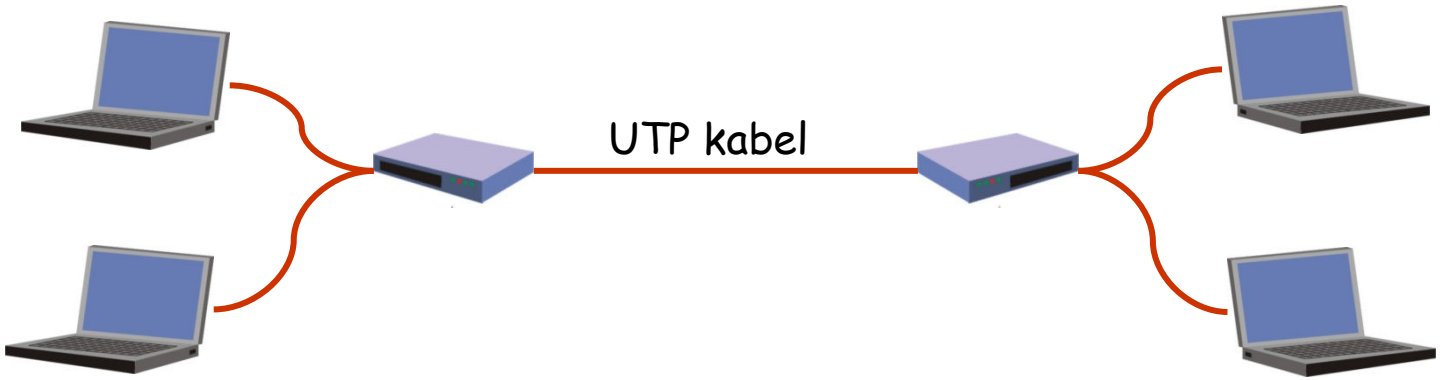
Zaštita integriteta bežične komunikacije

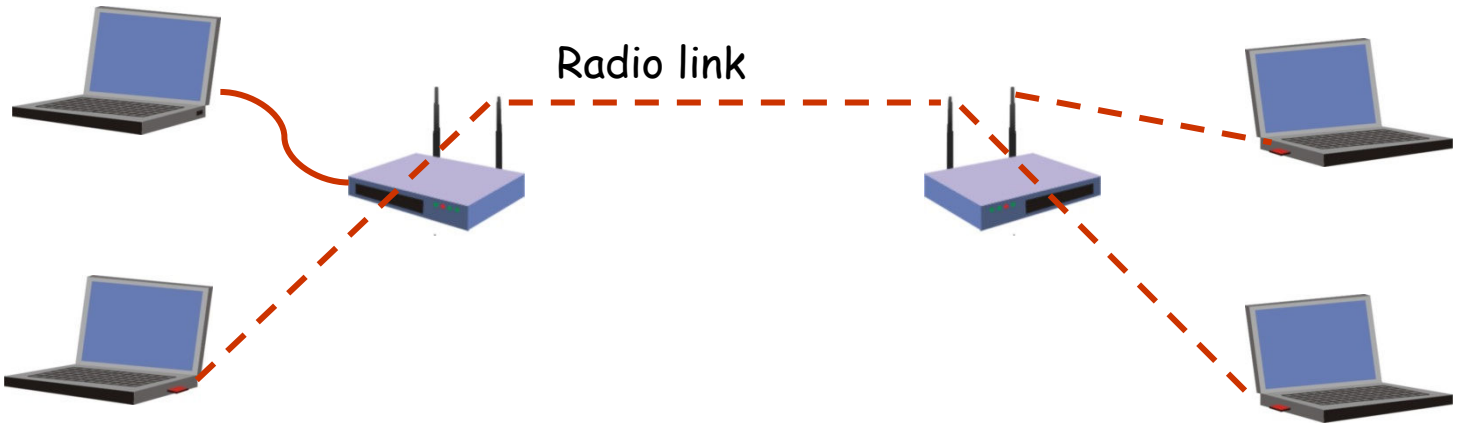
Autori:
Hrvoje Lozančić
Prof. dr. sc. Danko Kezić, dipl. ing.
Mr. sc. Anita Gudelj, prof.
Split, lipanj 2007.

