

# On the **Krack Attack**: Reproducing Vulnerability and a Software-Defined Mitigation Approach

Ramon dos Reis Fontes and Christian Esteve Rothenberg  
University of Campinas (UNICAMP)

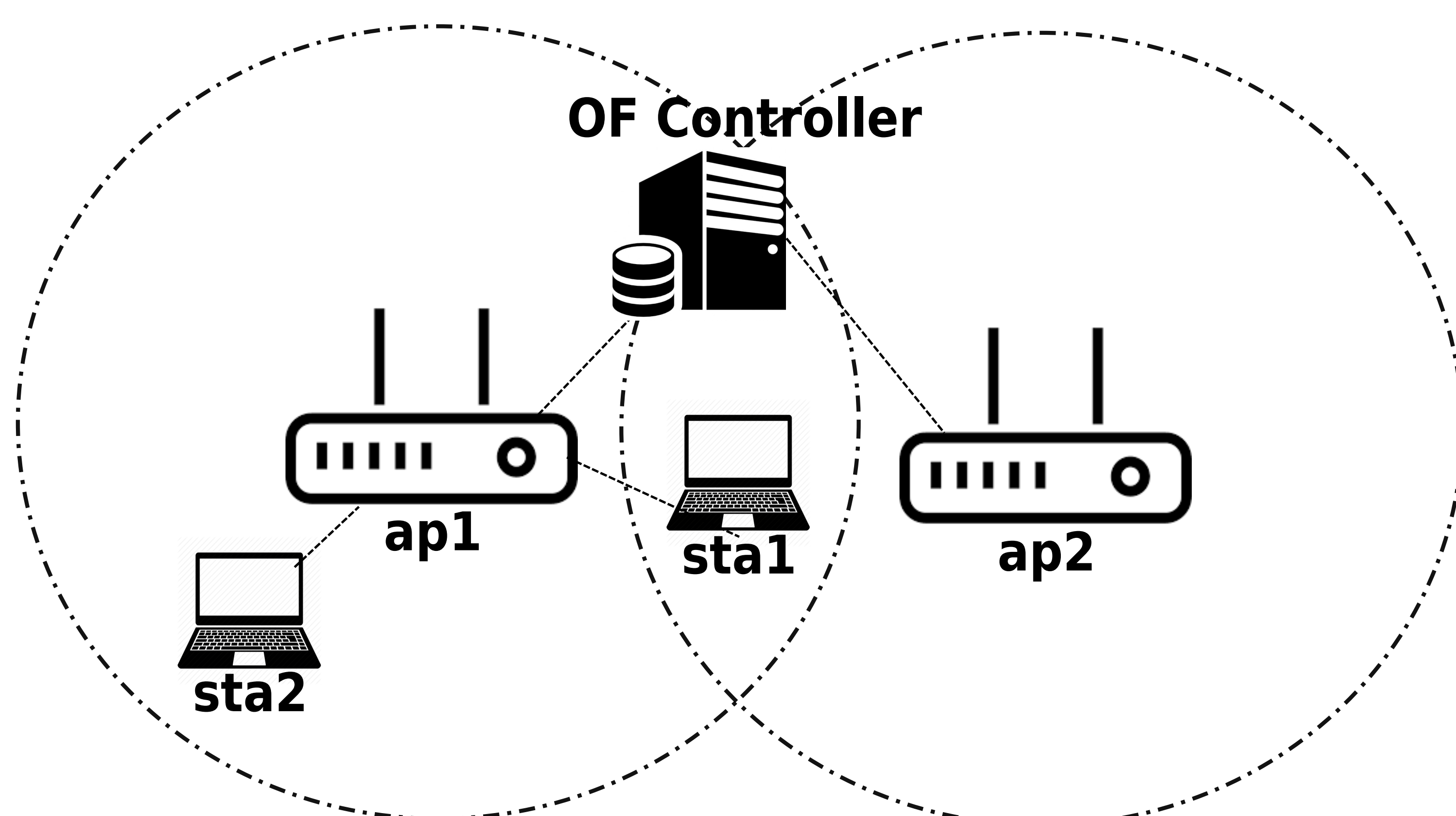


**Proof-of-concept:** Detecting and mitigating vulnerability on 802.11r Fast-BSS Transition (FT)

**Emulation Platform:** Mininet-WiFi - [github.com/intrig-unicamp/mininet-wifi](https://github.com/intrig-unicamp/mininet-wifi)

