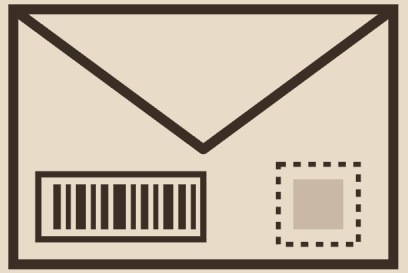
RIPE NCC INTERNET MEASUREMENT DAY · ALMATY · 3 NOVEMBER 2026

What does the disguise cost?



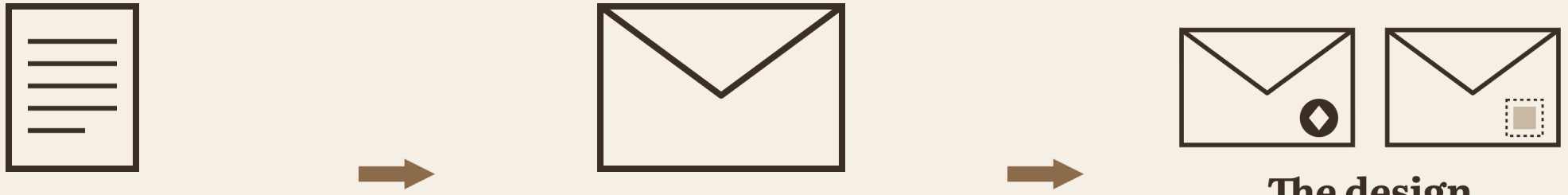
Separating encapsulation from camouflage in circumvention transports

Askar Oralkhan

Supervised by Temirlan Zhaxalykov

School of Information Technology and Engineering, KBTU, Almaty

A tunnel is a letter in an envelope



The letter

your traffic

The envelope

the outer connection

ENCAPSULATION

The design

what an observer sees

CAMOUFLAGE

TCP = registered letter. Lost → resent, and everything behind it waits.

UDP = ordinary letter. Lost → gone, and nothing waits.

THE PROTOCOLS

Four tunnels, four envelopes

	LOGO · SELF-IDENTIFYING	ORDINARY STAMP · CAMOUFLAGED
UDP outer ordinary letter	 **WireGuard** A standard VPN. Its fixed handshake names the protocol.	 **Hysteria2** Runs over QUIC and looks like an HTTP/3 website.
TCP outer registered letter	 **VLESS-plain** No disguise at all: our control.	 **REALITY** Borrows the TLS handshake of a real website.



Direct: no envelope at all, the baseline.

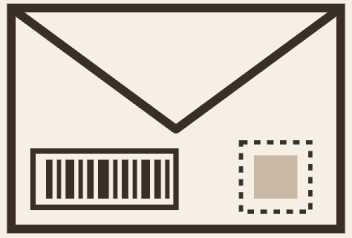
THE HYPOTHESIS

What everyone assumes: the design slows the mail

Hypothesis: the disguise is what makes stealth tunnels slow.

Practitioner lore says REALITY is slow because of its disguise — and we believed it too.

IF IT IS TRUE



REALITY

loses far more than

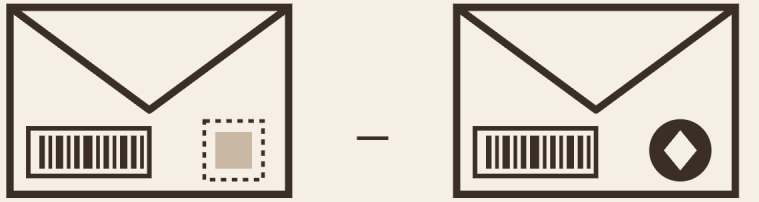


VLESS-plain

Same envelope, different design.

THE TEST

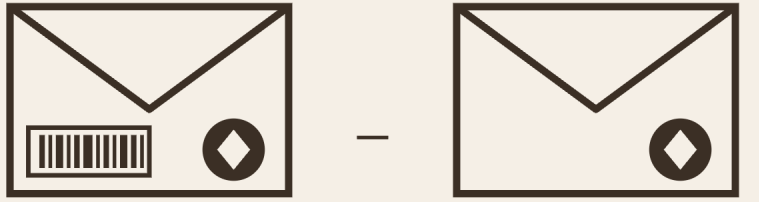
Change one thing at a time



REALITY − VLESS-plain =

the design

camouflage · same envelope, different design



VLESS-plain − WireGuard =

the envelope

encapsulation · same design, different envelope

VLESS-plain is REALITY with the disguise removed and nothing else changed. No earlier comparison we know of had this control.

