



HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Analiza Kismet alata

CCERT-PUBDOC-2004-09-91

A decorative graphic at the bottom of the page consisting of several concentric, semi-transparent white arcs on a light gray background, creating a sense of depth and movement.

CARNet CERT u suradnji s **LS&S**

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument, koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost** računalnih mreža i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Ovaj dokument predstavlja vlasništvo CARNet-a (CARNet CERT-a). Namijenjen je za javnu objavu, njime se može svatko koristiti, na njega se pozivati, ali samo u originalnom obliku, bez ikakvih izmjena, uz obavezno navođenje izvora podataka. Korištenje ovog dokumenta protivno gornjim navodima, povreda je autorskih prava CARNet-a, sukladno Zakonu o autorskim pravima. Počinitelj takve aktivnosti podliježe kaznenoj odgovornosti koja je regulirana Kaznenim zakonom RH.

Sadržaj

1. UVOD I PREGLED MOGUĆNOSTI	4
1.1. PODRŽANI OPERACIJSKI SUSTAVI	4
2. INSTALACIJA I KONFIGURACIJA	5
3. RAD S ALATOM	6
3.1. ALTERNATIVNA SUČELJA	7
4. GRAFIČKO MAPIRANJE MREŽA	8
5. DISTRIBUIRANI NAČIN RADA	11
6. KISMET KAO IDS SUSTAV.....	12
7. ZAKLJUČAK	14

1. Uvod i pregled mogućnosti

Kismet je alat koji omogućuje detekciju 802.11 bežičnih računalnih mreža, prisluškivanje bežičnog mrežnog prometa i detekciju neovlaštenih aktivnosti na ovakvim mrežama. Alat radi na drugom sloju OSI modela i identifikaciju mreža vrši na temelju pasivnog prikupljanja podataka koje one emitiraju u eter.

Zbog velikog broja mogućnosti, ovaj alat moguće je koristiti za različite primjene, kao što su npr.:

- Prisluškivanje mrežnog prometa i pohrana prikupljenih informacija u formatu kompatibilnom s Ethernet programom,
- Bilježenje osjetljivih WEP paketa u formatu kompatibilnom sa Aircrack alatom za probijanje Wep ključeva,
- Detekcija raspona IP adresa mreže,
- Otkrivanje skrivenih SSID oznaka mreža,
- Grafičko mapiranje bežičnih računalnih mreža pomoću GPS uređaja,
- Identifikacija tipa i modela pristupnih uređaja (engl. *access point*) i mrežnih kartica,
- Detekcija pristupnih uređaja sa tvorničkom konfiguracijom.

No, bez obzira na njegove brojne mogućnosti, najčešće primjene Kismet programskog paketa uključuju sljedeće aktivnosti:

- Wardriving skeniranje,
- Nadgledanje rada bežične računalne mreže,
- Postavljanje distribuiranog IDS sustava,
- Detekcija malicioznih pristupnih uređaja.

1.1. Podržani operacijski sustavi

Iako bi bez većih problema trebao raditi na svim Posix kompatibilnim sustavima, funkcionalnost Kismet programa na pojedinima od njih određena je postojanjem odgovarajućih upravljačkih programa za bežične mrežne kartice. Naime, prisluškivanje mrežnog prometa na bežičnim računalnim mrežama nešto je kompliciranije od iste radnje na žičanim mrežama. Dok je kod klasičnih mrežnih kartica za prisluškivanje mrežnog prometa potrebno jednostavno isključiti filtriranje paketa (engl. *promiscuous mod*), kod bežičnih mreža potrebni su posebni upravljački programi, koji su u stanju osim Ethernet mrežnog prometa prikupljati i prosljeđivati sav ostali bežični mrežni promet (*beacon* paketi, praćenje svih mrežnih kanala, itd.).

Zbog najvećeg izbora upravljačkih programa koji su u stanju prisluškivati bežični mrežni promet, kao najbolja platforma preporučuje se Linux operacijski sustav. Zadovoljavajući broj odgovarajućih upravljačkih programa moguće je pronaći i kod OpenBSD, FreeBSD, NetBSD i MacOSX sustava. Trenutno ne postoje odgovarajući javno dostupni upravljački programi za Microsoft Windows operacijske sustave, iako je na tim sustavima moguće instalirati centralni Kismet poslužitelj za distribuirani IDS sustav.

2. Instalacija i konfiguracija

Instalacijski postupak Kismet programa ne razlikuje se od tipične instalacije većine programa na Linux/Unix operacijskim sustavima. Pri postupku prevođenja izvornog koda koristi se `configure` skripta uobičajena za većinu *open source* projekata i prevođenje bi trebalo proteći bez problema ukoliko se koristi bilo koja modernija inačica `gcc` prevodioca.