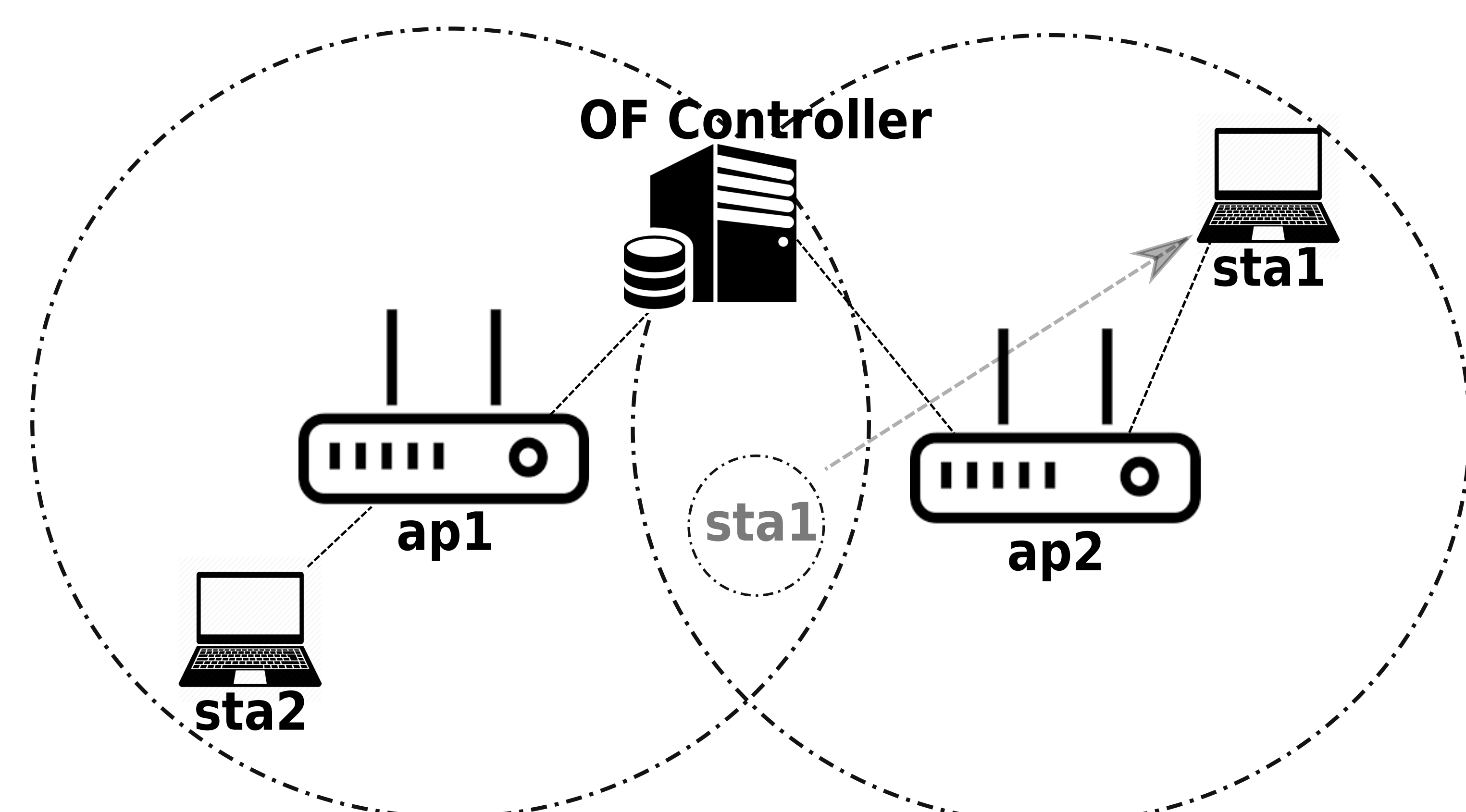
**OpenFlow Controller:** Extended version of Ryu - [github.com/ramonfontes/ryu](https://github.com/ramonfontes/ryu)

Scenario 01 (monitoring)



