Teknik och samhälle
Datavetenskap

Examensarbete
15 högskolepoäng, grundnivå

DDoS
Ett evolverande fenomen

DDoS
An evolving phenomenon

Emil Andersson

Examen: Kandidatexamen 180hp
Huvudämne: Datavetenskap
Program: Systemutvecklare
Datum: 2012-05-28

Handledare: Kristina von Hausswolff
Examinator: Bengt J. Nilsson

Sammanfattning

Internetfenomenet ”Distributed Denial of Service”, förkortat DDoS, beskrivs ofta som ett av de största hoten mot Internet idag. Genom att utnyttja den grundläggande strukturen i kommunikation mellan nätverk och datorer kan kriminella blockera och stänga ute webbplatser och -tjänster från användare, samtidigt som det är mycket svårt för offret och myndigheter att någonsin identifiera den eller de skyldiga. Enorma globala nätverk av ovetande människors infekterade datorer fjärrstyrs till att utföra angrepp mot alla sorters organisationer på Internet med olika motiv, som finansiella, politiska eller för ren vandalism. Syftet med det här arbetet är att göra en dagsaktuell kartläggning över läget kring DDoS-angrepp och titta på statistik över de mest förekommande angreppstyperna, och se om den nyare publicerade forskningen kan svara på de pågående och framträdande trender som kan ses. Sex forskningsartiklar väljs ut att jämföra med dessa trender för att se var mer forskning krävs. Resultatet visar att forskningen kring försvar mot HTTP-GET-angrepp är bristande, samt att den framträdande trenden där angreppen allt oftare använder sig av olika angreppstyper samtidigt inte har undersökts. Mer öppen forskning bör riktas mot dessa bristande områden.

Abstract

The Internet phenomenon ”Distributed Denial of Service”, in short DDoS, is often said to be one of the greatest threats to the Internet today. By abusing the foundation of inter-network and computer communication, criminals can block and shut out websites and services from users while making it very hard for the victim and the authorities to ever identify who was behind it. Enormous global networks made up of unknowing peoples' infected computers can be remotely controlled to conduct attacks against all sorts of organisations on the Internet with different motives, from financial or politic to sheer vandalism. The purpose of this study is to create an up-to-date mapping of the situation of DdoS-attacks and look at statistics of the most prevalent attack types, and to check if newly published research can answer the current and emerging trends that can be seen. Six research articles are chosen to compare with these trends to see where more research is required. The results show that the research around defense against HTTP-GET-attacks is lacking, and that the emergent trend of DDoS-attacks that make use of more than one attack type at the same time has not been examined. More open research should be directed to these lacking areas.

Innehållsförteckning

1 Inledning

Det moderna samhällets ökande beroende av datorteknologi för med sig både nya lösningar och nya sårbarheter. Automatiserade processer förenklar utförandet av sysslor och ärenden samtidigt som det lämnar en öppning för de som har kunskapen att manipulera dessa processer att utnyttja det för egen vinning. Antalet angrepp via datorer mot datorsystem (känt som ”cyberattacker”) ökar år för år eftersom det blir alltmer finansiellt fruktbart för kriminella att rikta sig mot företag, stora som små, som spenderar stora summor för att etablera sig på online-marknaden för att nå ett så stort antal kunder som möjligt. Cyberattacker ökar även i popularitet som ett verktyg för aktivism och personbrott eftersom privatpersoners närvaro på Internet blir allt större.

De typer av cyberangrepp som kriminella kan använda mot virtuella system är många och varierade. Ett sorts angrepp kallas för 'Denial of Service' (härefter förkortat till DoS), tillsammans med den mer storskalade varianten 'Distributed Denial of Service' (härefter DDoS), som utnyttjar Internets grundläggande struktur för att orsaka skada och förlust för offret.

1.1 Arbetet

Detta arbete är för en kandidatexamen inom datavetenskap vid Malmö högskola. Det är ett teoretiskt arbete i form av en litteraturöversikt som sammanfattar kunskap om cyberfenomenet DDoS och dess läge idag. En målsättning med arbetet är att det ska fungera som en plattform för vidare forskning kring DDoS. Arbetet skrivs huvudsakligen i tredje person.

Arbetet skrivs på rekommendation av svenska försvarsmakten.

1.2 Problemformulering

DDoS har varit ett problem för användare och tillhandahållare av nätverkstjänster under en lång tid. Angripare utnyttjar själva Internets underliggande struktur och kommunikation för att kunna blockera en tjänst eller plats för andra användare. För privatpersoner kan effekterna av en attack vara enbart störande, men för företag och organisationer som lagt stora pengar på att upprätthålla en front på Internet kan det vara förödande. DoS och DDoS har varit närvarande på Internet under en lång tid och de visar inga tecken på att försvinna oavsett vad som gjorts för att förhindra deras utförande – tvärtom visar statistik istället på att problemet är ökande i både frekvens och intensitet.

Som grund för arbetet finns följande frågeställning att besvara:

- Hur svarar den senaste fria forskningen inom DDoS-försvar på de trender som ses i dagsläget?

För att besvara frågeställningen ska arbetet sammanställa statistik kring de mest förekommande typerna av DDoS-angrepp och andra pågående trender, samt med hjälp av den publicerade oberoende forskningen försöka matcha populära angrepp mot existerande försvar.

1.3 Syfte

Syftet med arbetet är att skapa en sammanställning och översikt av dagsläget kring DDoS, de mest förekommande angreppstyperna och dess trender, och att matcha dem mot den senaste forskningen kring prevention och försvar. Det kommer att medföra en fördjupning inom ämnet, och resultatet kan sedan användas som en indikerare på oupptäckta områden som behöver mer uppmärksamhet och som en plattform för vidare forskning.

1.4 Avgränsningar

Området kring DDoS är brett och för att möjliggöra en fördjupning inom arbetets fokuss krävs avgränsningar.

- Arbetet behandlar vetenskapliga experimentstudier som påvisar olika tekniker för att bekämpa DDoS-angrepp i olika kontexter, med komplexa matematiska formler för att implementera de algoritmer som presenteras. Med tanke på min egen begränsade erfarenhet med liknande beräkningar ska arbetet inte gå ut på att nära beskriva eller utvärdera dessa formler, utan istället undersöka och presentera det tekniska utförandet.
- Forskningen som arbetet ska behandla är av den fritt tillgängliga typen (härefter refererad till som *den fria forskningen*) som finns tillgänglig genom högskolans bibliotek. Forskningen som bedrivs inom företag och hos andra intressenter är inte tillgänglig.
- DDoS är aktivt över Internet som på egen hand är ett stort område med många olika teknologier och protokoll som samspelar med varandra. Endast trådbunden Internetkommunikation är i fokus för arbetet. Det lägger heller inte någon vikt vid att särskilja molntjänster från andra tjänster, även om ett helt arbete skulle kunna skrivas om det också.
- DoS och DDoS är närbesläktade, men eftersom det sistnämnda är aktivt på en större skala och därmed allvarligare lägger arbetet direkt fokus på DDoS, och inte på DoS.

1.5 Disposition

I kapitel två (**Bakgrund**) presenteras termer, definitioner och kunskap som behövs för att förstå innebörden av DDoS-angrepp.

I kapitel tre (**Metod**) beskrivs arbetsmodellen som arbetet följer för att framställa resultatet utifrån de vetenskapliga artiklar som används. Kapitlet ger en översikt av processen och ett komplett resonemang kring urval i informationshämtningen.

I kapitel fyra (**Dagsläge**) presenteras den teoretiska bildning som är direkt relevant till att precisera vad det är arbetets resultat ska besvara utifrån frågeställningen.

I kapitel fem (**Resultat**) presenteras resultatet som arbetet utmynnar i sett till frågeställningen och teorin. Resultatet sammanställs till en enhetlig text som utgör en klarläggning av de områden som forskningsartiklarna berör.

I kapitel sex (**Diskussion**) diskuteras arbetets framställda resultat och metoden som används för att framställa resultatet.

I kapitel sju (**Slutsats**) dras slutsatser mellan resultatet som arbetet utmynnat i sett till frågeställningen, och förslag till framtida forskning ges.

2 Bakgrund

DDoS är ett skadligt fenomen som fortsätter att verka över Internet och förbrylla datavetare och säkerhetstekniker. Det här kapitlet presenterar de bakomliggande begrepp som behövs för att förstå DDoS-angrepp.

2.1 Distributed Denial of Service

Larry Rogers vid CERT (2004) beskriver DDoS-angrepp som en attack med syfte att göra en webbplats eller annan tjänst otillgänglig för användare. Alla resurser är ändliga, och med särskilt skrivna programverktyg genererar angriparen en tillräckligt stor mängd trafik mellan sig själv och platsen som ska anfallas för att den inte ska få någon möjlighet att behandla trafik från legitima användare.

