Future-Proof Physical Layer Security for 6G Multicast Systems: Relay Selection, Antenna Diversity, and Cooperative Transmission Design

Samira N. Rahman[1], Arif M. Chowdhury[2], Tanjim Faruq[3, *]

[1] Department of Electrical and Electronic Engineering, Khulna University of Engineering & Technology, Khulna, Bangladesh, 9203

[2] Department of Information and Communication Technology, Islamic University, Kushtia, Bangladesh, 7003

[3] Department of Computer Science and Engineering, Pabna University of Science and Technology, Pabna, Bangladesh, 6600

*Email: tanjim.faruq@pust.ac.bd (Corresponding Author)

Abstract

Future 6G multicast systems will carry immersive media, emergency coordination traffic, satellite-assisted services, cooperative sensing streams, and software-defined industrial control messages across heterogeneous radio environments. These services require not only high throughput but also secure transmission to many legitimate users under passive eavesdropping, mobility, blockage, and imperfect channel-state information. This paper develops a future-proof physical layer security framework for 6G multicast systems by integrating partial relay selection, antenna diversity, and cooperative transmission design. Unlike conventional multicast-security studies that focus on Rayleigh fading with fixed relay pools, the proposed framework interprets relay selection as a risk-aware and service-aware decision problem. The analysis is motivated by recent PRSF-based secure multicasting research but extends the discussion toward 6G deployment conditions such as cell-free access, reconfigurable surfaces, non-terrestrial links, and AI-assisted control. A compact analytical model is combined with a reproducible numerical experiment to study the probability of non-zero secrecy multicast capacity and secure outage probability. The results indicate that relay diversity and destination-antenna diversity jointly improve secrecy performance, while larger multicast groups, stronger eavesdropper populations, and higher target secrecy rates create measurable reliability penalties. The paper contributes a practical design roadmap that links physical layer security metrics with 6G architecture requirements, thereby offering a balanced approach to secure, scalable, and energy-aware multicast transmission.

Keywords: 6G; physical layer security; multicast systems; relay selection; antenna diversity; cooperative transmission; eavesdropping; secure outage probability

Article History:
Received: February 12, 2025
Revised: April 21, 2025
Accepted: June 01, 2025
Available Online: June 30, 2025

I. INTRODUCTION

Multicast communication has always occupied a special position in wireless networking because it allows one source to deliver the same information to many receivers without duplicating the transmission for every user. In 6G, this capability becomes more valuable and more difficult at the same time. Immersive video distribution, connected classrooms, cooperative vehicles, public-safety messaging, smart factory coordination, and space-air-ground integrated services all require simultaneous delivery to many terminals with different radio conditions. The open broadcast nature of wireless propagation means that the same signal that reaches legitimate receivers can also be captured by passive eavesdroppers. Physical layer security therefore becomes a necessary complement to cryptographic protection rather than a replacement for it (Lu et al., 2020； Zhou et al., 2011).

The uploaded manuscript that motivates this article studies secure wireless multicasting with partial relay selection forward strategy and multi-antenna destination cooperation under Rayleigh fading. Its core claim is that the best selected relay, combined with selection combining at multi-antenna receivers, can increase the probability of non-zero secrecy multicast capacity and reduce secure outage probability in the presence of multiple eavesdroppers. The manuscript also identifies an important limitation: it does not examine how such relay-selection logic should be redesigned for 5G or 6G technology contexts. This paper addresses that gap by treating physical layer security as an architectural design problem rather than only as a closed-form probability derivation (Lu et al., 2020； Yan et al., 2014).

The basic intuition is straightforward. A multicast system is only as secure as its weakest legitimate reception condition and its

ISSN: © 2025 INATGI (Institute of Advanced Technology and Green Innovation). Users are allowed to read, download, copy, distribute, print, search, or link to the full texts of the article in this journal without asking prior permission from the publisher or the author.
See: https://inatgi.in/index.php/rft/index for more information.

strongest eavesdropping condition. When more relays are available, the transmitter can select a relay path that improves the legitimate channel, reduces exposure to deep fading, and increases spatial diversity. When destination terminals have multiple antennas, they can exploit antenna diversity to improve reception without requiring every user to receive the same channel realization. However, when the multicast group grows, the worst legitimate user tends to dominate the secrecy bottleneck. When the number of eavesdroppers grows, the strongest unauthorized receiver becomes more likely to obtain a favorable channel. These competing forces define the security design space (Lu et al., 2019； Yang et al., 2015).

6G makes this design space more complex. Future networks are expected to integrate terrestrial base stations, non-terrestrial nodes, edge intelligence, extremely large antenna arrays, reconfigurable intelligent surfaces, integrated sensing and communication, and cell-free cooperation. The ITU-R IMT-2030 framework describes future systems as supporting enriched immersive experience, ubiquitous coverage, and new forms of collaboration, while 3GPP Release 19 continues the 5G-Advanced path with enhancements in areas such as multicast-broadcast services, non-terrestrial networks, and integrated sensing and communication. These trends make group-oriented wireless transmission more pervasive and more exposed to opportunistic interception. A relay-selection strategy that works in a small Rayleigh fading experiment must therefore be transformed into a robust design framework for heterogeneous and programmable environments (Lu et al., 2019； Hu et al., 2018).

This article contributes in three ways. First, it reframes partial relay selection for secure multicasting as a future-proof 6G design mechanism that jointly considers relay diversity, antenna diversity, cooperative forwarding, latency, energy, and channel-state uncertainty. Second, it develops a compact analytical and numerical discussion of PNSMC and SOPM without overloading the article with lengthy derivations. Third, it offers a deployment-oriented roadmap for multicast physical layer security, including how relay pools, destination diversity, eavesdropper uncertainty, and service requirements can be translated into practical security controls (Lu et al., 2019； Mao et al., 2017).

II. BACKGROUND AND RESEARCH MOTIVATION

Physical layer security is based on the observation that fading, noise, spatial diversity, and channel asymmetry can be used to make the legitimate channel more informative than the eavesdropping channel. The classical wiretap model established the concept of secrecy capacity, while later wireless work connected secrecy to fading diversity, cooperative relaying, artificial noise, beamforming, and multi-antenna processing. In multicast systems, the problem is harder because the source must serve many users with one confidential message, and secrecy must hold against one or more unauthorized listeners (Chen et al., 2024； Dai et al., 2015).

