

Decentralized Elliptic Curve Identity for Authenticated Software Defined Radio Mesh Messaging

Raymond Sebetoa Teboho Nyareli Mphahlela Thaba

Defence and Security

Council for Scientific and Industrial Research (CSIR)

Pretoria, South Africa

e-mail: RSebetoa@csir.co.za, TNyareli@csir.co.za, JThaba@csir.co.za

Abstract—Software Defined Radio mesh networks are useful for disconnected and mobile communication. However, a receiver still needs a way to verify the sender, ensure that the message was not changed, and reject old messages that are replayed. This paper combines a structured literature review with an offline experiment for a decentralized elliptic curve identity layer. The review covers security implementations for the Software Defined Radio physical layer, physical layer authentication and key generation, authentication in mobile and vehicular ad hoc networks, and trust systems based on blockchain. It identifies a gap between radio-layer protection, transmitter authentication, and cryptographic authentication at the message level for Software Defined Radio mesh systems. The proposed layer derives node identities from public keys, signs outgoing payloads, and verifies the trusted key list, signature, and replay state after the radio frame is recovered. The experiment measures payload growth, Low-Density Parity-Check block impact, payload efficiency, signing time, verification time, and security behavior for tampered, replayed, incorrect-key, and unknown-node messages. The results show that signing and verification complete in microseconds, while packet growth is the main cost for small payloads that make inefficient use of message blocks. The results indicate that decentralized elliptic curve authentication is practical for low-rate authenticated Software Defined Radio messaging when compact encoding, key identifiers, and batching are used to reduce airtime overhead.

Keywords—software defined radio; mesh networks; authentication; elliptic curve cryptography; decentralized identity.

I. INTRODUCTION

Software Defined Radio (SDR) makes it possible to implement adaptable communication waveforms and protocol logic in software rather than fixed hardware [1]. This flexibility is useful for mobile mesh networks that must operate in disconnected, infrastructure-limited, or rapidly changing environments. However, a flexible radio link also creates an authentication problem. A receiver must decide whether a decoded message came from a trusted node, whether the message was changed, and whether the message is new rather than replayed.

Many SDR security studies focus on physical layer confidentiality, jamming resistance, waveform adaptation, or interference resilience. Representative SDR studies include Multiple-Input Multiple-Output Singular Value Decomposition (MIMO-SVD) secrecy, full-duplex jamming, transmitter-fingerprint authentication, and channel-based key generation [3]–[10]. These topics are important, but they do not by themselves establish persistent node identity and message authenticity.

Error detection and forward error correction can show that a packet was recovered, but they do not prove that the packet came from a trusted sender. A malicious transmitter can still inject a correctly formed packet if the receiver has no cryptographic identity layer [3]–[10]. To determine whether the existing lines of work address the complete message-level problem, this paper first conducts a structured literature review and uses its findings to motivate the authentication layer evaluated later in the paper.

Centralized Public Key Infrastructure (PKI) can authenticate nodes, but it depends on certificate distribution, certificate path validation, and revocation checks that may not be available during disconnected mesh operation [2]. Earlier work on Mobile Ad Hoc Networks (MANETs) also shows that these networks cannot always depend on available trusted authorities, which led to self-organized public key management and secure routing approaches [11]–[13]. MANET and Vehicular Ad Hoc Networks (VANETs) studies address authentication in dynamic networks using certificates, identity-based methods, elliptic curves, certificateless signatures, and trust systems supported by blockchain [14]–[20]. However, these approaches solve different parts of the problem and can still depend on certificate authorities, roadside infrastructure, key generation centers, cluster-based trust, or protocol-level validation rather than an SDR message pipeline. The review in Sections II and III therefore tests the gap explicitly instead of assuming that message-level SDR authentication is absent.

This paper makes four focused contributions. First, it combines SDR security, physical layer authentication, MANET and VANET authentication, and trust systems based on blockchain into a layered gap analysis. Second, it proposes a decentralized elliptic curve identity model in which node identifiers are derived from public keys and messages are signed before SDR frame bundling. Third, it implements an offline secure envelope experiment that measures payload growth, Low-Density Parity-Check (LDPC) block impact, useful payload efficiency, signing time, and verification time. Fourth, it evaluates authentication behavior under valid, tampered, wrong-key, unknown-node, and replayed message cases. The novelty of this work is at the system-integration and evaluation level rather than in a new cryptographic primitive or authentication protocol: public-key-derived identity, Ed25519 signing, trusted-key lookup, and replay state are placed inside an SDR-style transmit and receive workflow, and their byte,

LDPC-block, and processing costs are measured.

The rest of this paper is organized as follows. Section II describes the literature review method. Section III reviews the main findings and identifies the research gap. Section IV presents the proposed identity layer and secure envelope. Section V describes the experiment. Section VI reports the results. Section VII discusses the threat model, trade-offs, and comparison with centralized approaches. Section VIII concludes the paper and identifies future work.