THE LAB

Our lab: a post office on a bad road

Sender
test traffic → tunnel client

the bad road
loses and delays letters, in each direction

Receiver
relay → an address reachable only through the tunnel

0 to 5 %
letters lost on the road, no delay

50 to 200 ms
round trip, nothing lost

7 setups
5 tunnels; the TCP ones with CUBIC and with BBR

5 × 30 s
runs per condition, interleaved, one session

One machine and an emulated road: not a real censor, not a real path.

THE METRICS

Four things we measured, and why

Calls and video: UDP sent at a constant 100 Mbit/s that never slows down

Downloads: bulk TCP, as fast as it can go, up to 1 Gbit/s



Lost letters

OBSERVED UDP LOSS

Calls can’t wait for a resend.



Delivered rate

DELIVERED UDP RATE

What actually arrives, not what was sent.



Download speed

TCP GOODPUT

For downloads, only total speed matters.



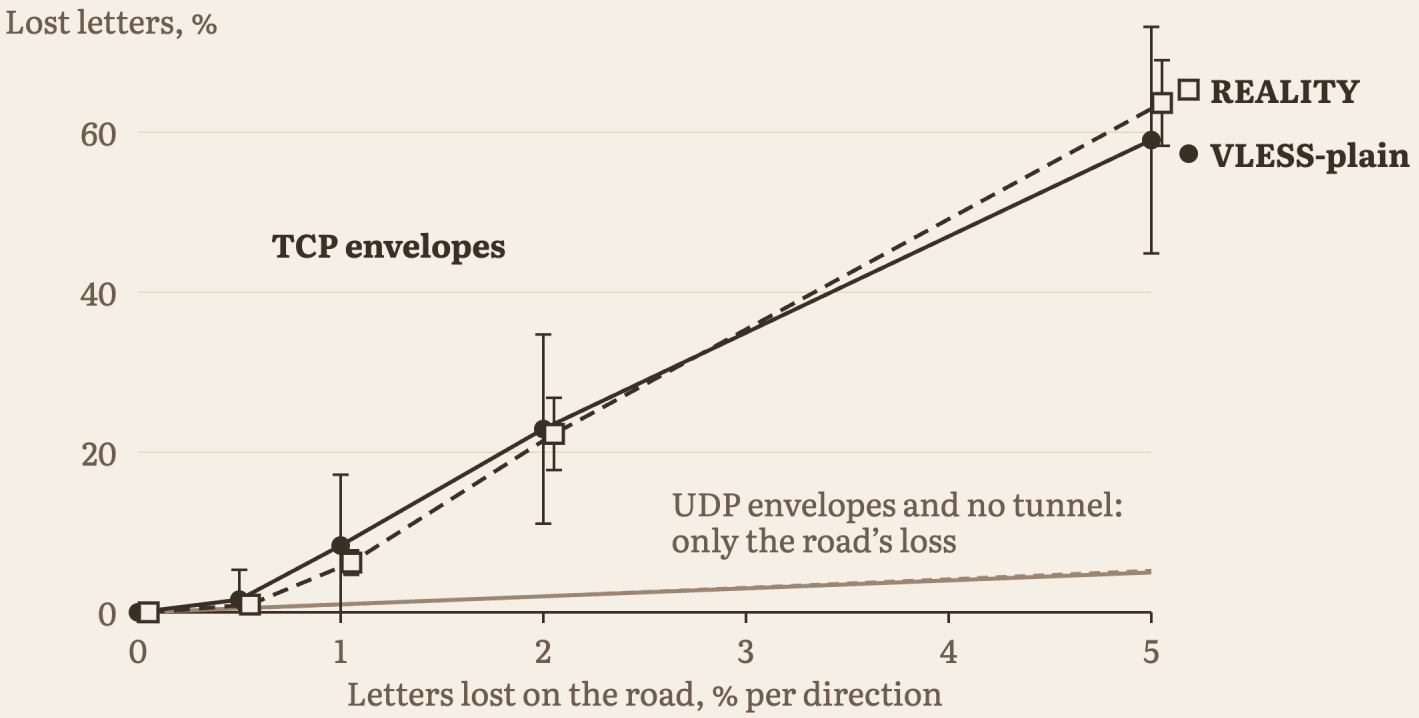
Delivery time

ECHO ROUND TRIP, 95TH PCT.

