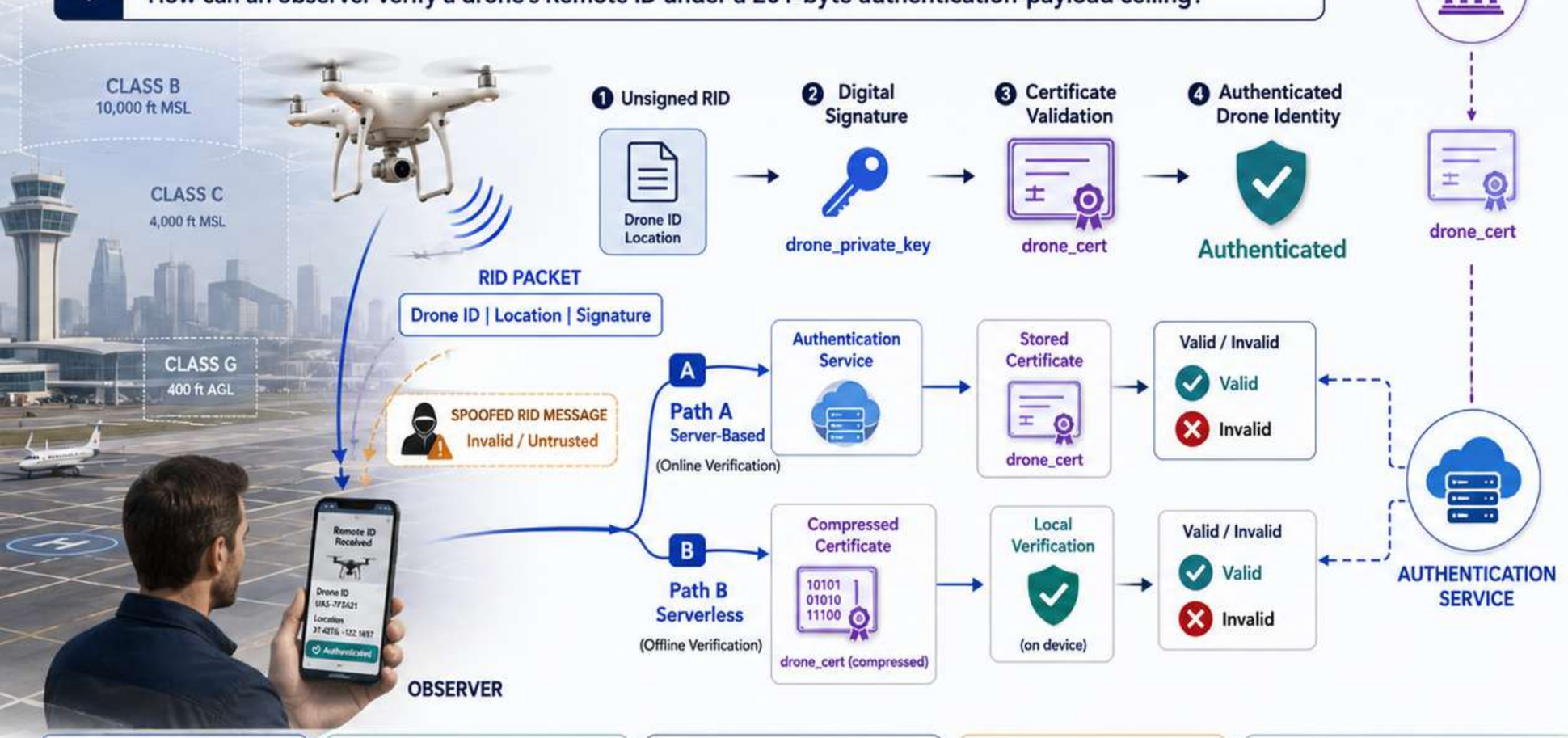
Authenticating UAV Broadcast Remote ID

Two ASTM-compliant PKI protocols for online and offline verification

MAIN RESEARCH QUESTION:
How can an observer verify a drone's Remote ID under a 201-byte authentication-payload ceiling?



