； Mao et al.,2018). For this reason, the present article does not assume that the most complex model is the best model. It favors interpretable ranking and compact ensemble learning because the decision must be made quickly and audited after deployment.

Explainability is not an optional feature in security analytics. A network operator must be able to understand why a relay was selected, why another relay was rejected, and whether the model is emphasizing the right kind of evidence. Model explanation methods such as local surrogate explanations and feature-attribution analysis

RESEARCH ARTICLE
Vol. 4, No. 1 (2026), pp. 40–55
DOI: 10.63646/jaiaa.2026.040104

are useful because they translate a prediction into a reasoned decision narrative (Ribeiro et al.,2016； Lundberg and Lee,2017). In the proposed framework, explanation is tied directly to engineering validation: if the model repeatedly selects relays because of irrelevant features, the deployment team can detect misalignment before security loss becomes severe.

From an application perspective, AI-assisted relay selection is most relevant to multicast services that are group-based, latency-sensitive, and security-sensitive. Examples include factory sensor clusters, remote medical monitoring groups, unmanned vehicle coordination, public-safety broadcast, and collaborative edge intelligence. These settings share a common structure: a source must reach multiple legitimate devices while the wireless medium remains observable. The proposed model is therefore not limited to one application sector. Its analytical logic can be adapted wherever relay diversity, receiver diversity, and eavesdropper exposure interact.

The framework also creates a bridge between communication theory and operational analytics. Communication theory supplies the target concepts, including secrecy capacity, outage probability, fading diversity, and relay advantage. AI analytics supplies adaptive ranking, feature interaction learning, risk scoring, and drift monitoring. Neither side is sufficient alone. A purely theoretical rule may be too rigid under changing operational conditions, while a purely data-driven model may ignore the physical meaning of security. The strongest design is hybrid: theory defines the objective, and AI improves the decision process.

Future 6G systems will increase the relevance of this hybrid design. Emerging networks are expected to include integrated sensing, edge AI, reconfigurable intelligent surfaces, ultra-reliable low-latency communication, and dense device connectivity (Lu and Zheng,2020； Saad et al.,2020； Calvanese Strinati et al.,2019). Under such conditions, a relay-selection mechanism will need to account for context, risk, and resource constraints in real time. The proposed framework should therefore be viewed as an early analytics template for a larger class of security-aware network intelligence systems.

The broader implication is methodological. AI applications should not be evaluated only by whether they increase prediction accuracy. In security-sensitive engineering contexts, the model must also be evaluated by whether it reduces risk, preserves interpretability, operates within latency boundaries, and remains reliable under distribution shift. This article therefore contributes an analytics-oriented manuscript structure: problem translation, feature design, simulation benchmark, interpretability assessment, and deployment governance. Such a structure can be reused for other AI-assisted communication-security problems.

AUTHOR CONTRIBUTIONS

Author	Contribution
Nabila Rahman	Conceptualization, methodology, writing - original draft, visualization
Fahim Ahmed	Simulation design, data curation, formal analysis, validation
Tariq Mahmud	Supervision, resources, writing - review and editing, project administration

DECLARATIONS

Conflicts of interest: The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this manuscript.

Data availability: The simulation configuration, aggregate benchmark tables, and generated scenario summaries are available from the corresponding author upon reasonable request. No personal or proprietary network data is distributed in this article.

Funding: This research received no external funding.

Ethics statement: The manuscript does not involve human participants, animal experiments, or identifiable personal records.

ABOUT THE AUTHORS

Nabila Rahman is affiliated with Jashore University of Science and Technology, Bangladesh. Her research focuses on AI analytics, wireless systems, and secure network intelligence.

Fahim Ahmed is affiliated with Hajee Mohammad Danesh Science and Technology University, Bangladesh. His research interests include cooperative wireless communications, physical-layer security, and simulation-based performance evaluation.

Tariq Mahmud is affiliated with Pabna University of Science and Technology, Bangladesh. His research addresses secure communication systems, machine-learning-assisted network optimization, and dependable multicast services.

REFERENCES

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

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

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

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

Csiszar, I., & Korner, J. (1978). Broadcast channels with confidential messages. IEEE Transactions on Information Theory, 24(3), 339-348. https://doi.org/10.1109/TIT.1978.1055892

Lu, Y. (2019). 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

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

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

Shannon, C. E. (1949). Communication theory of secrecy systems. Bell System Technical Journal, 28(4), 656-715. https://doi.org/10.1002/j.1538-7305.1949.tb00928.x

O'Shea, T. J., & Hoydis, J. (2017). An introduction to deep learning for the physical layer. IEEE Transactions on Cognitive Communications and Networking, 3(4), 563-575. https://doi.org/10.1109/TCCN.2017.2758370

Goldsmith, A. (2005). Wireless Communications. Cambridge University Press. https://doi.org/10.1017/CBO9780511841224

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

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

Ye, H., Li, G. Y., & Juang, B.-H. F. (2018). Power of deep learning for channel estimation and signal detection in OFDM systems. IEEE Wireless Communications Letters, 7(1), 114-117. https://doi.org/10.1109/LWC.2017.2757490