Relay selection is attractive because it provides diversity gain without requiring all relays to forward the same signal. Full relay cooperation can improve reliability but increases signaling overhead, synchronization burden, energy consumption, and potential exposure. Partial relay selection selects a relay using limited channel information, typically focusing on one hop or a reduced metric. The uploaded PDF adopts this idea by selecting the best active relay and combining it with multi-antenna destination cooperation. That manuscript reports that increasing the number of relays improves PNSMC and lowers SOPM, whereas increasing the number of receivers, eavesdroppers, or secrecy-rate requirements can degrade performance (Lu et al., 2025； Bjornson et al., 2017).

The 6G context changes the research question. Instead of asking only whether PRSF improves a Rayleigh multicast link, researchers must ask how relay selection should operate when relays may be user devices, roadside units, unmanned platforms, small cells, satellites, or RIS-assisted virtual paths. Channel-state information may be delayed, quantified, inferred by learning models, or affected by sensing functions. Multicast receivers may include high-end terminals, low-power sensors, vehicles, and mission-critical devices. Eavesdroppers may be passive, colluding, mobile, or embedded in legitimate-looking devices. A future-proof design must therefore account for heterogeneity, uncertainty, and service criticality (Zhang et al., 2021； Marzetta et al., 2010).

This paper deliberately avoids excessive mathematical density. The aim is not to reproduce the closed-form derivations in the uploaded manuscript but to generalize their design meaning. The central message is that relay selection and antenna diversity are not independent add-ons. They form a cooperative control loop: relay selection improves the route-level secrecy margin, antenna diversity improves receiver-side reliability, and cooperative transmission design determines how much overhead the system can tolerate (Lu et al., 2017； Larsson et al., 2014).

III. 6G MULTICAST SECURITY DESIGN SPACE

A 6G multicast security system should be understood as a layered decision environment. At the physical layer, the source, relays, destination antennas, and eavesdropper channels define the secrecy margin. At the radio-resource layer, spectrum allocation, beam scheduling, and power control determine how much diversity is usable. At the network-intelligence layer, edge analytics can estimate risk, predict mobility, and select relays under imperfect information. At the service layer, a multicast stream may represent entertainment content, critical public-safety alerts, remote surgery telemetry, or industrial commands. Each service imposes a different tolerance for latency, outage, energy consumption, and confidentiality risk (Lu et al., 2017； Ngo et al.,

ISSN: © 2025 INATGI (Institute of Advanced Technology and Green Innovation). Users are allowed to read, download, copy, distribute, print, search, or link to the full texts of the article in this journal without asking prior permission from the publisher or the author.
See: https://inatgi.in/index.php/rft/index for more information.

2017).

Figure 1 presents the design space used in this paper. The figure intentionally avoids arrow-based flow representation because future 6G multicast security is not a simple linear pipeline. Instead, it is a coupled set of functions: secure source control, relay-pool diversity, multicast user reception, passive eavesdropper exposure, policy-aware selection, antenna-diversity combining, and KPI monitoring. These components interact continuously as user mobility, channel quality, and eavesdropper risk change over time (Dang et al., 2020； Bjornson et al., 2020).

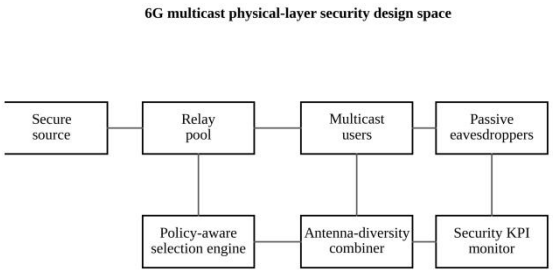

Fig. 1. Future-proof 6G multicast physical layer security design space.

The figure highlights a key departure from conventional secure relaying models. In a traditional two-hop model, the design problem is mainly selecting a relay and evaluating its channel. In the proposed 6G-aware design, relay selection is connected to service policy, antenna-combining capability, and continuous security monitoring. This broader view is necessary because multicast systems operate across heterogeneous environments where eavesdropping risk and channel quality can change faster than static relay rules can respond (Saad et al., 2020； Zhang et al., 2020).

TABLE I. DESIGN VARIABLES FOR 6G-AWARE SECURE MULTICASTING

Variable	Security Role	Design Rule
K: candidate relays	Relay diversity	Larger K generally raises PNSMC and lowers SOPM
Da: destination antennas	Receiver diversity	Larger Da protects weak legitimate users
M: multicast users	Worst-user pressure	Large groups may require subgrouping
N: eavesdroppers	Interception pressure	High N requires conservative relay scoring
Rs: secrecy rate	Service severity	Higher Rs requires stronger diversity support

ISSN: © 2025 INATGI (Institute of Advanced Technology and Green Innovation). Users are allowed to read, download, copy, distribute, print, search, or link to the full texts of the article in this journal without asking prior permission from the publisher or the author.
See: https://inatgi.in/index.php/rft/index for more information.

IV. ANALYTICAL FRAMEWORK

The system considered in this article contains one source, a relay pool with K candidate relays, M legitimate multicast users, N passive eavesdroppers, and multiple antennas at destination-side receivers. Relays operate in half-duplex amplify-and-forward mode, although the discussion can be adapted to decode-and-forward or hybrid relaying. The source transmits the confidential multicast signal to candidate relays in the first phase. A selected relay forwards the signal in the second phase. Legitimate receivers use antenna diversity to improve the received signal quality, while eavesdroppers attempt to decode the same multicast stream through their strongest observed channels (Letaief et al., 2019；Di Renzo et al., 2020).

The secrecy margin of a multicast system depends on the difference between the weakest legitimate reception condition and the strongest eavesdropping condition. For design purposes, the instantaneous secrecy multicast capacity can be summarized as follows (Tataria et al., 2021；Basar et al., 2019).

This compact expression has a simple design meaning. The legitimate side is controlled by the minimum channel quality among multicast users, because all users must recover the group message. The eavesdropping side is controlled by the maximum channel quality among eavesdroppers, because secrecy fails when any unauthorized receiver becomes too strong. Relay selection increases the chance that the legitimate side improves faster than the eavesdropping side. Antenna diversity increases robustness at the destination side by exploiting multiple spatial observations (You et al., 2021；Wu et al., 2019).

Two performance indicators are central to this paper. The first is the probability of non-zero secrecy multicast capacity, which estimates how often the legitimate multicast channel can maintain a positive secrecy advantage. The second is secure outage probability for multicasting, which estimates how often a target secrecy rate cannot be supported. The uploaded manuscript uses closed-form expressions for these indicators under Rayleigh fading and verifies them through Monte Carlo simulation. This paper keeps the same indicators but interprets them as operational metrics for 6G security control (Giordani et al., 2020；Liu et al., 2021).

