Anonymizer hálózatok elleni támadások

SZENTPÁL ZOLTÁN

Budapesti Műszaki és Gazdaságtudományi Egyetem, Távközlési és Médiainformatikai Tanszék
zoltan.szentpal@gmail.com

ZÖMBIK LÁSZLÓ

BME Távközlési és Médiainformatikai Tanszék, Ericsson Magyarország, R&D
laszlo.zombik@ericsson.com

Lektorált

Kulcsszavak: anonim kommunikáció, anonymizer hálózatok, privacy

Az anonymizer hálózatok két fő feladata egyrészt a felhasználók forgalmának és kommunikációs partnereinek elrejtése a helyi hálózatok elől, másrészt annak biztosítása, hogy a felhasználók kiléte és helyzete ismeretlen maradjon a távoli hálózatokban. Cikkünkben az anonymizer hálózatok korlátai kerülnek bemutatásra, ismertetünk egy támadási eljárást ezen hálózatok felhasználóinak anonimitása ellen. A támadás lényege, hogy a felhasználó kommunikációs partnerénél a forgalmat torzítjuk. Ezután a partnertől kiindulva, a forgalom torzítást detektálva a felhasználó helyzetét visszakövetjük.

1. Anonymizer hálózatok

A végpontok és a hálózati forgalom hitelesítése, valamint a forgalmazott adatok titkosítása nem képes védeni a felhasználókat olyan támadások ellen, melyek a felhasználók anonimitása ellen irányulnak. A csomagok IP fejlécének forrás cím – cél cím mezőpárja elegendő információt árul el a felhasználóról, ezért a felhasználó IP címét módosítani szükséges. Ezt többféleképpen lehet elérni, például hálózati címfordítással (Network Address Translation), vagy proxy szerverek használatával. Címfordítás esetén az IP címek, proxy szerverek esetén az IP címek és az IP csomagok forrásra jellemző tartalma lecserélődik. Proxy szerverek hálózatából anonymizer hálózatok épülnek fel, melyekben a forgalmat a proxy szerverek láncolatán keresztül továbbítják, esetlegesen titkosítva is azt *(1. ábra)*.

A proxy szerverekből felépült hálózatok lehetnek nyilvánosak, vagy zártak. Nyilvános proxy szervereket általában önkéntesek üzemeltetnek, ezért ezek a hálózatok gyakran kevésbé megbízható szolgáltatást nyújtanak.

A privát proxyk alkalmazása kedvezőbb a teljesítmény és sebesség szempontjából. Használatuk hátránya, hogy ez a megoldás lehetővé teszi az anonymizer hálózatot üzemeltető vállalat számára, hogy megfigyelje a felhasználók forgalmát.

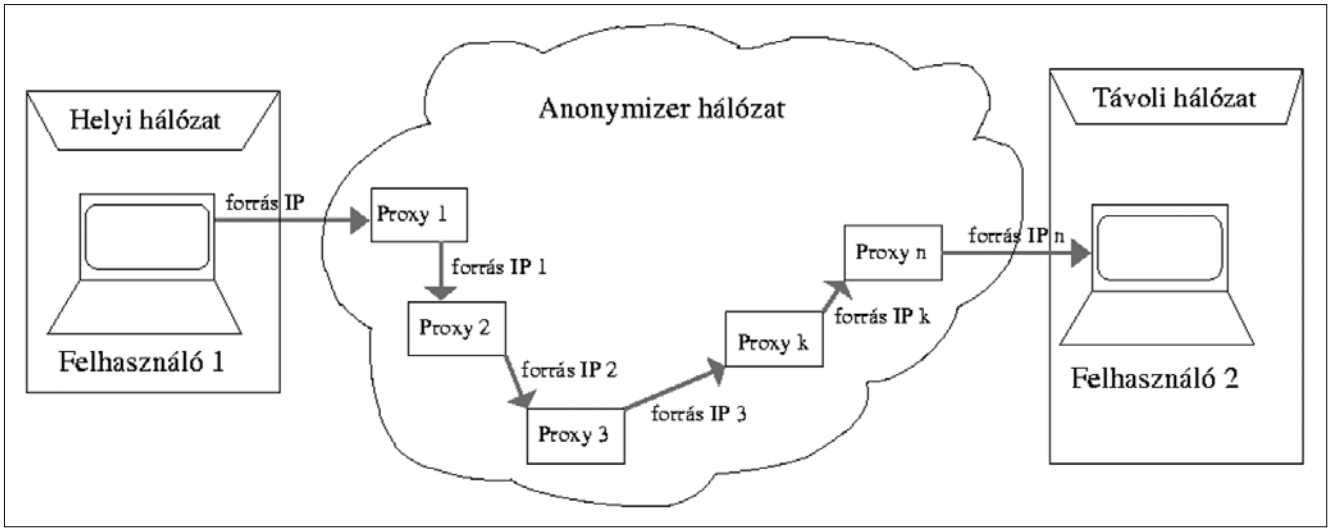
Számos kliens alkalmazás áll a felhasználók rendelkezésére, amelyek különböző anonymizer hálózatokat használnak, különböző mértékű anonimitást nyújtva a felhasználóknak. Sok közülük egyéb funkciókat is kínál (pl. a GhostSurf rendszer még anti-spyware alkalmazást is). Többségük Windows operációs rendszer alapú.

