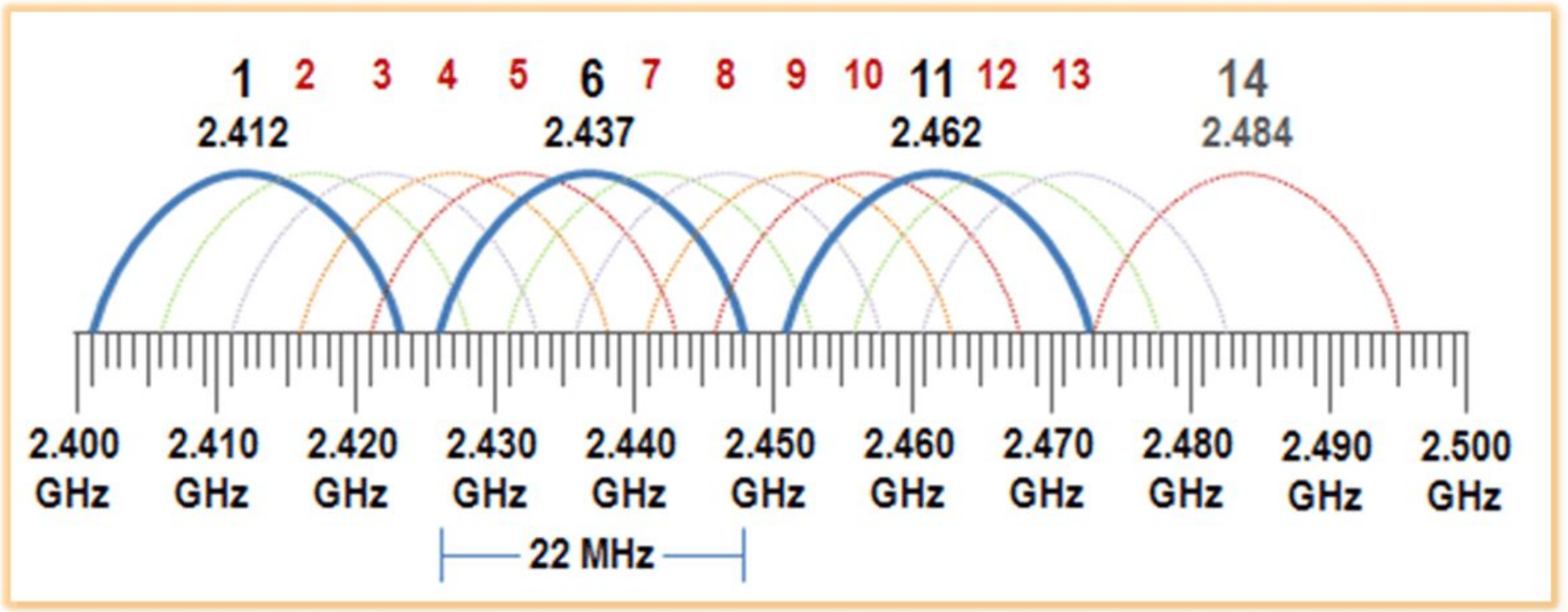
Безопасность беспроводных сетей

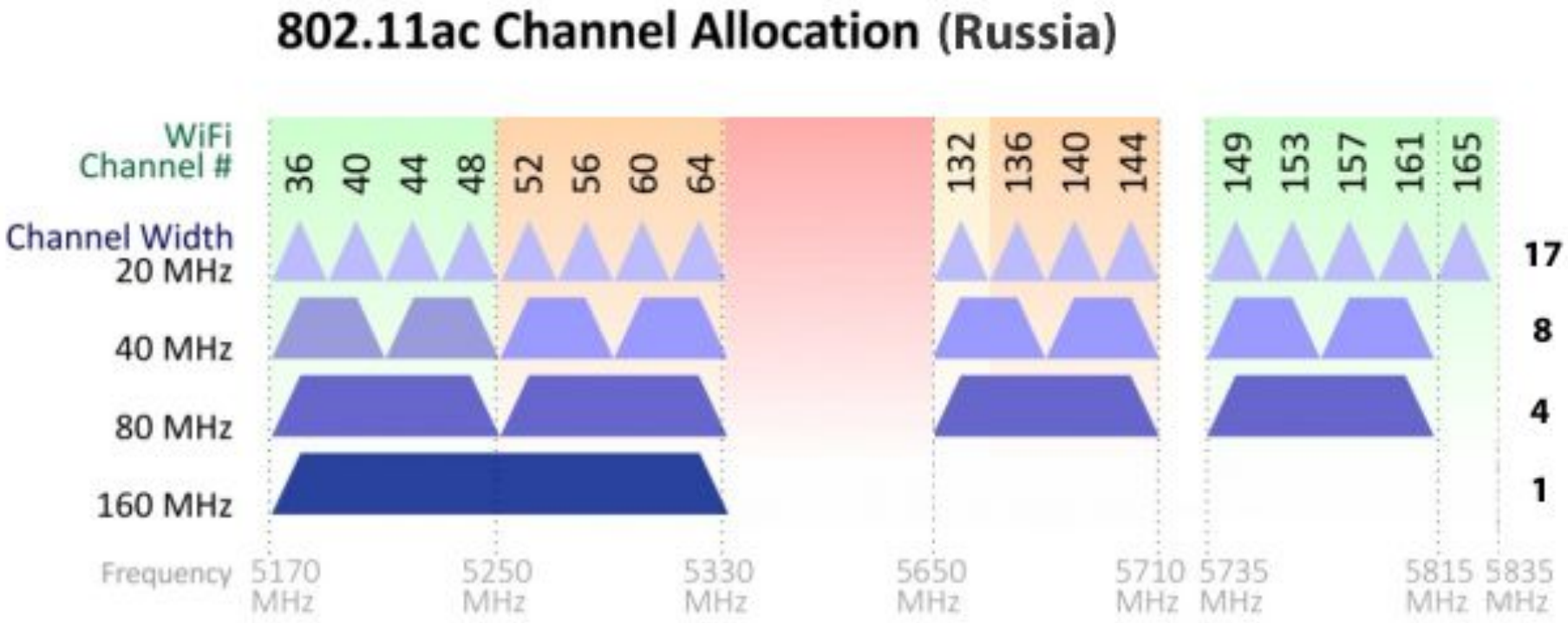
Группа стандартов IEEE 802.11

Wi-Fi generations					
	Wi-Fi 4	Wi-Fi 5	Wi-Fi 6	Wi-Fi 6E	Wi-Fi 7 (expected)
Launch date	2007	2013	2019	2021	2024
IEEE standard	802.11n	802.11ac	802.11ax		802.11be
Max data rate	1.2 Gbps	3.5 Gbps	9.6 Gbps		46 Gbps
Bands	2.4 GHz and 5 GHz	5 GHz	2.4 GHz and 5 GHz	6 GHz	1–7.25 GHz (including 2.4 GHz, 5 GHz, 6 GHz bands)
Security	WPA 2	WPA 2	WPA 3		WPA3
Channel size	20, 40 MHz	20, 40, 80, 80+80, 160 MHz	20, 40, 80, 80+80, 160 MHz	20, 40, 80, 80+80, 160 MHz	Up to 320 MHz
Modulation	64-QAM OFDM	256-QAM OFDM	1024-QAM OFDMA		4096-QAM OFDMA (with extensions)
MIMO	4x4 MIMO	4x4 MIMO, DL MU-MIMO	8x8 UL/DL MU-MIMO		16x16 MU-MIMO

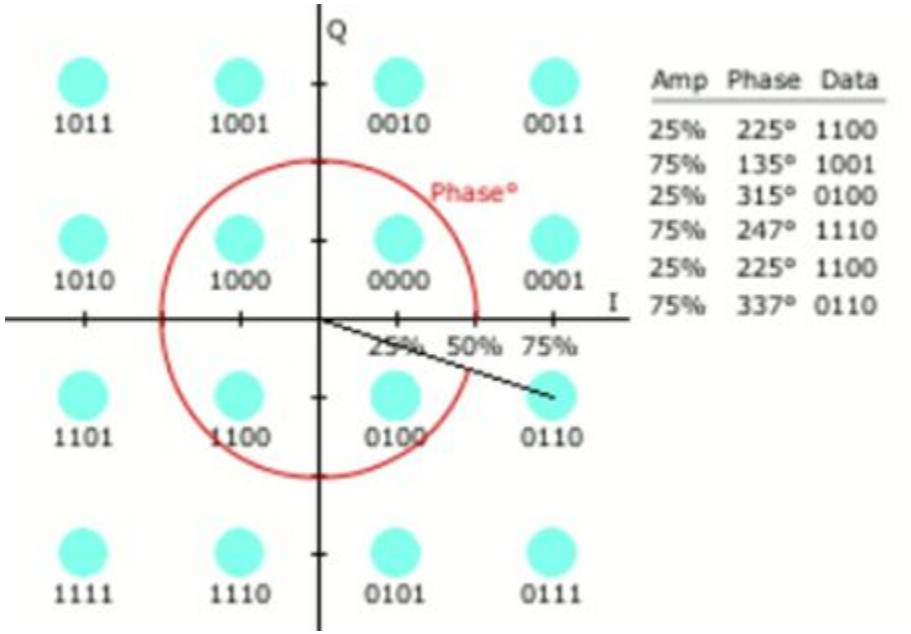
Частотные каналы (2,4 GHz)