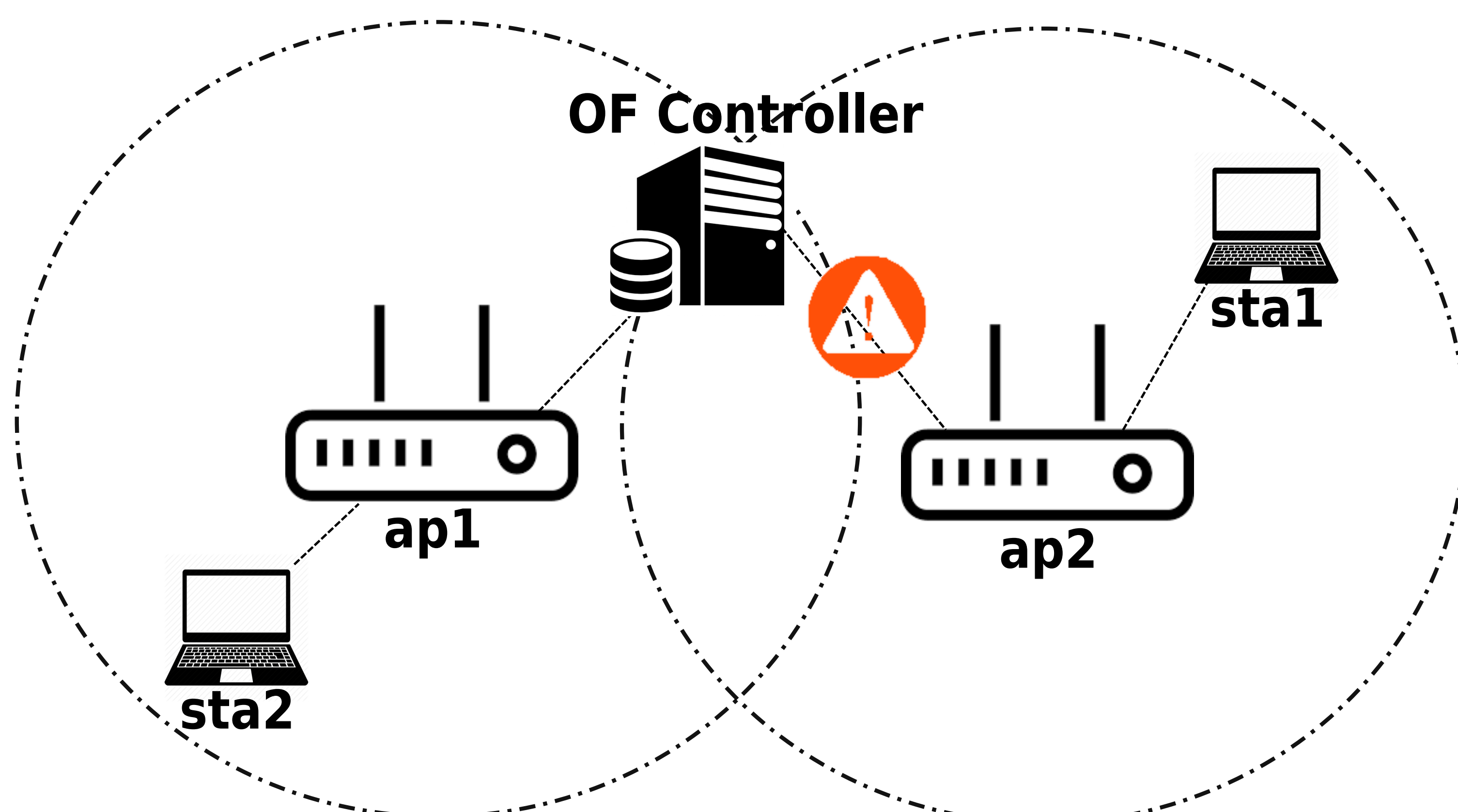
→ Both *sta1* and *sta2* are associated with *ap1*  
OF controller is equipped with a Wi-Fi interface working in monitor mode

Scenario 02 (monitoring)