Prije prevođenja aplikacije, potrebno je na sustavu instalirati sve eventualno potrebne biblioteke i eksterne aplikacije. U daljnim poglavljima navedene su biblioteke i aplikacije potrebne za rad pojedinih funkcionalnosti. Nakon instalacije potrebnih aplikacija i biblioteka, pokreće se `configure` skripta sa odgovarajućim opcijama. Opcije koje se zadaju, uključuju pojedine funkcionalnosti u prevedenu aplikaciju, a listu dostupnih opcija moguće je pregledati izdavanjem naredbe

```
#configure -help
```

Nakon što je paket ispravno konfiguriran, potrebno ga je prevesti izdavanjem naredbe `make` te instalirati pomoću naredbe `make install`.

Po uspješnoj instalaciji, paket je prije inicijalnog pokretanja potrebno konfigurirati. Konfiguracija Kismet programa obavlja se pomoću dvije datoteke (`kismet.conf` i `kismet_ui.conf`). Datoteka `kismet.conf` sadrži konfiguraciju kismet poslužitelja, dok se u datoteci `kismet_ui.conf` nalazi konfiguracija klijentskog sučelja za rad s polužiteljem. Obje datoteke uobičajeno se nalaze u direktoriju `/usr/local/etc/` i sadrže konfiguracijske varijable u jednostavnom obliku „varijabla=vrijednost“.

Osnovna konfiguracija sustava, dovoljna za normalan rad, svodi se na sljedeće korake:

- **Postavljanje `suiduser` korisničkog imena** – Kismet prilikom pokretanja posjeduje root ovlasti na sustavu, koje su mu neophodno potrebne da mrežnu karticu postavi u "Monitor" način rada i priključi se na sučelje za prisluškivanje paketa. Čim obavi sve neophodne radnje, program će odbaciti root ovlasti i preuzeti razinu ovlasti korisnika definiranog `suiduser` direktivom unutar konfiguracijske datoteke. Postavljanje navedene direktive neophodno je za ispravno pokretanje Kismet poslužitelja,
- **Podešavanje izvora paketa** – pomoću `source` direktive definira se izvor za prikupljanje paketa, tj. mrežna kartica pomoću koje se prisluškuje mrežni promet. Sintaksa ove direktive je sljedeća `source=tip_izvora,mrežno_sučelje,ime[,inicijalni_kanal]`. Važeći tipovi izvora mogu se pronaći u dokumentaciji programa pod poglavljem "Capture Sources", npr. za Cisco Aironet kartice izvor se definira kao 'cisco'. Iako većina korisnika posjeduje samo jednu bežičnu mrežnu karticu na računalu, ovom direktivom moguće je definirati proizvoljan broj izvora,
- **Podešavanje dozvole pristupa klijentima** – budući da Kismet radi u klijent poslužitelj načinu rada, potrebno je podesiti dozvole za spajanje klijentskim sučeljima. Ova vrijednost inicijalno je podešena tako da dozvoljava spajanje isključivo klijentima sa lokalnog računala, što u većini slučajeva odgovara. Ipak, ukoliko se klijent nalazi na udaljenom računalu, potrebno je definirati njegovu IP adresu,
- **Podešavanje direktorija za log zapise** – Kismet je inicijalno podešen tako da log poruke zapisuje u direktorij iz kojega je pokrenut. Ovakav način zapisivanja u većini slučajeva je nepoželjan, pa je pomoću direktive `logtemplate` potrebno definirati lokaciju proizvoljnog direktorija u koji će se zapisivati log poruke.

Klijentska aplikacija također zahtijeva određenu konfiguraciju, tj. podešavanje vrijednosti u datoteci `kismet_ui.conf`. Koraci podešavanja su sljedeći:

- **Definiranje lokacije i porta Kismet poslužitelja** – klijentska aplikacija inicijalno se pokušava spojiti na lokano računalo, uzimajući kao parametar uobičajeni port na kojem se nalazi Kismet poslužitelj. Ukoliko se poslužitelj nalazi na udaljenom računalu ili koristi nestandardni port, potrebno je podesiti ove parametre.
- **Podešavanje prikaza** – unutar konfiguracijske datoteke moguće je podesiti podatke o pronađenim mrežama koji će se ispisati na zaslonu. Inicijalne vrijednosti također zadovoljavaju u većini slučajeva.