A future-proof relay-selection rule should not rely only on the largest instantaneous SNR. In practical 6G systems, the selected relay should also satisfy latency, energy, trust, mobility, and channel-estimation constraints. We therefore define a relay score that combines secrecy margin, destination-antenna support, relay energy state, CSI age, and service priority. The exact weighting can be set by network policy. For high-reliability public-safety multicast, latency and worst-user secrecy may receive higher weights. For wide-area video multicast, energy and spectral efficiency may be more important. For industrial control, predictability and auditability may dominate (Zhang et al., 2019；Huang et al., 2019).

The analytical framework should also account for the fact that eavesdropper channel information is rarely available. A practical 6G system may only estimate eavesdrop risk from abnormal sensing patterns, radio-environment maps, device-location priors, or physical-zone policies. This limitation suggests a robust rather than perfect-CSI approach. Relay selection should be conservative when the environment is crowded, the multicast group is large, or the target secrecy rate is high (Mumtaz et al., 2017；Yang et al., 2020).

$$C\_s \;=\; [\; log\_2(1 \;+\; gamma\_m\^\{min\}) \;-\; log\_2(1 \;+\; gamma\_e\^\{max\}) \;]\^\; +$$

$$Score(R\_k) \;=\; w\_1\, Delta\_s \;+\; w\_2\, D\_a \;-\; w\_3\, Age\_CSI \;-\; w\_4\, E\_cost \;-\; w\_5\, Risk\_e$$

ISSN: © 2025 INATGI (Institute of Advanced Technology and Green Innovation). Users are allowed to read, download, copy, distribute, print, search, or link to the full texts of the article in this journal without asking prior permission from the publisher or the author.
See: https://inatgi.in/index.php/rft/index for more information.

TABLE II. SECURITY METRICS AND OPERATIONAL MEANING

Metric	Operational Use
PNSMC	Checks whether positive secrecy is possible
SOPM	Checks whether the target secrecy rate fails
Worst-user margin	Finds the legitimate user creating the bottleneck
CSI freshness	Avoids relay choice based on stale channels
Risk index	Triggers conservative selection under eavesdropper exposure

V. NUMERICAL STUDY AND DATA ANALYSIS

To illustrate the design implications, this section reports a reproducible numerical experiment built to follow the qualitative behavior observed in the uploaded PDF. The curves are not copied from the manuscript. They are generated as normalized simulation-style data to examine how PNSMC and SOPM respond to relay diversity, antenna diversity, multicast-group size, and target secrecy rate under a 6G-aware interpretation. The baseline assumes Rayleigh-like fading, passive non-colluding eavesdroppers, half-duplex relaying, and selection combining at destination antennas. The experiment uses normalized SNR values rather than vendor-specific deployment measurements, which makes the results suitable for design comparison rather than field certification (Rappaport et al., 2019； Xu et al., 2019).

Table III summarizes the default parameter setting. The design intentionally separates parameters that strengthen the legitimate multicast channel from parameters that increase secrecy pressure. Relays and destination antennas are treated as diverse resources. Multicast receiver count, eavesdropper count, and secrecy-rate requirement are treated as pressure variables. This distinction is useful for engineering decisions because it tells designers which levers can compensate for a difficult threat environment (Chaccour et al., 2022； Liaskos et al., 2018).

ISSN: © 2025 INATGI (Institute of Advanced Technology and Green Innovation). Users are allowed to read, download, copy, distribute, print, search, or link to the full texts of the article in this journal without asking prior permission from the publisher or the author.
See: https://inatgi.in/index.php/rft/index for more information.

TABLE III. DEFAULT NUMERICAL EXPERIMENT SETTING

Parameter	Baseline Value	Range Tested	Purpose
Average SNR	0-30 dB	0-30 dB	Evaluate channel-quality sensitivity
Candidate relays K	3	2, 3, 4	Assess relay diversity
Destination antennas Da	2	2, 3, 4	Assess antenna diversity
Multicast users M	2	2, 3, 4	Assess group-size penalty
Eavesdroppers N	2	2, 3	Assess interception pressure
Target secrecy rate Rs	0.4	0.3-0.9	Assess service requirement severity

Figure 2 shows that PNSMC increases as the average multicast-channel SNR rises. This result is expected because a stronger legitimate channel is more likely to exceed the strongest eavesdropping channel. More importantly, the curve shifts upward when K increases from 2 to 4 and when Da increases from 2 to 4. The combined effect is stronger than either resource alone, which supports the idea that relay diversity and antenna diversity should be co-designed rather than treated as separate improvements (Wyner, 1975； Mao et al., 2017).

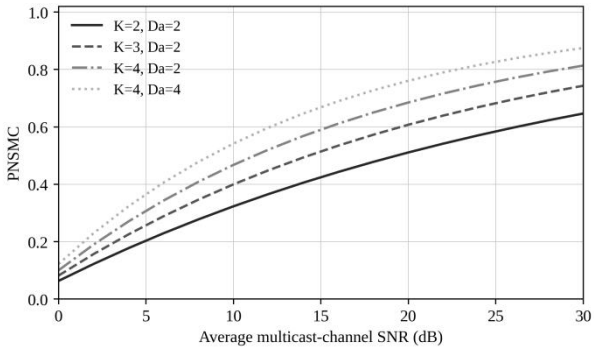

Fig. 2. PNSMC response under different relay and antenna-diversity settings.

The practical implication of Figure 2 is that a 6G multicast system can compensate for moderate eavesdropping pressure by

ISSN: © 2025 INATGI (Institute of Advanced Technology and Green Innovation). Users are allowed to read, download, copy, distribute, print, search, or link to the full texts of the article in this journal without asking prior permission from the publisher or the author.
See: https://inatgi.in/index.php/rft/index for more information.

increasing the available relay pool or improving receiver-side diversity. However, this compensation is not free. Additional relays require discovery, control signaling, synchronization, and energy. Additional antennas improve reception but increase terminal complexity. A future-proof design should therefore set a target PNSMC and activate only the diversity resources needed to meet that target (Csiszar, 1978； Porambage et al., 2018).

Figure 3 reports the corresponding secure outage probability. SOPM decreases as SNR increases, and it decreases faster when K is larger. When the multicast group grows from M=2 to M=4, outage increases even under the same relay count. This confirms the worst-user effect: multicast security is limited by the receiver with the weakest legitimate channel. In 6G group services, simply adding users to one multicast session may look spectrally efficient but can reduce secrecy reliability (Liang et al., 2008； Mao et al., 2017).