För att få tillgång till den datorkraft som krävs för att blockera en tjänst används en stor mängd datorer som samtidigt utför enskilda angrepp. Datorerna som ingår i ett angrepp är del av vad som kallas ett attacknätverk eller ett botnät, och allt som oftast är de infekterade av skadlig programvara som tillåter en ensam angripare att fjärrstyra datorerna till att utföra angrepp på dennes kommando, även om de enskilda datorernas ägare kan vara helt omedvetna om detta. Spridningen av denna programvara är nuförtiden helt automatisk, och de infekterade datorerna kan på egen hand hitta andra datorer med bristande säkerhet och infektera dem, vilket leder till botnätens ökande i storlek och kraft. (Rogers, 2004)

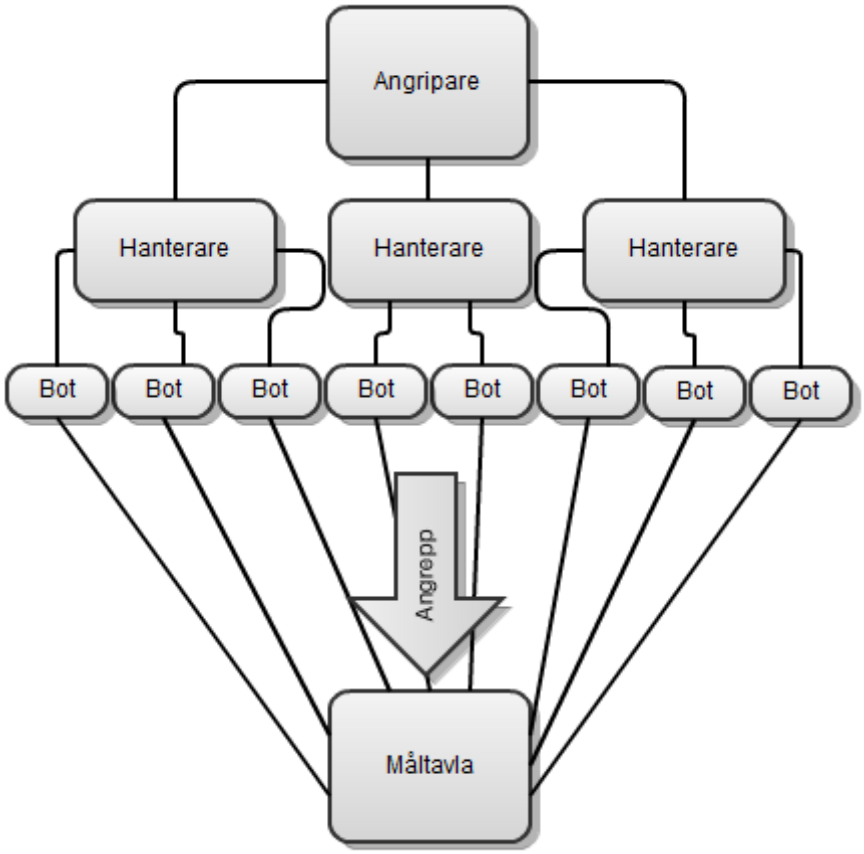

Bild 1. En typisk struktur på ett botnät där angriparen fjärrstyr infekterade datorer (bot) med hjälp av hanterare för att få de att på samma gång skicka trafik mot måltavlan i ett DDoS-angrepp.

2.2 DDoS-varianter

Gadot, Atad & Ben-Ezra (2012) vid säkerhetsföretaget Radware presenterar i sin årliga rapport om DDoS-angrepp två grupperingar av angrepp som tar sig an olika inriktningar: angrepp på nätverksnivå och angrepp på applikationsnivå. Båda sorters angrepp resulterar i att göra en tjänst otillgänglig för andra användare, men med olika tillvägagångssätt.

Mirkovic & Reiher (2004) beskriver angrepp på nätverksnivå som attacker vars mål är att förbruka bandbredden eller någon annan resurs som ett nätverk har tillgängligt för sin trafik, och på så sätt blockera åtkomsten av webbsidan eller tjänsten för andra användare. Distinkt för de flesta nätverksangrepp är den stora mängden trafik som används för att angripa ett nätverk, och igenom det kan angreppen upptäckas.

Mirkovic & Reiher (2004) fortsätter med att beskriva angrepp på applikationsnivå som attacker riktade mot en särskild applikation på en dator eller i ett system för att förbruka dess resurser. Till skillnad från angrepp på nätverksnivå är det inte nödvändigt så att ett angripet system i övrigt blir obrukbart för andra användare. Det finns svårigheter med att upptäcka angrepp på applikationsnivå eftersom de endast angriper en begränsad del av systemet och mängden trafik som utgör ett angrepp ofta är för låg för att vara möjliga att urskilja.

Gadot, m.fl. (2012) gör skillnad mellan trafikstorleken hos angrepp på nätverksnivå som ofta är intensiva i sin trafik, och angrepp på applikationsnivå som ofta håller en lägre profil. Detta beror på att resurserna som finns tillgängliga i ett systems applikationslager oftast är mindre än de som finns till för nätverket, och att angrepp på applikationsnivå därför kan använda en mindre mängd trafik för att uppnå samma effekt som ett angrepp på nätverksnivå.

2.3 Vad möjliggör DDoS-angrepp?

Mirkovic & Reiher (2004) skriver att det är den grundläggande strukturen av kommunikation över Internet som möjliggör DDoS-angrepp. Strukturen bygger på en *slutpunkt-till-slutpunktsparadigm* som dikterar att nätverket mellan sändare och mottagare endast har som syfte att transportera kommunikation på snabbast möjliga sätt, och efter det är det upp till de medverkande parterna i slutändarna att upprätthålla krav på kvalitet och säkerhet. De menar att detta öppnar upp möjligheten för en av de två parterna att missbruka kommunikationen till mottagaren eftersom det inte finns någon skyldighet hos det mellanliggande nätverket att agera mot ett illasinnat angrepp. Säkerheten på Internet blir en kollektiv insats mellan alla inblandade användare, vilket försvårar DDoS-prevention ytterligare: Sålänge som det finns sårbara datorer och system som kan användas av kriminella för att utföra angrepp så kommer DDoS att vara ett säkerhetshot.

Mirkovic & Reiher (2004) fortsätter med att säga att resurserna på Internet är ändliga. De gör en uppdelning mellan kommunikationskanaler som ofta besitter en stor bandbreddskapacitet för deras enda uppgift att möjliggöra förflyttning av stora mängder trafik på samma gång, och slutpunkter hos användare som på grund av kostnader besitter precis den bandbreddskapacitet som de beräknas använda. Detta gör att kanalerna kan forsla in en större mängd trafik i ett system hos användare än vad systemet är utrustat för att behandla.

Kommunikationen över Internet tvingar inte den sändande parten att identifiera sig själv för nätverket, vilket har gett upphov till den tidigare nämnda 'spoofing'-tekniken som ofta användas vid DDoS-angrepp. Kontrollen på Internet är även distribuerad till den del att det inte är möjligt att införa ett globalt verktyg eller en policy på grund av varierande lagar om privatliv och undersökningar. (Mirkovic & Reiher, 2004)

2.4 Problematik med att stoppa DDoS

Rogers (2004) beskriver tekniken 'IP spoofing' som tillåter angripare att dölja den egentliga avsändaradressen i deras trafik med en förfalskad adress. På så sätt kan de hålla sig anonyma både under och efter ett utfört angrepp.

Ari, m.fl. (2003) belyser problematiken med att särskilja vanlig trafik från ett renodlat angrepp. Man talar om 'flash crowds' som en händelse när en webbplats eller tjänst plötsligt får ett mycket större antal förfrågningar än vanligt under en kort tidsperiod, ofta i koppling med yttre faktorer. Exempelvis kan en mindre webbplats utsättas för en flash crowd om en länk till platsen publiceras på ett populärt offentligt forum eller en nyhetsplats. En sådan plötslig belastning kan komma att orsaka skada hos eller krascha ett oförberett system.

BBC (2006) rapporterade en händelse som inträffade under året 2006 när maskineriföretaget Universal Tube & Rollform Equipment vidtog juridisk handling mot videodelningssidan YouTube eftersom deras snarlika domännamn på webben (Utube.com & YouTube.com, tillsammans med den populära förkortningen av engelskans 'you' till endast 'u') resulterade i att mängder av tänkta YouTube-besökare av misstag navigerade till Utubes sida och överbelastade företagets bandbredd till kraschningspunkten. Företaget sade sig redan ha varit tvungna att flytta sin webbplats fem gånger för att ”vara steget före YouTube.com-besökarna” och att de behövt uppgradera sin bandbredd för dyra pengar på grund av det, trots att de varit aktiva på webben i tio år före YouTube.

2.5 Angreppsverktyg

DDoS-angrepp utförs med särkilda verktyg som tillåter angriparen att generera särskild trafik eller att på annat sätt manipulera kommunikationsprocessen mellan datorer. Gadot, m.fl. (2012) skriver i sin säkerhetsrapport om de fyra verktyg som uppskattats ha varit mest aktiva under året 2011.

2.5.1 LOIC

Low Orbit Ion Cannon (härefter förkortat LOIC) är ett 'open source'-verktyg som ursprungligen användes för att stresstesta nätverk genom att generera trafik på både nätverks- och applikationsnivå. En särskild funktion hos LOIC kallad 'Hive Mind Mode' tillåter verktyget att genom IRC-protokollet samla andra datorer som frivilligt använder verktyget och använda deras gemensamma kraft för att utföra DDoS-angrepp utan att på förhand behöva infektera de med programvara. Verktyget har använts flitigt men har också lett till ett flertal arresteringar runt om i världen eftersom det inte tillhandahåller automatisk anonymisering av användarens IP-adress. (Gadot, m fl. 2012)

2.5.2 Mobile LOIC

Mobile LOIC är en mobil webbaserad variant av LOIC med begränsade valmöjligheter och endast förmågan att generera HTTP-trafik. Verktyget besitter inte samma IRC-baserade funktioner som LOIC men är flexibelt eftersom det kan köras på de flesta moderna telefoner och i de flesta webbläsare. En annan styrka hos Mobile LOIC ligger i dess förmåga att genom webbläsaren som används generera äkta HTTP-anrop med metadata från webbläsaren. Andra verktyg som inte är webbaserade genererar trafik som lättare kan identifieras som ett angrepp eftersom de tvingas skapa egen metadata till sin trafik. (Gadot, m.fl. 2012)

2.5.3 R.U.D.Y

Verktyget R.U.D.Y (”Are You Dead Yet?”) använder sig av en alternativ attackmetod mot applikationslagret som kallas för '*slow rate attack*'. Verktyget kan utnyttja inbyggda svagheter i komponenter och orsaka förbrukning av resurser med en förhållandevis liten ström trafik från angriparen. Formulär i webbsidan identifieras och igenom dem skickas HTTP-POST-anrop från verktyget till servern, med den lilla särskildheten att anropet bryts ner till enskilda bytes som skickas en och en med tio sekunders väntetid mellan varandra. Webbservrar är enligt design tvungna att vänta på fullständiga HTTP-anrop innan de kan agera, och om angriparna öppnar tillräckligt många förbindelser med servern och utnyttjar R.U.D.Y genom de alla kan de tillgängliga resurserna förbrukas. (Gadot, m.fl. 2012)

2.5.4 THC-SSL-DoS

Verktyget THC-SSL-DoS som utvecklats av hackergruppen 'The Hacker's Choice', en förkortning för 'The Hacker's Choice Secure Sockets Layer Denial of Service', erbjuder ett unikt angreppssätt eftersom det angriper ytterligare ett lager mellan nätverks- och applikationslagren. SSLs arbetsuppgift är att skydda data som skickas mellan servrar eller mellan en server och slutanvändare. Detta utförs med ett så kallat ”hemligt handslag” som skapar en hemlig nyckel till innehållet i trafiken. Verktyget utnyttjar detta genom att påkalla en inbyggd funktion i protokollet som skapar en ny hemlig nyckel. Arbetet med att skapa en enda hemlig nyckel är en intensiv process för maskinen, och genom att gång på gång påtvinga skapandet av en ny nyckel kan en ensam angripare få systemet att förbruka 15 gånger mer resurser än vanligt (Gadot, m.fl., 2012). Enligt hackergruppen själva har verktyget tagits fram för att belysa problemet med föråldrad teknik, och genom att demonstrera dessa svagheter kan utvecklingen tvingas framåt i snabbare fart. (THC, 2011)

3 Metod

I det här kapitlet redogörs arbetsmodellen som arbetet följer för att framställa resultatet.