HIGHLIGHTS OF THE PAPER

01 ASTM CONSTRAINT ANALYSIS:
Remote ID message size, broadcast periodicity, AuthPage fragmentation, and effective 201-byte authentication-payload ceiling.

02 TWO PKI AUTHENTICATION PROTOCOLS:
Protocol 1 uses an online Authentication Service; Protocol 2 uses a compressed C509 certificate for direct offline verification.

03 FORMAL SECURITY VERIFICATION:
Tamarin verifies liveness, private-key secrecy, certificate integrity, and RID-message integrity for both protocols.

04 COMPLETE IMPLEMENTATION AND EVALUATION:
UAV hardware, Android observer app, and cloud service evaluated for latency, payload, energy, and network reliability.

Signing: 38.22 ms

Local verification: 4 ms

Server verification: 530 ms

Signing energy: 14.33 mJ

Local verification is approximately **132× faster** in the evaluated setup.

Standard PKI can authenticate Broadcast Remote ID, but online and offline verification make different trade-offs.

Computers & Security, 2026 DOI: 10.1016/j.cose.2026.105075

Why a Signed Drone ID Is Hard to Broadcast

Strong cryptography must fit inside strict ASTM message and timing limits

ASTM F3411-22a
Remote ID Standard

1 PUBLIC BROADCAST

Civil drone broadcasts Basic ID and Location to legitimate observer with smartphone; malicious receiver copies or modifies RID stream.

Remote ID is publicly receivable, so an unsigned message can be spoofed, modified, or replayed.

2 ASTM MESSAGE LIMIT

ASTM F3411-22a constrains the size and timing of RID transmissions.

RID Message

25 bytes

Message Pack

Maximum 9 messages

Static messages: generally every 3 s

Dynamic messages: generally every 1 s

3 AUTHPAGE STRUCTURE

Authentication Message uses AuthPages to carry authentication data within the RID Message and Message Pack limits.

AuthPage 0

Header fields	(fixed)
Authentication data	17 bytes

AuthPages 1–15

Header	(fixed)
Authentication data	23 bytes each

17 + 23 × 8 = 201 bytes

Effective authentication-payload ceiling

Authentication data may extend across multiple AuthPages; the nine-message-pack limit constrains what fits in one pack.

4 CERTIFICATE PROBLEM

A standard X.509 certificate is far larger than the available authentication payload within one Message Pack.

Standard DER X.509 Certificate

Typically 500–1000 bytes

vs.

Available Authentication Payload (One Message Pack)

{ }

201 bytes

Does not fit

5 TWO DESIGN OPTIONS

Given the ASTM constraints, there are two practical design pathies.

Server-Based:
Do not broadcast the certificate.

Serverless:
Compress the certificate and divide authentication data across message packs.

RESEARCH GAP

Existing PKI approaches do not directly account for ASTM payload limits, message fragmentation, periodic broadcasts, and practical end-to-end verification performance.

RESEARCH TAKEAWAY: The main challenge is not only signing the RID message; **it is transmitting everything needed for verification within the standard.**

ASTM F3411-22a constrains RID Message size (25 bytes), Message Pack size (maximum 9 messages), timing (static ~3 s, dynamic ~1 s), and Authentication Message structure (AuthPage). These limits make broadcasting a complete, verifiable, signed identity fundamentally difficult.

RID Message | Message Pack (max 9) | AuthPage | Authentication Message

Two Ways to Verify the Same Signed Remote ID

Compact online verification or larger offline verification

SHARED ENROLLMENT

Drone Owner or Operator → Generate key pair → Create CSR → Certification Authority, CA → Issue drone_cert → Install drone_private_key on Drone

Protocol 1 — Server-Based

Drone | Observer | Authentication Service | Stored Certificate

1. Drone signs RID.
2. Drone broadcasts RID + 64-byte signature.
3. Observer authenticates with Authentication Service.
4. Observer receives JWT.
5. Observer sends RID + signature + JWT.
6. Service validates JWT. RS256
7. Service retrieves drone_cert.
8. Service verifies signature. Ed25519

Service returns Valid / Invalid.