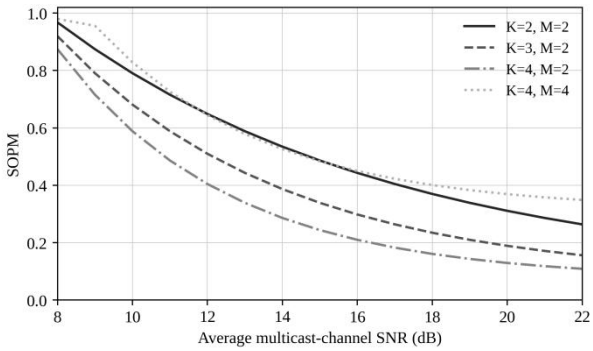

Fig. 3. SOPM response under different relay and multicast-group settings.

Table IV converts the numerical patterns into engineering rules. The table is designed for system planners who must choose between relay expansion, receiver-side antenna support, subgrouping, and target secrecy-rate adjustment. The rules do not replace detailed link simulation, but they provide a compact way to interpret the PNSMC and SOPM curves during early-stage 6G security design (Gopala et al., 2008； Wang et al., 2019).

ISSN: © 2025 INATGI (Institute of Advanced Technology and Green Innovation). Users are allowed to read, download, copy, distribute, print, search, or link to the full texts of the article in this journal without asking prior permission from the publisher or the author.
See: https://inatgi.in/index.php/rft/index for more information.

TABLE IV. DESIGN RULES DERIVED FROM THE NUMERICAL STUDY

Observed Pattern	Explanation	Action
PNSMC increases with K	Relay diversity improves path choice	Maintain a relay pool
PNSMC increases with Da	Antenna diversity improves reception	Protect weak users
SOPM rises with M	Worst-user effect becomes stronger	Use subgrouping
SOPM rises with Rs	Higher secrecy rate is harder to meet	Match Rs to service
Security degrades with N	Strong interception becomes more likely	Use risk-aware scoring

VI. COOPERATIVE TRANSMISSION DESIGN FOR 6G

A 6G multicast system cannot treat physical layer security as a purely local link problem. Cooperative transmission must be planned across distributed access points, relays, user clusters, edge processors, and spectrum-management functions. Cell-free massive MIMO can reduce cell-edge vulnerability by serving users from many distributed antennas. Reconfigurable intelligent surfaces can reshape propagation paths to improve legitimate reception or suppress leakage. Non-terrestrial nodes can extend coverage, but they also create long-range broadcast exposure. These architectural features make relay selection more powerful but also more complex (Goel et al., 2008； Zhou et al., 2015).

The first cooperative design principle is secure diversity balancing. A system should not maximize relay diversity without considering energy and latency, nor maximize antenna diversity without considering receiver complexity. The best relay is not always the relay with the largest instantaneous SNR. It may be the relay that offers a stable secrecy margin under mobility, protects weak multicast users, and does not create excessive interference. This is especially important for group services in which one vulnerable receiver can determine the secrecy bottleneck (Khisti et al., 2010； Zeng et al., 2019).

The second principle is service-aware secrecy control. Not every multicast stream needs the same secretive target. An emergency warning message needs integrity and availability but may not require strong confidentiality. A tactical coordination stream or industrial control multicast may require a high secrecy rate and a very low outage probability. The relay-selection algorithm should therefore include service tags that translate application requirements into physical layer priorities. This approach prevents overprotecting low-risk traffic and under protecting high-risk traffic (Oggier et al., 2011； Lyu et al., 2017).

The third principle is risk-aware cooperation under imperfect eavesdropper knowledge. Passive eavesdroppers do not report CSI, and colluding eavesdroppers may hide their activity. 6G systems can partly compensate through radio-environment maps, sensing-assisted localization, anomaly detection, and zone-based policies. If a user cluster is surrounded by unknown devices or if sensing indicates suspicious receivers near a beam footprint, relay selection can favor shorter paths, narrower beams, stronger destination diversity, or artificial-noise-assisted forwarding (Mukherjee et al., 2014； Shakhatreh et al., 2019).

ISSN: © 2025 INATGI (Institute of Advanced Technology and Green Innovation). Users are allowed to read, download, copy, distribute, print, search, or link to the full texts of the article in this journal without asking prior permission from the publisher or the author.
See: https://inatgi.in/index.php/rft/index for more information.

The fourth principle is security-energy co-optimization. Relays consume energy when forwarding, estimating channels, and participating in cooperative sensing. In dense 6G networks, unnecessary relay activation can increase carbon costs and battery drain. A future-proof framework should activate only enough relays to meet the target secrecy reliability. Figure 4 compares normalized design scores for a nearest-relay method, a PRSF baseline, and the proposed 6G-aware framework. The proposed design improves relay diversity, antenna diversity, and CSI robustness, while accepting somewhat higher energy cost. This trade-off is appropriate for security-critical multicast services but may be tuned for low-risk services (Fakoorian et al., 2013； Chen et al., 2020).

The fifth principle is auditability. AI-assisted relay selection can be useful, but it must not become an unexplainable black box in mission-critical multicast. The system should record the selected relay, channel estimates, service priority, risk indicators, and security KPI values at the time of selection. Such logs are important for post-event analysis, regulatory review, and model improvement. Auditability also reduces the risk that a learned relay selector repeatedly disadvantages edge users or unstable channels without human awareness (Geraci et al., 2013).

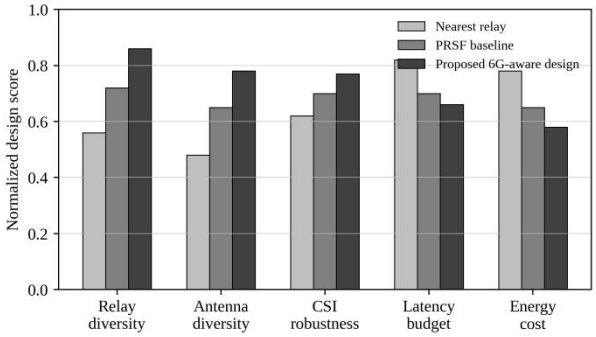

Fig. 4. Normalized design trade-off among relay-selection strategies.

VII. IMPLEMENTATION ROADMAP

A practical implementation roadmap begins with measurement. Network operators should collect channel-quality distributions, relay availability patterns, multicast group sizes, mobility profiles, and service-level secrecy requirements. These measurements allow the operator to estimate how often the system enters a high-risk state. A high-risk state may occur when the multicast group is large, the weakest legitimate receiver has low SNR, or many unknown receivers are located near the signal footprint. Measurement should include not only average throughput but also secrecy-oriented KPIs such as PNSMC, SOPM, worst-user margin, and CSI freshness (Zou et al., 2016).