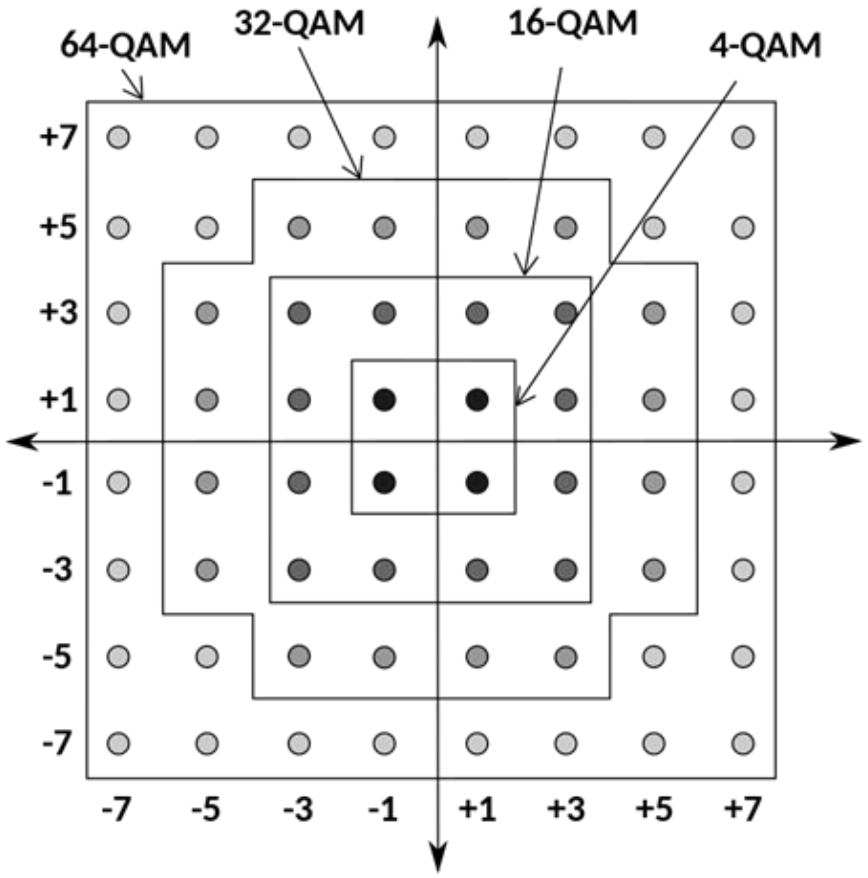


Частотные каналы (5 GHz)

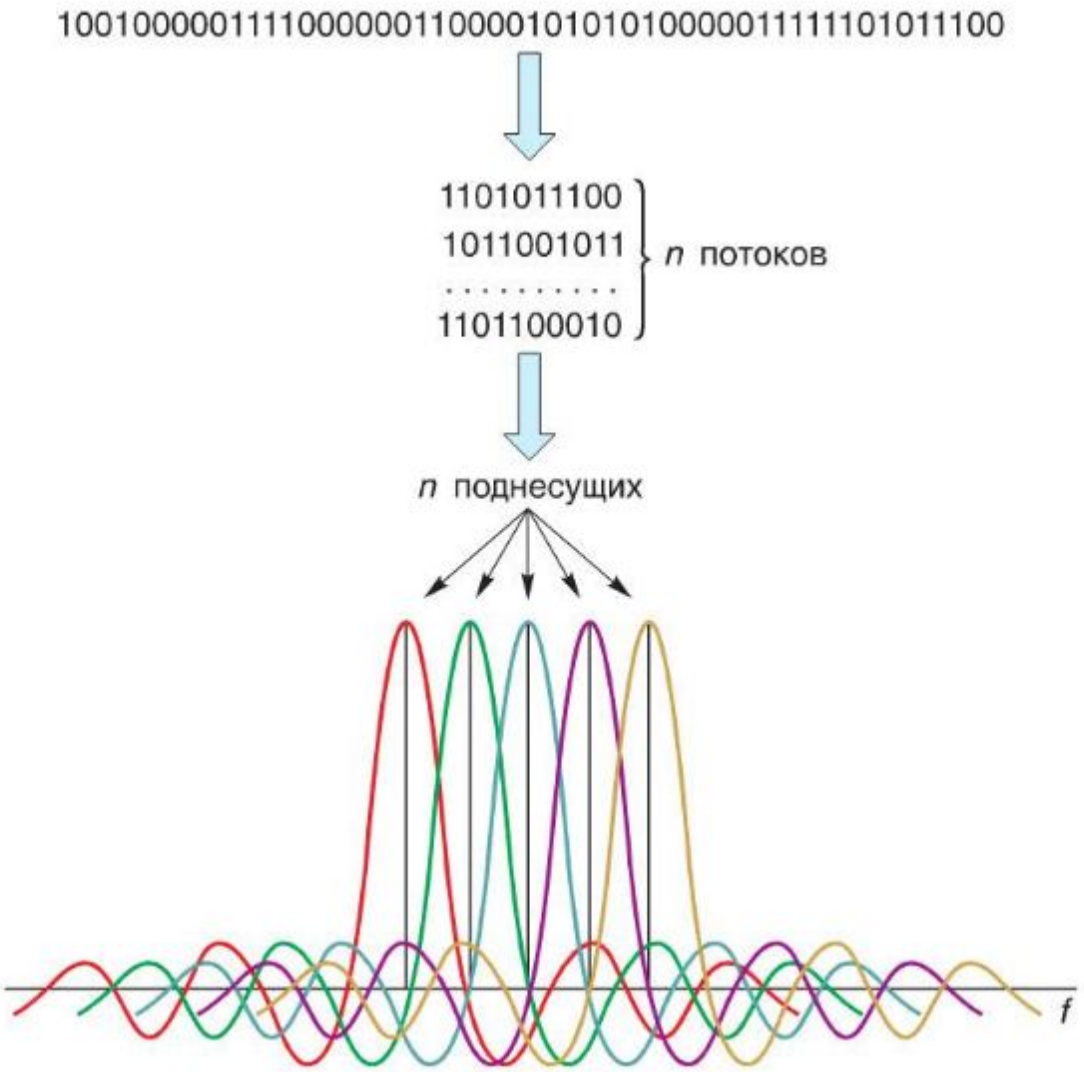


Квадратурная модуляция (QAM)





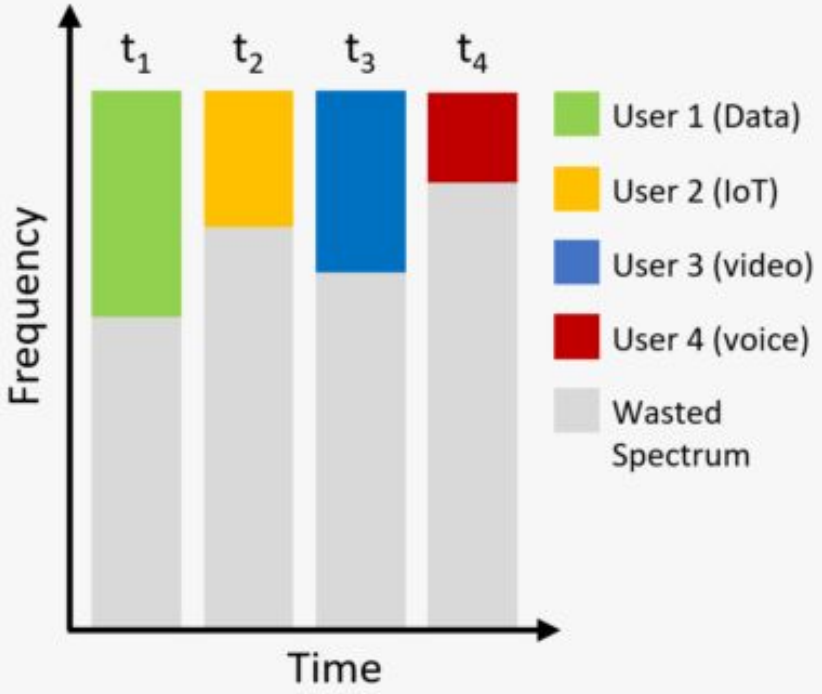
OFDM


10010000011110000001100001010101000001111110101110 0
1101011100
1011001011
. . . . . .
1101100010
n потоков
n поднесущих
f