II. REVIEW METHODOLOGY

A structured review was used to identify relevant studies on authentication, cryptographic identity, and security in SDR-based and decentralized wireless communication systems. The review followed the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) screening approach [25]. The publication window was 2015–2026 and the main databases were Institute of Electrical and Electronics Engineers (IEEE) Xplore and Scopus. The final literature-library export used for screening was generated on May 5, 2026, which is used as the review search cut-off date. Existing reviews cover important but narrower topics, including physical-layer security, digital-radio security, and identity-based VANET security [7][26][27]. The purpose of the present review is different: it asks whether these areas jointly provide a practical message-level authentication path inside an SDR mesh workflow and whether implementation cost is reported. Secondary review articles were used to position the study but were not counted among the 22 primary studies in the final synthesis.

A. Research Questions

The review was guided by three Research Questions (RQs). RQ1 asks which security and authentication mechanisms are used in SDR, MANET, and VANET communication. RQ2 asks which approaches can verify identity during disconnected operation without a continuously available central service. RQ3 asks whether the reviewed work combines message-level identity and replay protection with SDR-pipeline integration and reports communication or processing cost.

B. Search Strategy

Three Boolean search strings formed the core search protocol. Elliptic-Curve Cryptography (ECC) is abbreviated in S3 exactly as it was used in the search:

- S1:** (“software defined radio” OR “SDR”) AND (“physical layer security” OR “authentication”).
- S2:** (“mesh network” OR MANET OR “mobile ad hoc network”) AND (authentication OR “digital signature” OR “public key”) AND (identity OR trust OR “key management” OR certificate OR “certificate-less”).
- S3:** (“elliptic curve cryptography” OR ECC OR “identity-based cryptography”) AND (authentication OR “digital signature”) AND (“mesh network” OR MANET OR “ad hoc network”).

Database-specific syntax was used where required. In Scopus, the search was restricted to article title, abstract, and keywords; the archived IEEE Xplore search used the document search without a narrower field restriction. Year and publication-type filters were then applied consistently.

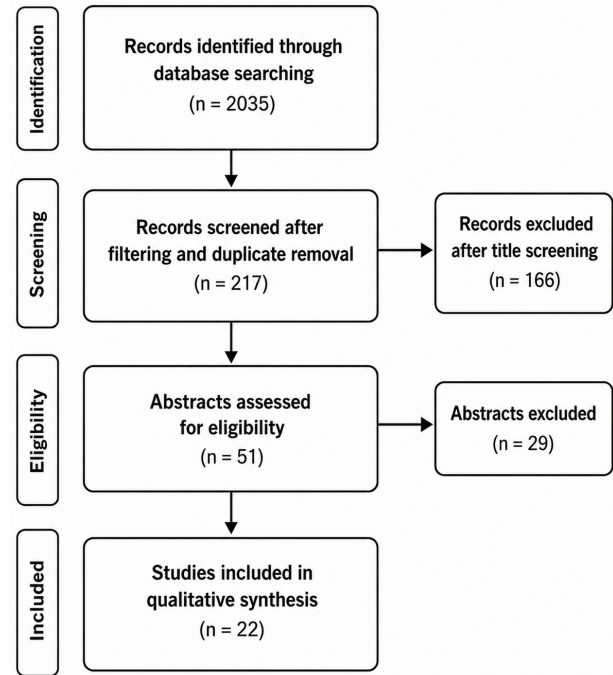


Figure 1. PRISMA style screening process used in the review.

C. Screening Process

The searches produced approximately 2035 records before duplicate removal and relevance filtering. After duplicate removal and filtering by publication year and keyword relevance, 217 papers were retained for title screening. Abstract screening reduced the set to 51 studies, and full-paper assessment produced a final set of 22 papers for review and comparison. Titles, abstracts, and full papers were assessed against the research questions, with priority given to studies that described an authentication or identity mechanism and its applicability to decentralized wireless communication. Figure 1 summarizes the selection process.

D. Inclusion and Exclusion Criteria

Studies were included if they addressed authentication, identity verification, trust establishment, digital signatures, mesh communication, MANETs, VANETs, SDR systems, decentralized wireless networks, lightweight cryptography, or deployable communication security. Studies were excluded if they focused only on channel capacity, throughput optimization, theoretical physical layer analysis, beamforming or other SDR signal-processing techniques without authentication relevance, cryptographic theory without communication use, unrelated cybersecurity domains, duplicate publications, or incomplete publications. The term “lightweight” was not used as an independent inclusion gate. It was recorded only when

a study explicitly targeted lightweight or resource-constrained operation and supported that claim with at least one efficiency measure, such as execution time, communication bytes, key or signature size, or cryptographic operation count.

E. Data Extraction

Each selected paper was grouped by network type, cryptographic method, authentication mechanism, identity model, dependence on centralized services, implementation environment, reported communication or computation cost, main contribution, and limitation. These fields map directly to RQ1–RQ3 and provide the basis for the structured synthesis reported in Table I.