JWT RS256 ••••••••

RID PACKET

Drone ID	Location	Signature (64 bytes)

JWT RS256 ••••••••

ADVANTAGES

- 64-byte authentication payload
- Drone does not broadcast certificate
- Observer does not store drone certificates

TRADE-OFFS

- Internet required
- Server availability required
- Token and network latency

Protocol 1: Smaller broadcast, higher infrastructure dependence

Protocol 2: Larger broadcast, near-real-time local verification

Protocol 2 — Serverless

Drone | Observer | ca_cert | C509 Certificate

1. Owner compresses drone_cert using C509.
2. Drone stores private key and compressed certificate.
3. Drone signs RID.
4. Drone broadcasts RID + signature.
5. Drone separately broadcasts compressed C509 certificate.
6. Observer decompresses certificate.
7. Observer verifies certificate using ca_cert.
8. Observer verifies RID signature locally. Ed25519
9. Observer accepts or rejects the drone.

ADVANTAGES

- Offline verification
- No Authentication Service
- Approximately 4 ms local verification

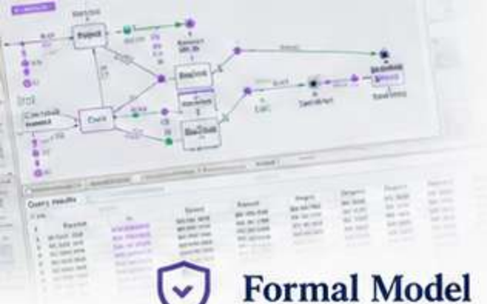
TRADE-OFFS

- 64 + 136 byte authentication payload
- Two message packs required
- Both packs must be received

RESEARCH TAKEAWAY: The protocols authenticate the same signed RID message but place the certificate-verification work in different locations.

From Security Proof to UAV Hardware

Tamarin verification and a complete Remote ID implementation



Formal Model → **Drone Module** → **Wireless Broadcast** → **Observer App** → **Authentication Server**

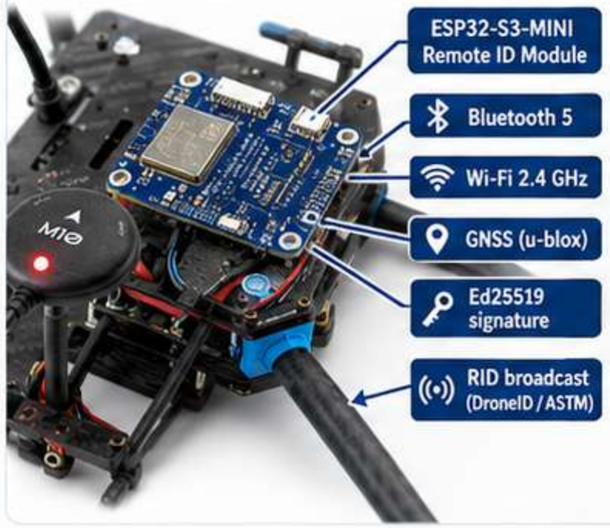
Tamarin security matrix

	Protocol 1	Protocol 2
Protocol Liveness	✓ Verified	✓ Verified
Private-Key Secrecy	✓ Verified	✓ Verified
Certificate Integrity	✓ Verified	✓ Verified
JWT Authenticity	✓ Verified	− Not Applicable
RID Message Integrity	✓ Verified	✓ Verified
Injective Agreement	✗ Not Verified	✗ Not Verified

Threat model (Dolev-Yao)

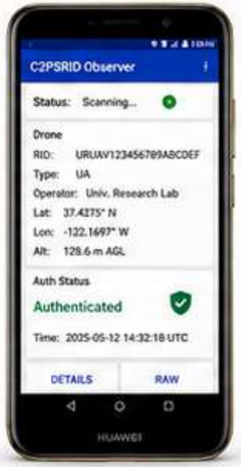
Dolev-Yao adversary may intercept, modify, delete, replay, and inject messages, but cannot forge signatures without the private key.