OFDM vs OFDMA

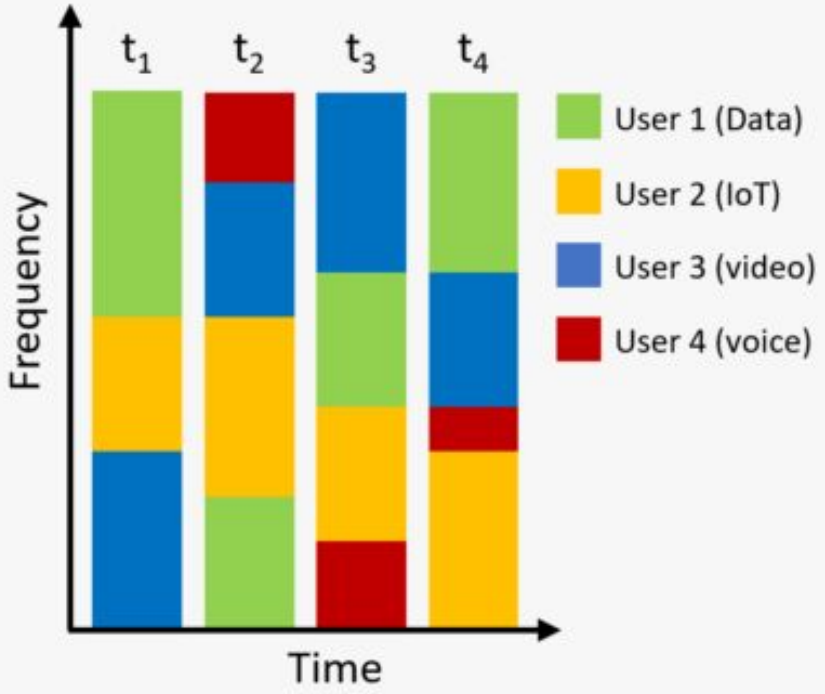
OFDM (Wi-Fi 2-5)

- One user packet per time segment
- Inefficient for small packets
- High voice/video delay

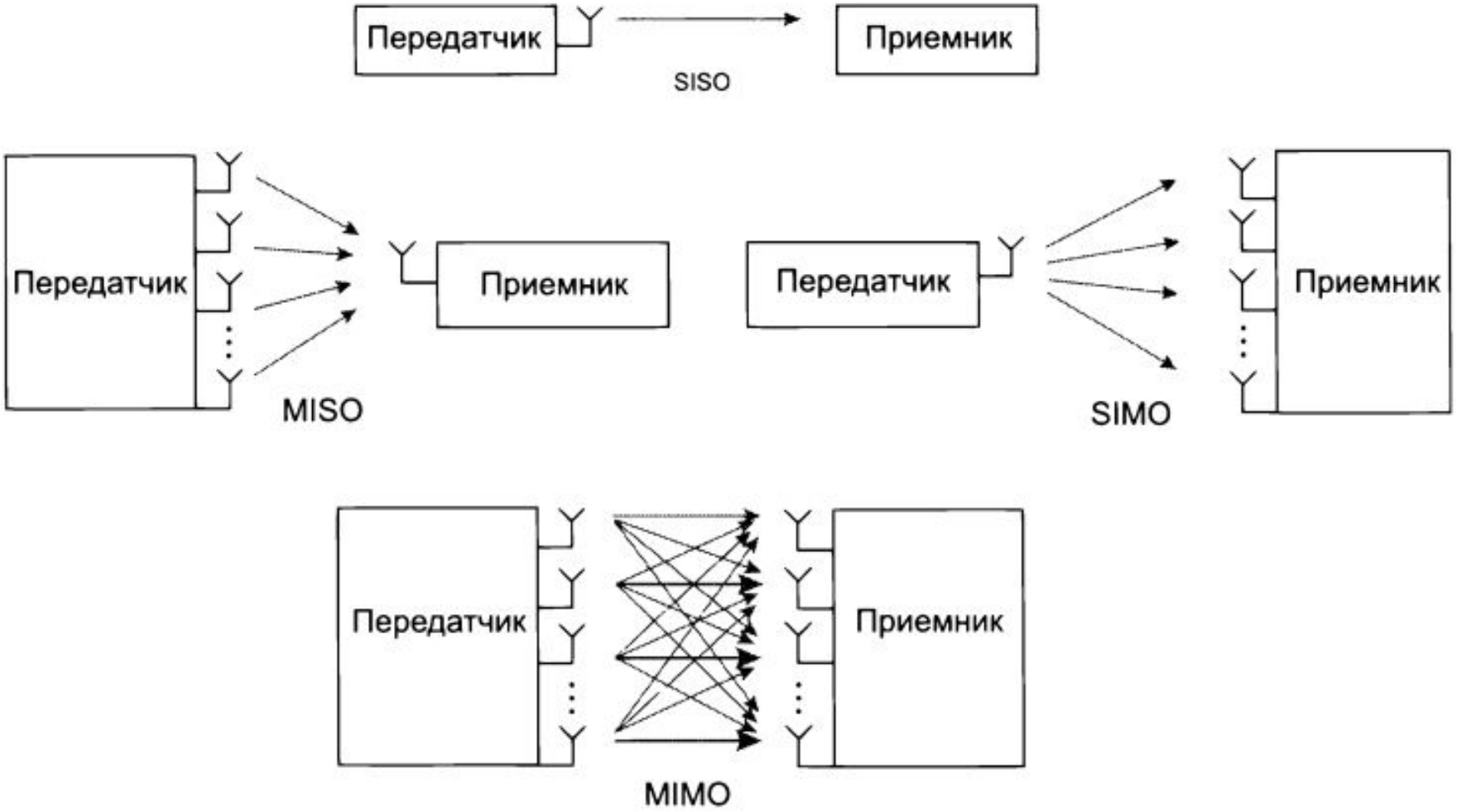


OFDMA (Wi-Fi 6)

- Multiple users packet per time segment
- Highly efficient
- Low voice/video delay



Антенны MIMO



Безопасность беспроводных сетей - специфика

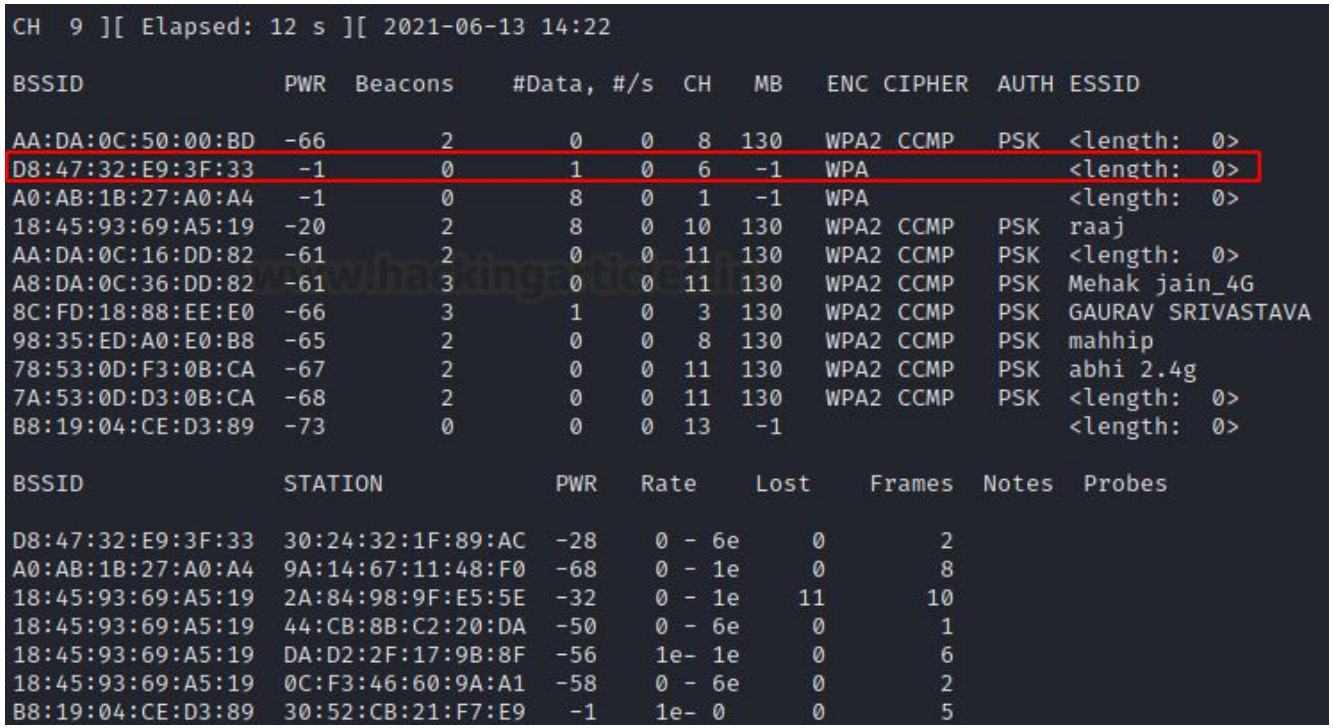
- Возможность бесконтактного доступа: подключение возможно из любой точки, где достаточна мощность сигнала.
- Принцип вещания: пакет передается в эфир, и устройства сами определяют, принимать пакет или нет.