III. REVIEW FINDINGS AND RESEARCH GAP

The review shows that the literature addresses several parts of the security problem, but most studies focus on separate layers of the communication stack. The final studies were grouped into four areas: SDR physical layer security, SDR physical layer authentication and key generation, MANET and VANET authentication, and trust systems based on blockchain or distributed ledgers. The groups are compared using the same extraction fields so that the research gap follows from the review evidence rather than from an unsupported assertion [3]–[20].

A. SDR Physical Layer Security

SDR and physical layer security research includes MIMO-SVD secrecy, full-duplex jamming, relay-assisted secrecy, device-to-device protection, and reconfigurable intelligent surface methods [3]–[8]. Several of these studies include SDR or hardware demonstrations, which confirms that security functions can be implemented at the radio layer. Their main target, however, is confidentiality, jamming resistance, or channel protection rather than persistent message identity. A recovered frame can therefore still require a separate decision about sender identity, deliberate modification, and replay.

B. SDR Physical Layer Authentication and Key Generation

Physical layer authentication moves closer to identity by using waveform or hardware properties. Verma et al. demonstrated transmitter fingerprint embedding on SDR, while Hu et al. evaluated channel-based key generation on an SDR-based Long Range (LoRa) platform [9][10]. These methods are useful, but fingerprinting can depend on hardware and channel behavior, while shared-key extraction does not by itself define a portable public-key node identity or replay state for forwarded mesh messages. The proposed message layer is therefore complementary to these radio-specific methods.

C. MANET and VANET Authentication

MANET and VANET research addresses authentication under mobility and intermittent connectivity. Foundational work considered self-organized public-key management and secure routing, while later schemes use ECC, identity-based cryptography, certificateless methods, signcryption, and privacy-preserving authentication [11]–[19]. These approaches

TABLE I. STRUCTURED SYNTHESIS OF THE REVIEWED LITERATURE.

Cluster	Main target	Implementation / dependency	Unresolved for this paper
SDR physical layer security [3]–[8]	Secrecy, jamming and channel protection	Several SDR/hardware demonstrations; identity is not the main target	Persistent message identity and replay state
SDR physical layer authentication and key generation [9][10]	Transmitter fingerprint or shared key material	SDR demonstrations; depends on channel or hardware properties	Portable public-key mesh identity and replay handling
MANET and VANET authentication [11]–[19]	Certificates, ECC, identity-based or certificateless authentication	Often assumes authorities, roadside units, key centers, or protocol/simulation validation	Integration with SDR framing and measured coded-message cost
Blockchain trust [20]	Distributed trust and cross-domain authentication	Requires ledger state, synchronization, storage, and consensus	Lightweight SDR integration without ledger maintenance

are relevant to SDR mesh operation, but many assume certificate authorities, roadside units, key-generation centers, cluster roles, or protocol/simulation validation. They therefore do not directly report how signed messages map into an SDR frame workflow or how authentication changes coded-message cost.

D. Trust Systems Based on Blockchain and Distributed Ledgers

Blockchain and distributed ledgers can reduce reliance on one central authority by maintaining shared trust records. VANET work has used this model for cross-domain authentication [20]. The trade-off is ledger synchronization, consensus, storage, and transaction exchange. For the present low-throughput disconnected SDR use case, direct signatures and local trusted-key lookup provide a simpler baseline when the immediate decision is whether a recovered message was signed by a trusted node and is fresh.

E. Gap Identified

Table I is the formal synthesis of the reviewed clusters and answers RQ1–RQ3. The table separates each cluster's main security target, dependence on supporting infrastructure, implementation evidence, and the property that remains unresolved for the present SDR mesh problem.

No study in the final reviewed set was identified as reporting all of the following together: public-key-derived node identity, signed message payloads, per-node replay state, placement inside an SDR transmit/receive workflow, and measured packet or coded-link cost. The research gap is therefore not the absence of SDR authentication research. It is the lack of a practical, evaluated integration of these properties for disconnected SDR mesh messaging. This paper addresses that narrower gap by implementing the message envelope and reporting its byte growth, LDPC block use,

useful payload efficiency, signing time, verification time, and rejection behavior.

IV. PROPOSED AUTHENTICATION LAYER

The proposed layer adds decentralized identity and message authentication above SDR frame recovery and below application message processing. It can be used with different SDR transports, but the evaluation focuses on the secure message envelope and its cost.

A. Node Identity

Each node owns an elliptic curve signing key pair. The node identifier is derived from a hash of the public key and mapped to that public key in a local trusted key list. This binds the compact identifier to the trusted key material while allowing routine verification to continue without an online certificate authority or distributed ledger. This follows the general idea of identities derived from public keys, as used in decentralized systems such as Bitcoin, where possession of the private key proves control over the related identifier [21]. A second mode, where the message includes the public key, was evaluated to quantify the additional cost of enrollment or discovery-style traffic.

B. Secure Envelope

A secure envelope contains the version, node identifier, sequence number, timestamp, payload, and digital signature. The signature is computed over the envelope fields that define the sender, replay state, and payload. The receiver parses the envelope, obtains the trusted public key associated with the node identifier, verifies the signature, checks the sequence number, and accepts the payload only if all checks succeed [22]. Ed25519 was selected as an established engineering choice, not as a novel primitive: it is standardized, uses a fixed 64-byte signature and 32-byte public key, and is directly supported by the OpenSSL interface used in the experiment.

