sk-High.net

Declassified Asset

DROPLET

Deployable Rooftop Observation & Passive Listening Exploitation Tool

Inspector Gadgets · skHighNet
Idea Credit: Randy Pesek

DROPLET — Deployable Rooftop Observation & Passive Listening Exploitation Tool

Product line: Inspector Gadgets (skHighNet) **Status:** Concept phase **Idea credit:** Randy Pesek

---

Executive Summary

DROPLET is a throwable, waterproof Bluetooth surveillance device that deploys in seconds — you throw it onto a roof, it catches in the gutter or valley, and it begins passive signal interception of every Bluetooth device in the building. No setup, no re-entry, no risk.

Current SDR drops are disposable toys with short battery life and no real protocol capture. DROPLET solves deployment, power, and signal interception in one hardened package. It's not a bug you place — it's a rock you throw.

---

1. Deployment: Throw-and-Stick, Zero Setup

Shape

Asymmetric teardrop/pyramid: - **Heavy end forward** — ballistic tip, aluminum core. Positions itself for impact on landing. - **Light tail stabilizes** in flight — TPU fin/flange catches on roof features. - **Center of mass** at forward 1/3rd. Like a throwing knife — predictable spin, lands heavy-side-first.

Catch Points

Designed to wedge into any of these: - **Gutters** — flange catches the lip, body sits inside or against the gutter channel - **Valley seams** — where two roof planes meet, wedge between them - **Ridge vents** — flange hooks the vent louver - **Shingle overlap** — slides under the edge of a course of shingles - **Solar panel frame** — magnet variant clamps to aluminum rail

Impact Survival

- **Shell:** TPU overmold over a milled aluminum core. Shore hardness 85A — stiff enough to protect, soft enough to absorb impact.
- **Drop rating:** 3m+ onto concrete. Rooftop drops are typically 1-2m. With margin.
- **Potted electronics:** Epoxy filled — no air gaps, no water paths, no component rattling. The board is a solid block inside the shell.

Camouflage

Color-matched to common roofing stock: - **Charcoal shingle** (most common asphalt) - **Terra cotta tile** (southwest) - **Galvanized gutter gray** - **Dark wood / cedar toned**

Surface textured to match roof gravel grit — matte finish, no reflection. The device looks like a roof pebble.

On the roof: invisible unless you're standing on the roof looking directly at it.

Magnetic Backup

Integrated rare earth magnet plate (N52): - Optional adhesive-backed steel washer for non-magnetic surfaces - Direct stick to metal roofs, gutter channels, HVAC units, satellite dishes - The magnet provides ~5lbs of pull — will not slide off a gutter in wind

---

2. Power Architecture — The Real Differentiator

Battery life is what kills every other device in this class. DROPLET doesn't compete on the same field.

Core MCU: nRF5340

Parameter	Value
Architecture	Dual-core Arm Cortex-M33 (1x app, 1x network)
BLE version	5.4 (LE Audio, AoA, advertising extensions)
Thread/Zigbee	Yes (network core)
Idle current	0.9 µA (system OFF, retained RAM)
Active TX current	~3.5 mA (BLE broadcasting)
RX current	~2.8 mA (active listening)
Wake time	< 1 µs from sleep

10-100x better idle power than an ESP32 (which pulls ~80mA even in deep sleep on some boards).

Power Budget

Sniff/record mode: nRF5340 active + SDR powered + MEMS recording: - Active: ~50 mA - Duty cycle: 10% (sniff 6 seconds every minute) - Average: ~5 mA average draw

Passive scan mode (BLE only): nRF5340 BLE listening only, SDR off: - Active: ~3 mA - Duty cycle: 20% - Average: ~0.6 mA

Deep sleep (standby): Timer wake every N hours for brief check-in: - Idle: ~1 µA - Wake duration: 100ms sync - Essentially negligible

Battery Config	Passive Scan	Sniff/Record	Standby
400 mAh LiPo (internal)	~28 days	~3.3 days	~45 years
400 mAh LiPo + solar trickle	Indefinite (light)	Indefinite (light)	—

Battery Config	Passive Scan	Sniff/Record	Standby
2000 mAh 18650 (external sled)	~138 days	~16 days	—

Solar trickle: Amorphous thin-film cell embedded in the top surface. Even under gutter overhang (partial sky view), generates 1-5 mA in daylight. Enough to offset standby + brief active windows indefinitely. Full sun: 15-20 mA — actively charges the battery during the day.