3.1 Ansats

Detta är ett teoretiskt arbete i form av en litteraturöversikt. Dess syfte är att med hjälp av publicerade vetenskapliga källor besvara arbetets frågeställning. Arbetets ansats är kvalitativ med syfte att tydligt belysa den fria forskningens täckande av de mest förekommande DDoS-angreppen. Det resulterar i en fördjupning i ämnet som bildar en plattform att påbörja vidare forskning från.

En alternativ ansats är att göra en litteraturöversikt med ett kvantitativt perspektiv. En sådan ansats ger en bredare överblick över området och säkerställer statistisk relevans i resultatet och dess slutsatser, men den gör det svårare att relatera resultatet direkt till det dagsaktuella läget.

Ett annat alternativ för att närma sig problemområdet är att utföra ett empiriskt arbete där data hämtas genom intervjuer, enkäter eller annat. Ett möjligt tillvägagångssätt i ett sådant arbete är att ta kontakt med folk i IT-försvarsbranschen och använda dem som datakällor för att framställa resultatet och besvara frågeställningen. Styrkan med en sådan ansats är möjligheten att genom personlig kontakt med erfarna yrkesmänniskor kunna ställa de frågor och följdfrågor som bäst ger svar på vad arbetet behandlar, utan att vara låst till vad den publicerade fria forskningen tillhandahåller. Svårigheten med en sådan ansats är att upprätta kontakt med ett tillräckligt antal villiga individer vid företag för att ge ett väl avvägt svar på arbetets frågeställning, och även att beakta hur individer som är anställda hos en aktör på marknaden kan vara begränsade i hur de får lov att svara enligt företagspolicyer.

Ytterligare ett alternativ för att utföra arbetet är att skapa en konstruerad testmiljö enligt relevant teori och bedöma utfallet genom tester som baseras på de försvarslösningar som presenteras genom den fria forskningen. Styrkan med en ansats som denna är att resultat och slutsatser kan knytas till stark evident data. Svagheten med en ansats som denna är möjliga problem som kan uppstå vid konstruerandet av testmiljön som behövs för att framställa resultatet. Konstruktionen och de följande testerna kräver även en god omfattning på områdets samlade kunskap för att forma relevanta testfall, vilket saknas i den fria forskningen idag.

Ansatsen som används för det här arbetet väljs på grund av möjligheten att skapa en samlad överblick över området, vilket saknas i dagsläget. Ett arbete på den här nivån har även begränsade resurser för utförandet vilket försvårar för alternativa ansatser. Ett arbete som baseras på vetenskaplig publicerad text kan även till sina styrkor räkna en god reliabilitet eftersom studierna har genomgått granskning från andra forskare inom området.

3.2 Arbetsprocess

Det här arbetet är en litteraturöversikt som hämtar data från den vetenskapliga litteraturen. Enligt Nilsson (2005) är en litteraturöversikt ett lämpligt arbete för det här tillfället eftersom den nuvarande erfarenhetsnivån inte tillåter en mer djupgående studie. Istället ger arbetet en möjlighet för fördjupning inom området. Vid ett empiriskt arbete vore risken stor att kunskapen som tillförs inte är något nytt eftersom kunskapsnivån är för låg, men genom att undersöka och tillvarata vad som redan gjorts inom området i en litteraturöversikt kan egna, nya slutsatser dras.

Arbetsprocessen för det här arbetet har hämtat inspiration från ett par olika källor. Friberg (2010) och Nilsson (2005) är de huvudsakliga metodkällorna.

Nedan är en bildlig representation av arbetsprocessen som arbetet följer.

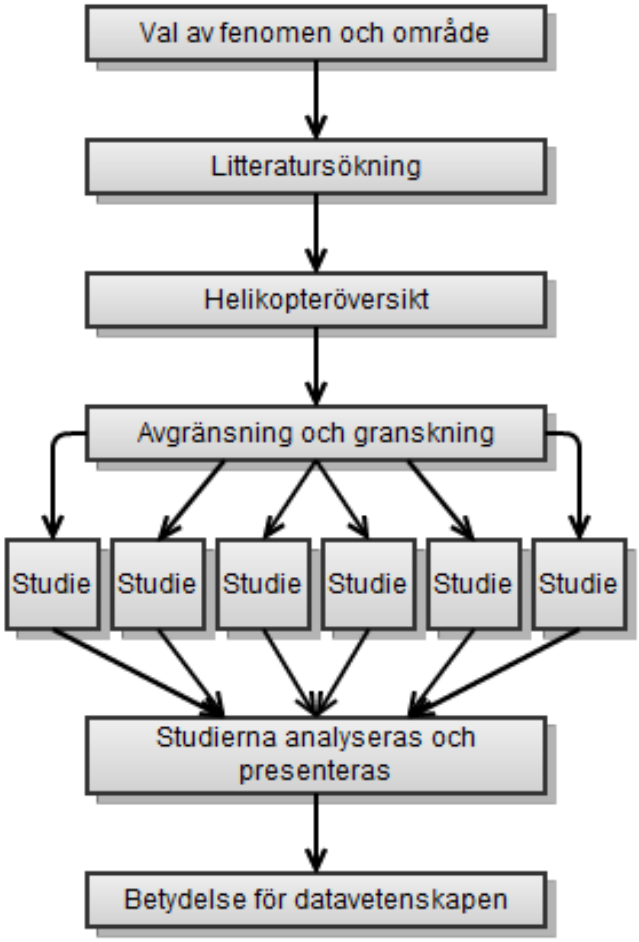

Bild 2: En visuell presentation av arbetets modell och genomförande.

Val av fenomen och område: Det första steget i litteraturöversikten är att finna ett område efter eget intresse. Till det här arbetet väljs fenomenet DDoS på grund av dess aktualitet och en önskan att titta närmare på det.

Litteratursökning: En bred digital litteratursökning görs för att ta reda på vad som finns publicerat inom området. Lämpliga informationskällor väljs och söktermer hålls breda.

Helikopterperspektiv: Ett helikopterperspektiv över sökresultaten från litteratursökningen hjälper till att finna andra aspekter som inte är självklara från början. Det handlar om att göra en övergripande beskrivning av det som finns publicerat på området. Relevant för arbetet är att den redan publicerade litteraturen till stor del är lösryckt och osammanhängande, något som en teoretisk sammanställning som det här arbetet är kan ordna.

Avgränsning och granskning: Efter att den teoretiska grunden för arbetet har lagts görs en avgränsning som i slutändan leder fram till ett konkret resultat. För det här arbetet görs en avgränsning till att titta på de mest framträdande angreppsvarianterna, och studier som hänger samman med dessa väljs ut och kvalitetsgranskas för att säkerställa deras vetenskapliga relevans.

Studierna analyseras och presenteras: Studierna läses igenom och sammanfattas. Innehållet i studierna grupperas tillsammans under lämpliga rubriker baserat på den teoretiska grunden för DDoS. Innehållet presenteras på ett sätt som kopplar det samman till arbetets frågeställning.

Betydelse för datavetenskapen: Arbetets betydelse för området diskuteras och motiveras. Särskilt intressant att diskutera om är vad resultatet bidrar till för kunskap och vilka nya frågor som väcks genom den.

3.3 Litteratur

Arbetet använder litteratur både till att kartlägga och beskriva trender inom DDoS och för att hitta aktuell forskning om försvar mot angreppen. Information från säkerhetsföretag i form av rapporter eller andra publiceringar används för att framställa statistik till det teoretiska avsnittet. Materialet som används för att framställa resultatet är hämtat genom databaserna *ACM Digital Library* och *IEEE*. Dessa väljs som informationskällor på grund av deras relevans till ämnet datavetenskap, och för att de finns fritt tillgängliga genom högskolan. För att besvara arbetets frågeställning används studier som presenterar och redogör för experimentella försök att på något sätt försvara mot DDoS i kontext till arbetets presenterade teori.

3.3.1 Sökning

Till en början görs en bred litteratursökning för att se över problemområdet, i enlighet med Friberg (2010). Allt eftersom dagsläget tydliggörs avgränsas området och litteratursökandet från att först skapa en överblick över det publicerade materialet kring DDoS vidare till att undersöka angrepp på nätverksnivå och applikationsnivå fram till TCP-SYN-angrepp och HTTP-GET-angrepp. Dessa sista termer förklaras närmare i teorin som följer i nästa avsnitt.

För sökprofiler se bilaga [1]. De artiklar som presenteras i sökprofilerna inkluderar de som i slutändan inte visade sig uppfylla det syfte som arbetet kräver och redovisas därför inte i resultatet, men de granskas ändå för en helhetsbild.