Угрозы:

- Сбор информации о сети / о подключенных устройствах.
- Подмена идентичности с целью доступа к сети / контроля над устройством.
- Отказ в обслуживании.

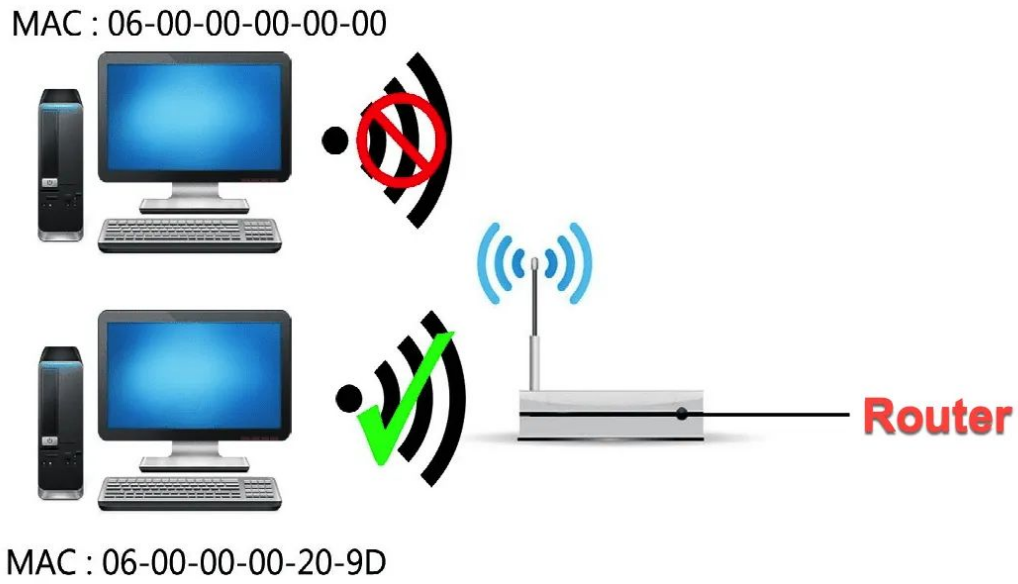
Скрытие SSID беспроводной сети

- SSID (Service Set Identifier) - уникальное имя, беспроводной сети
- Скрытый SSID не транслируется точкой доступа в Beacon Frames.
- Сеть со скрытым SSID не отображается в списке доступных, но может быть обнаружена при сканировании -> **метод является ненадежным**



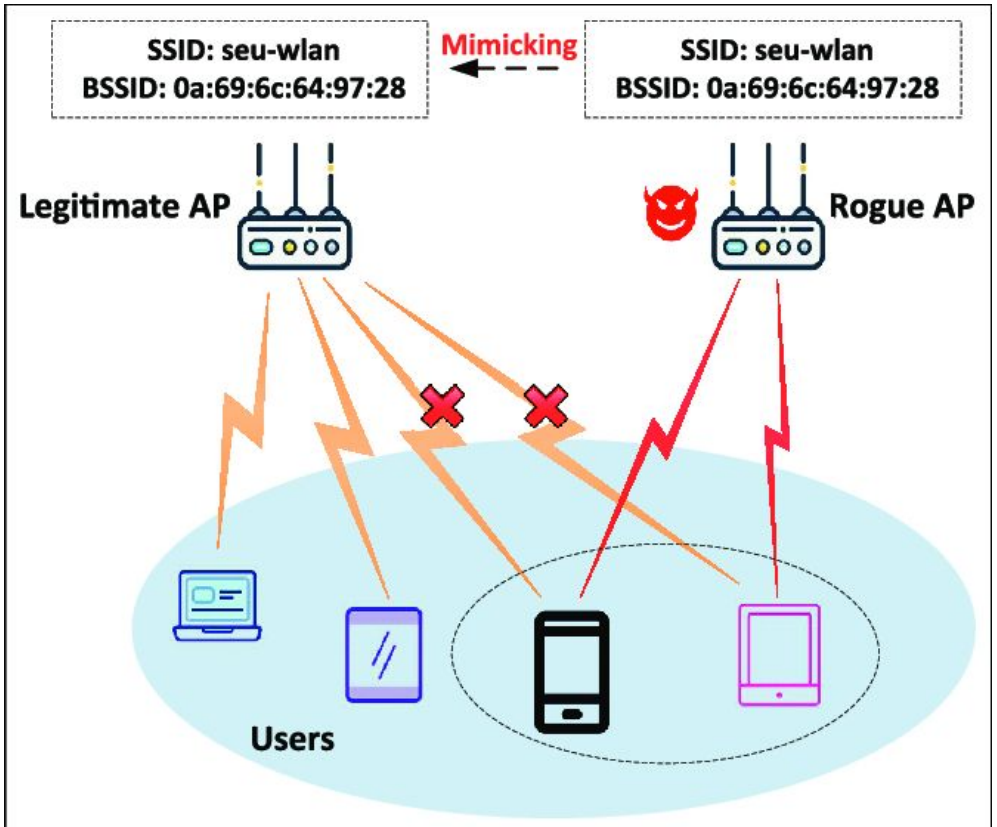
Фильтрация по MAC-адресу

- Запрет доступа к сети с использование использования черных / белых списков MAC
- **Эффективность низкая**: сканирование сети выявляет разрешенные MAC адреса в заголовках кадров



Rogue AP - фальшивые точки доступа

- Маскируются под легитимную точку доступа, клиент подключается к «известной» точке автоматически.
- Используются для перехвата данных с подключенных устройств.
- Защита - мониторинг эфира на предмет подозрительных устройств

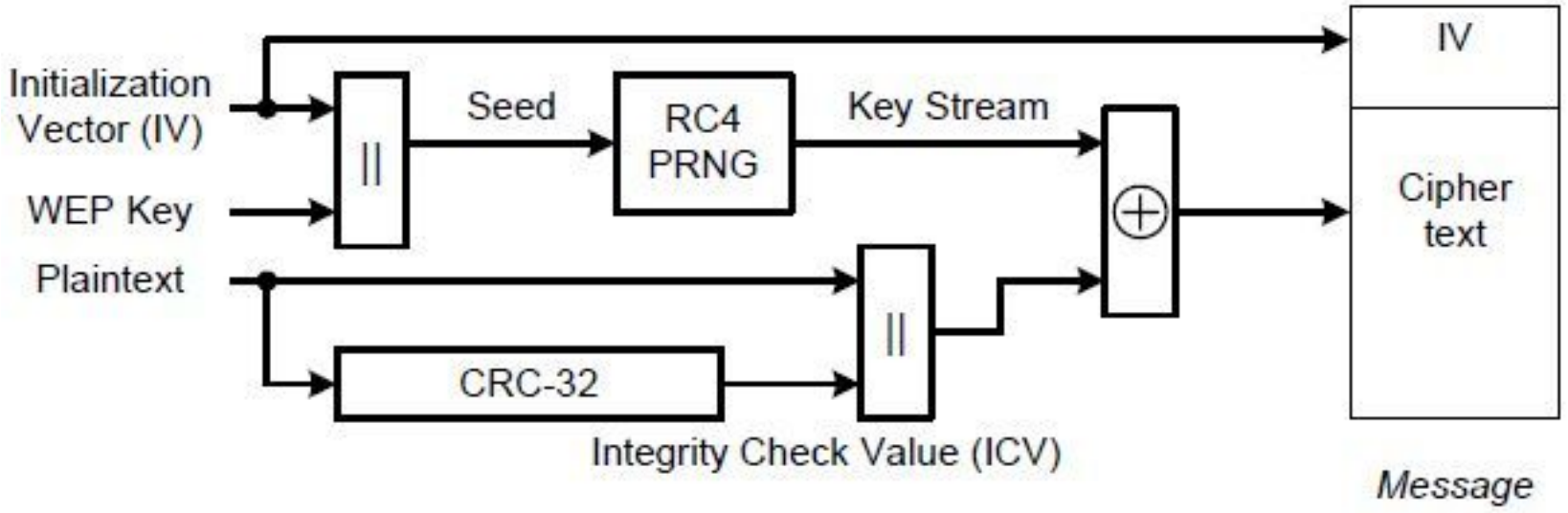


Стандарты безопасности беспроводных сетей

	WEP	WPA	WPA2	WPA3
Release Year	1999	2003	2004	2018
Encryption Method	Rivest Cipher 4 (RC4)	Temporal Key Integrity Protocol (TKIP) with RC4	CCMP and Advanced Encryption Standard (AES	Advanced Encryption Standard (AES)
Session Key Size	40-bit	128-bit	128-bit	128-bit (WPA3-Personal) 192-bit (WPA-Enterprise)
Cipher Type	Stream	Stream	Block	Block
Data Integrity	CRC-32	Message Integrity Code	CBC-MAC	Secure Hash Algorithm
Key Management	Not provided	4-way handshaking mechanism	4-way handshaking mechanism	Simultaneous Authentication of Equals handshake
Authentication	WPE-Open WPE-Shared	Pre-Shared Key (PSK) & 802.1x with EAP variant	Pre-Shared Key (PSK) & 802.1x with EAP variant	Simultaneous Authentication of Equals (SAE) & 802.1x with EAP variant

