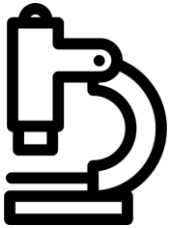
Testing and Improving the Correctness of Wi-Fi Frame Injection

Mathy Vanhoef [1], Xianjun Jiao [2], Wei Liu [2], and Ingrid Moerman [2]

[1] KU Leuven University, [2] Ghent University (Belgium)

Wi-Fi frame injection

Normally: kernel or network card constructs Wi-Fi frames



Research: want to construct custom (“raw”) Wi-Fi frames

How to inject frames?

Raw Wi-Fi frame to transmit

```
>>> sendp(RadioTap()/Dot11(addr1=...)/Dot11Deauth())
```

How to inject frames?

```
>>> sendp(RadioTap()/Dot11(addr1=...)/Dot11Deauth())
```

Radiotap header:

- To specify bitrate, channel bandwidth,…
- Parsed & removed by kernel (never actually transmitted)

Two possible monitor modes:

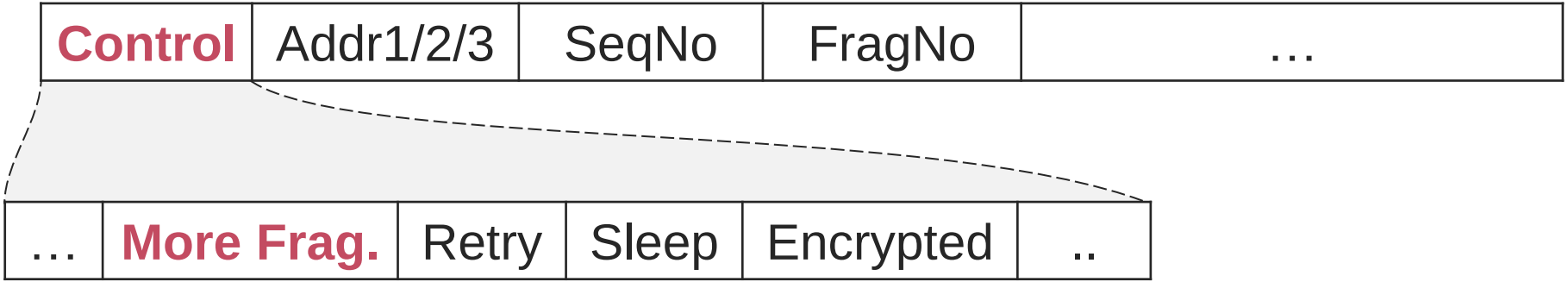
- **Pure mode**: network card is only used for injection
- **Mixed mode**: network card concurrently used as client or AP

Mixed mode example: FragAttacks

	SeqNo	FragNo		
header	s	0	…	Encrypted
header	s	1	…	**Plaintext**
header	s	2	…	**Plaintext**

1. Mixed mode: all network cards **overwrote Seq&FragNo**
   - Makes it impossible to detect vulnerable FragAttacks devices!
2. Pure mode: Atheros firmware **overwrote SeqNo**

