

Selvorganiserende læring av trafikkategorier i Bayesiansk pakkebasert IDS



Innledning

Innbruddsdeteksjonssystemer (IDS) brukes for å oppdage unormal aktivitet i et nettverk. Tradisjonelle IDS'er bruker gjerne signaturbasert deteksjon, som går ut på å "matche" nettverkstrafikken mot en forhåndsdefinert angrepsprofil. I motsetning til dette kan vi se på læringsbaserte IDS'er, som har som mål å lære seg hva som er normal nettverkstrafikk, for så å kunne blokkere for den unormale trafikken.

I denne oppgaven har vi fokusert på en læringsbasert IDS, og vi ser på hvordan vi kan bruke en Naiv Bayesiansk klassifikator for å lære seg hva som er normal og unormal nettverkstrafikk. For å kunne klare det er det vesentlig hvordan vi velger ut attributtene som skal brukes i klassifikatoren.

Attributtutvelgelse

Å velge attributter for bruk i en Naiv Bayesiansk klassifikator er meget viktig for å få en mest mulig nøyaktig klassifikator. Attributtene skal dannes av de 384 første bitene i pakken. Disse 384 bitene dekker IP og TCP/UDP header + de første bitene av pakkens innhold. Vi har tatt for oss 2 ulike tankeganger når det gjelder å velge attributter til klassifikatoren.

Semantisk grupperte attributter

Å gruppere bitene i attributter på bakgrunn av hvilken betydning de har, betegner vi som semantisk grupperte attributter. Denne metoden brukes når vi deler inn bitene i attributter som tilsvarer headerfeltene IP og TCP/UDP protokollen.

Avhengighetsbaserte attributter

Avhengighetsbaserte attributter dannes ved at vi ser på relasjonene mellom 2 og 2 bit i pakken, for deretter gruppere de bitene som har høyest gjensidig avhengighet. Avhengigheten defineres som:

$$\sum_{x=y=0}^1 P_{uv}(x,y) * \log \frac{P_{uv}(x,y)}{P_u(x) * P_v(y)}$$

Der

$$P_{uv}(x,y) = \frac{Ant_{xy}}{Totalantall}$$

Hvor Ant_{xy} er antall forekomster av kombinasjonen mellom 2 bits, og $Totalantall$ er total antall pakker.

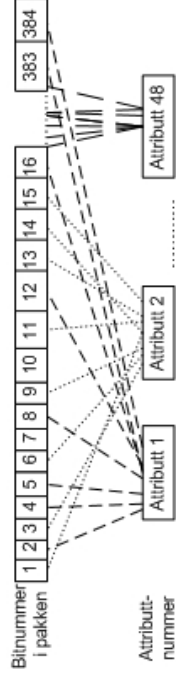
$$P_u(x) = \frac{Ant_x}{Totalantall}$$

Hvor Ant_x er antall ganger $x = 1$ og $Totalantall$ er totalt antall pakker.

$$P_v(y) = \frac{Ant_y}{Totalantall}$$

Hvor Ant_y er antall ganger $y = 1$ og $Totalantall$ er totalt antall pakker.

Ved å gruppere bit i attributter etter hvor avhengige de er av hverandre oppnår vi attributter som antar få verdier og dermed er gode å klassifisere på. Vi gjør forsøk med attributter der vi grupperer 8 og 8 bit, og der vi grupperer inntil 8 bit hvis de har sterk nok gjensidig avhengighet.



Figur 1. Eksempel på utvelgelse av bit ved bruk av bitavhengighets algoritme

Klassifisering

Når vi klassifiserer de innkommende pakkene vil de i utgangspunktet bli plassert i en av klassene Normal, DOS, Probe, U2R eller R2L. Pakken klassifiseres til trafikklassen som er mest sannsynlig, noe som kan bety at pakker havner i en klasse selv om den egentlig ikke bør havne der. Dette løser vi med å innføre en klasse vi kaller ukjent, der vi plasserer pakker som avviker fra gjennomsnittsverdien for klassen den først blir klassifisert som. Innføring av denne klassen fører til en økning av antall falske alarmer, men vi kan senke antallet feilklassifiseringer.

Falske alarmer og feilklassifiseringer

Falske alarmer oppstår når normaltrafikk klassifiseres som angrep. Dette er trafikk som da må behandles manuelt, og det er dermed hensiktsmessig å ha lavest mulig antall falske alarmer. Å senke antall falske alarmer fører til at antallet feilklassifiseringer øker. Det er derfor nødvendig og finne den optimale balansen mellom falske alarmer og feilklassifiseringer.

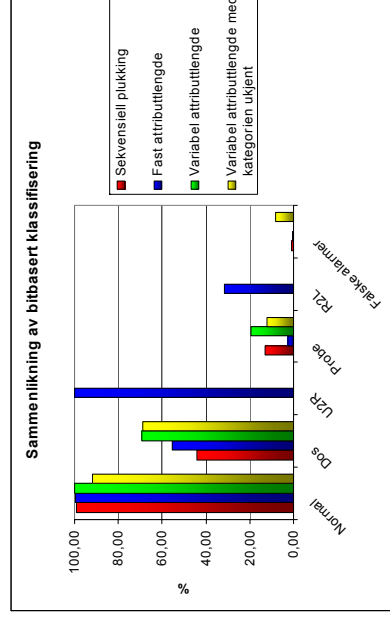
Resultater

Det er flere måter å vise nøyaktigheten til klassifikatoren på. Tabellen under viser hvor mange av angrepsinstanser som blir detektert.

	Instanser av angrep	Detektert	Ukjent	Resultat
Dos	5	4	1	100%
Probe	6	3	3	100%
U2R	3	0	2	67%
R2L	2	0	0	0%

Ser vi på prosentandelen av pakker i de ulike trafikkategoriene viser grafen i Figur 2 hvordan

de ulike avhengighetsbaserte klassifikatorene scorer.



Figur 2. Nøyaktighet av klassifikator med avhengighetsbaserte attributter

Konklusjon

Resultatene viser at vi ved riktig valg av attributter er i stand til å detektere en stor del av angrepene som initieres mot et nettverk. Det er da viktig å merke seg at vi med å detektere et angrep menes det at en eller flere av pakkene i angrepet detekteres. Hvis vi ser resultatene på pakkenivå vil vi kunne klassifisere 99,89 % av normaltrafikken, samtidig som det er relativt få falske alarmer. Vi viser også at det er mulig å justere forholdet mellom feilklassifiseringer og falske alarmer ved å justere hvor stor margin vi skal ha for klassen "ukjent".