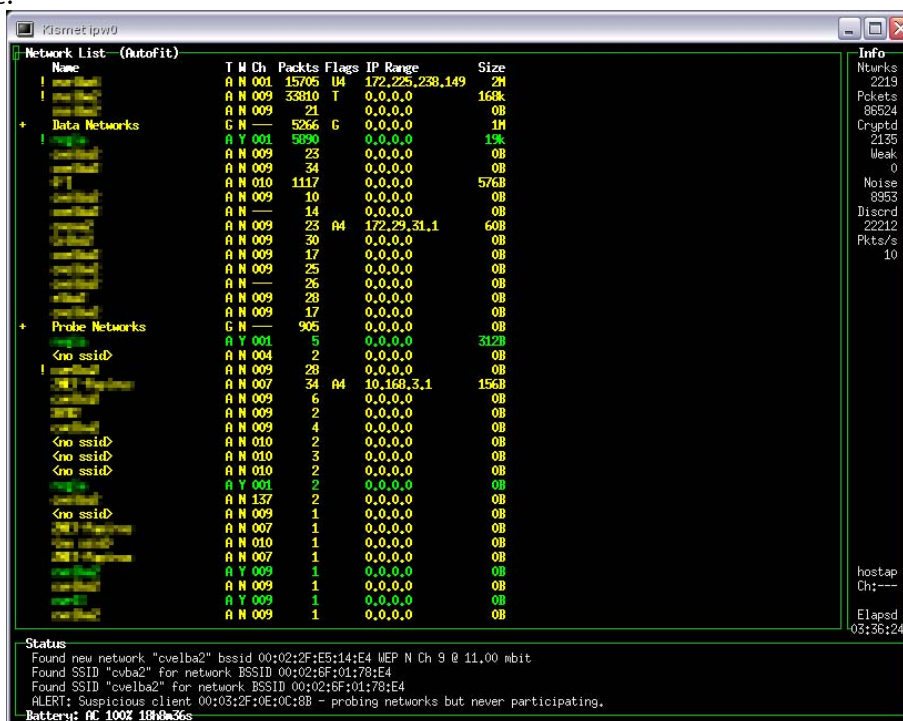
- **Podešavanje zvučnih signala** – sučelje sadrži i mogućnost podešavanja zvučnih upozorenja u slučaju detekcije malicioznih aktivnosti ili pronalaska nove mreže. U tu svrhu koristi se eksterna aplikacija za reprodukciju zvuka. Inicijalno podešena 'play' naredba u većini slučajeva zadovoljava potrebe.

Navedeni koraci dovoljni su za ispravan rad i skeniranje mreža. Dodatna konfiguracija potrebna je za ostale funkcionalnosti kao što su filtriranje paketa, distribuirani način rada, napredne IDS opcije, itd. Upute za podešavanje dodatnih opcija nalaze se u dokumentaciji programa, kao i komentarima unutar same konfiguracijske datoteke.

3. Rad s alatom

Nakon uspješne konfiguracije, alat se pokreće iz naredbenog retka upisivanjem naredbe `kismet`, što će pokrenuti kismet poslužitelj i odmah zatim klijentsku aplikaciju. Sučelje klijenta je u tekstualnom obliku (Nurses/Panels) i snalaženje u njemu je relativno intuitivno. Pomoć je dostupna pritiskom na tipku 'h', što će rezultirati popisom svih opcija za rad sa sučeljem.

Unutar glavnog prozora sučelja nalazi se popis svih detektiranih mreža (**Slika 1**), i općenite informacije o prikupljenim paketima. Donji dio prozora prikazuje najnovije podatke o pronađenim mrežama i upozorenja o neovlaštenim aktivnostima. Detektirane mreže moguće je sortirati na razne načine pritiskom na tipku 's', nakon čega se pritiskom na tipku 'i' mogu proučiti detalji odabrane mreže.



Slika 1: Glavni prozor Kismet sučelja

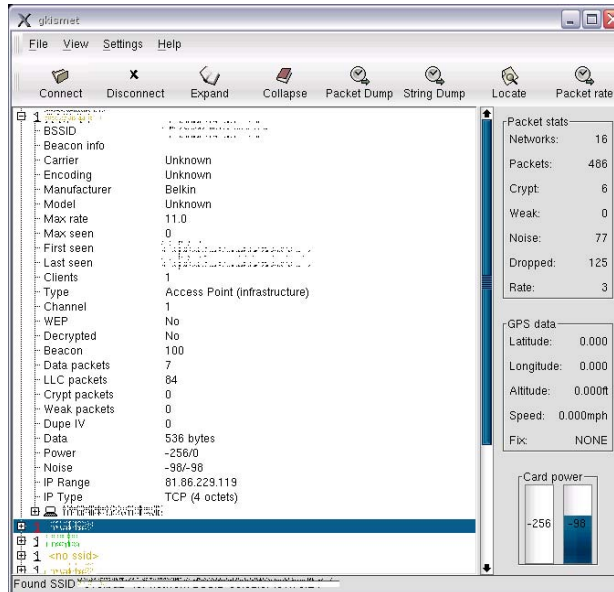
Kao dodatne opcije mogu se navesti sljedeće:

- Ispis klijenata pojedine mreže – znak 'c',
- Graf koji prikazuje količinu paketa u ovisnosti o vremenu – znak 'r',
- Prikaz tipova prikupljenih paketa za odabranu mrežu – znak 'p',
- Ispis tekstualnih nizova iz prikupljenih paketa – znak 'd',
- Ispis svih upozorenja o malicioznim aktivnostima – znak 'w',
- Prozor za precizno lociranje koordinata odabrane mreže.