Commodity hardware implementation



RID broadcast (ASD-BT / Wi-Fi Aware)

Android C2PSRID observer app



- Scan RID
- Show drone ID
- Show location
- Show authentication status

Authentication Service

- **JWT** verification
- certificate lookup
- Ed25519 signature verification
- database and cache

64-byte Ed25519 signature | 136-byte C509 certificate | HTTPS / WebSocket | RS256 JWT | 1000 trials per protocol configuration

Limitation: physical-source ambiguity

Legitimate drone signs and broadcasts RID message

Malicious rebroadcaster relays the message from a different location

Cryptography authenticates the signed message, but it **does not conclusively bind** that message to the nearby physical radio transmitter.

Potential mitigations

require AoA, RSSI, RF fingerprinting, or cross-sensor correlation.

The protocols are logically secure under the formal model, but physical-source identification remains an open problem.

What the Evaluation Shows

Latency, payload, energy, and network-scale authentication performance

1 TIMING AND PAYLOAD COMPARISON (Table 6)

	Protocol 1 Server-Based	Protocol 2 Serverless
Signing time	38.22 ± 0.003 ms	38.22 ± 0.003 ms
Verification time	530 ± 370.6 ms*	4 ± 0.0552 ms
Authentication payload	64 bytes	64 + 136 bytes
Offline capability	✗ No	✓ Yes

Local verification is approximately **132×** faster in the evaluated setup.

* Protocol 1 timing assumes the observer is already authenticated; login may add substantially more delay.

2 MESSAGE PACK CONSTRUCTION (Figure 5)

MESSAGE PACK 1 (150 bytes)

1. Identification page (25 B)
2. Location page (25 B)
3. AuthPage 0 – Signature (17 B)
4. AuthPage 1 – Signature (23 B)
5. AuthPage 2 – Signature (23 B)
6. AuthPage 3 – Signature (1 B)

(3–6: 64-byte signature fragmented)

- 6 messages × 25 bytes = 150 bytes
- Carries the 64-byte Ed25519 signature

Signature broadcast: every 1 second (Message Pack 1)

MESSAGE PACK 2 (175 bytes)

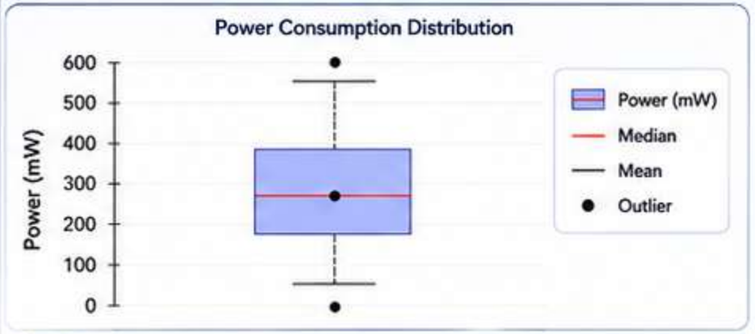
1. AuthPage 0 – Cert (17 B)
2. AuthPage 1 – Cert (23 B)
3. AuthPage 2 – Cert (23 B)
4. AuthPage 3 – Cert (23 B)
5. AuthPage 4 – Cert (23 B)
6. AuthPage 5 – Cert (23 B)
7. AuthPage 6 – Cert (4 B)

(1–7: 136-byte C599 certificate fragmented)