Bežične računalne mreže - uvod

- Klasična mreža

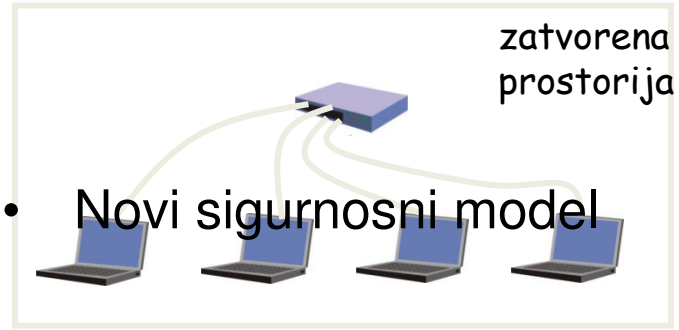


- Bežična mreža

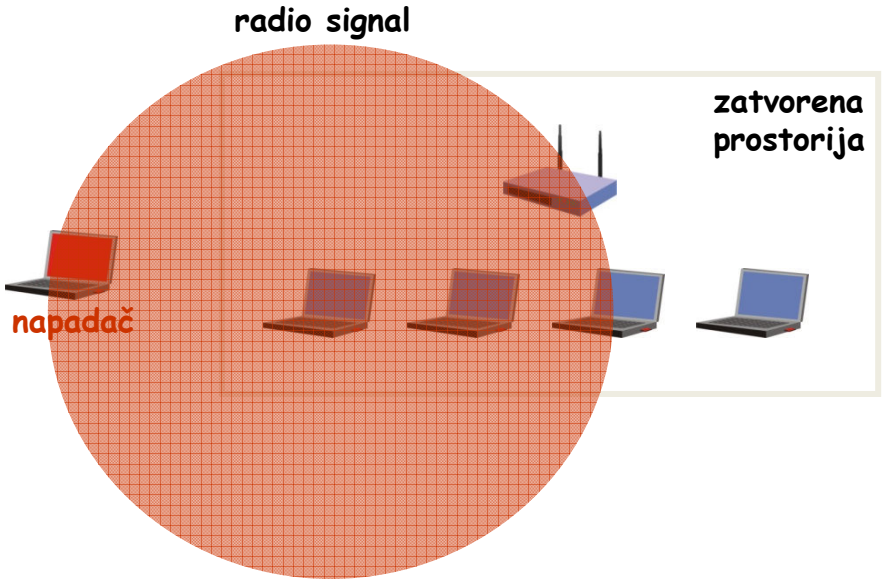


Bežične vs. klasične mreže

	klasična mreža	bežična mreža
jednostavnost	-	+
mobilnost	-	+
brzina	+	-
sigurnost	+	-