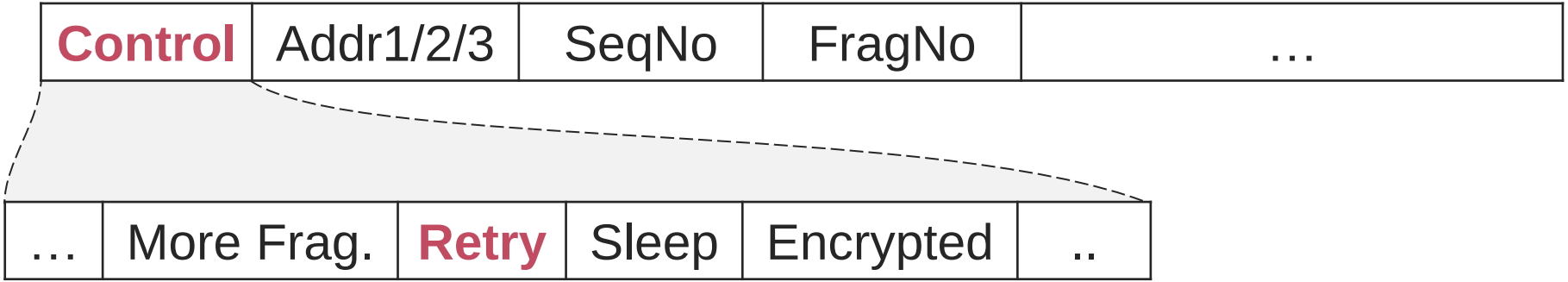
Wi-Fi frame structure



“More Frag.” flag: more fragments to follow

3. The Intel AC-3160 and RT5572 **didn’t transmit** injected frames that had the “More Frag.” flag set!

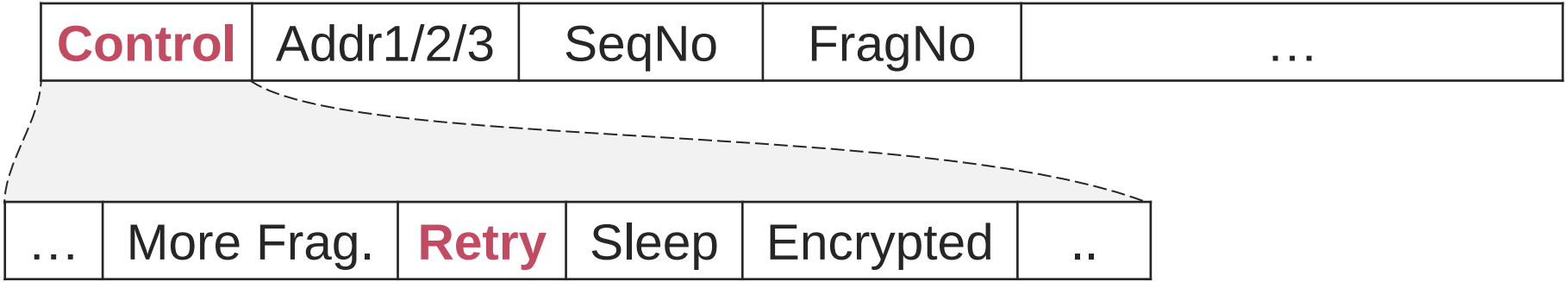
Wi-Fi frame structure



“Retry” flag: this is a retransmitted frame

4. Many network cards retransmit injected frames even after receiving an acknowledgement

Wi-Fi frame structure



“Retry” flag: this is a retransmitted frame

5. Many network cards don’t acknowledge received frames
   - Makes it impossible to connect with some APs

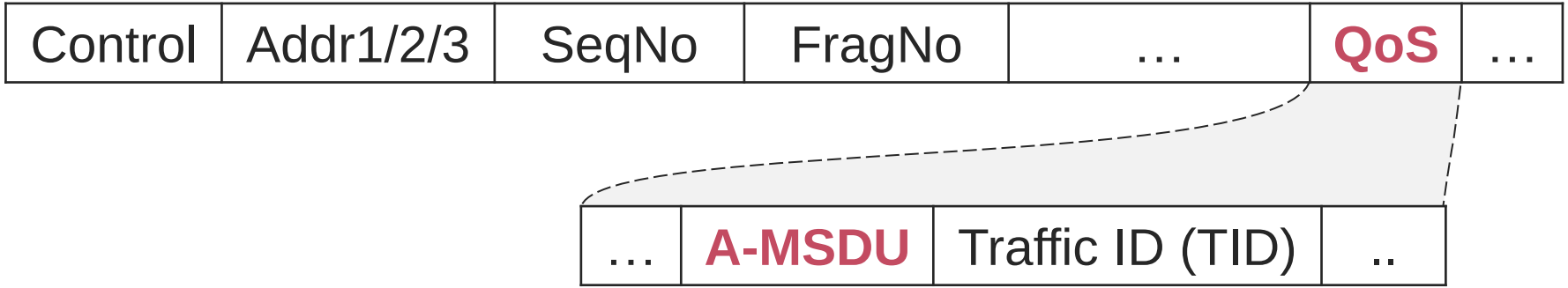
Wi-Fi frame structure

Control	**Addr1/2/3**	SeqNo	FragNo	…

Receiver, sender, and final destination MAC address

6. Intel AC-3160 in mixed mode: didn’t transmit frames with spoofed sender address

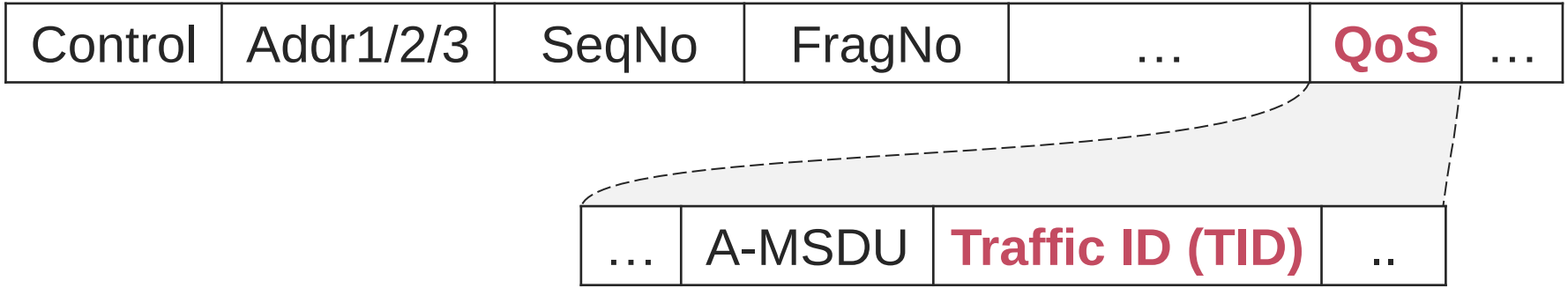
Wi-Fi frame structure



Whether this is an aggregated frame

7. Intel AC-3160 didn’t inject A-MSDU frames

Wi-Fi frame structure



Represents the frame's priority

8. Frames with different TID got reordered before being sent

And other bugs…

9. Handling clients in sleep mode
10. Unexpected Block Ack procedure
11. In mixed mode, the network card's hardware decryption removed the Packet No (replay counter) field
12. Mixed mode: injected plaintext frames were dropped by some drivers before authenticating