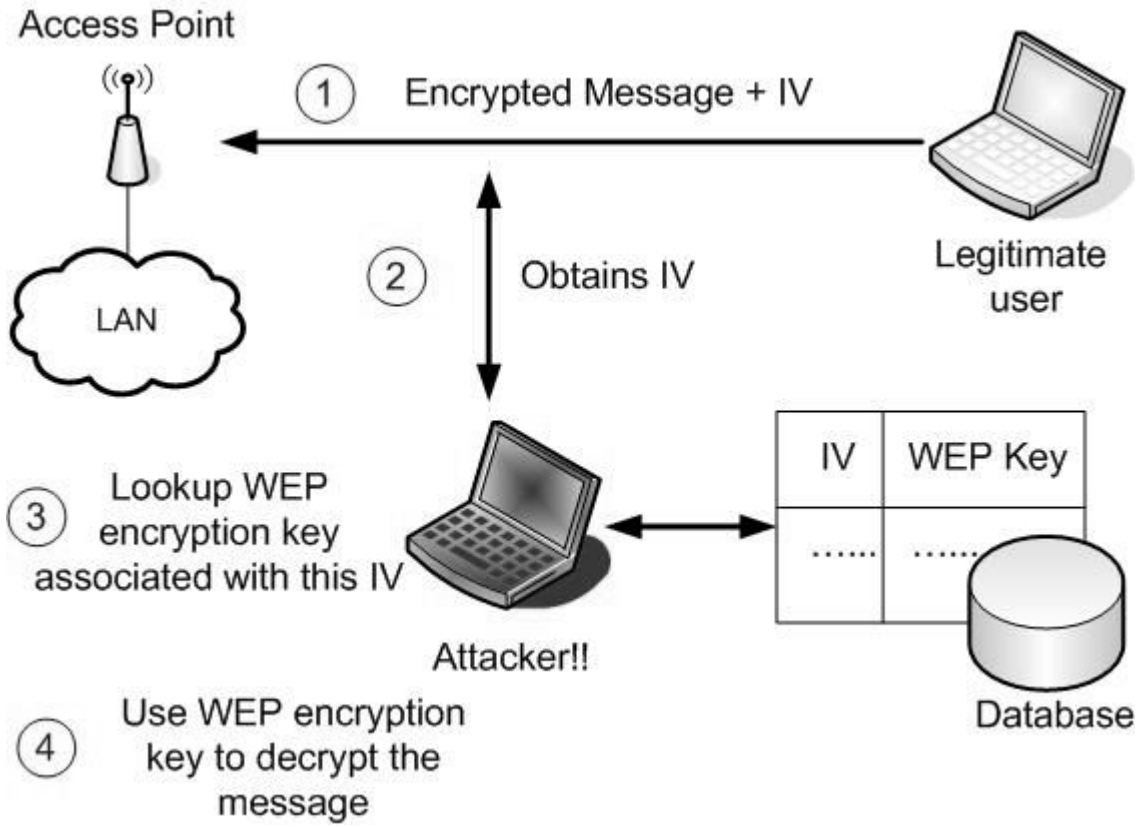
WEP (Wired Equivalent Privacy)

- В основе поточный шифр RC4. Длина ключа - 40 или 104 бита
- Используются для перехвата данных с подключенных устройств.
- Защита - мониторинг эфира на предмет подозрительных устройств



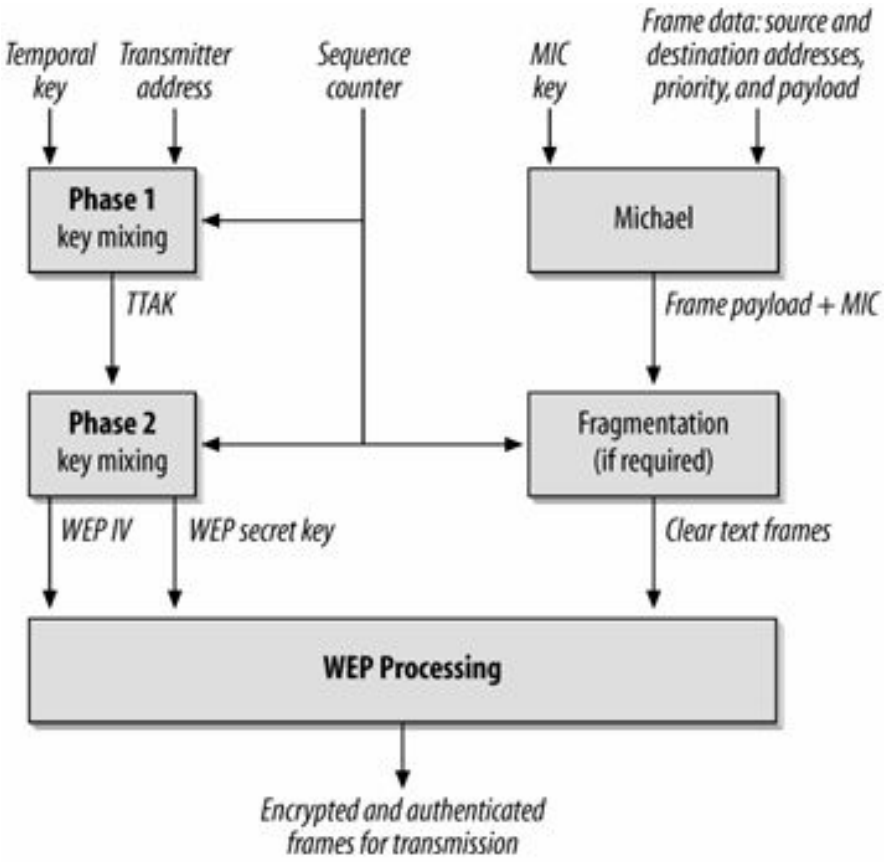
- В основе атаки - перехват и анализ кадров беспроводной сети.
- **В силу подверженности атакам считается устаревшим.**

Атака на WEP


Access Point
1
Encrypted Message + IV
LAN
2
Obtains IV
Legitimate user
3
Lookup WEP encryption key associated with this IV
IV
WEP Key
.....
.....
Attacker!!
Database
4
Use WEP encryption key to decrypt the message