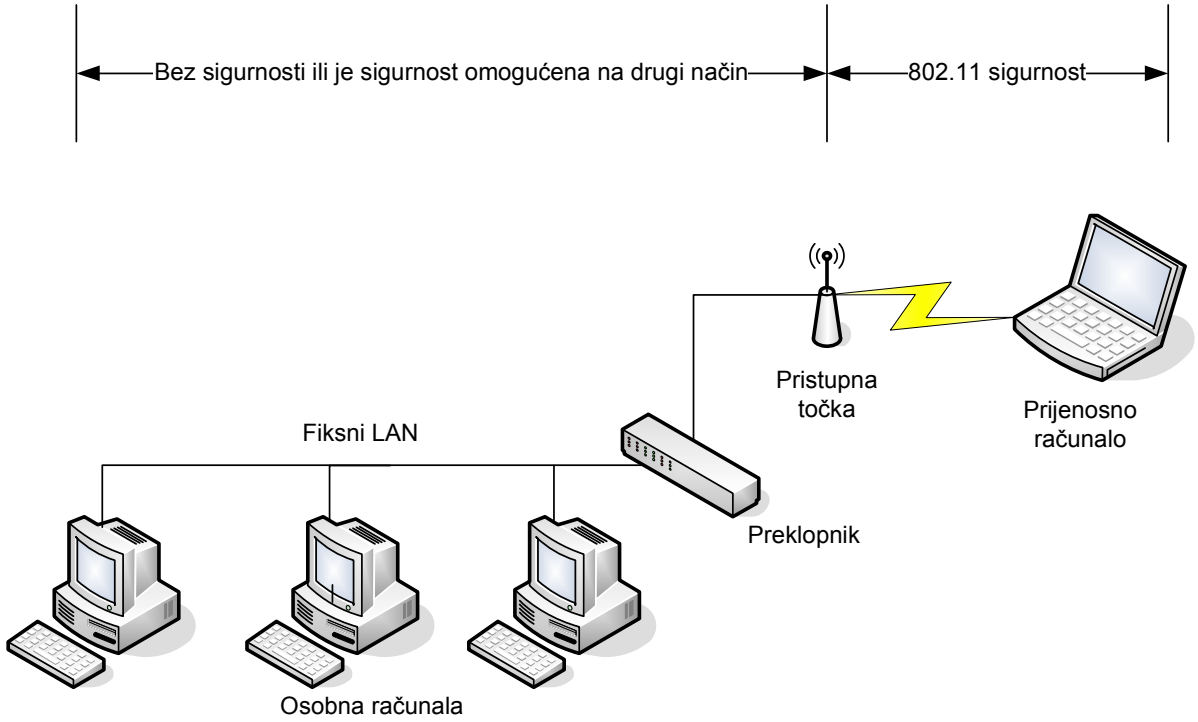


- Novi sigurnosni model



Wired Equivalent Privacy (WEP)

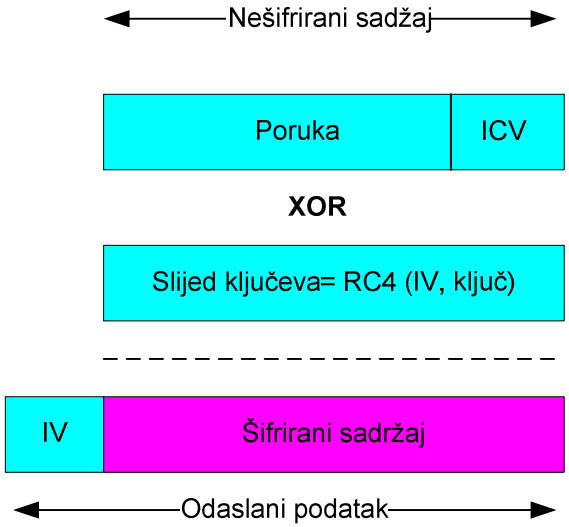
WEP je protokol koji štiti podatke na sloju podatkovne veze za vrijeme prijenosa između pristupne točke i klijenta.



WEP se bazira na tajnom ključu koji se dijeli između mobilne stanice i pristupne točke.

Šifrirani WEP okvir

Povjerljivošću i integritetom rukuje se istovremeno. Prije šifriranja, poruka prolazi kroz algoritam provjere integriteta, generirajući vrijednost provjere integriteta ICV .



Okvir i ICV su šifrirani, tako da ICV nije dostupna napadaču.

Sigurni WEP se kombinira s 24-bitnim inicijalizacijskim vektorom (IV) za kreiranje 64-bitnog RC4 ključa. IV se smješta u zaglavlje okvira radi omogućavanja dešifriranja poruke na prijemniku.

Konstrukcijski propust WEP zaštite

Okviri kojima se šalju poruke nisu šifrirani pa je napadač u mogućnosti doći do inicijalizacijskog vektora koji je korišten pri šifriranju.

Poznata mana svih algoritama šifriranja koji rade s tokom podataka (stream ciphers) je to da šifriranje dviju različitih poruka istim inicijalizacijskim vektorom daje informacije o samim porukama.

Ako je $C1 = P1 \text{ XOR } RC4(IV, ključ)$
i
$C2 = P2 \text{ XOR } RC4(IV, ključ)$
tada je
$C1 \text{ XOR } C2 = (P1 \text{ XOR } RC4(IV, ključ)) \text{ XOR } (P2 \text{ XOR } RC4(IV, ključ))$
$= P1 \text{ XOR } P2$

Provođenjem ekskluzivnog ILI na dva šifrirana bloka poništava se efekt zaštite.

Zahvaljujući ovom svojstvu mogući su mnogi načini napada !!!

WEP2

WEP2 je nastao nadograđivanjem WEP-a i s time je naslijedio neke slabosti.

Načinjene su preinake u duljini ključa, proširenjem na 128 bita te proširivanjem polja u kojemu se nalazi inicijalizacijski vektor koje je sada velik 128 bita.

No ostao je isti enkripcijski algoritam – RC4 i isti način upravljanja ključevima pa se može zaključiti da WEP 2 ne donosi velik pomak u poboljšanju sigurnosti.