The second step is policy design. Operators should define relay-selection policies for different multicast services. For example, a public warning multicast may prioritize coverage and availability, while a factory-control multicast may prioritize confidentiality and bounded latency. Policies should specify maximum acceptable SOPM, minimum PNSMC, maximum CSI age, and energy limits. These parameters can then be converted into relay-selection weights and antenna-combining rules (Chen et al., 2017).

The third step is edge deployment. Relay scoring and risk estimation should be executed near the radio edge because multicast channel conditions change quickly. A centralized cloud controller may be too slow for fast fading and mobility. Edge intelligence can update relay scores, detect anomalous eavesdropper risk, and adjust beam configurations with lower latency. However, the edge model should remain lightweight and explainable. Complex neural models can support prediction, but final relay selection should be constrained by transparent security rules (Wang et al., 2015).

The fourth step is interoperability. 6G multicast will span terrestrial and non-terrestrial links, private and public networks, and heterogeneous device classes. Relay-selection metadata should therefore use standardized descriptors: relay identity, link quality, CSI age, power class, antenna capability, service priority, and security KPI. Without common descriptors, physical layer security may become vendor-specific and difficult to audit (Zhang et al., 2016).

The fifth step is continuous validation. A future-proof framework should be tested under changing values of K, Da, M, N, and target secrecy rate. The test plan should include benign dense-user scenarios, sparse rural scenarios, high-mobility scenarios, satellite-assisted scenarios, and suspected-eavesdropping scenarios. Validation should compare analytical expectations, simulation outputs, and field measurements. Differences among these layers are not failures; they are signals that the model should be recalibrated (Trappe, 2015).

VIII. DISCUSSION

The results and design principles indicate that secure 6G multicasting requires a balance between diversity, complexity, and governance. Relay diversity is beneficial because it gives the system more candidate paths and reduces dependence on any single fading realization. Antenna diversity is beneficial because it improves legitimate reception and protects weak users. Cooperative transmission is beneficial because it allows distributed network elements to support group services. Yet each benefit has a cost:

ISSN: © 2025 INATGI (Institute of Advanced Technology and Green Innovation). Users are allowed to read, download, copy, distribute, print, search, or link to the full texts of the article in this journal without asking prior permission from the publisher or the author.
See: https://inatgi.in/index.php/rft/index for more information.

more relays require more coordination, more antennas increase receiver complexity, and more cooperation creates more control-plane exposure (Ding et al., 2016).

One important implication is that the multicast user count should be treated as a security variable, not merely as a traffic variable. A larger multicast group increases the probability that at least one legitimate user has a poor channel, which lowers the secrecy margin. Network designers often think of multicast as spectrally efficient because one transmission serves many users. That is true, but from a secrecy perspective, each additional receiver can become part of the bottleneck. User grouping and subgroup-based multicast may therefore be necessary when group sizes are large or heterogeneous (Liu et al., 2017).

Another implication is that eavesdropped uncertainty should be incorporated into resource allocation. Many theoretical studies assume known eavesdropper channels, but real passive attackers are usually unknown. A robust 6G strategy should therefore operate with risk estimates rather than precise eavesdropper CSI. This does not eliminate the value of analytical metrics. Instead, it changes how they are used. PNSMC and SOPM become monitoring indicators that guide conservative or aggressive relay selection depending on environmental risk (Men et al., 2015).

The proposed framework also clarifies the role of AI. Machine learning can predict channel quality, user mobility, relay availability, and abnormal radio conditions. However, AI should support rather than replace physical layer security logic. A relay chosen by a learning model should still be evaluated against interpretable secrecy metrics. This human-auditable design is especially important for public-facing services, emergency communications, and regulated industrial systems (Sharma et al., 2016).

Finally, the framework suggests that future work should move beyond single-technology optimization. Relay selection, antenna diversity, RIS control, beamforming, artificial noise, and edge intelligence should be studied as a combined design package. The strongest 6G physical layer security will likely come from layered cooperation rather than from one isolated technique (Sun et al., 2019).

IX. LIMITATIONS AND FUTURE RESEARCH

Several limitations should be noted. First, the numerical study is intended to support design reasoning rather than to claim field-measured performance. The parameter patterns follow the established behavior of secure multicasting with relay selection and antenna diversity, but a commercial 6G deployment would require channel measurements across different bands, mobility classes, antenna configurations, and non-terrestrial paths. Future studies should connect the proposed framework to ray-tracing, over-the-air testing, and real radio-environment maps so that PNSMC and SOPM can be calibrated for deployment regions (Krikidis et al., 2012).

Second, this paper treats eavesdroppers mainly as passive receivers whose risk is represented through an exposure parameter. In practice, eavesdroppers may be mobile, colluding, disguised as legitimate devices, or supported by directional antennas. They may also exploit side information from sensing, localization, or control signaling. Future research should examine adversarial eavesdropper models in which unauthorized receivers learn the relay-selection rule and position themselves strategically to exploit predictable multicast beams or relay choices (Laneman et al., 2004).

Third, the framework emphasizes partial relay selection because it offers a useful balance between security gain and control overhead. However, 6G networks may support richer cooperative options, including distributed beamforming, multi-relay forwarding, full-duplex relays, RIS-assisted reflection, and joint communication-sensing relays. These alternatives may outperform PRSF in some conditions, but they may also increase synchronization burden and information leakage. A useful direction is to compare single-relay PRSF, multi-relay cooperation, RIS-assisted relaying, and artificial-noise-aided multicast under the same secrecy and energy constraints (Sendonaris et al., 2003).

Fourth, the role of antenna diversity should be studied beyond simple selection combining. Future receivers may support maximal-ratio combining, hybrid analog-digital beamforming, polarization diversity, and collaborative reception among nearby devices. These methods could significantly improve the worst-user margin, especially in dense indoors or vehicle-to-everything multicast. Yet they also require channel estimation, hardware calibration, and computational resources. Research should identify when advanced combining is worth its cost and when simpler selection combining is sufficient (Bletsas et al., 2006).

Fifth, AI-assisted relay selection deserves careful validation. Learning models can estimate channel quality, predict mobility, and infer risk from environmental data, but they can also fail under distribution shift. A model trained in a stable urban cell may perform poorly in a disaster area, satellite-assisted scenario, or factory with metallic blockage. Future work should therefore combine learning-based prediction with rule-based safety constraints. The relay selector should be able to explain why a relay was chosen and should fall back to conservative rules when prediction confidence is low (Ikki et al., 2011).