3.3.2 Val av dokument och granskning

De studier som väljs ut genom relevans till teorin filtreras genom generella inklusions- och exklusionskriterier (Friberg, 2010). Studierna är publicerade tidigast från 2010 för att säkerställa färskheten i innehållet, och de är antingen på svenska eller engelska. Studierna redovisar sina metoder/lösningar och deras utfall från experiment kring försvar mot de typer av DDoS-angrepp som presenteras i teorin.

Många artiklar sorteras bort efter att abstraktet lästs eftersom deras syften visar sig vara annat än vad arbetet är intresserat av. Det kan handla om artiklar som undersöker DDoS i kontext av molntjänster, trådlösa nätverk eller annat, och alla de egenheter som kommer med därtill. De artiklar som bedöms vara relevanta för arbetet läses, granskas och presenteras i arbetets resultatavsnitt.

3.3.3 Etiska överväganden

Eftersom forskningsartiklarna är publicerade på ett annat språk än svenska, och ofta skrivna på delvis bruten engelska, ursäktar jag mig på förhand för möjliga oavsiktliga feltolkningar av innehållet.

En viktig reflektion att tänka på i arbetets sammanhang är att informationen som presenteras görs fritt tillgänglig för kriminella att använda. Materialet är annars endast fritt tillgängligt inom högskolans nätverk, men att agera efter detta genom att undanhålla relevant information står emot öppen forskning och kunskapsbildning. Arbetet ger dock inga direktiv till angreppsverktyg och annat som inte annars finns fritt tillgängligt genom rapporter och andra källor.

3.3.4 Analys

De studier som efter granskning används till att framställa resultatet i arbetet läses, förstås och presenteras på ett översiktligt sätt som visar om de besvarar problemet som ställs i arbetets frågeställning i förhållande till teorin. Detta struktureras i resultatavsnittet med hjälp av teorin omkring försvar mot DDoS. Artiklarna redovisas kort i följande matris.

3.4 Artikelmatris

Artikel, författare	Syfte	Resultat	Diskussion	Övrigt
A Mitigation model for TCP SYN flooding with IP Spoofing – L.Kavisankar, C.Chellapan (2011).	Att presentera en mitigationsmodell mot TCP-SYN-attacker med spoofade IP-adresser.	Metoden är användbar och effektiv, med endast en liten mängd extra overhead som krävs.	Metoden kan inte behandla UDP-angrepp på samma sätt. En enhetlig lösning för alla sorters angrepp behövs.	Inkluderad i TCP-SYN-delen under detektion & mitigation.
A Two-Tier Coordinated Defense Scheme against DDoS Attacks – C-L.Chen, C-Y.Chang (2011).	Att presentera en mitigationsmodell mot TCP-SYN-attacker.	Metoden är användbar och har styrka i sin skalbarhet och enkelhet att implementera.	Saknas.	Inkluderades i TCP-SYN-delen under detektion & mitigation, förutom informationen om 'Droptail'.
Avoiding DDoS with Active Management of Backlog Queues – M. Bellaïche, J-C. Grégoire (2011).	Att presentera en förändring i inställningarna för TCP-protokollet som effektiviserar hanteringen av väntande anslutningar.	De föreslagna förändringarna visar på prestandahöjning både under normala förhållanden och under angrepp.	TCP-tekniken har föråldrade aspekter hos sig idag. Den nya metoden visar förbättringar på alla fronter, tillsammans med en enkelhet att implementeras.	Inkluderad i TCP-SYN-delen under prevention.
Detecting DDoS Attacks with Hadoop – Y. Lee, Y.Lee (2011).	Att presentera två detektionsmodell-er mot HTTP-GET-angrepp grundad i ett öppet ramverk.	Metoderna är effektiva och mycket skalbara och enkla att implementera. De kan dock inte hantera processering i realtid p.g.a ramverkets inbyggda datahantering.	En lösning i realtid bör arbetas fram.	Inkluderad i HTTP-GET-delen. Den andra metoden valdes bort p.g.a icke-utförlig beskrivning.
Detection of HTTP Flooding Attacks in Multiple Scenarios – D, Das, U. Sharma, D.K. Bhattacharyya (2011)	Att presentera tre detektionsmodell-er mot HTTP-GET-angrepp i olika attackscenarier.	Modellerna visar sig vara effektiva och kan tillsammans försvara ett system mot olika sorters HTTP-GET-angrepp.	Tröskelvärdena som används i testerna bör standardiseras för att säkerställa modellernas relevans inom andra miljöer.	Inkluderad i HTTP-GET-delen. Den tredje presenterade modellen valdes bort p.g.a bristande förståelse från min sida.
Detection of HTTP-GET flood Attack Based on Analysis of Page Access Behavior – T. Yatagai, T. Isohara, I. Sasase (2007).	Att presentera två olika detektionsmodell-er mot HTTP-GET-angrepp.	Modellerna visar på blandade resultat, där ingen av de ger ett helt perfekt resultat.	Saknas.	Inkluderad i HTTP-GET-delen. Studien valdes trots sitt publiceringsdatum p.g.a dess relevans för ämnet och en brist på andra artiklar.

4 Dagsläge

I det här kapitlet presenteras den relevanta teori som arbetet relaterar sitt resultat till i förhållande till frågeställningen.

4.1 DDoS idag

Här presenteras information från säkerhetsrapporter och andra publiceringar av säkerhetsföretag. Informationen används till att presentera dagsläget kring DDoS-angrepp och till att peka på trender inom angreppen.

4.1.1 DDoS-statistik

Prolexic är ett säkerhetsföretag som presenterar angreppsstatistik i sin rapport från det första kvartalet av 2012. Här under presenteras ett urval av statistiken från Prolexics rapport, med fokus på de mest förekommande angreppstyperna. Prolexic gör inte någon skillnad mellan angrepp på nätverksnivå eller applikationsnivå i sin statistik, men för tydlighets skull presenteras informationen här uppdelad i de två olika kategorierna.

Tabell 1: Statistik från Prolexic (2012a) angående de mest förekommande angreppstyperna under början av 2012.

Angreppstyp				
Nätverksnivå			**Applikation.**	
SYN Floods	**UDP Floods**	**ICMP Floods**	**GET Floods**	**Annat**
25%	15%	20%	20%	20%

Jämfört med statistik som presenteras i Prolexics rapport från det fjärde kvartalet av 2011 (Prolexic, 2012b) har TCP-SYN-angrepp gått om UDP-angrepp och ICMP-angrepp och blivit det mest förekommande angreppet på nätverksnivå sedan det fjärde kvartalet av 2010. På applikationsnivå har HTTP-GET-angrepp varit det tveklöst mest förekommande under samma tid.

Gadot, m.fl. (2012) redovisar i sin rapport fördelningen mellan nätverksangrepp och applikationsangrepp under 2011. Här under presenteras de tre vanligast förekommande varianterna på varje nivå.

Tabell 2: Statistik från Radware angående fördelningen mellan angreppstyper under 2011. Det skrivs inte ut tydligt i rapporten, men det är sannolikt att det som Gadot, m.fl. (2012) benämner enbart som ”HTTP” är HTTP-GET-angrepp, baserat på annan text i rapporten.

Angreppstyp							
Nätverksnivå				**Applikationsnivå**			
Totalt	**TCP**	**UDP**	**ICMP**	**Totalt**	**HTTP**	**HTTPS**	**DNS**
46%	25%	7%	6%	**54%**	21%	13%	9%

Arbor Networks (2012) redovisar data från sitt globala system ATLAS ('Active Threat Level Analysis System'), det första i sitt slag, som analyserar hot och angrepp runt hela världen, bland annat DDoS-angrepp. Statistik från de senaste 24 timmarna kring angreppskällor och mål, attacktyper och fördelningar är tillgänglig, och uppdateras i löpande takt. Till det här arbetet hämtas statistik från ATLAS under en sextondagarsperiod mellan mars och april i intervaller om 24 timmar

för att visa på färska siffror kring DDoS-aktiviteten idag. Här under presenteras statistik från ATLAS inhämtat under en period mellan mars och april. Ett urval ur statistiken görs för att påvisa de mest förekommande angreppstyperna på både nätverksnivå och applikationsnivå. Som med Prolexics rapport delas statistiken ursprungligen inte upp mellan angreppskategorier, men i det här arbetet görs det för översikts skull.

Tabell 3: Statistik från ATLAS angående antal angrepp under en period mellan mars och april, med en uppdelning mellan prevalenta angreppsmetoder.

Angreppstyp			
Nätverksnivå		**Applikations.**	
TCP-SYN	**UDP**	**DNS**	**Annat**
38%	21%	9%	34%

4.1.2 Statistiktolkning

De tre statistiska källorna är eniga om att TCP-SYN-angrepp är det vanligast förekommande angreppet på nätverksnivå idag. Statistiken från Gadot, m.fl. (2012) och Prolexic (2012) är eniga om att HTTP-angrepp är den absolut vanligaste attacken på applikationsnivå. Värt att notera är hur Arbor Networks (2012) ATLAS-system inte redovisar någon data kring HTTP-angrepp. Detta kan möjligen förklaras genom att ATLAS, enligt Nazario[1], hämtar in sin information genom utsatta tröskelvärden för trafik, och att angrepp på applikationsnivå som HTTP-GET-angrepp inte genererar tillräckligt mycket trafik för att ge ett utslag, i enlighet med vad Gadot, m.fl (2012) skriver.

4.1.3 Synliga trender

Gadot, m.fl. (2012) skriver att själva DDoS-angreppen befinner sig i förändring. Den äldsta varianten av DDoS-angrepp är den som angriper på nätverksnivå för att förbrukar bandbredd, men på senare tid har angrepp på applikationsnivå blivit allt mer populära som ett alternativ som inte alls kan bekämpas på samma sätt. De beskriver också i sin rapport uppmärksammade DDoS-attacker från 2011 som har använt sig av olika angreppsmetoder på samma gång (så kallat en ”multi-vector attack”, härefter MVA), där angrepp på nätverks- och applikationsnivå utförts samtidigt och mot samma mål. Denna framträdande trend hos DDoS-angrepp beskrivs som att de blir allt mer ”APT” (kort för ”Advanced Persistent Threat”). Detta betyder att angreppen blir mer och mer sofistikerade och skickligt utförda. Dobbins och Morales (2012) vid Arbor Networks stödjer detta i företagets årliga säkerhetsrapport från 2012 med påståendet att en ökande popularitet hos angrepp på applikationsnivå är en bidragande faktor till trenden.