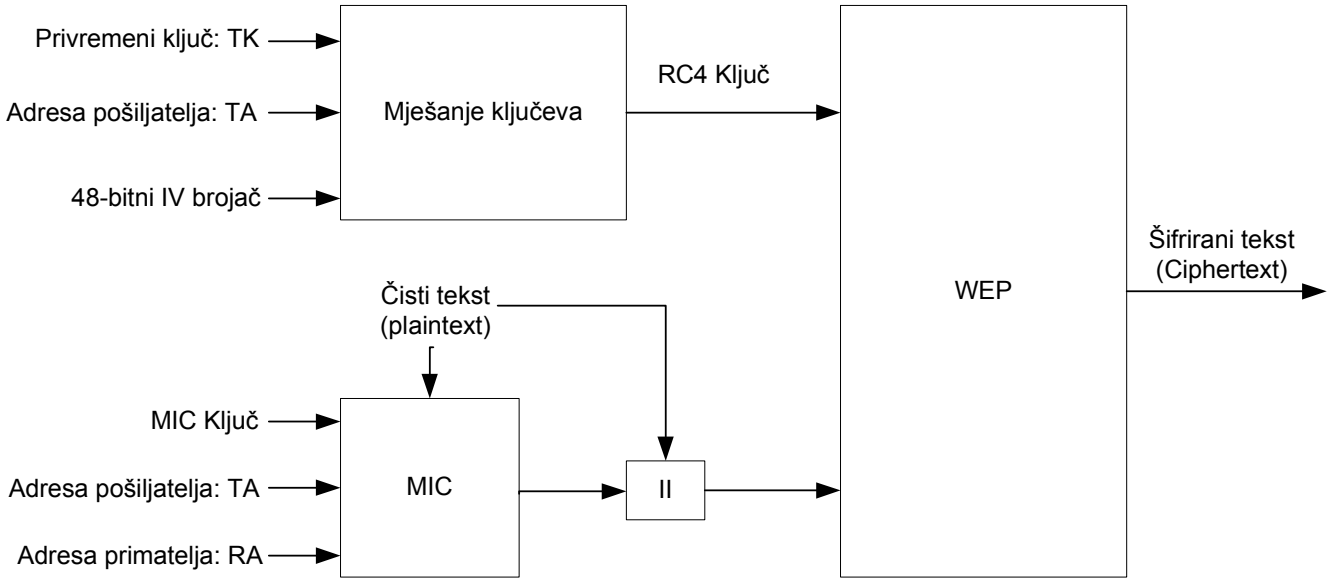
Očito je postojanje velikog broja napada na WEP (u praksi uspješno izvedivi).

To govori u prilog činjenici da je WEP, kao standard, krajnje nesiguran.

Potrebno ga je što zamijeniti sigurnijim i boljim standardom koji bi u uklonio navedene propuste.

Sigurnosni mehanizmi - WPA

WPA je standard koji pokušava riješiti nedostatke WEP-a. WPA standard je poznat od prije kao Safe Secure Network (SSN). Primjenjiv je u kućnim i malim uredima, ali najveću moć pokazuje implementiran u velikim konfiguracijama



WPA je ovojnica WEP-a koja osigurava da par (TK, IV) koristi samo jedan pošiljatelj i poboljšava integritet WEP okvira primjenjujući nelinearnu funkciju integriteta poruke.

Sigurnosni mehanizmi – WPA2

WPA 2 je nadogradnja na WPA i jedina razlika među njima je što se kao algoritam šifriranja koristi AES, a ne RC4. AES je prihvaćen kao službeni algoritam šifriranja NIST-a (National Institute of Standards and Technology).

Ovakav način zaštite je upotrebljiv i u IBSS (Independent Basic Service Set) načinu rada bežičnih mreža kada klijenti komuniciraju izravno jedan s drugim bez posredovanja pristupne točke. Duljina ključeva u AES-u je 128, 192 ili 256 bita.

No WPA 2 donosi i značajna materijalna ulaganja u novu mrežnu opremu jer je sadašnja preslaba, da bi mogla bez značajnijeg pada performansi omogućiti rad korisnicima. Uzrok tome su veliki sklopovski zahtjevi AES-a. Svaka organizacija bi trebala procijeniti je li isplativo takvo ulaganje u mrežnu opremu.

Sigurnosni propusti WPA zaštite

Napad preuzimanjem autentifikacije se zasniva na prisiljavanju korisnika da se ponovno autentificira.

Napad je jako jednostavan i samo treba natjerati korisnika da se odlogira i ponovno prijavi. Tada se snima proces ponovne prijave korisnika na računalo napadača.

Nakon završene autentifikacije, koristi se brute-force dešifriranje snimljenih podataka u potrazi za wpa ključem.