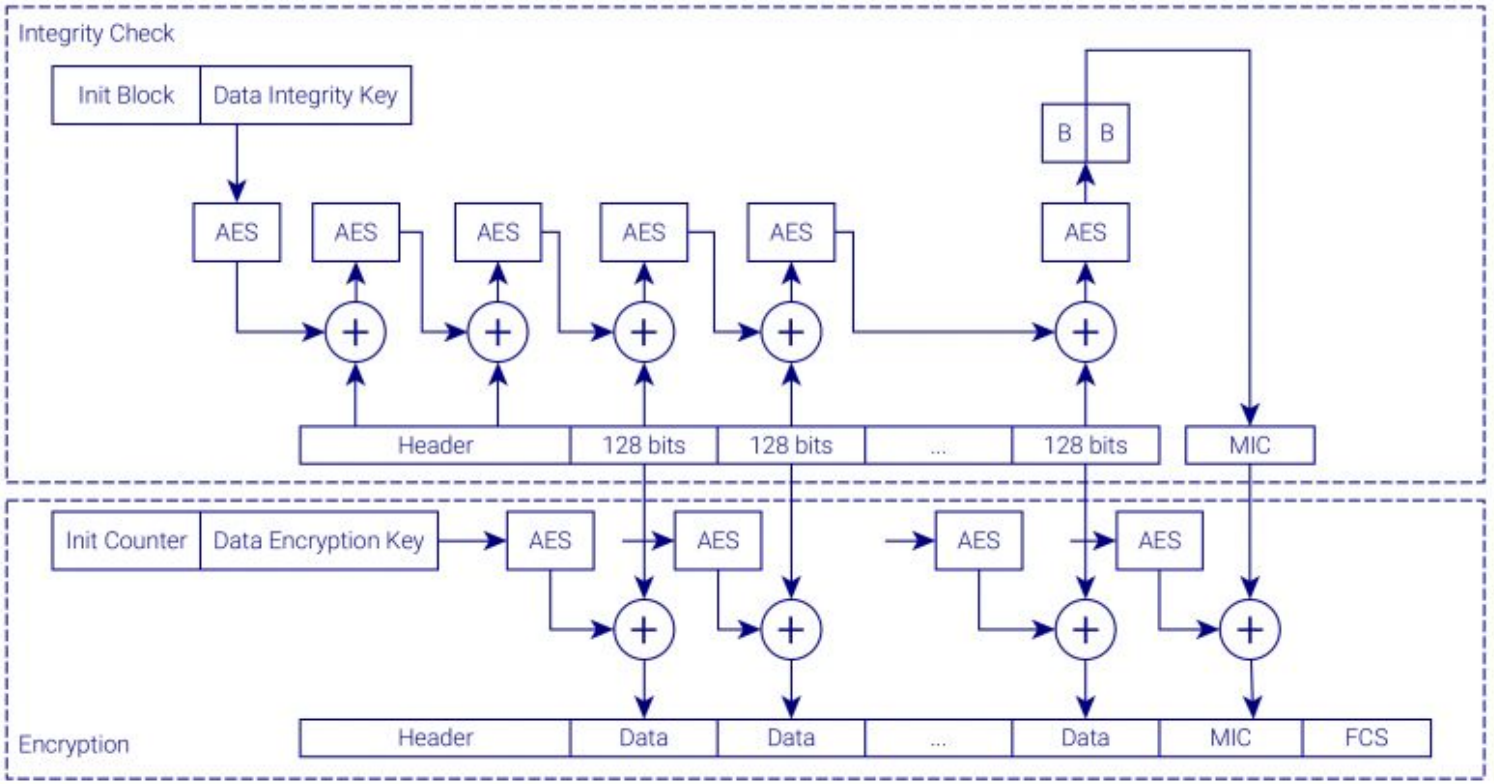
WPA (Wi-Fi Protected Access)

- протокол 802.1x
- протокол EAP — расширяемый протокол аутентификации
- протокол TKIP — протокол целостности ключей во времени
  - шифрование аналогично WEP, но ключи являются динамическими
- MIC — криптографическая проверка целостности пакетов

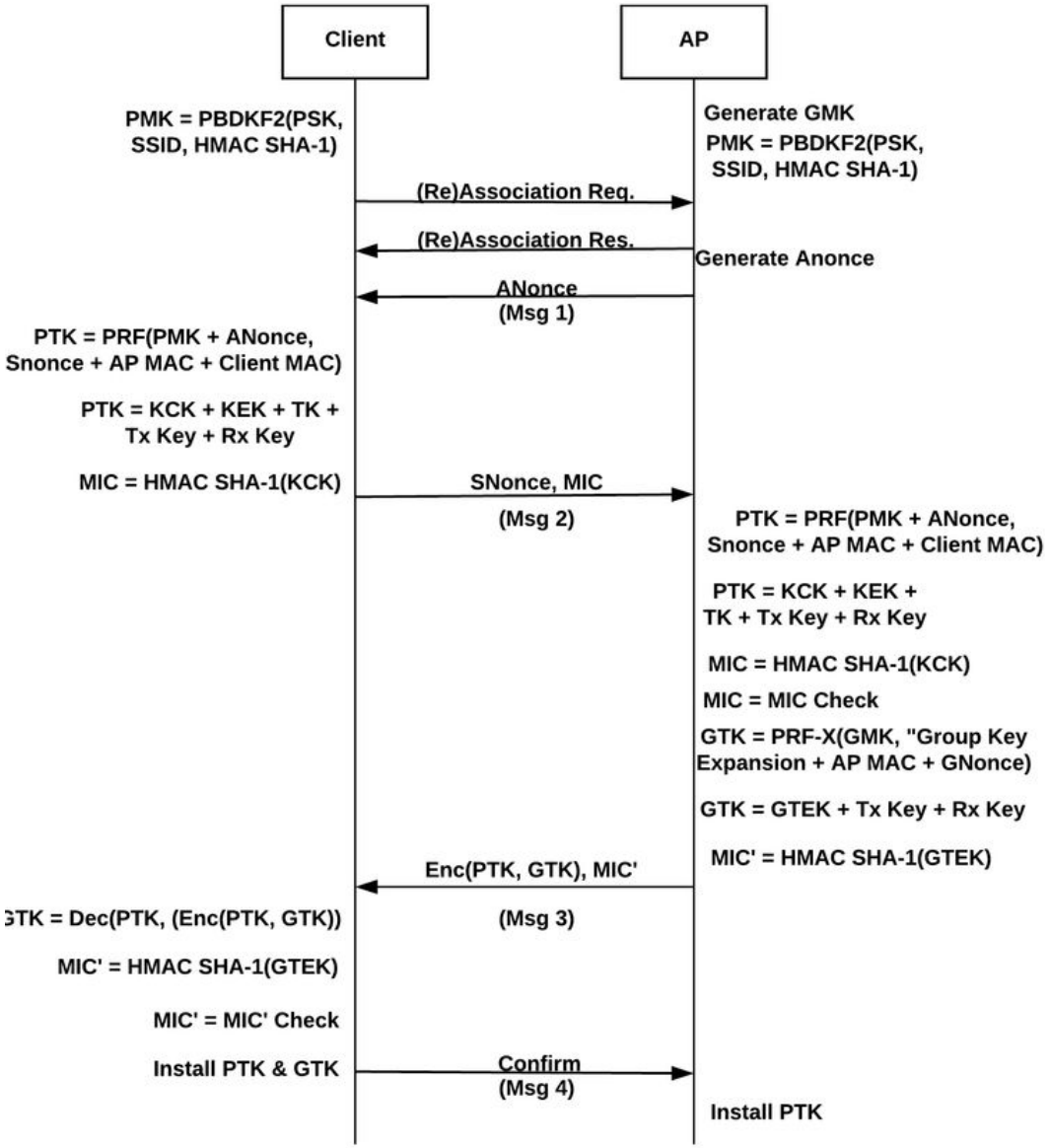


WPA2

- введен стандартом IEEE 802.11i-2004
- использует CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) и алгоритм шифрования AES (длина ключа 128 бит)
- использует метод 4-кратного рукопожатия (4-way handshake)



WPA2-PSK (4-way handshake)