Gadot, m.fl. (2012) fortsätter med att DDoS-angrepp överlag verkar användas mer och mer som bara ett steg i större sammanhang. Ett exempel på detta är när Sony Pictures under 2011 utsattes för ett storskaligt DDoS-angrepp som sedan följdes upp av attacker med mål att stjäla information, troligtvis utförda av samma grupp.

Sammanfattningsvis kan följande relevanta trender identifieras ur den statistik och information som presenterats.

- TCP-SYN-angrepp är den vanligast förekommande attacken på nätverksnivå.

1Jose Nazario, Ph.D. Manager of Security Research, Arbor Networks, e-post den 26 mars 2012.

- HTTP-GET-angrepp är den vanligast förekommande attacken på applikationsnivå.
- Angrepp blir allt mer MVA, alltså att angripare kan använda sig av olika sorters DDoS-attacker på samma gång mot ett offer.

4.2 TCP-SYN-angrepp

En normal TCP-förbindelse mellan maskiner bygger på något som kallas för en trevägshandskakning där den första parten (klienten) kontaktar den andra parten (servern) med ett SYN-anrop (kort för 'synchronize') och den andra parten svarar med ett SYN-ACK-meddelande (kort för 'synchronize acknowledge') för att bekräfta anropet. Den första parten ska då avsluta handskakningen med ett ACK-meddelande tillbaka till den andra parten, och efter det har de båda upprättat en förbindelse. Per protokollets design väntar den andra parten på det avslutande ACK-meddelandet från den första parten, och pågående försök till förbindelser lagras i en kö som oftast töms ut snabbt eftersom processen i vanliga fall är snabb. Väntande anslutningar förkastas om servern efter upprepade återförsändelser av SYN-ACK-meddelandet fortfarande inte fått ett ACK-meddelande tillbaka. Ett DDoS-angrepp utnyttjar dock denna design genom att förfalska avsändardressen genom IP spoofing hos de SYN-anrop som skickas till den andra parten, vars SYN-ACK-meddelanden aldrig kommer att få några svar eftersom de förfalskade adresserna inte leder någonstans. Väntekön kommer därför inte att kunna tömmas inom rimlig tid, och legitima användare kommer inte att kunna upprätta förbindelser med tjänsten. (Cisco, 2006)

Bild 3: En visuell presentation över en lyckad TCP-anslutning (vänster) och ett TCP-angrepp (höger). Angreppet fungerar på så sätt att serverns SYN-ACK meddelande inte besvaras. Väntekön kommer att fyllas med sådana väntande anslutningar, och legitima användare kommer inte att kunna nå tjänsten.

4.3 HTTP-GET-angrepp

HTTP-GET är en inbyggd metod i HTTP-protokollet som används för att hämta en resurs som klienten efterfrågar, exempelvis en individuell sida på en webbplats (w3, 2004). Das, Sharma & Bhattacharyya (2011) skriver att serversidans arbetsprocess är förhållandevis resurskrävande i förhållande till klientens, och ett HTTP-GET-angrepp utnyttjar detta genom att göra ett stort antal GET-anrop för att förbruka resurser. Ett angrepp som utnyttjar HTTP-protokollet skiljer sig från andra attacker på så sätt att det tekniskt sett följer de regler som finns för protokollet. Angreppet kräver en upprättad förbindelse och gör GET-anrop precis som vanliga klienter, men i en större mängd och snabbare takt beroende på vilken strategi som angriparen tillämpar. Ett angrepp kan använda sig av trafik som skickas med slumpmässig intensitet eller istället hålla en låg takt och endast tillfälligt skicka en stor mängd anrop, och på så sätt hålla ett lägre genomsnittligt värde på sin mängd trafik för att försvåra för försvarsmekanismer. De nämner även att ett angrepp kan försöka imitera 'flash crowds' som presenteras tidigare i bakgrundskapitlet.

4.4 DDoS-försvar

Tre termer används vanligen i sammanhanget DDoS-försvar. Dessa är de följande, med definitioner hämtade från den svenska Nationalencyklopedin (2012):

- *Detektion:* upptäckt, ertappning eller påvisning av existens av något fördolt med exempelvis en detektor.
- *Mitigation:* lindring eller minskning.
- *Prevention:* förhindrande eller förebyggande.

Detektion syftar till att upptäcka och lokalisera ett pågående angrepp, mitigation till att mildra och begränsa skadan som ett angrepp orsakar och prevention till att förhindra angreppet på förhand.

5 Resultat

I det här kapitlet redovisas lösningarna ur de sex studier som väljs ut för att framställa resultatet sett ur förhållande till frågeställningen och teorin. Resultatet grupperas efter angreppstyp och försvarskategori.

5.1 TCP-SYN-angrepp

De tre första studierna behandlar försvar specifikt mot TCP-SYN-angrepp.

5.1.1 Detektion och mitigation

Kavisankar och Chellappan (2011) presenterar en lösning för detektion och mitigation av TCP-SYN-angrepp med hjälp av sin metod ”TCP probing for Reply Argument Package” där ett flertal komponenter samarbetar.

En avkännare (”probe”) markerar inkommande SYN-paket från klienter och bifogar extra instruktioner i korresponderande avgående SYN-ACK-paket från servern. Instruktionerna handlar om att göra någon specifik ändring i inställningarna på det ACK-paket som förväntas skickas tillbaka, eller att skicka om det markerade SYN-paketet igen. Om klienten följer dessa instruktioner visar det på att den IP-adress som klientens paket visar är legitim. Om klienten inte följer instruktionerna utan istället skickar nya paket utan de efterfrågade förändringarna antas IP-adressen som angetts vara spoofad och dess trafik skadlig eftersom de avgående SYN-ACK-paketen inte mottagits. En paketanalysator registrerar transporten av paket och ska verifiera att ett flöde av paket har följt instruktionerna som givits av avkännaren. Med hjälp av verifieringen ska slutligen en detektor antingen acceptera eller dumpa paketflödet beroende på om flödet bedöms vara legitimt eller inte.

Detta är en metod som genom tester visar sig vara effektiv både på att upptäcka och att mildra angrepp. Den utnyttjar de givna resurser som finns i systemet utan att tillföra mycket extra overhead.

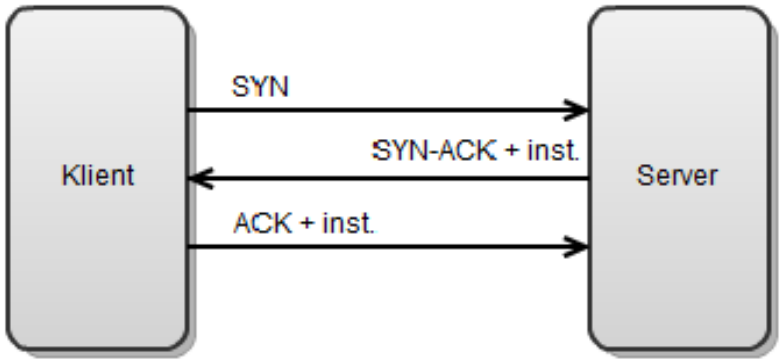

Bild 3: en visuell presentation av Kavisankars och Chellappans (2011) lösning när den hanterar en legitim klient. Om instruktionerna (inst.) som skickas med SYN-ACK-meddelandet inte besvaras kommer trafiken från klienten att dumpas.

Chen och Chang (2011) presenterar en annan lösning för detektion och mitigation av angrepp. Metoden använder sig av två enskilda försvarsmetoder för detektion som används i lager på varandra. Den första bygger på kvotbaserad mätning på inkommande trafik och den andra på mätning av längden på väntekön för oavklarade TCP-anslutningar hos servern. Metoden implementerar två trafikfilter i form av routrar som placeras på olika platser i nätverket. Det första filtret placeras i utkanten av systemets nätverk och det andra filtret så nära servern som möjligt.

Det första trafikfiltret använder kvotbaserad mätning och granskar inkommande trafikflöden för att se om de kan identifieras som skadliga med hjälp av kontinuerligt uppdaterade flödeslistor som delas genom hela systemet. På förhand identifierbar skadlig trafik dumpas. Ickeskadlig trafik registeras i flödeslistorna om de inte redan finns, och statistik förs över flödenas antal lyckade och misslyckade sändelser för att beräkna om det finns grund för att misstänka ett flöde som skadligt, varpå resultatet loggas.

Det andra trafikfiltret använder kölängdbaserad mätning med hjälp av köhanteringsmetoden ”Random early detection”, kort RED. RED dumpar slumpmässigt paket inlagda i kön i en takt som baseras på belastningen kön befinner sig under, där fler paket dumpas ju större köns arbetsbörda är. Förhållandet mellan det totala antalet paket i väntekön, inklusive de som slumpmässigt dumpas, och antalet paket som slumpmässigt dumpats registreras och kontrolleras, och om ett flöde visar på siffror som faller utanför givna tröskelvärden ifrågasätts dess legitimitet. Om det ifrågasatta flödet sedan det första trafikfiltret loggats som misstänkt kommer det att flaggas som skadligt i flödeslistorna, vilket låter det första trafikfiltret dumpa all inkommande trafik från den källan.

Tester av lösningen genomförs i olika sammanhang. Det första och det andra trafikfiltret testas enskilt och tillsammans, med utfallet att RED på egen hand inte är ett lämpligt skydd mot angrepp. Tillsammans med det första filtret visade RED dock god prestanda tack vare den fördelade arbetsbördan mellan trafikfiltren och enkelheten i att beräkna trafikflödenas kvot av misslyckade sändelser och vänteköns storlek.