The identity derivation and message signature can be expressed as

$$\begin{aligned} ID_i &= H(PK_i), \\ \sigma_i &= \text{Sign}(SK_i, m), \end{aligned} \quad (1)$$

where PK_i is the public key of node i , SK_i is the matching private key, $H(\cdot)$ is a cryptographic hash function, m is the message, and σ_i is the digital signature. A message is accepted only when

$$\text{Verify}(PK_i, m, \sigma_i) = 1 \quad (2)$$

and the node is trusted and the sequence number is fresh.

The relative packet overhead for a payload of size P bytes is computed as

$$O_p = \frac{T - P}{P} \times 100, \quad (3)$$

where T is the total serialized envelope size.

C. Receiver Decision Logic

The receiver applies a strict accept or reject policy. A message is accepted only if the node identifier is known, the signature verifies under the trusted public key, and the sequence number is newer than the last accepted value for that node. A monotonic sequence number was chosen because it requires only small per-node state and can be checked while disconnected; the timestamp provides additional freshness context without making online time synchronization the sole replay defense. A message can therefore be rejected even if the lower layer channel code reconstructs it correctly. This separation is important because forward error correction improves reliability, while the signature establishes authenticity [22][24].

V. EXPERIMENTAL METHOD

The experiment was designed to evaluate cryptographic cost and behavior rather than live radio performance. This avoids mixing packet authentication results with unrelated channel effects, such as carrier frequency offset, sampling rate offset, fading, or timing recovery errors.

A. Communication Stack and Frame Structure

The proposed authentication layer is placed before SDR framing at the transmitter and after frame recovery at the receiver. The target SDR stack used by the project is summarized in Table II. The application payload is first placed inside the secure envelope. The resulting authenticated message is then fragmented if needed, protected with Cyclic Redundancy Check (CRC) fields, encoded with LDPC forward error correction, framed using a Short Training Sequence (STS), Long Training Sequence (LTS), and 32-bit synchronization word, and modulated using $\pi/4$ Differential Quadrature Phase Shift Keying (DQPSK). On reception, the order is reversed: synchronization and demodulation recover the coded frame, LDPC decoding and CRC checks recover the bytes, and the cryptographic layer then verifies the sender identity, signature, and replay state.

TABLE II. TARGET SDR MESSAGE STACK USED FOR THE AUTHENTICATED PIPELINE.

Layer or field	Role in the pipeline
Application payload	Text or telemetry message to be sent
Secure envelope	Node identifier, sequence number, timestamp, payload, and Ed25519 signature
Fragment and CRC fields	Fragment header, fragment integrity check, and object-level integrity check
Forward error correction	LDPC coding with $k = 1152$ information bits and $n = 2304$ coded bits
Frame synchronization	Short training sequence, long training sequence, and 32-bit synchronization word
Modulation	$\pi/4$ -DQPSK target waveform for the SDR modem
Receiver checks	Demodulation, LDPC decoding, CRC checks, trusted key lookup, signature check, and replay check

The CRC fields and LDPC decoder address transmission errors, while the digital signature addresses authenticity. A

packet can pass lower layer error checks and still be rejected by the authentication layer if it is from an unknown node, has a bad signature, or reuses an old sequence number. This separation is important because link reliability and message trust are different decisions.

B. Implementation

The authentication layer was implemented offline as a C++17 experiment. Ed25519 signing and verification were performed using the OpenSSL high-level cryptographic interface [22][23]. The SDR-style message pipeline used an LDPC block model with $k = 1152$ information bits and $n = 2304$ coded bits, consistent with a rate-one-half forward error correction configuration [24]. The experiment did not transmit live radio frequency signals.

The measured payload sizes were 16, 25, 64, 128, 256, 512, and 1024 bytes. Each cryptographic timing result was averaged over 10,000 iterations. Three transmission modes were evaluated: plaintext without authentication, signed key identifier envelope, and signed envelope with the public key included in the message. Figure 2 shows the byte-level frame layout together with the transmit and receive processing order used in the experiment.

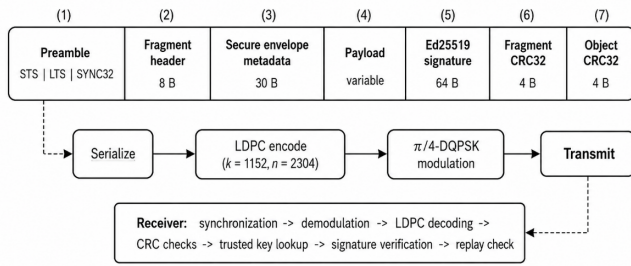


Figure 2. Authenticated SDR frame structure used in the offline experiment.

The preamble supports frame acquisition, while the CRC fields check recovered fragments and objects before the trusted-key, signature, and replay checks are applied.

C. Experimental Platforms

Two offline environments were used. The Windows workstation represents a typical desktop development platform. The isolated sandbox provides a repeatable baseline with different resource constraints. Table III summarizes both environments.