3.1. Alternativna sučelja

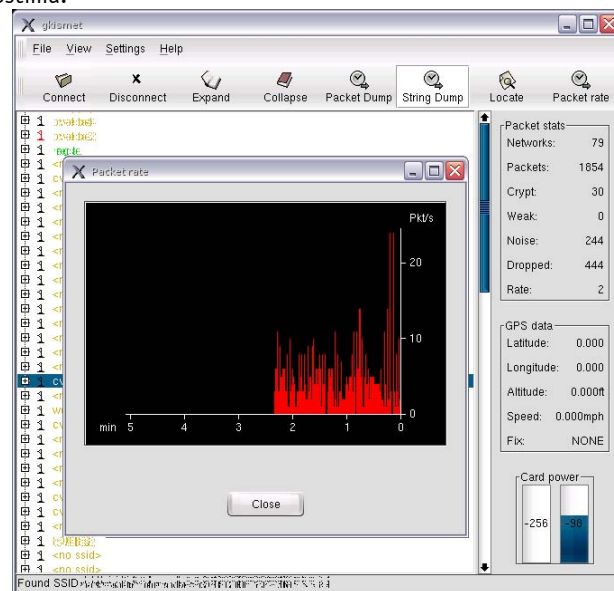
Osim standardnog kismet kljenta s ncurses/panels sučeljem, moguće je koristiti i alternativne klijente čija su sučelja namijenjena za rad u grafičkim okruženjima. Podaci o raspoloživim alternativnim klijetima nalaze se na Web stranici Kismet alata (<http://www.kismetwireless.net/links.shtml>).

Kao jedno od stabilnijih i kvalitetnijih sučelja, pokazalo se gkismet sučelje temeljeno na Gnome Desktop okruženju.



Slika 2: Glavni prozor gkismet kljenta

Gkismet sučelje je po svojoj funkcionalnosti gotovo identično tekstualnom Ncurses sučelju, ali je rad u njemu puno ugodniji i određene funkcije, poput prikaza količine prometa, su mnogo bolje riješene. Kao najveći nedostatak ovog sučelja može se navesti nedostatak kvalitetne podrške za upozorenja o malicioznim aktivnostima.



Slika 3: Prikaz količine prometa u grafičkom sučelju

4. Grafičko mapiranje mreža

Jedna od naprednih mogućnosti Kismet alata je i iscrtavanje položaja detektiranih mreža na zadanim zemljopisnim kartama. Ova opcija najčešće se koristi kod *wardriving* skeniranja, ali moguće ju je iskoristiti i za određivanje položaja napadača u slučaju primjene Kismet-a kao distribuiranog IDS sustava. Kismet prikuplja podatke o svom položaju putem GPS uređaja spojenog na računalo i na temelju njih određuje položaj detektirane pristupne točke, koju potom ucrtava na zadane mape.

Za korištenje ove funkcionalnosti potrebne su neke eksterne aplikacije i biblioteke koje se dodatno instaliraju. Ukratko, potrebni su sljedeći alati:

- GSPD (<http://russnelson.com/gpsd>) - GSPD je poslužitelj koji provjerava serijske portove računala u potrazi za priključenim GPS uređajima. Ukoliko je GPS uređaj priključen, GSPD parsira prikupljene podatke i čini ih dostupnim ostalim aplikacijama putem TCP sučelja. Kismet je u mogućnosti prikupljati podatke sa GSPD poslužitelja na lokalnom sustavu ili sa udaljenih računala, putem klasičnog žičanog ethernet-a.
- Imagemagick (<http://www.imagemagick.org/>) - Imagemagick je biblioteka za generiranje grafičkih datoteka, koja podržava razne danas dostupne formate datoteka. Korištenjem ove biblioteke, Kismet iz obrađenih GPS mapa generira gotove slike. Za ispravan rad, na sustav je potrebno instalirati Imagemagick inačice 5.4.7 ili noviji.
- Expat (<http://expat.sourceforge.net>) - Expat je programska biblioteka koja se koristi za procesiranje XML biblioteka. Pomoću ove biblioteke `gpsmap` parsira izlazne datoteke Kismet-a koje su zapisane u XML formatu. Za ispravan rad potrebno je koristiti Expat paket inačice 1.95 ili noviji.
- GMP (<http://www.swox.com/gmp/>) - GMP je biblioteka koju Kismet koristi pri izvođenju matematičkih kalkulacija visoke preciznosti, potrebnih za generiranje GPS mapa.