A late letter is as bad as a lost one.

RESULT 1 OF 3 · CALLS AND VIDEO

The envelope decides what arrives; the design doesn't



Observed UDP loss · outer TCP on CUBIC · 5 runs, bars = 95 % interval

HYPOTHESIS

Falsified

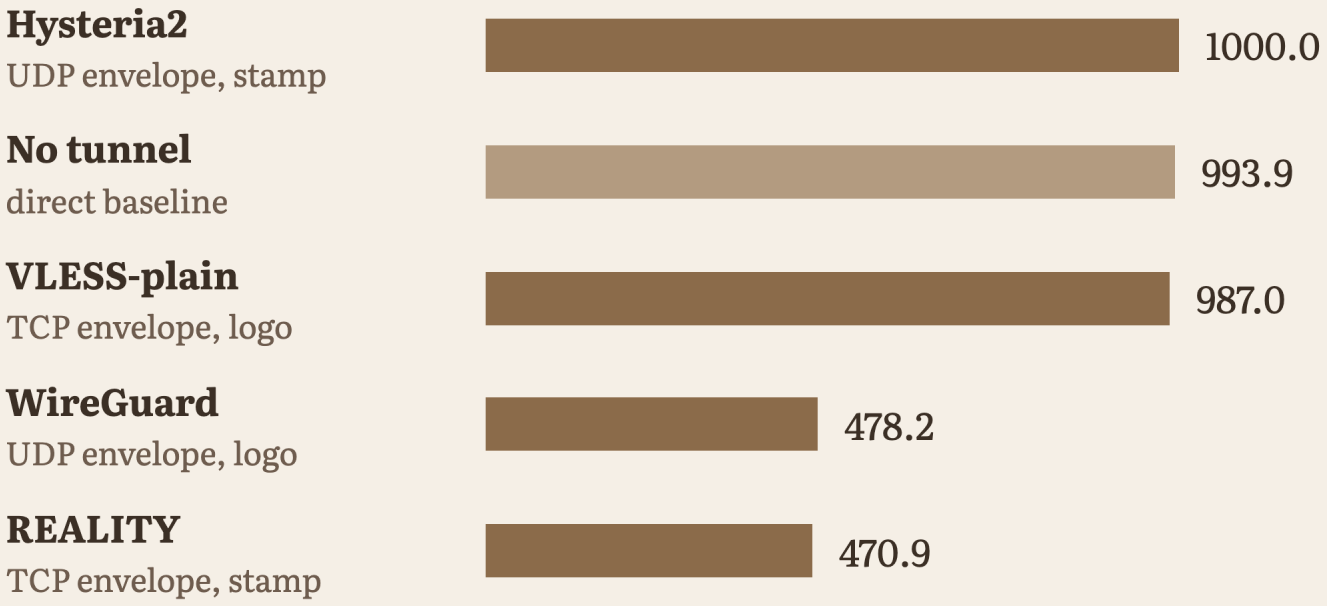
for calls and video

Same envelope, same curve. The disguise adds no difference we can measure.

A TCP envelope waits for every resend. The mailroom shelf overflows and letters are thrown away — none are lost on the road itself.

RESULT 2 OF 3 · DOWNLOADS

For downloads, a TCP envelope can even help



Download speed (TCP goodput) at 2 % road loss, Mbit/s · outer TCP on CUBIC

A clerk re-sends for you

The TCP envelope ends your connection locally and re-sends lost letters itself. WireGuard carries your own TCP end to end, so every loss slows you down.