13. Mixed mode: Intel cards only provide frames belonging to the network it is connected to

Fixes: updated Radiotap standard

- Flag to indicate SeqNum should not be overwritten
- Flag to indicate frame shouldn’t be reordered

Use these in all your future Wi-Fi experiments:

```
RadioTap(present="TXFlags",
    TXFlags="NOSEQ+ORDER")
```

Fixes: code patches

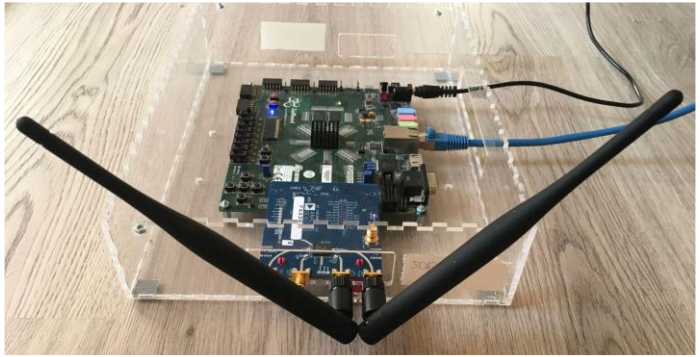
- Implemented Radiotap updates in Linux kernel
- Including some bug fixes

Part of Linux **kernel 5.11** and above

- Modified Atheros firmware to preserve sequence number

Fixes: openwifi

1. Update openwifi to support Radiotap updates
2. Openwifi now supports KRACK and FragAttack tools ☺



Evaluation

- FragAttacks variant: inject plaintext frame **before** authenticating
- Patches assure frame is sent before (not after!) authenticating

Discovered **three new vulnerable devices**:

Device	While authenticating	After authenticating
OnePlus 6	Unicast & broadcast	/
Pixel 4 XL	Unicast	/
Huawei Y6’	Unicast & broadcast	Unicast & broadcast

Thank you! Questions?

- Created tool to test Wi-Fi frame injection
- `RadioTap(present="TXFlags", TXFlags="NOSEQ+ORDER")`
- Linux **kernel 5.11+** improves injection
- Openwifi now supports FragAttack tool

https://github.com/vanhoefm/wifi-injection