Cover, T. M., & El Gamal, A. A. (1979). Capacity theorems for the relay channel. IEEE Transactions on Information Theory, 25(5),

572-584. https://doi.org/10.1109/TIT.1979.1056084

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

Tse, D., & Viswanath, P. (2005). Fundamentals of Wireless Communication. Cambridge University Press. https://doi.org/10.1017/CBO9780511807213

Sun, H., Chen, X., Shi, Q., Hong, M., Fu, X., & Sidiropoulos, N. D. (2018). Learning to optimize: Training deep neural networks for wireless resource management. IEEE Transactions on Signal Processing, 66(20), 5438-5453. https://doi.org/10.1109/TSP.2018.2866382

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

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

Gopala, P. K., Lai, L., & El Gamal, H. (2008). On the secrecy capacity of fading channels. IEEE Transactions on Information Theory, 54(10), 4687-4698. https://doi.org/10.1109/TIT.2008.928990

Zappone, A., Di Renzo, M., Debbah, M., Lam, T. T., & Qian, X. (2019). Model-aided wireless artificial intelligence: Embedding expert knowledge in deep neural networks for wireless system optimization. IEEE Vehicular Technology Magazine, 14(3), 60-69. https://doi.org/10.1109/MVT.2019.2921612

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

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

Barros, J., & Rodrigues, M. R. D. (2006). Secrecy capacity of wireless channels. IEEE International Symposium on Information Theory, 356-360. https://doi.org/10.1109/ISIT.2006.261613

Mao, Q., Hu, F., & Hao, Q. (2018). Deep learning for intelligent wireless networks: A comprehensive survey. IEEE Communications Surveys & Tutorials, 20(4), 2595-2621. https://doi.org/10.1109/COMST.2018.2846401

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

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

Dong, L., Han, Z., Petropulu, A. P., & Poor, H. V. (2010). Improving wireless physical layer security via cooperating relays. IEEE Transactions on Signal Processing, 58(3), 1875-1888. https://doi.org/10.1109/TSP.2009.2038412

Chen, T., & Guestrin, C. (2016). XGBoost: A scalable tree boosting system. Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 785-794. https://doi.org/10.1145/2939672.2939785

Liang, Y., Poor, H. V., & Shamai, S. (2008). Secure communication over fading channels. IEEE Transactions on Information Theory, 54(6), 2470-2492. https://doi.org/10.1109/TIT.2008.921678

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/10.1080/17517575.2025.2541199

Tekin, E., & Yener, A. (2008). The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming. IEEE Transactions on Information Theory, 54(6), 2735-2751. https://doi.org/10.1109/TIT.2008.921715

Ribeiro, M. T., Singh, S., & Guestrin, C. (2016). Why should I trust you? Explaining the predictions of any classifier. Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 1135-1144. https://doi.org/10.1145/2939672.2939778

Huang, J., & Swindlehurst, A. L. (2011). Robust secure transmission in MISO channels based on worst-case optimization. IEEE Transactions on Signal Processing, 60(4), 1696-1707. https://doi.org/10.1109/TSP.2011.2181666

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

Rudin, C. (2019). Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead. Nature Machine Intelligence, 1, 206-215. https://doi.org/10.1038/s42256-019-0048-x

Wang, X., & Poor, H. V. (2003). Wireless communication systems: Advanced techniques for signal reception. Prentice Hall. https://doi.org/10.1017/S0263574704221137

Lundberg, S. M., & Lee, S.-I. (2017). A unified approach to interpreting model predictions. Advances in Neural Information Processing Systems, 30. https://doi.org/10.48550/arXiv.1705.07874

He, K., Zhang, X., Ren, S., & Sun, J. (2016). Deep residual learning for image recognition. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 770-778. https://doi.org/10.1109/CVPR.2016.90

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

Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., & Bengio, Y. (2014). Generative adversarial nets. Advances in Neural Information Processing Systems, 27. https://doi.org/10.48550/arXiv.1406.2661

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.3109

Breiman, L. (2001). Random forests. Machine Learning, 45, 5-32. https://doi.org/10.1023/A:1010933404324

Calvanese Strinati, E., Barbarossa, S., Gonzalez-Jimenez, J. L., Ktenas, D., Cassiau, N., Maret, L., & Dehos, C. (2019). 6G: The next frontier. IEEE Vehicular Technology Magazine, 14(3), 42-50. https://doi.org/10.1109/MVT.2019.2921162

Friedman, J. H. (2001). Greedy function approximation: A gradient boosting machine. Annals of Statistics, 29(5), 1189-1232. https://doi.org/10.1214/aos/1013203451

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

Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., Kaiser, L., & Polosukhin, I. (2017). Attention is all you need. Advances in Neural Information Processing Systems, 30. https://doi.org/10.48550/arXiv.1706.03762