TABLE III. EXPERIMENTAL PLATFORMS.

Item	Windows workstation	Isolated sandbox
Operating system	Windows 11 Home	Debian GNU/Linux 13 (Trixie)
Processor	Intel Core i7-9750H at 2.60 GHz	2 vCPUs at 2.60 GHz
Memory	32 GB	4 GB
Compiler	GCC 15.2.0	GCC 14.2.0
Cryptography	OpenSSL 3.6.1	OpenSSL 3.5.5
Radio mode	Offline only	Offline only

The two platforms were used only to compare processing cost; the differences in processor and memory are not used to make radio-performance claims.

VI. EXPERIMENTAL RESULTS

This section reports the experimental results. The main finding is that computation is not the main cost in the tested desktop-class environments. Packet growth and the related coded-link bit cost dominate, especially for small telemetry messages.

A. Payload Growth and Coding Impact

Table IV shows the payload growth for the signed key identifier mode. The key identifier envelope adds 94 bytes to each tested payload. This includes 30 bytes of metadata and a 64 byte Ed25519 signature. Because the public key is not included in every key identifier message, the overhead remains constant across payload sizes.

TABLE IV. SIGNED KEY IDENTIFIER ENVELOPE OVERHEAD AND CODING IMPACT.

Payload bytes	Total bytes	Overhead bytes	Overhead percent	LDPC blocks
16	110	94	587.50	1
25	119	94	376.00	1
64	158	94	146.88	2
128	222	94	73.44	2
256	350	94	36.72	3
512	606	94	18.36	5
1024	1118	94	9.18	8

The relative overhead is severe for very small messages. A 25-byte text payload expands to 119 bytes, which is a 376.00 percent overhead. However, the relative cost decreases as payload size increases. A 1024-byte payload expands to 1118 bytes, which is 9.18 percent overhead. Figure 3 shows this trend and also shows that including the public key in every message increases the fixed overhead from 94 bytes to 126 bytes.

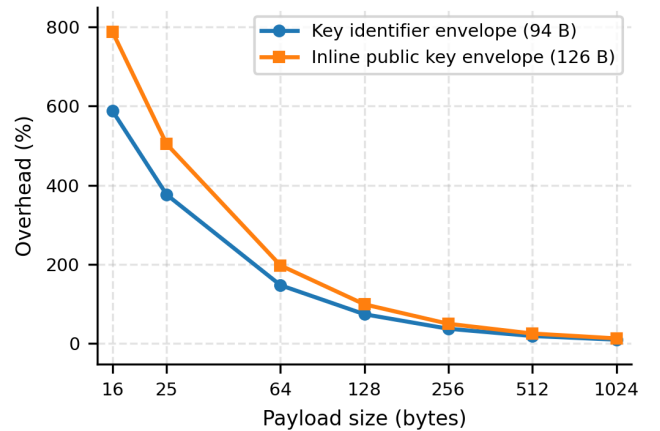


Figure 3. Envelope overhead for key identifier and inline public key modes.

The coding impact follows from the number of information bits available per LDPC block. A 64-byte plaintext message uses one coding block, while its signed key identifier envelope requires two coding blocks. A 512-byte plaintext payload uses four blocks, while the signed envelope requires five. This

shows that authentication overhead affects not only stored packet size, but also channel airtime and useful payload efficiency.

B. Cryptographic Latency

Table V compares signing and verification time for the signed key identifier mode. The Windows workstation achieved lower average latency than the isolated sandbox. Signing required approximately 80 to 85 microseconds on Windows and 117 to 130 microseconds in the sandbox. Verification required approximately 109 to 111 microseconds on Windows and 162 to 168 microseconds in the sandbox.

TABLE V. AVERAGE SIGNED KEY IDENTIFIER CRYPTOGRAPHIC LATENCY.

Payload bytes	Win. sign us	Win. verify us	Sandbox sign us	Sandbox verify us
16	85	109	119	167
25	81	109	118	168
64	80	110	117	164
128	80	110	117	167
256	81	109	117	166
512	82	110	118	162
1024	84	111	130	168

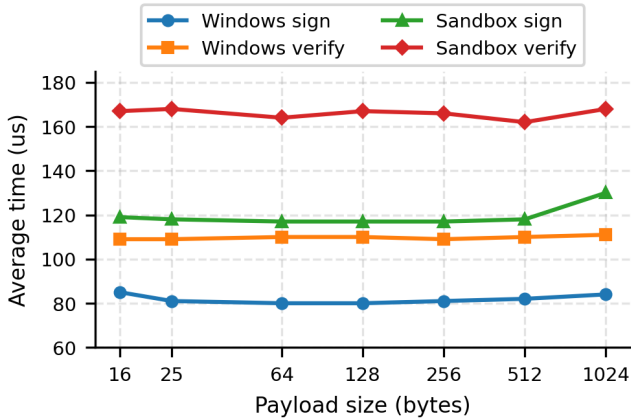


Figure 4. Signing and verification time on the two offline platforms.