- 7 messages × 25 bytes = 175 bytes
- Carries the 136-byte compressed C509 cert

Certificate broadcast: every 3 seconds (Message Pack 2)

3 ENERGY CONSUMPTION (Figure 6)

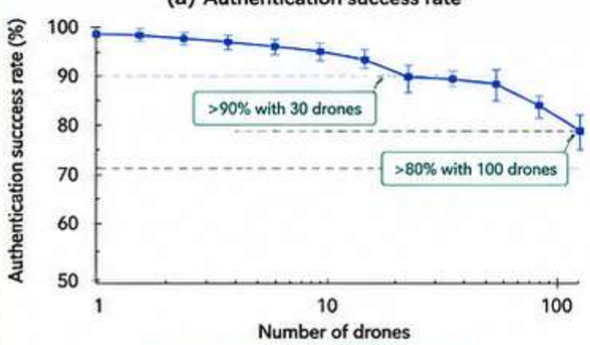


- Median power: **375 mW**
- Measured range: **260–450 mW**
- Signing energy: **14.33 mJ** per RID signature

Ed25519 signing introduces limited energy overhead on the ESP32-S3-MINI prototype.

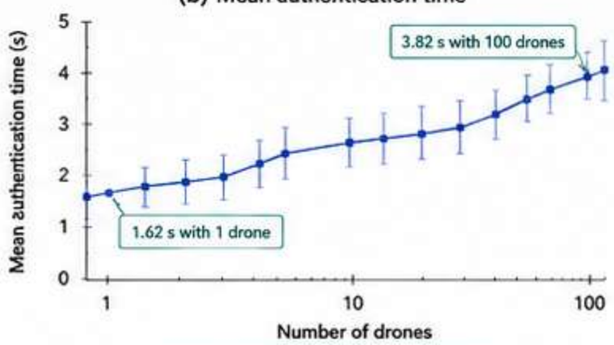
4 NETWORK SIMULATION PERFORMANCE (ns-3)

(a) Authentication success rate



97–100% success at low densities

(b) Mean authentication time



Latency grows with drone density

SIMULATION SETUP

ns-3 · 500 m × 500 m open area · 1–100 drones · 10–25 m/s Gauss-Markov mobility · BLE and Wi-Fi broadcast in parallel · 100 Monte Carlo trials per population (900 total trials) · 10-second observation window

TRADE-OFF SUMMARY

Protocol 1 — Server-Based

- 64-byte authentication payload
- Compact broadcast footprint
- No certificate in broadcast
- No certificate storage on observer
- Requires Internet connectivity
- Depends on server availability
- Token and network latency

Protocol 2 — Serverless

- 64 + 136 byte authentication payload
- Fast local verification (~4 ms)
- No Internet or server required
- Supports offline operation
- Two message packs required
- Both packs must be received
- Observer must store CA certs

FINAL RESEARCH CONCLUSION

ASTM-compliant Broadcast Remote ID authentication is feasible using standard PKI and commodity hardware, but system designers must choose between smaller broadcasts and offline resilience.

⚠ LIMITATIONS

- No cryptographic proof of physical transmitter identity
- Android observer platform only
- Server and token dependency in Protocol 1
- Limited certificate-payload headroom (201-byte ceiling)
- ns-3 uses an approximate BLE model
- Ideal open-air simulation may be optimistic
- ~80% success at 100 drones is insufficient for high-assurance deployment

CAUSE-AND-EFFECT CHAIN

ASTM constraints (25-byte messages, 9 messages per pack, 201-byte auth ceiling) → Signed RID (Ed25519 signature 64 bytes) → Choose server or local verification (Protocol 1 or Protocol 2) → Validate certificate and signature (CA trust + Signature check) → Authenticate the message (Valid or Invalid) → Manage payload, latency, and availability trade-offs

FINAL TAKEAWAY: Small broadcast or offline verification—both are possible, but each has a different operational cost.

Computers & Security, 2026 | DOI: 10.1016/j.cose.2026.105075