Otpornost na Brutal force napade

Izračun trajanja brute force napada uz brzinu od 100 ključeva u sekundi na dužinu ključa od :

8 znakova, vrijeme dešifriranja je 25 dana.
9 znakova, vrijeme dešifriranja je 21 mjesec.
10 znakova, vrijeme dešifriranja je 46 godina.

Daljnja ilustracija o značenju dužine ključa nije potrebna.

Ipak, ovaj model zaštite ipak ima fizičke granice, a vrijeme dešifriranja se skraćuje zbog brzine računala.

Stoga ova zaštita ipak ne nudi konačno rješenje.

Open source riješenja za wireless napade

Open source riješenje koja se koriste za Wireless napade su sljedeća:

1. Kismet [*http://www.kismetwireless.net/*](http://www.kismetwireless.net/)
Puna funkcionalnost unutar Windows OS platforme.
2. Aircrack [*http://www.aircrack-ng.org/*](http://www.aircrack-ng.org/)
Potpuna funkcionalnost unutar Linux OS-a distribucije.
3. Knoppix STD 0.1 [*http://s-t-d.org/index.html*](http://s-t-d.org/index.html)
CD bootabilna distribucija Linuxa sa integriranim alatima.
4. Kismac [*http://binaervarianz.de/*](http://binaervarianz.de/)
Najbolja aplikacija za razbijanje WPA zaštite. Radi samo pod OSX platformom.

SMJERNICE RAZVOJA ZAŠTITE

- Nove smjernice razvoja zaštite u bežičnim sustavima dijelom odbacuju dosadašnji pristup isključivo enkripcijske zaštite. Zbog stalnog unapređenja mogućnosti računala, vrijeme za brutal force napad se smanjuje.
- Do sada se taj problem rješavao na način da se podiže složenost enkripcije, složenost inicijalizacijskog vektora, vektora integriteta ili hash funkcije. To u konačnosti nije rješenje jer ne nudi konačni model.
- Dolazimo do paradoksa pri kojem će okviri razmjene podataka u budućnosti imati veći teret na strani enkripcije i verifikacija, nego li na strani samog korisnog sadržaja kojeg se prenosi. Stoga su nužna nova rješenja.

Optimal Message Transfer Autenticator

Zasnovan je na vizualnoj provjeri poruke.

Hash je algoritam koji je određeni paket podataka u stanju prikazati određenim heksadecimalnim brojem.

Svaki podatak ima jedinstveni hash “otisak prsta“, jedinstven za svaki podatak. Na osnovu hasha korisnik može provjeriti autentičnost poruke.

Ovaj pristup je nedavno uzdrmala grupa znanstvenika iz Kine koji su na osnovu hasha, uspjeli izmijeniti, izraditi novi paket identične vrijednosti.

Rješenje je odmah ponuđeno. Promjeniti varijablu kojom se hash izračunava sa 128 bitne vrijednosti na 129, 130 bitnu itd.

No to ne može biti konačno rješenje.

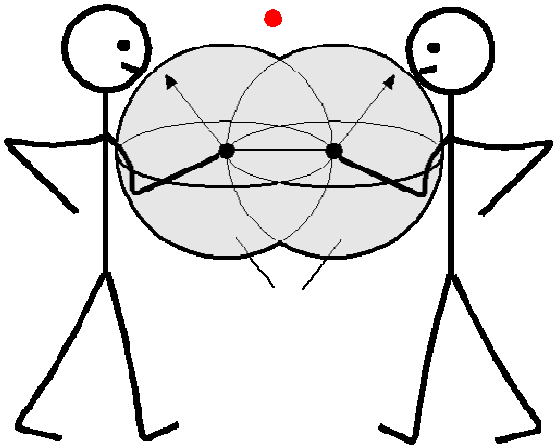
Integrity regions (I regions)

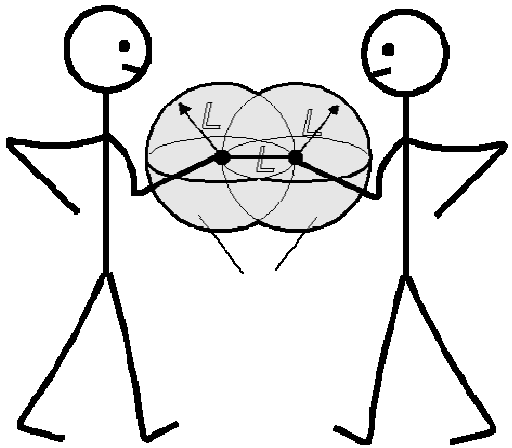
- Zasnovan je na provjeri pozicije s koje je odaslan signal.
- Prethodna rješenja sa kontrolom radiousa emitiranja AP i GPS verifikacijom radious server su odbačena, izigrana.
- Stoga se pristupilo verifikaciji korisnika, odnosno njegove pozicije unutar zadane regije, koristeći ultrazvučni mjerač, koji mjeri s odstupanjem od najviše 1 cm.