Figure 4 shows that latency depends on the platform, while packet overhead is deterministic. The small increase at the largest payload size does not change the main conclusion. On both platforms, signing and verification remained below 200 microseconds for all tested payloads. Therefore, in low-rate telemetry messaging, the processing cost of the digital signature is unlikely to be the main bottleneck on desktop-class processors.

C. Useful Payload Efficiency

The experiment also computed useful payload efficiency as the original payload bits divided by the coded link bits required to carry the message. The efficiency is limited by both packet size and the fixed LDPC block size. Figure 5 shows the block-aware efficiency curves for plaintext and signed key identifier messages, with markers indicating the payload sizes tested in the experiment.

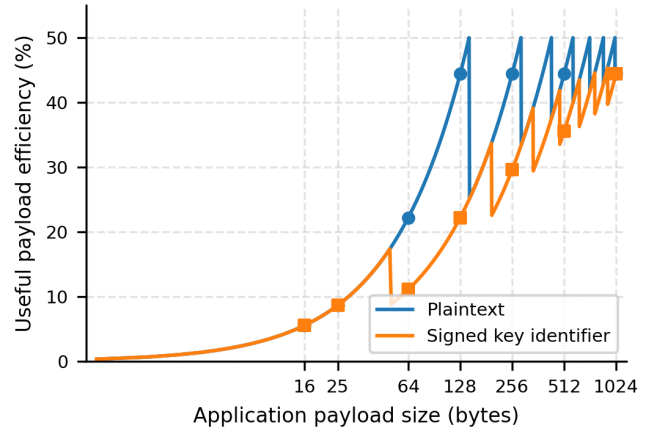


Figure 5. LDPC block-aware useful payload efficiency for plaintext and signed messages. Markers show the tested payload sizes, and each drop shows where an additional LDPC block is required.

The signed message is least efficient for small payloads because the fixed 94-byte authentication overhead consumes a large part of the coded block capacity. For 25 bytes, both plaintext and signed key identifier modes still require one coding block, but most of the coded block carries authentication metadata rather than application data. For 64 bytes, the signed message crosses into a second coding block, reducing useful payload efficiency from 22.22 percent to 11.11 percent. The practical lesson is that message batching and compact binary encoding are important when signatures per message are used on narrowband links.

D. Security Behavior

In addition to size and latency measurements, the receiver logic was tested using six message cases: valid message, payload tamper, signature tamper, unknown node, wrong public key, and replay. These cases were selected to test authenticity, payload integrity, trusted key enforcement, and replay rejection. Table VI reports the receiver decision for each security behavior test. The valid message was accepted. Payload tampering and signature tampering were rejected by signature verification. Messages from unknown nodes were rejected by the trusted key lookup. A message signed under the wrong public key was rejected as a bad signature. A repeated sequence number was rejected as a replay.

TABLE VI. AUTHENTICATION BEHAVIOR UNDER ADVERSARIAL MESSAGE CASES.

Case	Expected result	Observed result
Valid signed message	Accept	Accepted
Payload tamper	Reject	Bad signature
Signature tamper	Reject	Bad signature
Unknown node	Reject	Unknown node
Wrong public key	Reject	Bad signature
Replay sequence	Reject	Replay rejected

These results confirm the intended separation between transmission reliability and message authenticity. A lower layer checksum or forward error correction decoder can confirm

that bytes were recovered, but it cannot decide whether the bytes came from a trusted sender. The signed envelope adds that decision point.

VII. DISCUSSION AND THREAT MODEL

The review and experimental results show that decentralized elliptic curve authentication can be integrated into an offline SDR-style message pipeline with low processing cost. However, they also show a clear downside: authentication metadata significantly increases airtime for small payloads.

A. Threat Model

The proposed framework assumes a decentralized wireless mesh in which adversaries may spoof node identities, inject rogue packets, modify payloads, retransmit captured packets, or attempt to forward unauthenticated traffic. Table VII summarizes the threats addressed by the proposed layer.

TABLE VII. THREAT MODEL AND MITIGATION SCOPE.

Threat	Description	Mitigation
Spoofing	Rogue node impersonates a legitimate participant	Public key identity and signature verification
Replay	Captured packet is retransmitted	Sequence number and timestamp checks
Message tamper	Payload modified in transit	Digital signature verification
Unknown node	Packet from untrusted participant	Trusted key lookup
Compromised key	Private key stolen	Future revocation and re-enrollment
Jamming	Wireless channel disruption	Complementary SDR protection

Wideband jamming and denial of service are outside the direct scope of the cryptographic layer and must be handled using complementary SDR techniques [3]–[10].

B. Benefits and Costs

The main benefit is that verification does not require infrastructure once the receiver has the sender's trusted public key. Message verification does not require an online certificate authority, an active certificate status service, or a shared network database. This is important for disconnected mesh networks in which a node may have to accept or reject messages while isolated from fixed infrastructure [2].