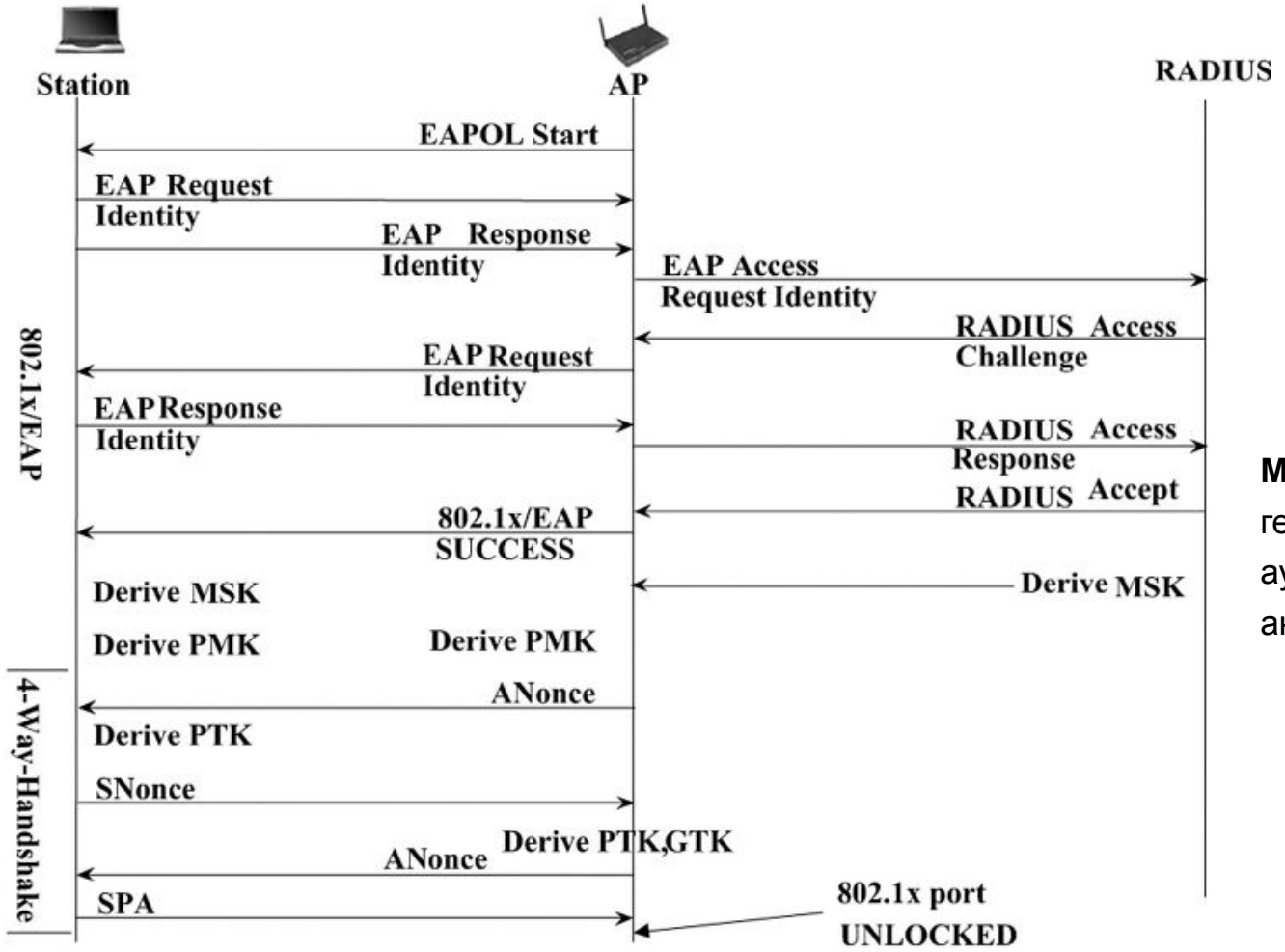


- **Попарный мастер-ключ PMK** - вычисляется сторонами до начала соединения на основе предварительного ключа **PSK**
- **Попарный передаточный ключ PTK** - вычисляется сторонами в процессе соединения
- **Структура PTK**

- ***Key Confirmation Key (KCK)*** - для проверки целостности кадров EAPOL (хэндшейка)
- **Key Encryption Key (KEK)** - для шифрования кадров EAPOL (хэндшейка)
- **Temporal Key (TK)** - для шифрования данных после установления соединения
- **MIC Tx / MIC Rx** - для проверки целостности данных от точки доступа / от клиента

*Похожим образом (но только на точке доступа) вычисляются **групповые ключи GMK и GTK** для защиты кадров broadcast и multicast.*

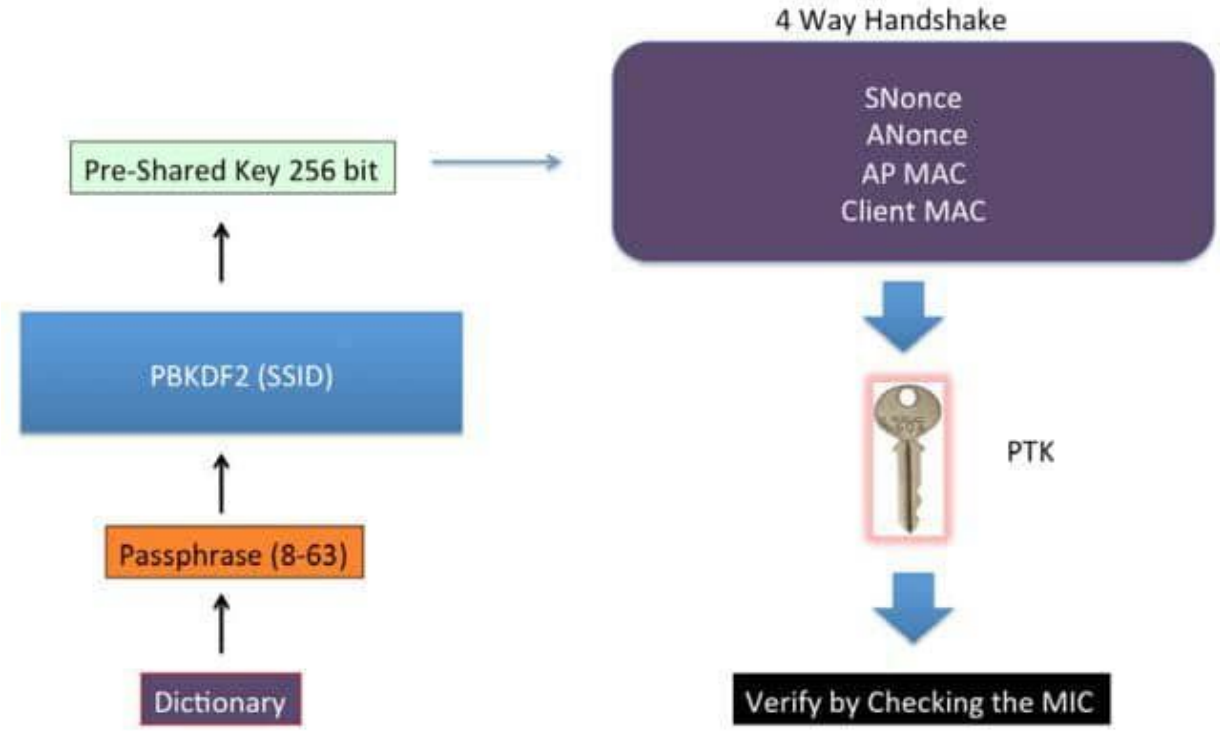
WPA2 802.1x/EAP

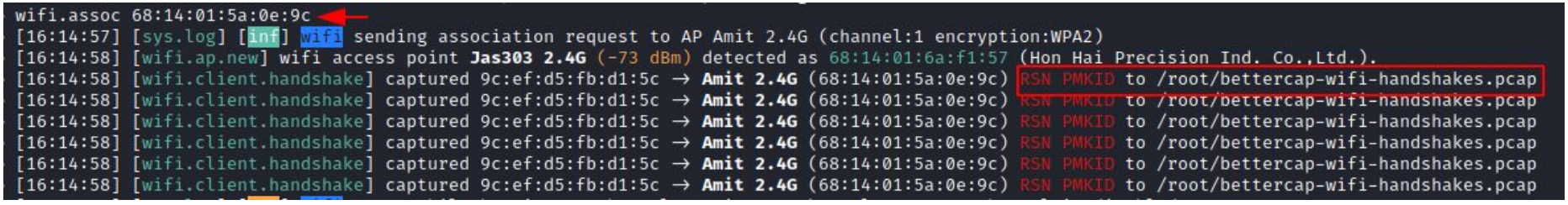


MSK (Master Session Key) - генерируется сервером аутентификации и играет роль, аналогичную PSK

WPA/WPA2 bruteforce (на перехваченных данных хэндшейка)

- для перехвата может потребоваться деаутентифицировать подключенного клиента.
- перебор паролей ведется по словарю (готовому либо сгенерированному)





WPA/WPA2 bruteforce (на перехваченных данных PMKID)

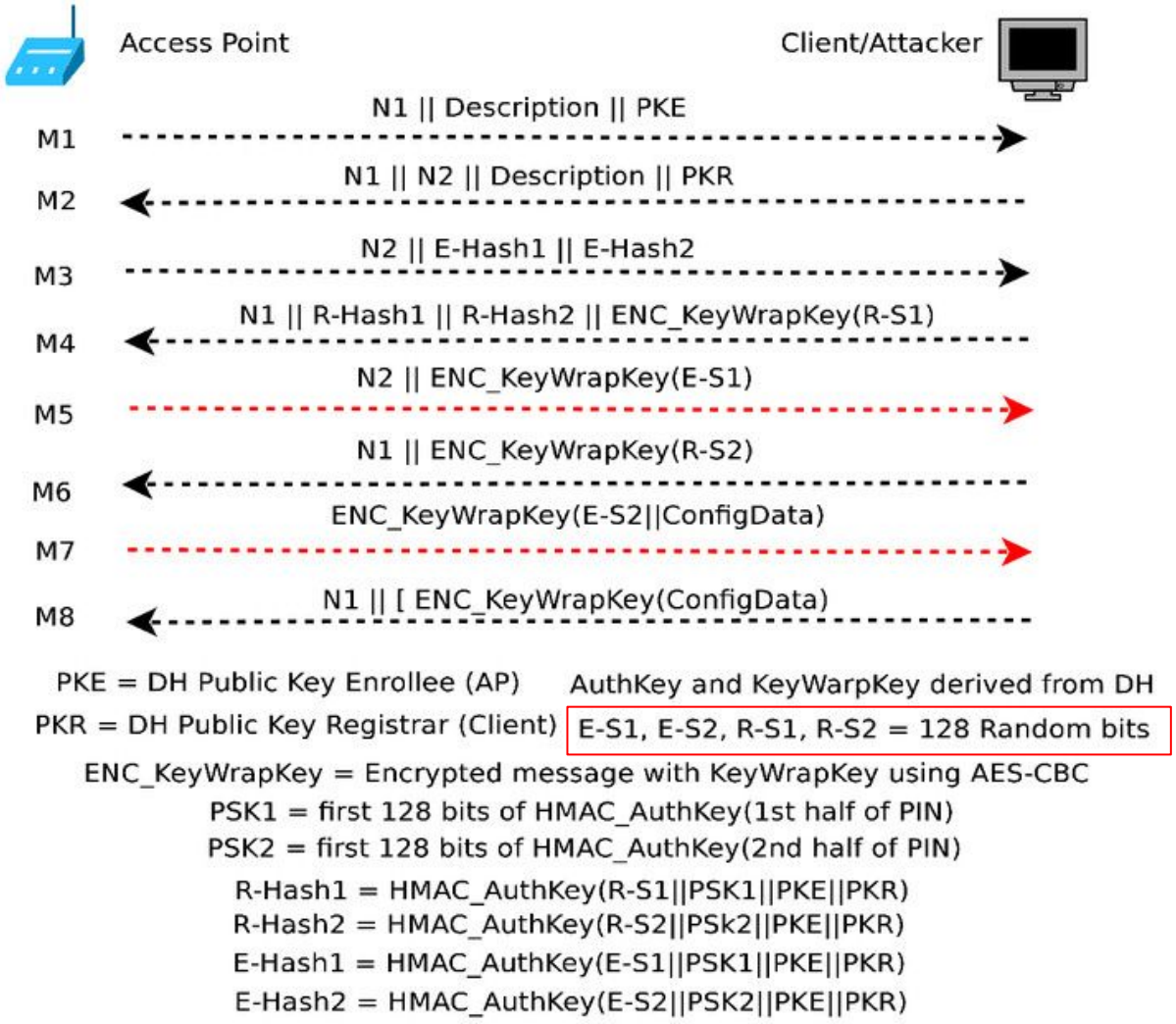
- Pairwise Master Key Identifier Dump (PMKID) - передается для обеспечения роуминга в Wi-Fi-сетях, использующих несколько точек доступа (стандарт 802.11r)
- не требует наличия подключенных клиентов
- методика перебора аналогична атаке по хэндшейку