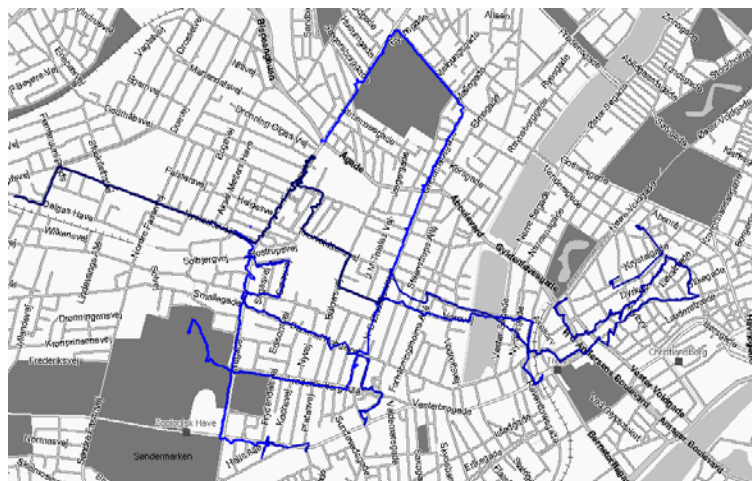
Za generiranje grafičkih datoteka i ucrtavanje položaja pronađenih mreža na mape, koristi se pomoćni alat unutar kismet paketa pod nazivom `gpsmap`. Ovaj alat procesira `netxml` i `gpsxml` datoteke generirane od strane Kismet-a i pomoću dobivenih podataka ucrtava položaj pronađenih mreža na mapi. Mape na koje će se ucrtavati prikupljeni podaci mogu se dohvatiti od raznih izvora (npr. MapBlast, Tiger, Terraserver, EarthMaps, itd.), a postoji i mogućnost korištenja mapa vlastite izrade.

Sintaksa naredbe za generiranje mapa je sljedeća:

```
#gpsmap [opcije] -g konfiguracijska_datoteka -o izlazna_datoteka
```

Izlazna datoteka tj. rezultat obrade podataka je mapa sa ucrtanim položajima detektiranih mreža. Cjelokupan popis opcija koje se koriste prilikom pokretanja `gpsmap` alata može se pronaći u njegovim man stranicama, a njihova primjena odnosi se uglavnom na izgled i format generirane slike. Prilikom generiranja slike, navažnije je odabrati metodu ucrtavanja tj. prezentiranja prikupljenih podataka, jer o tome uvelike ovisi konačan izgled slike. `Gpsmap` nudi izbor između sljedećih metoda ucrtavanja:

- **Track drawing** – na temelju podataka dobivenih od Kismet poslužitelja, na mapi se iscrtava krivulja koja opisuje kretanje senzora prilikom skeniranja.



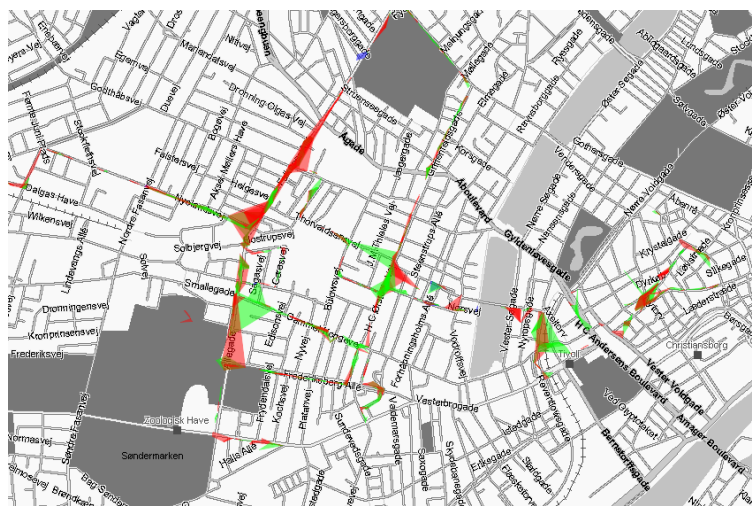
Slika 4: Track drawing prikaz

- **Bounding rectangle** – na mapu se ucrtava pravokutnik koji omeđuje ekstremne točke detektirane bežične mreže.
- **Range circle** – na temelju podataka o središtu mreže i njenih ekstremnih točaka, procjenjuje se prosječan domet mreže, koji se predstavlja ucrtanim krugom na karti. Ova metoda nije potpuno precizna, ali u većini slučajeva u zadovoljavajućoj mjeri određuje domet mreže.