The main trade-off is packet growth. For small telemetry updates, the fixed signature and metadata cost can be larger than the payload itself. This suggests three engineering responses. First, related telemetry fields should be batched into a single signed payload where latency requirements allow it. Second, compact binary serialization should be preferred over verbose text serialization formats. Third, the key identifier mode should be used for routine traffic after public keys have been distributed, while messages that include the public key should be reserved for enrollment, discovery, or recovery procedures.

C. Comparison With Centralized Solutions

A centralized certificate approach can provide mature lifecycle management, policy enforcement, and revocation, but it requires certificate handling and access to trust status information [2]. The proposed design trades some of that management structure for disconnected operation. In the proposed model, trusted key population, public key distribution, and key revocation become operational responsibilities of the mesh system. The approach is most appropriate when disconnected verification is more important than centralized administrative convenience.

D. Limitations and Future Physical Layer Evaluation

The evaluation is intentionally limited to offline authentication behavior and coded message cost; it does not report live radio frequency throughput or field range. The current results nevertheless map directly to the target physical layer at the coding boundary because every additional LDPC information block requires a fixed 2304 coded bits before modulation. For example, the 64-byte plaintext payload fits in one information block, while its signed key-identifier envelope requires two. Radio impairments cannot reduce this deterministic authentication cost, while packet loss or retransmission can only increase the effective airtime cost. Live SDR validation will therefore measure authenticated delivery ratio, end-to-end latency, packet loss, and retransmission behavior under additive noise, carrier frequency offset, sampling rate offset, timing error, interference, and multi-hop forwarding. This keeps the present contribution focused on authentication integration and cost, while field robustness remains part of the future physical layer evaluation.

VIII. CONCLUSION AND FUTURE WORK

This paper presented a structured review, architecture proposal, and offline experiment for decentralized elliptic curve identity in authenticated SDR mesh messaging. The review found that existing SDR security research often emphasizes physical layer confidentiality, while MANET and VANET authentication literature often assumes centralized infrastructure, backup trust services, or simulation-level validation [3]–[20]. The proposed layer addresses the identified gap by binding messages to identities derived from public keys and applying signature verification, trusted key lookup, and replay checks after SDR frame recovery.

The experimental results support three conclusions. First, the authentication layer successfully rejected tampered payloads, tampered signatures, unknown nodes, wrong-key messages, and replayed messages. Second, signing and verification completed in microseconds on the tested platforms, indicating that computation was not the main bottleneck in this experiment. Third, packet growth was the dominant downside, especially for small telemetry payloads. The 25-byte payload expanded to 119 bytes in key identifier mode, while a 1024-byte payload expanded to 1118 bytes. This shows that decentralized authentication is practical for low-rate SDR

messaging, but payload batching and compact encoding are important.

Future work will evaluate the authenticated pipeline over live SDR hardware using authenticated delivery ratio, end-to-end latency, packet loss, and retransmission rate under additive noise, carrier frequency offset, sampling rate offset, timing recovery error, interference, and multi-hop forwarding. Future work should also investigate public key enrollment, key rotation, compromise recovery, and revocation procedures that preserve disconnected operation.