Saad, W., Bennis, M., & Chen, M. (2020). A vision of 6G wireless systems: Applications, trends, technologies, and open research problems. IEEE Network, 34(3), 134-142. https://doi.org/10.1109/MNET.001.1900287

Kingma, D. P., & Welling, M. (2014). Auto-encoding variational Bayes. Proceedings of the International Conference on Learning Representations. https://doi.org/10.48550/arXiv.1312.6114

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). https://doi.org/10.1080/17517575.2024.2397630

Mnih, V., Kavukcuoglu, K., Silver, D., Rusu, A., Veness, J., Bellemare, M., Graves, A., Riedmiller, M., Fidjeland, A. K., Ostrovski, G., Petersen, S., Beattie, C., Sadik, A., Antonoglou, I., King, H., Kumaran, D., Wierstra, D., Legg, S., & Hassabis, D. (2015). Human-level control through deep reinforcement learning. Nature, 518, 529-533. https://doi.org/10.1038/nature14236

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). https://doi.org/10.1080/17517575.2024.2448003

Schulman, J., Wolski, F., Dhariwal, P., Radford, A., & Klimov, O. (2017). Proximal policy optimization algorithms. arXiv preprint arXiv:1707.06347. https://doi.org/10.48550/arXiv.1707.06347

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

Doshi-Velez, F., & Kim, B. (2017). Towards a rigorous science of interpretable machine learning. arXiv preprint arXiv:1702.08608. https://doi.org/10.48550/arXiv.1702.08608

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

Silver, D., Huang, A., Maddison, C. J., Guez, A., Sifre, L., Van Den Driessche, G., Schrittwieser, J., Antonoglou, I., Panneershelvam, V., Lanctot, M., Dieleman, S., Grewe, D., Nham, J., Kalchbrenner, N., Sutskever, I., Lillicrap, T., Leach, M., Kavukcuoglu, K., Graepel, T., & Hassabis, D. (2016). Mastering the game of Go with deep neural networks and tree search. Nature, 529, 484-489. https://doi.org/10.1038/nature16961

Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. Journal of Network and Computer Applications, 60, 19-31. https://doi.org/10.1016/j.jnca.2015.11.016

LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. Nature, 521, 436-444. https://doi.org/10.1038/nature14539

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

Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153-1176. https://doi.org/10.1109/COMST.2015.2494502

Hochreiter, S., & Schmidhuber, J. (1997). Long short-term memory. Neural Computation, 9(8), 1735-1780. https://doi.org/10.1162/neco.1997.9.8.1735

Diro, A. A., & Chilamkurti, N. (2018). Distributed attack detection scheme using deep learning approach for Internet of Things. Future Generation Computer Systems, 82, 761-768. https://doi.org/10.1016/j.future.2017.08.043

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

Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. IEEE Symposium on Security and Privacy, 305-316. https://doi.org/10.1109/SP.2010.25

Jiang, W., Han, B., Habibi, M. A., & Schotten, H. D. (2021). The road towards 6G: A comprehensive survey. IEEE Open Journal of the Communications Society, 2, 334-366. https://doi.org/10.1109/OJCOMS.2021.3057679

Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. IEEE Transactions on Emerging Topics in Computational Intelligence, 2(1), 41-50. https://doi.org/10.1109/TETCI.2017.2772792

Zappone, A., Di Renzo, M., & Debbah, M. (2020). Wireless networks design in the era of deep learning: Model-based, AI-based, or both? IEEE Transactions on Communications, 67(10), 7331-7376. https://doi.org/10.1109/TCOMM.2019.2924010

Goodfellow, I. J., Shlens, J., & Szegedy, C. (2015). Explaining and harnessing adversarial examples. International Conference on Learning Representations. https://doi.org/10.48550/arXiv.1412.6572

Li, B., Fei, Z., & Zhou, C. (2018). Physical-layer security in space information networks: A survey. IEEE Internet of Things Journal, 7(1), 33-52. https://doi.org/10.1109/JIOT.2019.2943900

Sutton, R. S., & Barto, A. G. (2018). Reinforcement Learning: An Introduction. MIT Press. https://doi.org/10.7551/mitpress/10859.001.0001

You, X., Wang, C.-X., Huang, J., Gao, X., Zhang, Z., Wang, M., Huang, Y., Zhang, C., Jiang, Y., Wang, J., Zhu, M., Sheng, B., Wang, D., Pan, Z., Zhu, P., Yang, Y., Liu, Z., & Zhang, P. (2021). Towards 6G wireless communication networks: Vision, enabling technologies, and new paradigm shifts. Science China Information Sciences, 64, 110301. https://doi.org/10.1007/s11432-020-2955-6

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

Lu, Y. (2017). 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

Lu, Y. (2017). 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

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

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

Yin, S., Ding, S. X., Xie, X., & Luo, H. (2014). A review on basic data-driven approaches for industrial process monitoring. IEEE Transactions on Industrial Electronics, 61(11), 6418-6428. https://doi.org/10.1109/TIE.2014.2301773

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. Computer Networks, 54(15), 2787-2805. https://doi.org/10.1016/j.comnet.2010.05.010