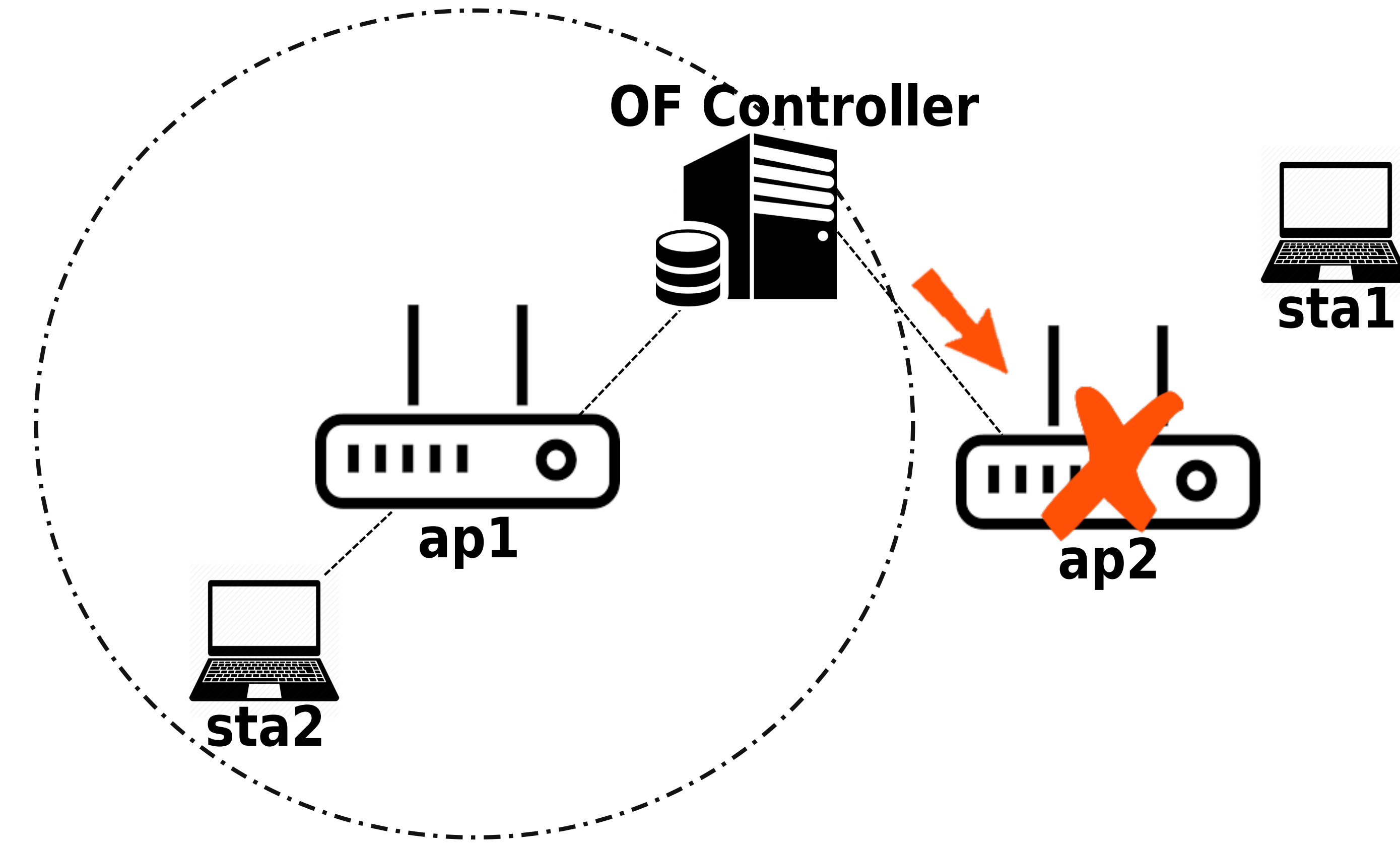
→ *sta1* roams to *ap2*

Scenario 03 (detected vulnerability)



→ OF Controller detects vulnerability on *ap2* during the Fast Transition (FT) handshake

Scenario 04 (mitigation strategy)



→ OF Controller turns *ap2* off  
• Other mitigation strategies:  
isolating the AP dataplane  
warning the user / stations (e.g. HTTP/DNS redirection)



Watch The  
Video Demo



INFORMATION & NETWORKING  
TECHNOLOGIES RESEARCH &  
INNOVATION GROUP

Reproduce Paper  
Experiments