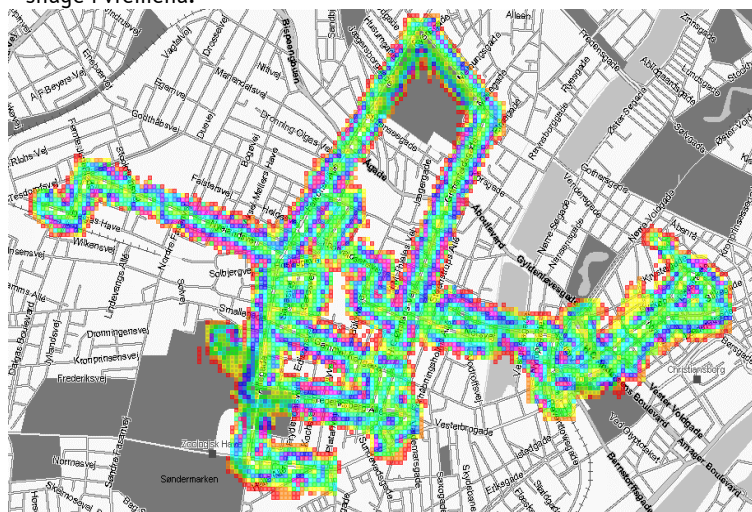
Slika 5: Range circle prikaz

- **Convex hull** – ovakav tip mape prikazuje stvarni domet mreže i njenu usmjerenost.



Slika 6: Convex Hull prikaz

- **Scatter plot** – iscrtava točku za svaki detektirani uređaj.
- **Power interpolation** – ovaj prikaz predstavlja mrežu polja koje označavaju snagu mreže na određenim mjestima. Prilikom generiranja ovkvoq tipa prikaza, postupkom interpolacije određuje se snaga mreže na onim mjestima gdje nije izravno izvršeno mjerenje. Kako bi ovaj prikaz bio što vjerniji realnoj situaciji, poželjno je uzeti uzorke signala sa lokacija pravilno raspoređenih po čitavom području skeniranja. Potrebno je napomenuti kako generiranje ovog tipa mape konzumira veće količine procesorske snage i vremena.

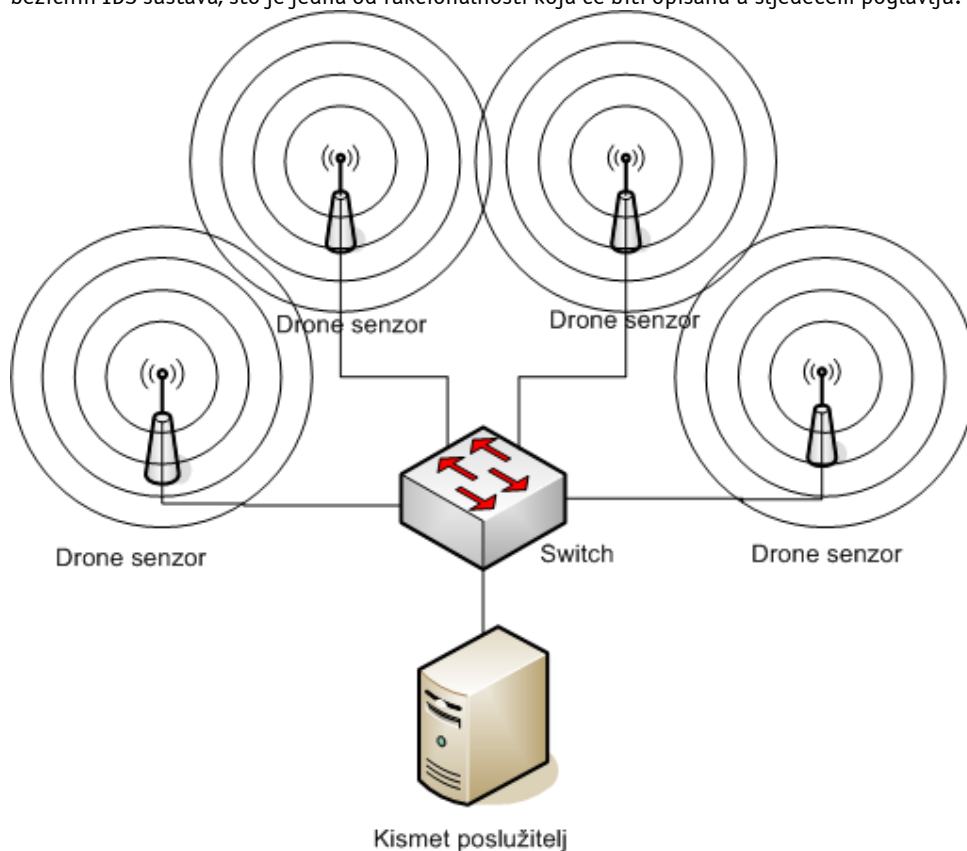


Slika 7: Power interpolation prikaz

- **Network center** – jednostavan prikaz, u kojem je točkom označeno središte svake detektirane mreže. Položaj središta određuje se kao srednja vrijednost ekstremnih točaka mreže.
- **Labels** – ovom opcijom uključuje se označavanje ucrtanih mreža njihovim SSID oznakama.
- **Legend** – u uglu mape ucrtava se legenda koja definira koordinate, skalu i ostale bitne detalje vezane uz generiranu mapu.