5.1.2 Prevention

Bellaïche och Grégoire (2011) presenterar en lösning för prevention av TCP-SYN-angrepp genom en förändring i time-out-inställningarna som kommer som standard med TCP-protokollet. Istället för den fasta tidsramen ska en dynamisk uträkning av en lämplig time-out-tid beräknas för varje utomstående trafikkälla genom observation av tiden det tar att avsluta kompletta handskakningar från det nätverk som trafikkällan kommer från. Denna genomsnittliga tid ska uppdateras i realtid, med tillägg för villkor av eventuella nödvändiga omförsändelser. Den nödvändiga storleken på väntekön beräknas också genom tester och observationer.

Lösningens validitet bekräftas i tester genomförda med två olika flöden: ett med ett avsiktligt högt antal time-out-händelser och ett med bara ett fåtal sådana. Lösningen visar på ett litet antal falskpositiva identifieringar, och observationer bekräftar att den ursprungliga tidsramen för en time-out som finns som standard i protokollet är onödigt stor. Belastningen på kön blir mindre med den nya lösningen, och med flödet som innehåller många time-outs visar metoden på en minskning av 50% av vänteköns storlek och belastning. De olika flödena visar på olika behov i vänteköns storlek, men i båda fallen undviker den nya metoden en överbelastning av väntekön när den utsätts för ett simulerat angrepp genom att mer effektivt hantera de väntande anslutningarna i kön.

5.2 HTTP-GET-angrepp

De resterande tre studierna behandlar försvar specifikt mot HTTP-GET-angrepp.

5.2.1 Detektion

För detektion av HTTP-GET-angrepp föreslås olika metoder. Lee och Lee (2011) utvecklar en detektionsmodell med hjälp av Hadoop, ett 'open source'-ramverk av Apache som tillåter distribuering av arbetsbörda mellan ett stort antal datorer. Ramverket används idag för att hantera stora beräkningar av flera framstående aktörer på Internet, så som Amazon, Facebook och Ebay.

Metoden använder tröskelvärden som i förväg beräknats genom lagrad data över en period för att sammanställa ett genomsnittsvärde att jämföra inkommande trafik med. Varje unik klient får en tidsstämpel som användas för att kontrollera hur många HTTP-GET-anrop denne gör till servern under observationstiden. Balansen mellan antalet anrop från klienten och antalet svar på anrop från servern till klienten med det på förhand bestämda tröskelvärdet, och därefter kan flödet flaggas som ett angrepp ifall klienten ligger i för stor obalans med servern i förhållandet mellan anrop och svar.

Metodens effektivitet bekräftas i simulerade tester med ett varierande antal maskiner som genom Hadoop delar på arbetsbördan att beräkna balansvärden mellan klienter och servern eller servrarna, beroende på scenariot. Ett större antal datorer hanterar större mängder information bättre. Metoden visas vara mycket skalbar i och med det distribuerade arbetssättet, beräkningens låga komplexitet och dess enkelhet att implementera i miljöer som redan använder Hadoop. Detektionen av angrepp sker dock inte i realtid eftersom ramverket använder sig av satsvis bearbetning.

Das, m.fl. (2011) presenterar en annan lösning för detektion av angrepp. Deras lösning inriktar sig mot angrepp inom olika tänkbara scenarier. Det första scenariot förutsätter ett angrepp med oregelbunden frekvens på anropen. Ett tröskelvärde beräknas genom att logga ankomsttakten av anrop från legitima klienter över en period för att finna den högsta enskilda ankomsttakten. Denna väljs ut som tröskelvärde och jämförs med ankomsttakten som hämtas in från varje klient i realtid under körning. De flöden som överstiger tröskelvärdet flaggas som angreppstrafik.

Ett annat scenario behandlar ett angrepp som använder en pulserande mängd trafik som stundvis uppnår en hög ankomsttakt men som annars håller ett lågt snittvärde på ankomsttakten. Ett tröskelvärde beräknas genom att hämta loggad information ur en databas och generera mönster ur ankomsttakten av loggade anrop. Ur dessa sammanställs ett övergripande mönster som används för att beräkna ett legitimt mönster som man jämför med mönster som skapas av flöden från klienter under körning. Om en klients mönster visas vara felaktigt i jämförelse med det beräknat legitima mönstret flaggas trafiken som angreppstrafik.

Lösningens två algoritmer undersöks genom simulerade tester där tröskelvärden beräknats genom data från en universitetsserver. I det första scenariot beräknades tröskelvärdet per kvartal och algoritmens effektivitet beräknades vara 100%. Det andra scenariot visade på ett mönster hos angreppstrafiken som alltid föll inom särskilda parametrar, och algoritments effektivitet mättes även här till att vara 100%, men det beror helt och hållet på den faktiska relevansen hos tröskelvärdet som används, vilket gör det viktigt att fastställa värdets riktighet.

Yatagai, Isohara & Sasase (2007) redovisar en annan lösning som beskriver två algoritmer för detektion av angrepp. Lösningen lägger fokus på besökares beteende på en webbplats. Den första algoritmen tittar på klienters bläddringshistorik över webbplatsens sidor. Angreppstrafik ska upptäckas genom att se återkommande mönster bland de klienter som styrs av samma botnät. IP-adressen för varje unik klient lagras, och om ett tillräckligt stort antal klienter visar på samma mönster i sin sökhistorik ska deras HTTP-GET-anrop dumpas.

Lösningens andra algoritm bygger på att titta på hur länge en klient befinner sig på en given webbsida i förhållande till informationsmängden som presenteras på den. Ett genomsnittsvärde räknas ut från loggad data över tidigare besökare på webbplatsen, och mot detta värde jämförs klienter under en pågående körning. De klienter som visas tillbringa för lite tid på enskilda sidor flaggas som angripare.

Lösningens resultat i tester visar på blandade utfall. Den första algoritmen visar sig olämplig för att upptäcka angrepp eftersom den uppvisar ett stort antal falsk-negativa mätningar där den släpper igenom angripare som om de vore legitima användare. Den andra algoritmen visar bättre resultat vad gäller detektion av angrepp men antalet falsk-positiva mätningar visar att den även stänger ute vissa legitima användare som om de vore angripare.

Som en i övrigt intressant beaktelse är studien som beskriver lösningen ovan den enda av många bekantade texter, även utanför de som används till att framställa resultatet, som inte uppvisar ett genomgående positivt resultat.

5.3 MVA-angrepp

Ingen funnen studie har presenterat någon lösning för att försvara ett system mot MVA-DDoS-angrepp.

6 Diskussion

I det här kapitlet diskuteras resultatet som arbetet leder fram till, samt arbetsmodellen som strukturerar arbetet.

6.1 Resultatdiskussion

Resultatet som kan framställas ur texterna som valts ut visar att den nyaste fria forskningen är begränsad i sin möjlighet att svara på de hot som just nu är mest utbredda. Varken mitigation eller prevention av HTTP-GET-angrepp besvaras i någon utav texterna, eller i någon annan studie som gick att finna innanför inklusionskriterierna. Antalet studier som undersökts i arbetet är dock för litet för att säga att det inte finns någon lösning överhuvudtaget, men det finns en synlig brist på det i proportion till uppmärksamheten som TCP-SYN-angrepp får.

En annan märkbar lucka i den fria forskningen kring DDoS-försvar är kunskap om den framträdande trenden att angreppen allt oftare använder sig av olika angreppstyper på en och samma gång. Jag tror att det området kommer att kräva särskild uppmärksamhet, eftersom en teknik för att försvara mot TCP-SYN-angrepp inte nödvändigtvis kan samarbeta med en teknik för att försvara mot HTTP-GET-angrepp på samma gång, beroende på implementation och resurshantering. För att fastställa ett försvar mot sådana MVA-angrepp bör skyddslösningen testas inom samma system mot alla tänkbara angrepp i kombination med varandra, och inte lösryckt mot ett sorts angrepp i taget som annars är vanligt inom de studier som undersökts.

Det är dock viktigt att nämna att IT-säkerhetsbranschen är ett område med mycket pengar involverat i privata företag där forskning kan föras i hemlighet från omvärlden för att kunna erbjuda tekniker och strategier till försvar mot DDoS. Sådan forskning finns inte att ta del av gratis och därför har ämnet inte undersökts åt det hållet, även om det dock kanske visat på en annan bild av dagsläget.

En observation är att de absolut flesta experimentstudier redovisar genomgående positiva resultat i sina tester att stoppa DDoS-angrepp i olika kontexter. DDoS fortsätter dock trots detta att nämnas bland de största hoten i cybervärlden idag. Den teoretiska biten i arbetet redovisar hur DDoS-angrepp utnyttjar den underliggande strukturen av datorkommunikation för att sabotera utförandet, och däri ligger antagligen den stora svårigheten med att bekämpa det. Experimentet som genomfördes av Bellaïche och Grégoire (2011) visar på att en förändring i inställningarna av hur TCP-protokollet hanterar väntande anslutningar hade en reell effekt som försvar mot DDoS-angrepp. Sådana preventionslösningar tror jag är att föredra framför enbart mitigationslösningar som istället försöker släta över bakomliggande ineffektivitet eftersom de angriper källan av problemet och inte endast symptomen av det. Sedan ligger en annan del av problemet i att ovetande individers datorer kan infekteras och utnyttjas i stora botnät av kriminella grupper. För att stävja detta är en större medvetenhet hos befolkningen nödvändig för att minska botnätens kraft och på så sätt bekämpa DDoS-angrepp.

6.2 Metoddiskussion

För ett teoretiskt arbete på den här nivån känns den följda arbetsmodellen lämplig. Om ett liknande arbete ska utföras i framtiden kommer modellen att tillämpas igen, med några förändringar mot personliga preferenser. Teoretiska arbeten inom datavetenskap är inte lika vanliga som empiriska arbeten, och det gick inte att finna något direkt relevant ramverk för att utföra arbetet. Den här typen av arbete är vanligare inom vårdvetenskapen.