A legnépszerűbb anonymizer hálózatok:

– Steganos Internet Anonym Pro 7 [1]
– Bypass Proxy Client [2]
– Anonymizer 2004 [3]
– MorphMix [4]
– GhostSurf 2005 Platinum [5]
– Tor [6]

Cikkünkben az utolsó két anonymizer hálózaton mutatjuk be az általunk megvalósított támadásokat. Ezeket a hálózatokat a következőkben röviden ismertetjük.

1. ábra Anonymizer hálózatok elvi felépítése



1.1. GhostSurf 2005 Platinum

A GhostSurf 2005 Platinum egy olyan szoftver-gyűjtemény, amely a felhasználók személyes adatainak védelmét és anonimitását segíti elő. A program zárt forráskódú (a vizsgálat során a program ingyenes próbaverzióját használtuk), és csak Microsoft Windows operációs rendszeren fut. A kliens szoftver zárt anonymizer hálózatot használ. A GhostSurf rendszer TCP feletti alkalmazásokat támogat. A kliens alkalmazás és a proxy szerver közötti kommunikáció során lehetőség van SSL/TLS titkosítás használatára is.

1.2. Tor

A Tor anonymizer rendszer a legtöbb, manapság népszerű operációs rendszert támogatja. Nyílt forráskódú, ingyenes szoftver. A Tor egy önkéntesek által karbantartott, elosztott, anonim szerverhálózatot használ. Ehhez a hálózathoz bárki csatlakozhat szerver üzemeltetőként, természetesen csak akkor, ha elegendő sávszélesség áll a rendelkezésére. A hálózatba bekerülő csomagok véletlenszerű útvonalon haladnak a hálózat szerverei között, ezért egy adott megfigyelési pontban lehetetlen megállapítani egy csomag forrás és cél címét. A csomagok küldése előtt a felhasználó kliensprogramja kiválaszt egy útvonalat a hálózat véletlenszerűen kiválasztott szerverei között, az üzeneteket Onion Routing használatával továbbítja *(2. ábra)*.

A kliensnek az aktuális szerverlánc összes szerverével létezik közös kulcsa (*K_ai,* ahol *„a”* a kliens, *„i”* a szerverlánc i-edik szervere). A kliens *„m”* csomag küldése előtt azt mindegyik kulccsal titkosítja, kezdve a legutolsó szerver kulcsával. A legkülsőbb titkosítást a legközelebb lévő szerver kulcsával végzi a kliens, ahogy az az ábrán is látható. Így egy adott szerver csak a csomag visszafejtése után fogja megtudni, hogy hova továbbítsa a csomagot, vagyis hogy melyik a következő szerver a láncban. Az útvonal összes szervere csak az őt megelőző (neki továbbító), és az őt követő szerverrel kommunikál, vagyis egyetlen egy szerver sem ismeri a csomagok teljes útvonalát.