5. Distribuirani način rada

Kismet je u mogućnosti raditi i kao distribuirani alat. Ideja ovakvog načina rada je instalacija velikog broja jednostavnih i hardveski minimalno zahtjevnih senzora, koji će prikupljati podatke i prosljeđivati ih na obradu centralnom poslužitelju. Takav pristup odgovara i zahtjevima za realizaciju modernih bežičnih IDS sustava, što je jedna od funkcionalnosti koja će biti opisana u sljedećem poglavlju.



Slika 8: Kismet u distribuiranom načinu rada

Komponenta Kismetova zadužena za prikupljanje i prosljeđivanje podataka naziva se `kismet_drone`. Drone poslužitelj pokreće se pomoću naredbe `kismet_drone` i za svoju konfiguraciju koristi `kismet_drone.conf` datoteku. Format i opcije u konfiguracijskoj datoteci gotovo su identične onima u konfiguracijskoj datoteci samog kismet poslužitelja (`kismet.conf`). Unutar konfiguracijske datotke potrebno je podesiti mrežni port na kojem će drone poslužitelj prosljeđivati prikupljeni mrežni promet (opcija `tcpport`), kao i adresu centralnog poslužitelja kojem je dozvoljen pristup podacima (opcija `allowedhosts`). Ostatak konfiguracije identičan je konfiguraciji klasičnog kismet poslužitelja, uz napomenu da su kod drone načina rada podržane sve mrežne kartice koje su podržane kod klasičnog Kismet poslužitelja, kao i mogućnost prikupljanja podataka sa više mrežnih kartica istovremeno. Osim toga, svaki udaljeni senzor moguće je podesiti tako da prisluškuje odabrani mrežni kanal i ovisno o kartici, odabrani mrežni standard (npr. 802.11a ili 802.11b).

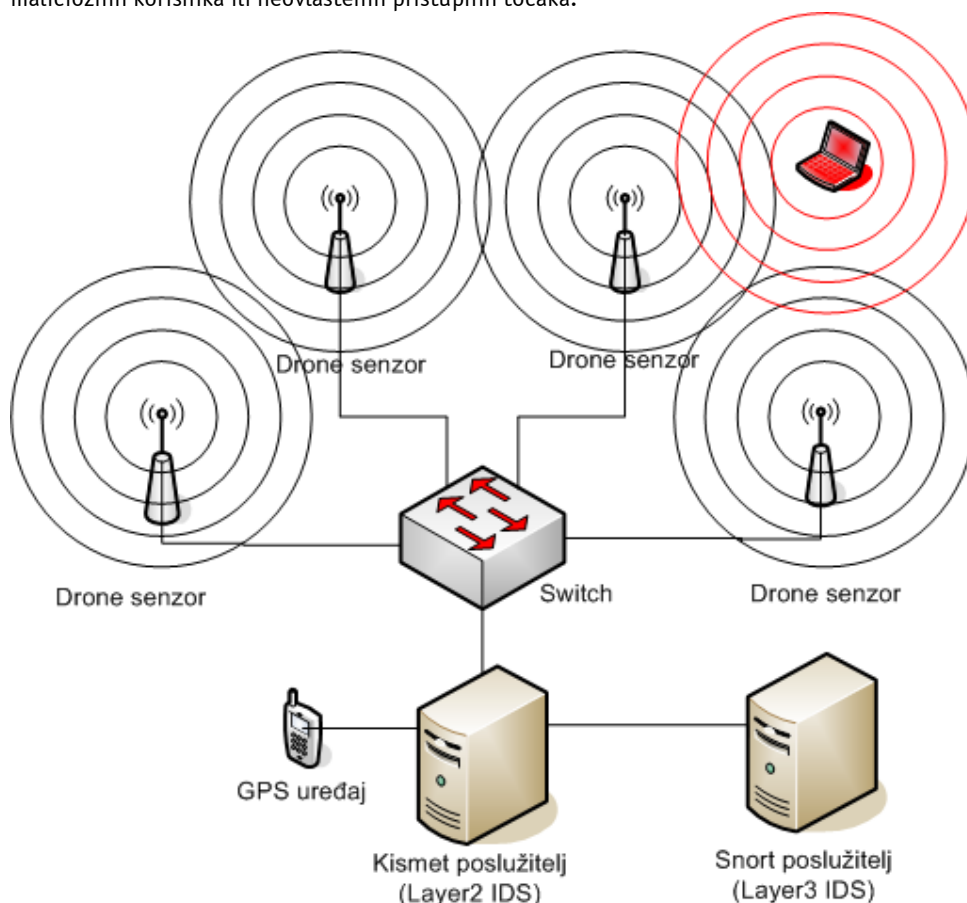
Kismet poslužitelj konfiguriran tako da prikuplja podatke sa svih `kismet_drone` senzora na lokalnoj mreži, sve podatke, tj. uočeni mrežni promet, sprema u jedinstvenu datoteku i po potrebi generira upozorenja o neovlaštenim aktivnostima u pojedinim dijelovima mreže. Sav prikupljeni promet moguće je, korištenjem fifo opcije u konfiguracijskoj datoteci, prosljeđiti i na daljnju analizu nekom eksternom IDS sustavu koji radi na trećem sloju OSI modela (npr. `snort`).