Solar Integration

- **Cell type:** Amorphous silicon (a-Si) — works in low/diffuse light, partial shade, dawn/dusk
- **Output:** 5V @ 22 mA peak in full sun, ~1-3 mA in overcast
- **Placement:** Embedded flush in the top face of the shell
- **View angle:** 30° tilt built into shell shape — catches more light than flat-on-roof

Result: In any deployment that gets partial sky view (gutter edge, valley, ridge vent), DROPLET's battery stays topped off indefinitely. Solar charging covers the entire passive-scan power budget in 2-3 hours of daylight.

---

3. Signal Capability

This is where DROPLET separates from dumb BLE sniffers.

Hardware Stack

Component	Role	Power
nRF5340	BLE host + app processor	~3 mA active
SDR frontend (MAX2839 or SiLabs EZRadio)	BT Classic + broad spectrum capture	~20 mA active
MEMS microphone (bottom-facing)	Audio capture	~1 mA
64 MB SPI flash (W25Q512)	Onboard storage	~5 mA write, 0 idle
Semtech SX1262	LoRa radio (exfil)	~15 mA TX, ~1 mA RX

BT Classic Sniffing

Paired Bluetooth headsets and speakers in the home broadcast predictable HCI traffic. DROPLET:

1. Scans for BT Classic inquiries/page scans
2. Identifies known device addresses from paired devices
3. If a headset is actively connected, captures unencrypted portions of HCI traffic
4. If pairing mode is detected, can attempt known-pairing-attack or relay

Practical impact: Capture audio stream from a headset paired to a phone in the house if: - The headset is in discovery/pairing mode - The connection uses legacy pairing (not Secure Simple Pairing) - DROPLET successfully MITMs the reconnection

Limitations: Modern BT 5+ headsets use Secure Simple Pairing + encryption. Audio stream capture requires the pairing key. This is the advanced play — not guaranteed, but worth attempting.

BLE Passive Tracking

DROPLET passively logs every BLE MAC address it hears: - Phones (iOS, Android) - Smart watches (Apple Watch, Garmin, Fitbit) - Fitness trackers (Oura, Whoop) - Asset tags (AirTags, Tile, Samsung SmartTag) - Smart home devices (thermostats, locks, sensors)

Output: A time-stamped device map of the building — who is present, what devices they carry, when they come and go, and what BLE relationships exist (device A is always near device B = they belong to the same person).

Broad Spectrum SDR Scan (Periodic)

DROPLET can be programmed to do a full spectrum survey once per hour/day/on-command:

- **WiFi (2.4/5 GHz):** SSID discovery, client detection, channel utilization
- **Zigbee/Thread (2.4 GHz):** Smart home sensor networks, lightbulbs, plugs
- **Baby monitors / wireless cams:** Identify analog and digital video feeds
- **Microwave / oven interference:** Patterns of use
- **Cellular faint signals:** Approximate carrier presence

Purpose: Maps the full wireless environment of the building — not just BLE. You know what's on, when it's on, and if something new suddenly appears (irregular phone, unauthorized device).

Audio Recording

Bottom-facing MEMS microphone with acoustic port in the shell.

- **Not constant recording** — storage is 64MB, not infinite
- **Voice-activity triggered:** Recording only when speech is detected above ambient
- **Pairing-event triggered:** Records a 30-second clip when any new BT pairing occurs in range
- **Command-triggered:** LoRa command "record_audio for 60 seconds" — manual override
- **Compression:** Opus codec at 16kbps — ~120 KB per minute, holds ~8 hours of voice

---

4. Exfil — Multiple Paths, Zero Trust

LoRa (Primary)

Parameter	Value
Radio	Semtech SX1262
Frequency	915 MHz ISM (US) / 868 MHz (EU)
TX power	+22 dBm (max)
Range	1-5 km LOS (urban), 5-15 km (suburban/rural)
Data rate	200-500 bytes per minute (SF10, 125kHz)
Protocol	LoRaWAN or custom point-to-point

Enough bandwidth for: - Telemetry packets (battery, temp, device count): every 10 minutes - BLE device list updates: every 4 hours - Audio clips (compressed): one 30s clip per payload, delivered when channel is open

You can sit in a car a block away or at a coffee shop across town and receive real-time data.