Integrity regions (I regions)

- Korisnici će sami biti u mogućnosti kontrolirali veličinu svoje zaštićene regije prijenosa, a eventualni napadač će se morati naći unutar te regije i proći korisničku provjeru.
- Primatelj Napadač Pošiljatelj

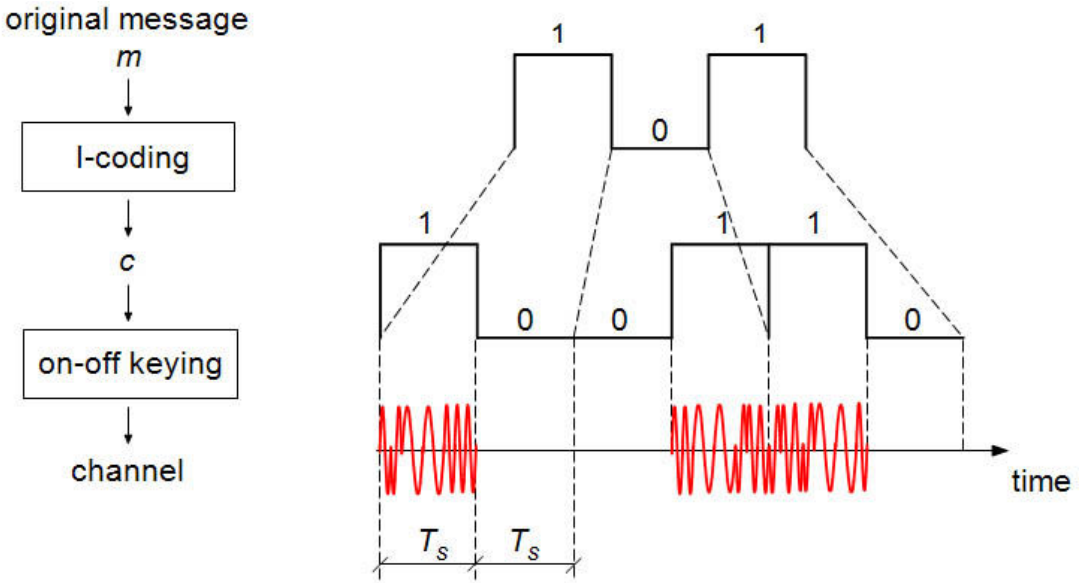
Primatelj Napadač Pošiljatelj





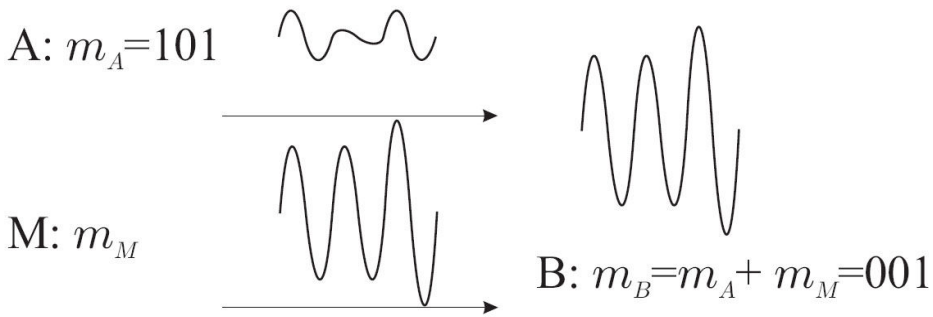
Integrity codes (I codes)

- Zasnovani su na teškoći ostvarivanja cilja da se ukloni trag emitiranog signala, emitiranjem signala protufaze i protuvrijednosti.
- informacija se prijenosi na način da se postojanjem ili nepostojanjem signala u određenom vremenskom intervalu definira stanje 1 ili 0.
- Svaka se 1 Manchester kodom pretvara u 10 odnosno 0 u 01.