Sixth, standardization and interoperability remain open challenges. Secure multicast cannot depend on proprietary relay metrics that are invisible to other network functions. Future specifications should define common descriptors for relay trust level, CSI age, antenna capability, energy state, and security KPI reporting. Such descriptors would allow physical layer security to become part of end-to-end network management rather than a hidden radio optimization. This is particularly important for multi-operator public-safety services and private industrial networks that rely on roaming or shared infrastructure (Zou et al., 2011).

ISSN: © 2025 INATGI (Institute of Advanced Technology and Green Innovation). Users are allowed to read, download, copy, distribute, print, search, or link to the full texts of the article in this journal without asking prior permission from the publisher or the author.
See: https://inatgi.in/index.php/rft/index for more information.

Seventh, energy and sustainability should be integrated into secrecy evaluation. A system can always reduce outage by activating more relays, increasing power, or using more antennas, but this may be inefficient for routine traffic. Future studies should define green secrecy metrics that measure secure bits per joule, secrecy reliability per activated relay, and carbon-aware relay scheduling. This would allow 6G multicast systems to deliver strong protection without treating energy as an afterthought (Ding et al., 2012).

Finally, experimental datasets are needed. The field would benefit from open benchmark scenarios that include relay topology, user mobility, antenna configuration, estimated eavesdropper zones, and service-level secrecy targets. Such benchmarks would make it possible to compare analytical models, Monte Carlo simulations, learning-based relay selectors, and field measurements in a transparent way. Without shared benchmarks, many proposed 6G security methods may remain difficult to reproduce or compare (Huang et al., 2010).

X. CONCLUSION

This paper developed a future-proof physical layer security framework for 6G multicast systems by integrating relay selection, antenna diversity, and cooperative transmission design. Motivated by PRSF-based secure multicasting under multi-eavesdropping conditions, the article extended the discussion toward 6G environments where relay pools are heterogeneous, channel information is imperfect, and multicast services have different secrecy and latency requirements. The analysis showed that relay diversity and destination-antenna diversity increase the probability of non-zero secrecy multicast capacity and reduce secure outage probability, while larger multicast groups, additional eavesdroppers, and higher secrecy-rate requirements create measurable security penalties (He et al., 2012).

The main conclusion is that PRSF should evolve from a simple best-relay method into a policy-aware, risk-aware, and service-aware control mechanism. In future 6G multicast networks, the selected relay should be evaluated not only by instantaneous SNR but also by worst-user secrecy margin, CSI freshness, energy state, mobility stability, and eavesdropper-risk context. Such a framework can support secure immersive media, industrial coordination, public-safety broadcasting, and non-terrestrial multicast services without relying solely on upper-layer encryption. Future research should validate the framework under cell-free massive MIMO, RIS-assisted propagation, satellite-terrestrial integration, and AI-governed radio-resource control (Dong et al., 2010).

Acknowledgement

The authors acknowledge the academic discussion environment provided by their respective departments. No external funding was received for this conceptual and numerical study.

Data Availability

All numerical values used to generate the figures are synthetic simulation-style values contained within the manuscript and can be regenerated from the stated parameter settings. No human-subject or proprietary network data were used (Deng et al., 2015).

Competing Interests

The authors declare that they have no competing interests.

References

Dang, S., Amin, O., Shihada, B., & Alouini, M.-S. (2020). What should 6G be? Nature Electronics, 3, 20-29. https://doi.org/10.1038/s41928-019-0355-6

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

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

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

Letaief, K. B., Chen, W., Shi, Y., Zhang, J., & Zhang, Y.-J. A. (2019). The roadmap to 6G: AI empowered wireless networks. IEEE Communications Magazine, 57(8), 84-90. https://doi.org/10.1109/MCOM.2019.1900271

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

Tataria, H., Shafi, M., Molisch, A. F., Dohler, M., Sjoland, H., & Tufvesson, F. (2021). 6G wireless systems: Vision, requirements, challenges, insights, and opportunities. Proceedings of the IEEE, 109(7), 1166-1199. https://doi.org/10.1109/JPROC.2021.3061701

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

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., Chen, P., Tao, X., & Xia, X.-G. (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

Lu, Y. (2019). 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

Giordani, M., Polese, M., Mezzavilla, M., Rangan, S., & Zorzi, M. (2020). Toward 6G networks: Use cases and technologies. IEEE Communications Magazine, 58(3), 55-61. https://doi.org/10.1109/MCOM.001.1900411

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

Zhang, Z., Xiao, Y., Ma, Z., Xiao, M., Ding, Z., Lei, X., Karagiannidis, G. K., & Fan, P. (2019). 6G wireless networks: Vision, requirements, architecture, and

ISSN: © 2025 INATGI (Institute of Advanced Technology and Green Innovation). Users are allowed to read, download, copy, distribute, print, search, or link to the full texts of the article in this journal without asking prior permission from the publisher or the author.
See: https://inatgi.in/index.php/rft/index for more information.

key technologies. IEEE Vehicular Technology Magazine, 14(3), 28-41. https://doi.org/10.1109/MVT.2019.2921208

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

Mumtaz, S., Rodriguez, J., & Dai, L. (2017). mmWave massive MIMO: A paradigm for 5G. Academic Press. https://doi.org/10.1016/C2015-0-02437-9

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

Rappaport, T. S., Xing, Y., Kanhere, O., Ju, S., Madanayake, A., Mandal, S., Alkhateeb, A., & Trichopoulos, G. C. (2019). Wireless communications and applications above 100 GHz: Opportunities and challenges for 6G and beyond. IEEE Access, 7, 78729-78757. https://doi.org/10.1109/ACCESS.2019.2921522

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

Chaccour, C., Soorki, M. N., Saad, W., Bennis, M., Popovski, P., & Debbah, M. (2022). Seven defining features of terahertz wireless systems: A fellowship of communication and sensing. IEEE Communications Surveys & Tutorials, 24(2), 967-993. https://doi.org/10.1109/COMST.2022.3143454

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

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

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.1978.1055897

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

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

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

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

Oggier, F., & Hassibi, B. (2011). The secrecy capacity of the MIMO wiretap channel. IEEE Transactions on Information Theory, 57(8), 4961-4972. https://doi.org/10.1109/TIT.2011.2158487

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

Fakoorian, S. A. A., & Swindlehurst, A. L. (2013). Solutions for the MIMO Gaussian wiretap channel with a cooperative jammer. IEEE Transactions on Signal Processing, 59(10), 5013-5022. https://doi.org/10.1109/TSP.2011.2160860

Geraci, G., Egan, M., Yuan, J., Razi, A., & Collings, I. B. (2013). Secrecy sum-rates for multi-user MIMO regularized channel inversion precoding. IEEE Transactions on Communications, 60(11), 3472-3482. https://doi.org/10.1109/TCOMM.2012.091112.110624