BLE Relay (Secondary)

When you're within ~50m of the target: - DROPLET dumps the entire flash contents over BLE GATT (custom service) - Transfer rate: ~5-10 KB/s - 64 MB flash dumps in ~2-3 hours while you sit nearby - Partial dump by date range supported

Mesh Relay (Future)

Multiple DROPLETs on multiple roofs form a LoRa mesh: - One unit with a clear shot to your receiver relays for the rest - Extends range well beyond single-hop LoRa limits - Broadcasts GPS coordinates of each relay hop - Network auto-discovers — drop units, they self-organize

Store-and-Forward Default

Always: 1. Records to onboard flash (64 MB, 30-day rolling buffer) 2. Exfil attempts on every exfil opportunity (LoRa ping BLE scan) 3. Once data is confirmed delivered by the receiver, marks flash as consumed 4. If no exfil in 30 days, oldest data is overwritten

No data loss if the pickup window is missed. The device has months of buffer.

---

5. Stealth — Active Camouflage

RF Silence at Idle

- **No periodic beacons.** The device does nothing that advertises its presence.
- **No "check-in" pings.** No heartbeat. No "I'm still here."

- **RF frontend completely powered down.** Zero emissions measurable by any consumer device.
- The device is a rock until you wake it.

Randomized Activity Windows

When scheduled sniffing is active: - Not on a fixed timer — adds +/- 30% jitter to all timing - Sniff duration varies: 4-12 seconds per window - SDR on-time is short and unpredictable from outside

No pattern to fingerprint. A spectrum analyzer watching for a consistent sequence won't find one.

Scheduled Operation

- Default: only active during programmed hours (configurable)
- Example: 9 PM - 6 AM — when people are home, BT headsets are paired, conversations are happening
- Daytime: deep sleep, solar charging, no RF activity

The schedule is also tunable per weekday — no sense sniffing an empty house during office hours.

Self-Destruct Chain

Trigger	Action
LoRa command `wipe`	Erase flash, zero all sectors
LoRa command `brick`	Wipe flash + set deep-sleep lock (irreversible until battery drain)
No LoRa signal for N days	Auto-wipe flash (dead-man switch)
Tamper detection	If shell is pried open, light detected by internal photodiode triggers immediate wipe + brick
Physical destruction	Device contains a small chemical reaction (reactant A + B mix when shell breaks, turning everything to slag). Not included in v1.

Design principle: If anyone recovers DROPLET, they get a dead, blank, bricked piece of epoxy with no identifiable data, no firmware, no identifying marks. It tells them nothing.

---

6. Build Path

v1 — Proof of Concept

Component	Source	Est. Cost
nRF5340 DK (dev kit)	Nordic Semi	$40
MEMS mic + breakboard	Adafruit SPH0645LM4H	$7
SPI flash W25Q512	Digikey	$6
LoRa module + breakboard	Adafruit RFM95	$20
Battery 400 mAh LiPo	Adafruit	$8
Prototype shell (3D print TPU)	Print	$2
Total		**$83**

Goal: Functional prototype. Hand-soldered, breadboard first, then perfboard. Test on your own roof for a week. Validate deployment shape, impact survival, BLE sniffing, audio recording, LoRa exfil range.

v2 — Field Prototype

Component	Source	Est. Cost
Custom PCB (4-layer, nRF5340 + SDR)	JLCPCB	$20/board
SDR frontend MAX2839	Digikey	$12
Solar cell (a-Si, 0.5W)	Voltaic	$15
Milled aluminum core	Protolabs	$50 (first, $10 after)
TPU overmold	Protolabs	$100 (first, $15 after)
Assembly	Hand	Free
Total		**~$200 (first), ~$60 (after)**

Goal: Field-deployable. Smaller, solar-integrated, properly potted. SDR onboard for spectrum scanning. 3-5 units built, tested in different environments (urban, suburban, rural).

v3 — Production

Component	Source	Est. Cost
Custom PCB (assembled)	JLCPCB/PCBWay	$12/board (qty 100)
Injection-molded TPU shell + aluminum core	Protolabs	$8/unit (qty 100)
Battery 400 mAh (custom shape)	Adafruit or custom	$4
Full assembly	Contract manufacturer	$15/unit
Total BOM		**~$40/unit (qty 100)**

Goal: Reliable, repeatable, sellable or deployable in volume. Color variants. Configurable firmware (BLE-only scan vs SDR full, Lora vs cellular exfil, etc.).

Target price: $150-250 per unit (comparable to a mid-range SDR but with all the integration and deployment work done).