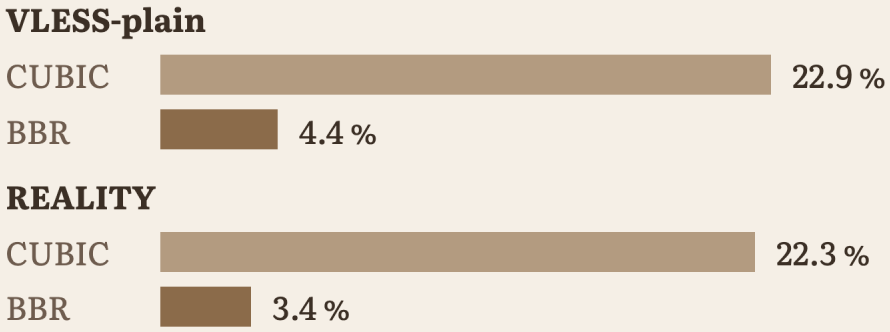
One gap

Here REALITY got half of VLESS-plain's speed. Result 3 shows what happens to it.

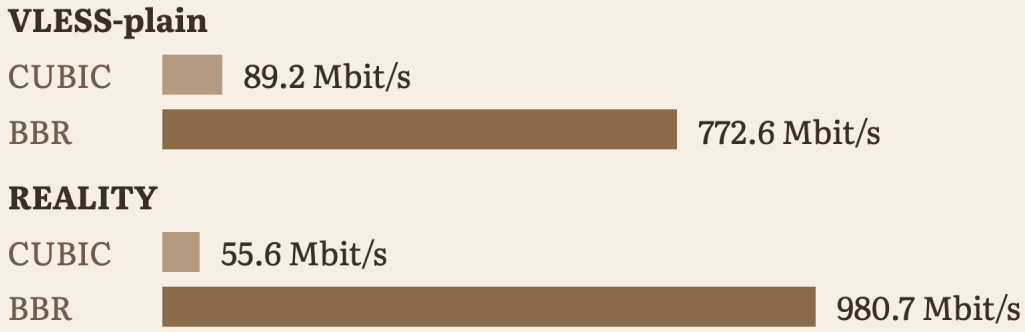
The clerk’s policy matters more than the design

One change only: the outer TCP’s congestion controller. **CUBIC** panics at every lost letter; **BBR** keeps a steady pace.

Lost letters at 2 % road loss



Download speed at 5 % road loss



The gap from Result 2 disappears: with BBR, REALITY and VLESS-plain both download at about 1 Gbit/s.

Three traps in our own post office

The shelf was too small

A delay test turned into a loss test: Linux's default queues and buffers dropped letters.

35 % → 4 %

seen → after raising the defaults

Every session gave a different answer

Same tunnel, same machine, same settings. The cause is still open.

20.6 to 46.1 %

loss at 2 % road loss, five sessions

The tool timed the wrong trip

iperf3 timed the trip to the local clerk, not the road.

1.3 ms vs 200 ms

reported vs real round trip

Fixes: raise and record host defaults · compare only within one session · read receiver-side numbers. All nine traps are reproducible.

WHO CAN USE THIS

What to do with the result

Network operators

Calls breaking up under loss? Check the envelope first, not the disguise.

Expect downloads through a TCP envelope to hold up better than through a VPN.

Tool builders and users

Carry calls in UDP envelopes where they get through.

On a TCP envelope, switch the congestion controller to BBR at both ends.

People who measure

Raise and record the host’s default queues and buffers.

Compare only within one session, and keep failed runs.

CONCLUSION AND FUTURE WORK

It’s the envelope, not its design

WHAT WE FOUND

1. The envelope costs tens of points of loss; the disguise, a few at most.
2. For downloads, a TCP envelope can even help.
3. On a TCP envelope, the congestion controller matters more than the disguise.

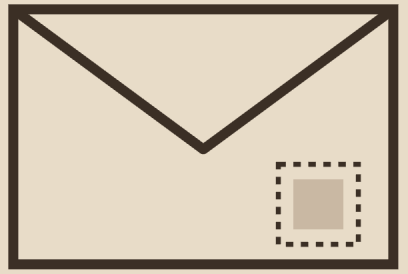
WHAT COMES NEXT

- → Where the loss starts: the sending rate at which a TCP envelope begins to drop letters.
- → Real paths: test the result outside the lab.
- → The disguise as a fingerprint: REALITY’s handshake timing and its post-quantum key share.

Limits: one machine · emulated loss and delay · one implementation (sing-box) · single flows · 5 runs per condition

Thank you

Questions, and real-path vantage points, are very welcome.



Askar Oralkhan

a.oralkhan@kbtu.kz

Supervised by Temirlan Zhaxalykov · School of Information Technology and Engineering, KBTU

Harness and data
will be released.