REFERENCES

- [1] J. Mitola, "The software radio architecture", *IEEE Communications Magazine*, vol. 33, no. 5, pp. 26–38, 1995. DOI: 10.1109/35.393001.
- [2] D. Cooper et al., *Internet x.509 public key infrastructure certificate and certificate revocation list profile*, RFC 5280, 2008. DOI: 10.17487/RFC5280.
- [3] J. Madeira, J. Guerreiro, and R. Dinis, "A software defined radio implementation of physical layer security using MIMO-SVD", in *2022 International Young Engineers Forum in Electrical and Computer Engineering*, 2022, pp. 75–79. DOI: 10.1109/YEF-ECE55092.2022.9850114.
- [4] A. Silva, M. A. C. Gomes, J. P. Vilela, and W. K. Harrison, "SDR testbed of full-duplex jamming for secrecy", in *2020 12th International Symposium on Communication Systems, Networks and Digital Signal Processing*, 2020, pp. 1–3. DOI: 10.1109/CSNDSP49049.2020.9249552.
- [5] N. T. Y. Linh, C. D. T. Thai, V. N. Q. Bao, and H. V. Hoa, "Physical layer security in multi-hop relay networks with modified dijkstra's routing algorithms", in *2020 7th NAFOSTED Conference on Information and Computer Science*, 2020, pp. 405–410. DOI: 10.1109/NICS51282.2020.9335844.
- [6] F. Zhu, F. Gao, T. Zhang, K. Sun, and M. Yao, "Physical-layer security for full duplex communications with self-interference mitigation", *IEEE Transactions on Wireless Communications*, vol. 15, no. 1, pp. 329–340, 2016. DOI: 10.1109/TWC.2015.2472527.
- [7] R. Kaur et al., "A survey on reconfigurable intelligent surface for physical layer security of next-generation wireless communications", *IEEE Open Journal of Vehicular Technology*, vol. 5, pp. 172–199, 2024. DOI: 10.1109/OJVT.2023.3348658.
- [8] T. N. Balan, A. C. Balan, and F. D. Sandu, "SDR implementation of a D2D security cryptographic mechanism", *IEEE Access*, vol. 7, pp. 38 847–38 855, 2019. DOI: 10.1109/ACCESS.2019.2904909.
- [9] G. Verma, P. Yu, and B. M. Sadler, "Physical layer authentication via fingerprint embedding using software-defined radios", *IEEE Access*, vol. 3, pp. 81–88, 2015. DOI: 10.1109/ACCESS.2015.2398734.
- [10] Y. Hu, D. Xu, and T. Zhang, "Implementation and evaluation of physical layer key generation on SDR based LoRa platform", in *2023 IEEE 98th Vehicular Technology Conference*, 2023, pp. 1–5. DOI: 10.1109/VTC2023-Fall60731.2023.10333718.
- [11] J.-P. Hubaux, L. Buttyan, and S. Capkun, "The quest for security in mobile ad hoc networks", in *Proceedings of the ACM International Symposium on Mobile Ad Hoc Networking and Computing*, 2001, pp. 146–155. DOI: 10.1145/501416.501437.
- [12] S. Capkun, L. Buttyan, and J.-P. Hubaux, "Self-organized public-key management for mobile ad hoc networks", *IEEE Transactions on Mobile Computing*, vol. 2, no. 1, pp. 52–64, 2003. DOI: 10.1109/TMC.2003.1195151.
- [13] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks", in *Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking*, 2002, pp. 12–23. DOI: 10.1145/570645.570648.
- [14] U. K. Verma, S. Kumar, and D. Sinha, "A secure and efficient certificate based authentication protocol for MANET", in *2016 International Conference on Circuit, Power and Computing Technologies*, 2016, pp. 1–7. DOI: 10.1109/ICCPCT.2016.7530346.
- [15] D. S. Gupta, S. K. H. Islam, and M. S. Obaidat, "A secure identity-based deniable authentication protocol for MANETs", in *2019 International Conference on Computer, Information and Telecommunication Systems*, 2019, pp. 1–5. DOI: 10.1109/CITS.2019.8862037.
- [16] R. Kumar, Y. Shiv, V. Kumar, and M. Wairiya, "An authentication technique in mobile ad hoc network using elliptic curve cryptography", in *2018 8th International Conference on Cloud Computing, Data Science and Engineering*, 2018, pp. 14–15. DOI: 10.1109/CONFLUENCE.2018.8442504.
- [17] V. S. Janani and M. S. K. Manikandan, "CRT-KM: Chinese remainder theorem based key management scheme for securing ad-hoc networks", in *2015 IEEE International Conference on Signal Processing, Informatics, Communication and Energy Systems*, 2015, pp. 1–5. DOI: 10.1109/SPICES.2015.7091501.
- [18] K. A. Yadav, S. H. Islam, G. P. Biswas, and D. S. Gupta, "Hyperelliptic curve cryptography-based lightweight privacy-aware secure authentication scheme for VANETs", in *Advances in Computer and Computational Sciences*, 2018, pp. 461–471. DOI: 10.1007/978-981-10-8575-8_10.
- [19] W.-K. Chiang and W.-Y. Wang, "An efficient certificateless signcryption for mutual and batch authentication in vehicular ad-hoc networks (VANETs)", *Peer-to-Peer Networking and Applications*, vol. 18, no. 4, p. 206, 2025. DOI: 10.1007/s12083-025-02018-4.
- [20] W. Wang, Y. Zhao, D. Liu, and H. Huang, "A blockchain-enhanced cross-domain handover authentication scheme for vehicular ad-hoc networks", *Ad Hoc Networks*, vol. 189, p. 104 248, 2026. DOI: 10.1016/j.adhoc.2026.104248.
- [21] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system", [retrieved: August, 2026], 2008. [Online]. Available: <https://bitcoin.org/bitcoin.pdf>.
- [22] S. Josefsson and I. Liusvaara, *Edwards-curve digital signature algorithm*, RFC 8032, 2017. DOI: 10.17487/RFC8032.
- [23] OpenSSL Project, "OpenSSL: Cryptography and SSL/TLS toolkit", [retrieved: August, 2026], 2026. [Online]. Available: <https://www.openssl.org/>.
- [24] R. G. Gallager, "Low-density parity-check codes", *IRE Transactions on Information Theory*, vol. 8, no. 1, pp. 21–28, 1962. DOI: 10.1109/TIT.1962.1057683.
- [25] M. J. Page et al., "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews", *BMJ*, vol. 372, n71, 2021. DOI: 10.1136/bmj.n71.
- [26] M. Dansarie, "Security issues in special-purpose digital radio communication systems: A systematic review", *IEEE Access*, vol. 12, pp. 91 101–91 126, 2024. DOI: 10.1109/ACCESS.2024.3420091.
- [27] M. A. Al-Shareeda, M. Anbar, S. Manickam, A. Khalil, and I. H. Hasbullah, "Security and privacy schemes in vehicular ad-hoc network with identity-based cryptography approach: A survey", *IEEE Access*, vol. 9, pp. 121 522–121 531, 2021. DOI: 10.1109/ACCESS.2021.3109264.