Antalet studier som används är i den lägre änden av spektrumet enligt Nilsson (2005), men på grund av det låga utbudet av studier som är så specifikt inriktade mot det avgränsade område som

presenteras i teorin anser jag att de uppfyller det som arbetet behöver. Friberg (2010) nämner dock detta som en svaghet med arbetsmodellen, att en liten mängd relevant litteratur begränsar arbetet. För att säkerställa en färsk översikt av forskningsområdet gjordes valet att arbetet endast skulle behandla studier från 2010 och framåt, förutom ett undantag som gjordes med en studie från 2007 som valdes eftersom den refererades till från andra lästa texter, och för att den var inriktad precis mot området. I eftertanke vore det nog en bra idé att titta på inkludera fler studier från längre tillbaka än 2010 för att kunna fånga fler relevanta artiklar och få fler trådar att följa.

Valet av informationskällor är också faktorer att betänka vid ett litteraturarbete som detta eftersom sökresultaten kan variera stort från källa till källa.

Spridningen av texterna som undersökts, både de som används till resultatet och de som studerats tidigare men som inte valdes ut, är begränsad mestadels till asien. Resultatet i studierna är dock framförda som vetenskapliga artiklar för en internationell konferens och publik, vilket ger de ett globalt perspektiv.

Ett alternativt sätt att framställa resultatet i arbetet är att fokuserade mindre på att presentera de faktiska lösningarna och istället framhäva resultaten ur ett större antal artiklar. Min egen reflektion kring detta är att själva resultatet hade varit snarlikt, men mer underbyggt.

6.3 Diskussion om studierna

Studierna som används för att framställa resultatet är alla framförda på ett snarlikt sätt. Lösningarna som presenteras testas och utvärderas med hjälp av simulerade miljöer och angrepp. Lösningen som framfördes i studien av Das, m.fl. (2011) använder sig av en universitetsserver för att hämta nödvändiga värden för att utvärdera effektiviteten i deras metod, och själva angreppet utförs med en attacksimulator från Strom Security. Lösningen från Kavisankar och Chellappan (2011) använder en bladserver (en nedskalad och modulär serverdator som kan uppgraderas efter specifika behov) och ett egetutvecklat angreppsverktyg för att simulera ett TCP-SYN-angrepp och undersöka hur väl deras metod fungerar. Andra lösningar, som de som framförs av Yatagai, m.fl. (2011) och Lee och Lee (2011), använder en dedikerad testmiljö kallat en testbädd som är utrustad med verktyg för vetenskapliga mätningar. Att testa och utvärdera föreslagna lösningar med hjälp av simulationer är definitivt det vanligaste tillvägagångssättet för att påvisa nya idéer och deras meriter. Simulerade miljöer speglar inte den verkliga omgivningen fullständigt, men att utföra tester av nya lösningar i skarpa situationer är riskabelt och, beroende på informationen som finns i systemet som tillåts angripas, oetiskt.

Studierna som används är de som går att finna bland den fria forskningen genom de valda informationskällorna som även faller inom inklusionsparametrarna. De härrör direkt till frågeställningen och teorin som arbetet presenterar. Andra texter som möjligtvis är användbara att ha med i resultatet är sådana som är mer generella i sitt område, som att titta på försvar mot DDoS-angrepp på nätverksnivå överlag och inte endast mot TCP-SYN-angrepp, och detsamma för angrepp på applikationsnivå. Detta lägger dock ett större krav på omkringliggande kunskap för att kunna dra slutsatser genom texter som inte är specifikt riktade mot det avgränsade ämnet. TCP-SYN-angrepp och HTTP-GET-angrepp är dock välkända fenomen idag med mycket bedriven forskning kring dem. Lösningar på samma problem som det Kavisankar och Chellappan (2011) presenterar kan finnas i studien av Liu och Sheng (2008), och i studien av Schuba, Krsul, Kuhn, Spafford, Sundaram & Zamboni (1997) från längre bak i tiden. Problemet som Bellaïche och Grégoire (2011) presenterar en lösning för i sin studie om att utvärdera ett nytt sätt att hantera väntekön för TCP-anslutningar har andra studier granskat sedan tidigare, exempelvis av Jaiswal, Iannaccone, Diot, Kurose och Towsley (2004). Likt studien av Yatagai, m.fl. (2011), har Lu och Yu (2006) experimenterat med detektion av HTTP-angrepp genom besökares beteende på en webbplats.

7 Sammanfattning

Med stöd från det som arbetet redovisar anser jag att den fria forskningen kring DDoS har fler områden att utforska. Resultatet visar på en brist på mitigations- och preventionsförslag mot specifikt HTTP-GET-angrepp, och en brist på forskning kring försvar mot det växande problemet av MVA-DDoS-angrepp. Det är möjligt att den privat förda forskningen redan besitter dessa svar, men den fria forskningen erbjuder en större spridning som öppnar upp utvecklingsmöjligheter från olika, varierande håll. Samtidigt finns det dock en nackdel med den fria forskningen, i och med att även angriparna får ta fri del av den och se de framsteg som görs.

Arbetets styrka ligger i att det presenterar de synligaste aspekterna av DDoS-fenomenet som det ser ut idag, och vart de senaste forskningsinsatserna ligger. Arbetet tar sin start vid en kunskapsnivå på ett lägre plan och leder fram till en förankrad helhetsbild och ett resultat som visar vart mer uppmärksamhet bör riktas. På så sätt fungerar arbetet som både ett fördjupningsarbete och som en plattform att utföra vidare forskning från. På samma sätt kan dock missförstånd och felaktiga tolkningar göras i uppgiften att kartlägga området, samt en oavsiktlig simplifiering av ämnets bredd. Detta är arbetets möjliga svaghet.

7.1 Vidare forskning

Mer ingående arbeten kring de olika framstående angreppstyperna, och då framförallt HTTP-GET-angrepp, föreslås som framtida forskning för att mer detaljerat kartlägga läget kring angreppen. Arbeten som istället konstruerar ett eller flera scenarier för att sedan testa en föreslagen lösning är också viktiga för att ge konklusiva bevis på effektivitet, även om de har en snävare ansats än ett litteraturarbete som detta.

Vidare undersökning kring hur försvar mot olika sorters angrepp kan samverka tillsammans är nödvändig för att besvara problemet kring DDoS. Den positiva förändring som visades i Bellaïche och Grégoires (2011) studie där TCP-protokollet hanterade väntande anslutningar mer effektivt ger grund till påståendet att forskning kring effektivisering av teknologi som fortfarande är aktuell också är ett värdefullt område.

Referenser

Arbor Networks (2012). ATLAS. Tillgänglig på Internet: http://atlas.arbor.net/
[Hämtat 12.03.19-12.04.05]
(Notis: This information was obtained from Arbor Networks' ATLAS Initiative on date(s) 12.03.19-12.04.05 and permission to republish has been obtained. ATLAS initiative data is dynamic and therefore, the information may have changed since the date of publication of the data. © Arbor Networks, Inc. ALL RIGHTS RESERVED. Atlas is a trademark of Arbor Networks, Inc.)

Ari, I., Hong, B., Miller, E., Brandt, S. & Long, D. (2003). Managing Flash Crowds on the Internet. *11th IEEE/ACM International Symposium on Modeling, Analysis and Simulation of Computer Telecommunications Systems, 2003. MASCOTS 2003.* Tillgänglig på Internet: 10.1109/MASCOT.2003.1240667
[Hämtad 12.03.19]

BBC (2006). YouTube sued by sound-alike site. Tillgänglig på Internet: http://news.bbc.co.uk/2/hi/business/6108502.stm
[Hämtad 12.03.19]

Bellaïche, M. & Grégoire, J-C. (2011). Avoiding DDoS with Active Management of Backlog Queues. *5th International Conference on Network and System Security (NSS), 2011.* Tillgänglig på Internet: 10.1109/ICNSS.2011.6060021
[Hämtad 12.04.17]

Chen, C-L. & Chang, C-Y. (2011). A Two-Tier Coordinated Defense Scheme against DDoS Attacks. *International Conference on Computer Science and Service System (CSSS), 2011.* Tillgänglig på Internet: 10.1109/CSSS.2011.5974535
[Hämtad 12.04.17]

Cisco (2006) Defining Strategies to Protect Against TCP SYN Denial of Service Attacks. Tillgänglig på Internet: http://www.cisco.com/application/pdf/paws/14760/4.pdf | http://www.cisco.com/en/US/tech/tk828/technologies_tech_note09186a00800f67d5.shtml
[Hämtad 12.04.03]

Das, D., Sharma, U. & Bhattacharyya, D.K. (2011). Detection of HTTP Flooding Attacks in Multiple Scenarios. *Proceedings of the 2011 International Conference on Communication, Computing & Security.*
Tillgänglig på Internet: 10.1145/1947940.1948047
[Hämtad 12.04.29]

Dobbins, R. & Morales, C. (2012). Worldwide Infrastructure Security Report 2011 Volume VII. Tillgänglig på Internet: http://www.arbornetworks.com/report
[Hämtad 12.03.19]

Friberg, F. (Red.) (2010). Dags för uppsats – vägledning för litteraturbaserade examensarbeten. Studentlitteratur AB; Elanders Beijing Printing Co. Ltd, China.