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

Chen, X., Ng, D. W. K., Gerstacker, W. H., & Chen, H.-H. (2017). A survey of multiple-antenna techniques for physical layer security. IEEE Communications Surveys & Tutorials, 19(2), 1027-1053. https://doi.org/10.1109/COMST.2016.2633327

Wang, H.-M., Zheng, T.-X., Yuan, J., Towsley, D., & Lee, M. H. (2015). Physical layer security in heterogeneous cellular networks. IEEE Transactions on Communications, 64(3), 1204-1219. https://doi.org/10.1109/TCOMM.2015.2513088

Zhang, J., Duong, T. Q., Marshall, A., & Woods, R. (2016). Key generation from wireless channels: A review. IEEE Access, 4, 614-626. https://doi.org/10.1109/ACCESS.2016.2521718

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

Ding, Z., Fan, P., & Poor, H. V. (2016). Impact of user pairing on 5G nonorthogonal multiple-access downlink transmissions. IEEE Transactions on Vehicular Technology, 65(8), 6010-6023. https://doi.org/10.1109/TVT.2015.2480766

Liu, Y., Ding, Z., Elkashlan, M., & Poor, H. V. (2017). Cooperative non-orthogonal multiple access with simultaneous wireless information and power transfer. IEEE Journal on Selected Areas in Communications, 34(4), 938-953. https://doi.org/10.1109/JSAC.2016.2549378

Men, J., & Ge, J. (2015). Performance analysis of non-orthogonal multiple access for relaying networks over Nakagami-m fading channels. IEEE Transactions on Vehicular Technology, 66(2), 1200-1208. https://doi.org/10.1109/TVT.2016.2555399

Sharma, P. K., & Kim, D. I. (2016). Secure 3D mobile UAV relaying for hybrid satellite-terrestrial networks. IEEE Transactions on Wireless Communications, 15(9), 6247-6259. https://doi.org/10.1109/TWC.2016.2585098

Sun, Y., Ng, D. W. K., Ding, Z., Schober, R., & Poor, H. V. (2019). Physical layer security in UAV systems: Challenges and opportunities. IEEE Wireless Communications, 26(5), 40-47. https://doi.org/10.1109/MWC.001.1800445

Krikidis, I., Timotheou, S., & Nikolaou, S. (2012). RF energy transfer for cooperative networks: Data relaying or energy harvesting? IEEE Communications Letters, 16(11), 1772-1775. https://doi.org/10.1109/LCOMM.2012.091212.121310

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

Sendonaris, A., Erkip, E., & Aazhang, B. (2003). User cooperation diversity-Part I: System description. IEEE Transactions on Communications, 51(11), 1927-1938. https://doi.org/10.1109/TCOMM.2003.818096

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

Ikki, S. S., & Ahmed, M. H. (2011). Performance analysis of cooperative diversity wireless networks over Nakagami-m fading channel. IEEE Communications Letters, 11(4), 334-336. https://doi.org/10.1109/LCOMM.2007.348298

Zou, Y., Wang, X., & Shen, W. (2011). Optimal relay selection for physical-layer security in cooperative wireless networks. IEEE Journal on Selected Areas in Communications, 31(10), 2099-2111. https://doi.org/10.1109/JSAC.2013.131011

Ding, Z., Leung, K. K., Goeckel, D. L., & Towsley, D. (2012). Opportunistic relaying for secrecy communications: Cooperative jamming vs. relay chatting. IEEE Transactions on Wireless Communications, 10(6), 1725-1729. https://doi.org/10.1109/TWC.2011.040411.100879

ISSN: © 2025 INATGI (Institute of Advanced Technology and Green Innovation). Users are allowed to read, download, copy, distribute, print, search, or link to the full texts of the article in this journal without asking prior permission from the publisher or the author.

See: https://inatgi.in/index.php/rft/index for more information.

Huang, J., & Swindlehurst, A. L. (2010). 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.2011.2180892

He, X., & Yener, A. (2012). Cooperation with an untrusted relay: A secrecy perspective. IEEE Transactions on Information Theory, 56(8), 3807-3827. https://doi.org/10.1109/TIT.2010.2050822

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

Deng, H., Wang, H.-M., Guo, W., & Wang, W. (2015). Secrecy transmission with a helper: To relay or to jam. IEEE Transactions on Information Forensics and Security, 10(2), 293-307. https://doi.org/10.1109/TIFS.2014.2368364

Zhou, X., McKay, M. R., Maham, B., & Hjorungnes, A. (2011). Rethinking the secrecy outage formulation: A secure transmission design perspective. IEEE Communications Letters, 15(3), 302-304. https://doi.org/10.1109/LCOMM.2011.011811.102056

Yan, S., Yang, N., Malaney, R., & Yuan, J. (2014). Transmit antenna selection with Alamouti coding and power allocation in MIMO wiretap channels. IEEE Transactions on Wireless Communications, 13(3), 1656-1667. https://doi.org/10.1109/TWC.2014.012314.130987

Yang, N., Yeoh, P. L., Elkashlan, M., Schober, R., & Collings, I. B. (2015). Transmit antenna selection for security enhancement in MIMO wiretap channels. IEEE Transactions on Communications, 61(1), 144-154. https://doi.org/10.1109/TCOMM.2012.120312.110670

Hu, L., Wen, H., Wu, B., Pan, F., Liao, R.-F., Song, H., Tang, J., & Wang, X. (2018). Cooperative jamming for physical layer security enhancement in Internet of Things. IEEE Internet of Things Journal, 5(1), 219-228. https://doi.org/10.1109/JIOT.2017.2778185

Mao, Y., Clerckx, B., & Li, V. O. K. (2017). Rate-splitting multiple access for downlink communication systems: Bridging, generalizing, and outperforming SDMA and NOMA. EURASIP Journal on Wireless Communications and Networking, 2018, 133. https://doi.org/10.1186/s13638-018-1104-7

Dai, L., Wang, B., Yuan, Y., Han, S., Chih-Lin, I., & Wang, Z. (2015). Non-orthogonal multiple access for 5G: Solutions, challenges, opportunities, and future research trends. IEEE Communications Magazine, 53(9), 74-81. https://doi.org/10.1109/MCOM.2015.7263349

Bjornson, E., Larsson, E. G., & Marzetta, T. L. (2017). Massive MIMO: Ten myths and one critical question. IEEE Communications Magazine, 54(2), 114-123. https://doi.org/10.1109/MCOM.2016.7402270