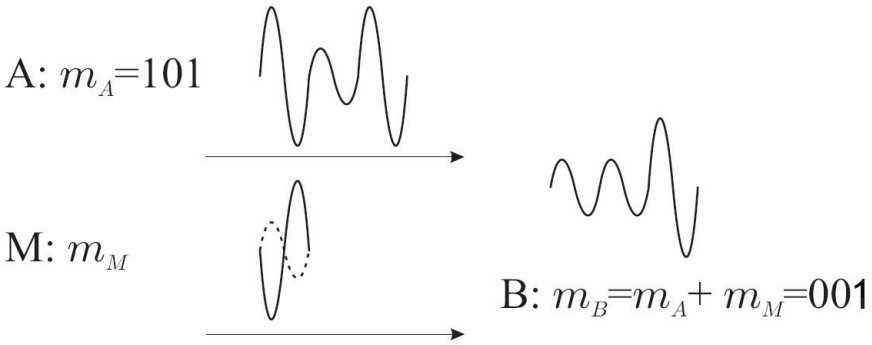


Integrity codes (I codes)

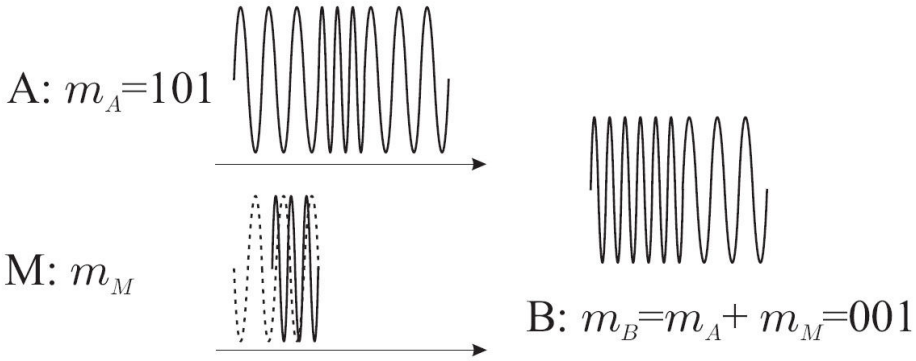
Amplitudna modulacija



Frekvencijska modulacija

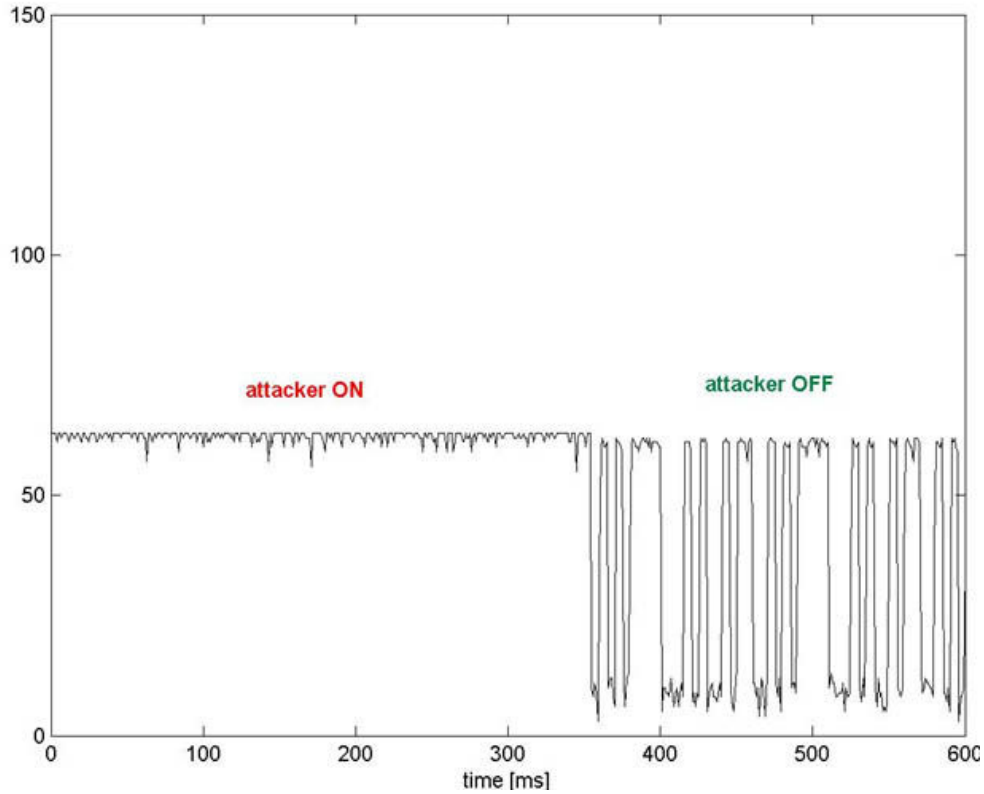


Signal shadowing



Integrity codes (I codes)