Potrebno je napomenuti da se komunikacija drone poslužitelja i centralnog poslužitelja za obradu prikupljenih podataka odvija na lokalnoj mreži u nekriptiranom obliku. Na taj način, kompletan

bežični mrežni promet, moguće j prisluškivati i na lokalnoj računalnoj mreži. Zbog toga se, u svrhu zaštite podataka, preporučuje klasično tuneliranje paketa preko SSH poslužitelja.

6. Kismet kao IDS sustav

Na temelju prethodno opisanog klijent-poslužitelj, odnosno distribuiranog modela rada Kismet alata, moguće je izgraditi jednostavan i jeftin bežični IDS sustav. Kismet generira upozorenja na temelju otisaka specifičnih programskih paketa (netstumbler skeniranje, korištenje airjack alata, itd.) te statističkih analiza (velik broj neuobičajenih paketa, itd.). Baza otisaka, kao i rad Kismet-a kao IDS sustava fokusira se prvenstveno na detekciju malicioznih aktivnosti na drugom OSI mrežnom sloju, dok se za detekciju na ostalim mrežnim slojevima (prvenstveno trećem) koristi mogućnost proslijeđivanja prometa eksternim IDS sustavima (Slika 9). U kombinaciji sa mapiranjem detektiranih mreža pomoću GPS uređaja i `gpsmap` alata, Kismet IDS sustav omogućuje vrlo jednostavno lociranje malicioznih korisnika ili neovlaštenih pristupnih točaka.



Slika 9: Distribuirani IDS sustav izveden pomoću Kismet alata

Neke od nepravilnosti u mrežnom prometu, koje Kismet prepoznaje, obuhvaćaju:

- Netstumbler upiti – u namjeri da otkrije SSID oznaku mreže, Netstumbler alat šalje specifične pakete. Ovo je vrlo pouzdan način za otkrivanje korisnika koji pokušavaju skenirati bežičnu mrežu i doći do podataka o konfiguraciji pristupnih uređaja.
- Pokušaj probijanja SSID oznake pomoću Wellenreiter alata – Wellenreiter alat za skeniranje mreža pokušava brute force napadom otkriti vrijednosti skrivenih SSID oznaka. Ovo je također vrlo pouzdan način otkrivanja malicioznih korisnika.
- Detekcija AirJack alata – AirJack alat za provođenje MitM (engl. Man in the Middle) napada koristi specifičan SSID, kojeg je vrlo lako prepoznati i na taj način uočiti maliciozne aktivnosti na mreži.

- Pojava Probe response paketa sa vrijednošću SSID parametra jednakoj nuli – mnogi bežični mrežni uređaji osjetljivi su na primanje ovakvih paketa, koji najčešće uzrokuju prekid rada uređaja. Pojava ovakvih paketa potencijalno ukazuje na provođenje DoS napada na bežičnu mrežu.
- Promjena kanala na pristupnom uređaju – budući da je temelj mogućih Man in the Middle napada preusmjerenje korisnika na lažni pristupni uređaj koji se nalazi na drugom kanalu, ovakve pojave na mreži mogu se s opravdanjem smatrati sumnjivima.

Iako primarno namijenjena upotrebi u statičkim IDS sustavima, ova funkcionalnost Kismet-a može se iskoristiti i prilikom *wardriving* skeniranja. Međutim, zbog specifičnih uvijeta koji nastaju kod takovih tipova skeniranja, potrebno je uzeti u obzir mogućnost generiranja velikog broja lažnih uzbuna.

7. Zaključak

Kismet trenutno predstavlja najbolji izbor pri odabiru alata za praćenje i analizu mrežnog prometa na 802.11 računalnim mrežama. Iako njihov broj raste iz dana u dan, slični konkurentski programi zaostaju količinom podržanih opcija, kao i jednostavnošću instalacije i upotrebe. Velik broj grafičkih sučelja razvijenih za upravljanje Kismetom, čini ga pogodnim za implementaciju na najrazličitije sustave (od ručnih računala do različitih Unix/Linux poslužitelja).

Mogućnost integracije s GPS uređajima i grafičkog prikaza položaja detektiranih bežičnih mreža (ili klijentskih računala) svoju najveću primjenu nalazi prilikom izvođenja *wardriving* skeniranja ali i prilikom implementacije Kismet-a kao jednostavnog i jeftinog IDS rješenja. Korištenju Kismet-a kao IDS sustava, u prilog ide i činjenica da ga je zbog klijent-poslužitelj modela, po kojem je izveden, vrlo lako moguće skalirati i rasporediti tako da pokrije cijelo traženo područje.