---

7. Variants

DROPLET-S (Solar) — Indefinite Deployment

- Top-shell amorphous solar cell as standard
- No battery swap needed
- Indefinite operation with any daylight
- SDR disabled by default in low-light conditions
- Best for: permanent installations, long-term monitoring

DROPLET-C (Cellular) — No Range Limit

- Replaces LoRa with LTE-M / NB-IoT cellular module
- No need for a receiver nearby
- Data goes direct to cloud
- Battery life: ~14 days (cellular is power-hungry)
- Best for: one-shot missions where you can't LoRa

DROPLET-P (Passive) — Lowest Cost, Pure BLE

- Strips SDR frontend entirely
- BLE passive scan only
- Audio via MEMS mic (no stream capture)
- Exfil via BLE relay only (no LoRa, no cellular)
- Battery: 400mAh LiPo, ~30 days
- Cost target: $25/unit (qty 100)
- Best for: saturation deployment — throw 10 of these on a block

DROPLET-X (Extended) — Larger Battery, Longer Deployment

- 18650 sled (2000mAh)
- All features enabled (SDR, audio, spectrum scan, LoRa)
- ~138 days passive scan, ~16 days active sniffing
- Larger shell (roughly 2x volume)
- Best for: deep-cover long-term ops

---

8. Competition Analysis

Device	Price	Battery	BT Sniff	SDR	Deploy	Audio	Exfil
Flipper Zero	$169	7 days	BLE only	No	Hand-place	No	BT/USB
Hak5 Packet Squirrel	$80	USB	No	No	Plug in	No	USB
Ubertooth One	$120	USB	BT Classic	No	Cable	No	USB
Custom ESP32 bug	$15	2-3 days	BLE only	No	Hand-place	Mic	BT
DROPLET v3	**$150-250**	**30 days+**	**BT Classic + BLE**	**Yes**	**Throw**	**Yes**	**LoRa/ BT**
DROPLET-S	**$200-300**	**Indefinite**	**BT Classic + BLE**	**Yes**	**Throw**	**Yes**	**LoRa/ BT**

No existing device combines throw-deployment, SDR, battery life, audio, and multi-path exfil in a single package. Every competitor falls short in at least 2 of these 5 dimensions.

---

9. OPSEC & Operational Considerations

Pre-Deployment

- Device is built and flashed in a Faraday environment
- No test transmissions before deployment
- Serial numbers, MAC addresses, and labels: none. Device has no identifying markings.
- Firmware is compiled from a builders-only branch, never pushed to public repos
- LoRa packets are encrypted (AES-256-GCM) with a key that lives only on the builder's machine and the receiver

Deployment

- Throw from a distance. Do not handle the unit with bare hands (gloves).
- Deploy at a time when you're not surveilled / the area has low traffic
- Multiple deployment points within the same mission create pattern risk — vary your timing
- Note GPS coordinates of deployment for exfil alignment (your LoRa receiver needs approximate range)

Active Operations

- DROPLET does not respond to any BLE inquiry or connect request from unknown devices
- The LoRa frequency is in the ISM band and looks like any other IoT sensor traffic
- Scheduled operation windows reduce exposure risk

- No geofencing or GPS onboard (GPS is a detectable signal and uses power) — range-based targeting only

Post-Deployment / Recovery

- Recovery of a deployed unit is a risk. If recovery is attempted:
- Send `wipe` command via LoRa immediately
- If wiped, the device is inert — harmless to recover
- If unrecoverable, dead-man switch auto-wipes after N days
- Do not deploy in jurisdictions where this device violates local surveillance laws. **This document is for educational and authorized security testing only.**

---

10. Bill of Materials (v3, qty 100)

Category	Item	Cost/Unit
MCU + BLE	nRF5340 + antenna matching	$8.00
SDR	MAX2839 + balun + filter	$12.00
LoRa	SX1262 + matching	$4.00
Audio	MEMS mic + acoustic port seal	$2.00
Storage	W25Q512 (64MB)	$3.00
Power	400mAh LiPo	$4.00
Solar	a-Si cell 5V/22mA	$3.00
Magnets	N52 10mm disc	$0.50
Shell	Injection molded TPU + aluminum core	$8.00
PCB	4-layer HDI, assembled (JLCPCB)	$12.00
Epoxy	Thermal potting compound	$1.00
Misc	Passives, connectors, RF shields	$3.00
Total BOM		**$60.50**
Assembly labor (contract)		$15.00
Testing + QC		$10.00
Total Unit Cost		**$85.50**
Target Retail		**$200-300**

Concept Credit

Randy Pesek — original idea, product vision, naming

This document is a concept exploration, not a build guide. Circuit design, PCB layout, firmware development, and regulatory compliance (FCC, ISED, CE) are required before any production run.