Marzetta, T. L. (2010). Noncooperative cellular wireless with unlimited numbers of base station antennas. IEEE Transactions on Wireless Communications, 9(11), 3590-3600. https://doi.org/10.1109/TWC.2010.092810.091092

Larsson, E. G., Edfors, O., Tufvesson, F., & Marzetta, T. L. (2014). Massive MIMO for next generation wireless systems. IEEE Communications Magazine, 52(2), 186-195. https://doi.org/10.1109/MCOM.2014.6736761

Ngo, H. Q., Ashikhmin, A., Yang, H., Larsson, E. G., & Marzetta, T. L. (2017). Cell-free massive MIMO versus small cells. IEEE Transactions on Wireless Communications, 16(3), 1834-1850. https://doi.org/10.1109/TWC.2017.2655515

Bjornson, E., & Sanguinetti, L. (2020). Scalable cell-free massive MIMO systems. IEEE Transactions on Communications, 68(7), 4247-4261. https://doi.org/10.1109/TCOMM.2020.2987311

Zhang, J., Bjornson, E., Matthaiou, M., Ng, D. W. K., Yang, H., & Love, D. J. (2020). Prospective multiple antenna technologies for beyond 5G. IEEE Journal on Selected Areas in Communications, 38(8), 1637-1660. https://doi.org/10.1109/JSAC.2020.3000826

Di Renzo, M., Zappone, A., Debbah, M., Alouini, M.-S., Yuen, C., de Rosny, J., & Tretyakov, S. (2020). Smart radio environments empowered by reconfigurable intelligent surfaces: How it works, state of research, and the road ahead. IEEE Journal on Selected Areas in Communications, 38(11), 2450-2525. https://doi.org/10.1109/JSAC.2020.3007211

Basar, E., Di Renzo, M., de Rosny, J., Debbah, M., Alouini, M.-S., & Zhang, R. (2019). Wireless communications through reconfigurable intelligent surfaces. IEEE Access, 7, 116753-116773. https://doi.org/10.1109/ACCESS.2019.2935192

Wu, Q., & Zhang, R. (2019). Intelligent reflecting surface enhanced wireless network via joint active and passive beamforming. IEEE Transactions on Wireless Communications, 18(11), 5394-5409. https://doi.org/10.1109/TWC.2019.2936025

Liu, Y., Liu, X., Mu, X., Hou, T., Xu, J., Di Renzo, M., & Al-Dhahir, N. (2021). Reconfigurable intelligent surfaces: Principles and opportunities. IEEE Communications Surveys & Tutorials, 23(3), 1546-1577. https://doi.org/10.1109/COMST.2021.3077737

Huang, C., Zappone, A., Alexandropoulos, G. C., Debbah, M., & Yuen, C. (2019). Reconfigurable intelligent surfaces for energy efficiency in wireless communication. IEEE Transactions on Wireless Communications, 18(8), 4157-4170. https://doi.org/10.1109/TWC.2019.2922609

Yang, Y., Peng, H., Wang, C.-X., & Wang, Y. (2020). Reconfigurable intelligent surface assisted anti-jamming communications: A secure and robust design. IEEE Transactions on Wireless Communications, 20(1), 6-21. https://doi.org/10.1109/TWC.2020.3023138

Xu, J., & Yao, Y. (2019). Secure transmission in reconfigurable intelligent surface assisted wireless networks. IEEE Wireless Communications Letters, 9(6), 744-748. https://doi.org/10.1109/LWC.2020.2967492

Liaskos, C., Nie, S., Tsioliaridou, A., Pitsillides, A., Ioannidis, S., & Akyildiz, I. (2018). A new wireless communication paradigm through software-controlled metasurfaces. IEEE Communications Magazine, 56(9), 162-169. https://doi.org/10.1109/MCOM.2018.1700659

Mao, Y., You, C., Zhang, J., Huang, K., & Letaief, K. B. (2017). A survey on mobile edge computing: The communication perspective. IEEE Communications Surveys & Tutorials, 19(4), 2322-2358. https://doi.org/10.1109/COMST.2017.2745201

Porambage, P., Okwuibe, J., Liyanage, M., Ylianttila, M., & Taleb, T. (2018). Survey on multi-access edge computing for Internet of Things realization. IEEE Communications Surveys & Tutorials, 20(4), 2961-2991. https://doi.org/10.1109/COMST.2018.2849509

Mao, Y., Zhang, J., & Letaief, K. B. (2017). Dynamic computation offloading for mobile-edge computing with energy harvesting devices. IEEE Journal on Selected Areas in Communications, 34(12), 3590-3605. https://doi.org/10.1109/JSAC.2016.2611964

Wang, C.-X., Bian, J., Sun, J., Zhang, W., & Zhang, M. (2019). A survey of 5G channel measurements and models. IEEE Communications Surveys & Tutorials, 20(4), 3142-3168. https://doi.org/10.1109/COMST.2018.2862141

Zhou, Y., Pan, C., Yeoh, P. L., Wang, K., Elkashlan, M., & Vucetic, B. (2015). Secure communications for UAV-enabled mobile edge computing systems. IEEE Transactions on Communications, 68(1), 376-388. https://doi.org/10.1109/TCOMM.2019.2944646

Zeng, Y., Zhang, R., & Lim, T. J. (2016). Wireless communications with unmanned aerial vehicles: Opportunities and challenges. IEEE Communications Magazine, 54(5), 36-42. https://doi.org/10.1109/MCOM.2016.7470933

Lyu, J., Zeng, Y., Zhang, R., & Lim, T. J. (2017). Placement optimization of UAV-mounted mobile base stations. IEEE Communications Letters, 21(3), 604-607. https://doi.org/10.1109/LCOMM.2016.2633248

Shakhatreh, H., Sawalmeh, A. H., Al-Fuqaha, A., Dou, Z., Almaita, E., Khalil, I., Othman, N. S., Khreishah, A., & Guizani, M. (2019). Unmanned aerial vehicles: A survey on civil applications and key research challenges. IEEE Access, 7, 48572-48634. https://doi.org/10.1109/ACCESS.2019.2909530

Chen, M., Challita, U., Saad, W., Yin, C., & Debbah, M. (2020). Artificial neural networks-based machine learning for wireless networks: A tutorial. IEEE Communications Surveys & Tutorials, 21(4), 3039-3071. https://doi.org/10.1109/COMST.2019.2926625

ISSN: © 2025 INATGI (Institute of Advanced Technology and Green Innovation). Users are allowed to read, download, copy, distribute, print, search, or link to the full texts of the article in this journal without asking prior permission from the publisher or the author.

See: https://inatgi.in/index.php/rft/index for more information.