PMKID = HMAC-SHAI-128(PMK, “PMK Name” | MAC_AP | MAC_STA)

PMK = PBKDF2(Passphrase, SSID, 4096)

```
wifi.assoc 68:14:01:5a:0e:9c
[16:14:57] [sys.log] [inf] wifi sending association request to AP Amit 2.4G (channel:1 encryption:WPA2)
[16:14:58] [wifi.ap.new] wifi access point Jas303 2.4G (-73 dBm) detected as 68:14:01:6a:f1:57 (Hon Hai Precision Ind. Co.,Ltd.).
[16:14:58] [wifi.client.handshake] captured 9c:ef:d5:fb:d1:5c → Amit 2.4G (68:14:01:5a:0e:9c) RSN PMKID to /root/bettercap-wifi-handshakes.pcap
[16:14:58] [wifi.client.handshake] captured 9c:ef:d5:fb:d1:5c → Amit 2.4G (68:14:01:5a:0e:9c) RSN PMKID to /root/bettercap-wifi-handshakes.pcap
[16:14:58] [wifi.client.handshake] captured 9c:ef:d5:fb:d1:5c → Amit 2.4G (68:14:01:5a:0e:9c) RSN PMKID to /root/bettercap-wifi-handshakes.pcap
[16:14:58] [wifi.client.handshake] captured 9c:ef:d5:fb:d1:5c → Amit 2.4G (68:14:01:5a:0e:9c) RSN PMKID to /root/bettercap-wifi-handshakes.pcap
[16:14:58] [wifi.client.handshake] captured 9c:ef:d5:fb:d1:5c → Amit 2.4G (68:14:01:5a:0e:9c) RSN PMKID to /root/bettercap-wifi-handshakes.pcap
[16:14:58] [wifi.client.handshake] captured 9c:ef:d5:fb:d1:5c → Amit 2.4G (68:14:01:5a:0e:9c) RSN PMKID to /root/bettercap-wifi-handshakes.pcap
```

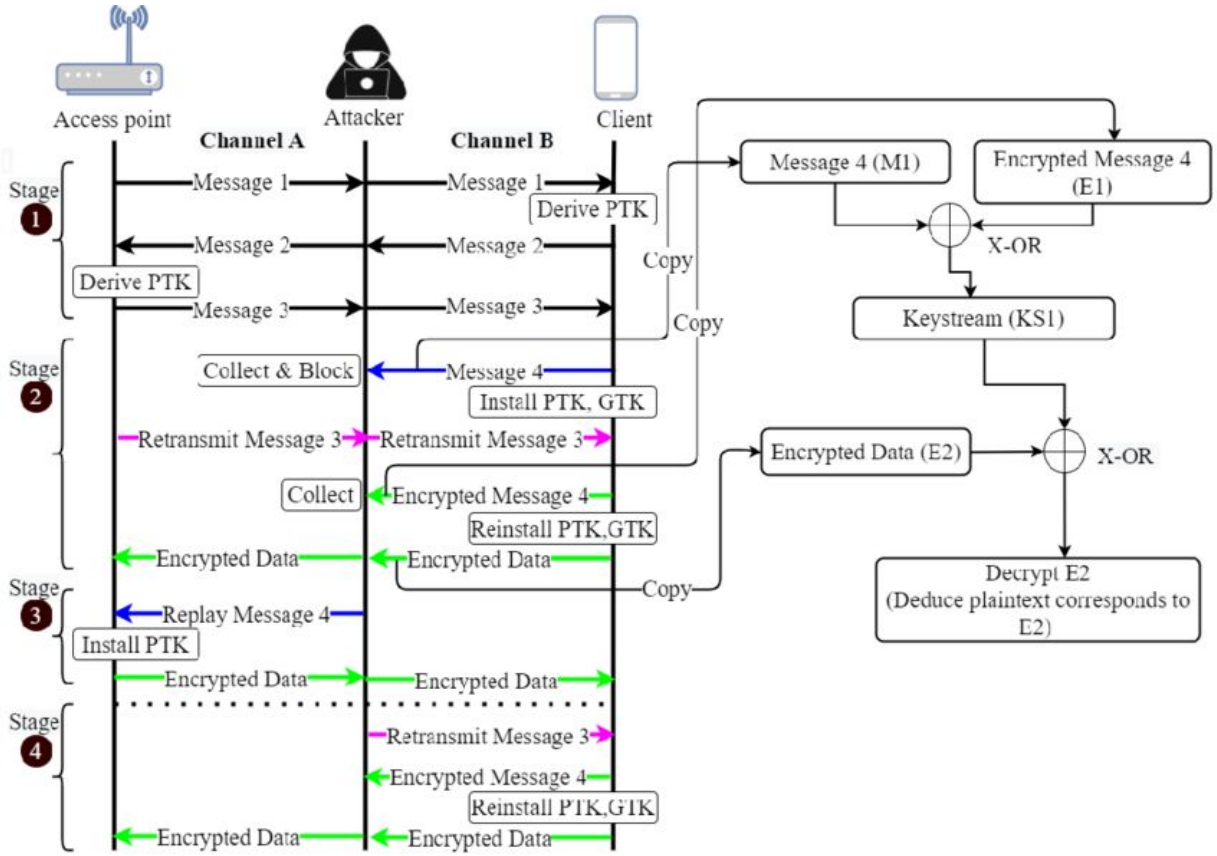
Использование уязвимостей WPS



- PKE, PKR, Authkey, E-Hash1, E-Hash2 перехватываем из сообщений M1, M2, M3
- E-S1 и E-S2 генерируются псевдослучайной функцией. Она же ранее генерирует N1 на 1 этапе
- В ряде моделей оборудования функция уязвима к брутфорсу, т. е. значения E-S1 и E-S2 детерминированы
- Отправляем все данные в хэш функцию и сравниваем каждый новый pin с (E-Hash1 и E-Hash2).
- В итоге перебора получаем WPS PIN точки доступа

Атака с переустановкой ключа (KRACK)

- На третьем этапе 4-этапного рукопожатия злоумышленник имеет возможность выполнить повторную отправку последовательности и ослабить уровень защиты соединения.
- Результатом атаки может стать перехват трафика, спуфинг или фальсификация данных.



WPA3

- Стандарт **IEEE 802.11-2016**
- **Одновременная аутентификация равных (SAE)** - работает на основании предположения о равноправности устройств. Любая из сторон может отправить запрос на соединение, и потом они начинают независимо отправлять удостоверяющую их информацию (противодействие KRACK).
- **Прямая секретность (PFS)** - невозможность расшифровать ранее перехваченные данные ключом, скомпрометированным позднее.
- **192-битное шифрование** (AES-256-GCM + HMAC-384)
- Поддержка **Opportunistic Wireless Encryption (OWE)** для открытых сетей - при подключении устройство пытается зашифровать канал передачи, а иначе переходит к незашифрованной связи. Ключ шифрования согласуется по DH (ephemeral).