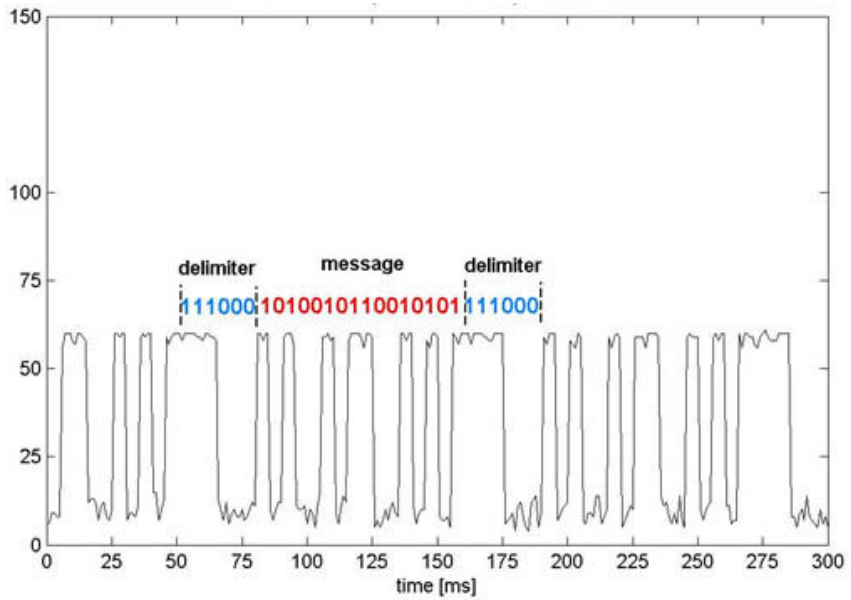
- Zbog trajanja signala od 5 ms, realno je nemoguće nekim generatorom vala, poništiti tragove signala, obrtanjem faze na način da se takav signal maskira i umjesto njega generira lažni, što je osnova za napad.



Integrity codes (I codes)

- Svaki slog podataka odvaja se delimiterom. Delimiter je najkraća moguća sekvenca koja nije ponovljiva u Manchester kodu. Između dva delimitera prenosi se slog podataka, a prijenos je završen kada je oglašen delimiter.

$$\mathcal{S} = \{0, 1, 00, 01, \ldots, \underbrace{11\ldots1}_{k}\}, \; \mathcal{C} = \{01, 10, 0101, 0110, \ldots, \underbrace{1010\ldots10}_{2k}\}$$



ZAKLJUČAK

- U analizi sigurnosti, WEP nije zadovoljio niti jedan od tri cilja s kojim je stvoren: provjera korisnika, zaštita privatnosti podataka te autorizacija korisnika. Impresivan broj različitih mogućih napada, od kojih su mnogi i praktično uspješno izvedeni, samo potvrđuje činjenicu nesigurnosti tog standarda.
- Jednako tome WEP 2 zaštita nije ponudila bitno bolje rješenje. Današnjim metodama WEP zaštita se “razbija” za 30 minuta, nakon čega napadač ima pristup mrežnim resursima, što je nedopustivo.

ZAKLJUČAK

- U ovom trenutku pravi odabir zaštite, kako za kućne bežične mreže tako i za korporativne bežične mreže, bila bi kombinacija više sigurnosnih mjera:

- 1. Uporaba WPA sigurnosne zaštite (u korporacijama ključ treba ostaviti nepoznat krajnjem korisniku).

- 2. MAC filtriranje korisnika na AP. (prikladnije za manje mreže, zbog manjeg broja izmjena i zamjena aktivnih mrežnih adaptera).

- 3. Prilagodba radijusa emitiranja signala pristupne točke na minimum koji pokriva područje organizacije ili kućne bežične mreže.

ZAKLJUČAK

- Ipak, WPA zaštita ima u konačnosti propust, koji će biti sve izraženiji kako se budu razvijale mogućnosti računala koja se bave dešifriranjem. Stoga su nove smjernice razvoja:

- Message authentication,
- I region,
- I codes.

- Nove metode ovim su načelno postavljene, a praktična rješenja i primjena se tek očekuju.