Gadot, Z., Atad, M. & Ben-Ezra, Y. (2012). 2011 Global Application & Network Security Report.
Tillgänglig på Internet:
http://www.radware.com/workarea/showcontent.aspx?ID=1628921
[Hämtad 12.03.16]

Jaiswal, S., Iannaccone, G., Diot, C., Kurose, J. & Towsley, D. (2004). Inferring TCP Connection Characteristics Through Passive Measurements. *INFOCOM 2004. Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies.*
Tillgänglig på Internet: 10.1109/INFCOM.2004.1354571
[Hämtad 12.05.09]

Kavisankar, L. & Chellappan, C. (2011). A Mitigation model for TCP SYN flooding with IP Spoofing. *International Conference on Recent Trends in Information Technology (ICRTIT), 2011*. Tillgänglig på Internet: 10.1109/ICRTIT.2011.5972435
[Hämtad 12.04.17]

Kim, W., Jeong, O., Kim, C. & So, J. (2010). On Botnets. Proceedings of the 12th International Conference on Information Integration and Web-based Applications & Services.
Tillgänglig på Internet: 10.1145/1967486.1967488
[Hämtad 12.02.24]

Lee, Y. & Lee, Y. (2011). Detecting DDoS Attacks with Hadoop. *Proceedings of The ACM CoNEXT Student Workshop.* Tillgänglig på Internet: 10.1145/2079327.2079334
[Hämtad 12.04.29]

Liu, P-E. & Sheng, Z-H. (2008). Defending against tcp syn flooding with a new kind of syn-agent. *2008 International Conference on Machine Learning and Cybernetics.*
Tillgänglig på Internet: 10.1109/ICMLC.2008.4620589
[Hämtad 12.05.09]

Lu, W-Z. & Yu, S-Z. (2006). An HTTP Flooding Detection Method Based on Browser Behavior. *2006 International Conference on Computational Intelligence and Security.*
Tillgänglig på Internet: 10.1109/ICCIAS.2006.295444
[Hämtad 12.05.09]

Mirkovic, J. & Reiher, P. (2004). *A taxonomy of DDoS attack and DDoS defense mechanisms.* ACM SIGCOMM Computer Communication Review.
Tillgänglig på Internet: 10.1145/997150.997156
[Hämtad 12.03.19]

Nationalencyklopedin (2012). detektera. **http://www.ne.se/sve/detektera** | mitigation. **http://www.ne.se/engelsk-ordbok/mitigation/511579** | prevention. **http://www.ne.se/lang/prevention**.
[Hämtad 12.05.10]

Nilsson, M. (2005). Den systematiska litteraturstudien som vetenskapligt fördjupningsarbete i omvårdnad. Ersta & Sköndal högskola; Ersta Diakonisällskap, kontorsservice.

Prolexic (2012a). Prolexic Attack Report Q1 2012. Tillgänglig på Internet: http://www.prolexic.com/attackreports/index.html
[Hämtad 12.04.27]

Prolexic (2012b). Prolexic Attack Report Q4 2011. Tillgänglig på Internet: http://ww1.prweb.com/prfiles/2012/02/07/9172148/Prolexic%20Attack%20Report%20Q411-020612.pdf
[Hämtad 12.04.27]

RioRey (2011) RioRey Taxonomy of DDoS Attacks. Tillgänglig på Internet: http://www.riorey.com/x-resources/2011/RioRey_Taxonomy_DDoS_Attacks_2.2_2011.pdf | http://www.riorey.com/resources-learnmore.html
[Hämtad 12.04.04]

Rogers, L. (2004) What is a Distributed Denial of Service (DDoS) Attack and What Can I Do About It? CERT. Tillgänglig på Internet: http://www.cert.org/homeusers/ddos.html
[Hämtad 12.05.07]

Schuba, C.L., Krsul, I.V., Kuhn, M.G., Spafford, E.H., Sundaram, A. & Zamboni, D. (1997). Analysis of a Denial of Service Attack on TCP. *Proceedings., IEEE Symposium on Security and Privacy, 1997.* Tillgänglig på Internet: 10.1109/SECPRI.1997.601338
[Hämtad 12.05.09]

The Hacker's Choice (2011). Tillgänglig på Internet: http://www.thc.org/thc-ssl-dos/
[Hämtat 12.04.02]

Yatagai, T., Isohara, T. & Sasase, I. (2007). Detection of HTTP-GET flood Attack Based on Analysis of Page Access Behavior. *IEEE Pacific Rim Conference on Communications, Computers and Signal Processing, 2007.*
Tillgänglig på Internet: 10.1109/PACRIM.2007.4313218
[Hämtad 12.04.29]

Bilagor

Bilaga 1 – sökprofiler

Här under namnges de artiklar som framstod som relevanta under arbetets gång, även fast de inte används till att framställa arbetets resultat. De artiklar som används till resultatet är markerade med en asterisk. Dubletter visas inte.

Sökprofil 1 Sökord: DDoS Begränsning: publicerat 2010-2012 Datum: 12.04.17	Sökkälla: IEEE Träffar: 261
Titel	Klassifikation
A two-tier coordinated defense scheme against DDoS attacks*	*Nätverksnivå, detektion & mitigation*
Distributed defense of distributed DoS using pushback and communicate mechanism	*Nätverksnivå, prevention*
Defending systems Against Tilt DDoS attacks	*Applikationsnivå (CPU), detektion*
NBHU-based method to counter quiet DDoS attacks (Nätverksnivå, mitigation)	*Nätverksnivå, mitigation*
Discriminating DDoS attack traffic from flash crowd through packet arrival patterns	*Detektion*
A rate limiting mechanism for defending against flooding based distributed denial of service attack	*Detekion & mitigation*
Detecting Application Denial-of-Service Attacks: A Group-Testing-Based Approach	*Applikationsnivå, detektion*
Mantlet Trilogy: DDoS Defense Deployable with Innovative Anti-Spoofing, Attack Detection and Mitigation	*Nätverksnivå, detektion & mitigation*
A Cooperative Mechanism to Defense against Distributed Denial of Service Attacks	*Mitigation*
CoDe — An collaborative detection algorithm for DDoS attacks	*Nätverksnivå, detektion*
Avoiding DDoS with active management of backlog queues*	*Nätverksnivå (TCP-SYN), prevention*

Mitigating DDoS attacks with transparent and intelligent fast-flux swarm network	*Molntjänst, mitigation*
TrustGuard: A flow-level reputation-based DDoS defense system	*Nätverksnivå, detektion*
Low-Rate DDoS Attacks Detection and Traceback by Using New Information Metrics	*Low-rate, detektion*
DDoS flooding attack detection through a step-by-step investigation	*Nätverksnivå, detektion & mitigation*
A new relative entropy based app-DDoS detection method	*Applikationsnivå, detektion*
Lightweight DDoS flooding attack detection using NOX/OpenFlow	*Flood, detektion*
An efficient anti-DDoS mechanism using flow-based forwarding technology	*Prevention*
Throttling DDoS attacks using discrete logarithm problem	*Applikationsnivå, mitigation*
Entropy-based input-output traffic mode detection scheme for DoS/DDoS attacks	*Detektion*
Multi-Agent pattern recognition mechanism for detecting distributed denial of service attacks	*Detektion*
CALD: Surviving Various Application-Layer DDoS Attacks That Mimic Flash Crowd	*Detektion, applikationsnivå (flash crowds)*
Distinguishing the Master to Defend DDoS Attack in Peer-to-Peer Networks	*P2p, prevention*
Detection of Low-rate DDoS Attack Based on Self-Similarity	*Low-rate, detektion*
Early Warning System for DDoS Attacking Based on Multilayer Deployment of Time Delay Neural Network	*Detektion*
DDoS Detection Technique Using Statistical Analysis to Generate Quick Response Time	*Detektion*
A novel improved compositive	*Detektion & mitigation*

DDoS defence system	
A real-time DDoS attack detection and prevention system based on per-IP traffic behavioral analysis	*Dätverksnivå, detektion*

Sökprofil 2 Sökord: DDOS mitigat* Begränsning: publicerat 2010-2012 Datum: 12.04.17	Sökkälla: IEEE Träffar: 26
Titel	Klassifikation
A mitigation model for TCP SYN flooding with IP spoofing*	*Nätverksnivå (TCP), detektion & mitigation*
Using whitelisting to mitigate DDoS attacks on critical Internet sites	*Mitigation*

Sökprofil 3 Sökord: DDOS mitigat* Begränsning: publicerat 2010-2012 Datum: 12.04.17	Sökkälla: IEEE Träffar: 38
An Effective Method for Defense against IP Spoofing Attack	*Blockera spoofade adresser*

Sökprofil 4 Sökord: Distributed DOS Begränsning: publicerat 2010-2012 Datum: 12.04.17	Sökkälla: IEEE Träffar: 116
Mitigating Distributed Denial of Service Attacks in Multiparty Applications in the Presence of Clock Drifts	*Applikationsnivå?, mitigation*
Game theory-based defense mechanisms against DDoS attacks on TCP/TCP-friendly flows	*Nätverksnivå (TCP), prevention*
Adaptive Selective Verification: An Efficient Adaptive Countermeasure to Thwart DoS Attacks	*Nätverksnivå, mitigation*
A Distributed Intrusion Detection System against flooding Denial of Services attacks	*Nätverksnivå, detektion (distribuerat)*
Preventing Denial of Service Attacks in Government E-Services Using a New Efficient Packet Filtering Technique	*Nätverksnivå(?), prevention*
Hop Count Based Packet Processing Approach to Counter DDoS Attacks	*Upptäcka spoofade adresser, detektion*
A Puzzle-Based Defense Strategy Against Flooding Attacks Using Game Theory	*Fyra olika strategier mot floods*

Sökprofil 4

Sökord: DDOS Begränsning: publicerat 2010-2012 Datum: 12.04.29 Fokus: HTTP-GET-angrepp	Sökkälla: ACM Träffar: 242
Detecting DDoS attacks with Hadoop*	*Applikationsnivå (HTTP-GET), detektion*
Dual-level defense for networks under DDoS attacks	*Detektion*
Detecting fraudulent use of cloud resources	*Molntjänst, detektion*
Detection of HTTP flooding attacks in multiple scenarios*	*Applikationsnivå (HTTP-GET), detektion*
Distributed denial of service is a scalability problem	*Diskussion*
Mitigating denial of service attack using CAPTCHA mechanism	*Nätverksnivå, mitigation*

Sökprofil 5 Sökord: DDoS Begränsning: publicerat 2000-2012 Datum: 12.04.29 Fokus: HTTP-GET-angrepp	Sökkälla: IEEE Träffar: 839
Detection of HTTP-GET flood Attack Based on Analysis of Page Access Behavior*	*Applikationsnivå (HTTP-GET), detektion*
DDoS-Shield: DDoS-Resilient Scheduling to Counter Application Layer Attacks	*Applikationsnivå (HTTP-GET?), detektion & mitigation*