A Tor rendszer csak TCP kapcsolatokat kezel, azonban bármely SOCKS-ot támogató alkalmazással képes együttműködni. A Tor hálózatot, a magánszemélyeken kívül, számos szervezet használja világszerte, például az Amerikai Egyesült Államok Haditengerészete is. Sok vállalat a hagyományos VPN (Virtual Private Network) hálózatuk biztonságosabbá tételére alkalmazza. Törvényszéki nyomozók a kormányzati IP címek elrejtésére használják a Tor rendszert, így a nyomozások során látogatott és megfigyelt honlapok weblogjában nem a saját IP címeik fognak szerepelni.

A forgalom analízisen alapuló támadások hatásosak az anonymizer hálózatok felhasználóinak anonimitása ellen. Tehát ezzel meghatározható, hogy ki kivel folytat kommunikációt egy nyilvános hálózaton keresztül, akkor is, ha a csomagokat titkosították és a fejléceket álcázták. A cikkben egy ilyen támadás megvalósítását mutatjuk be, élő anonymizer hálózatokon.

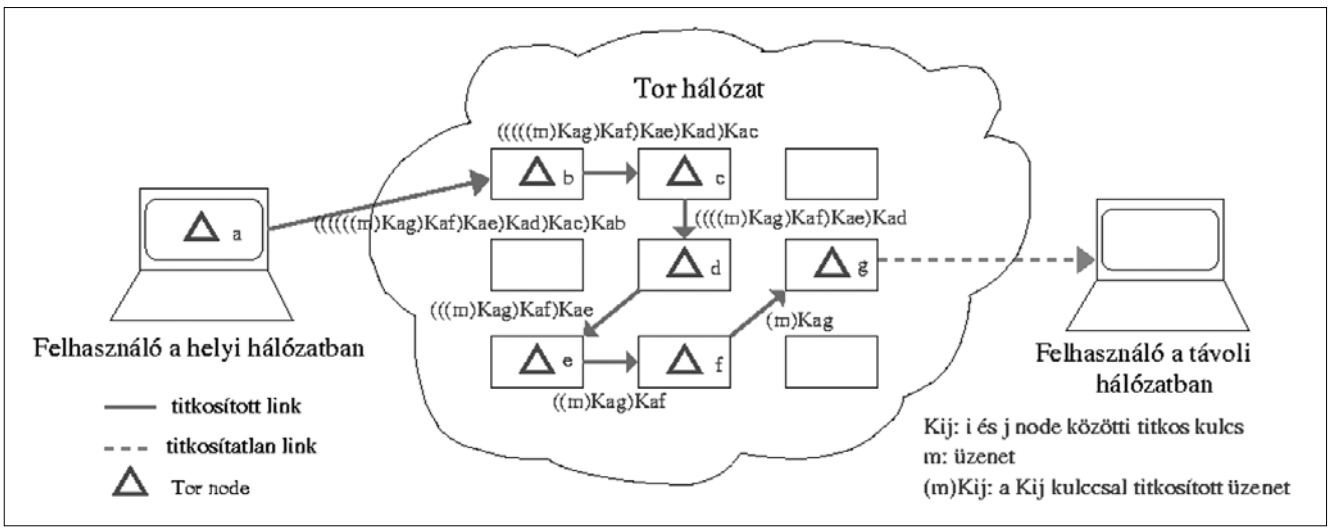
A támadás elméleti hátterét a második, a támadás megvalósításának részleteit a harmadik fejezetben ismertetjük. A negyedik fejezetben az anonymizer hálózatokban mért eredményeinket mutatjuk be.

2. A támadás elméleti háttere

Az ismertetésre kerülő támadás a támadó által készített mérőjel frekvenciatartománybeli vizsgálatán alapul. A hálózatban a bufferelés, a csomagok sorrendjének felcserélése, az üzenetküldési késleltetés változása, valamint a csomagvesztés nemlineáris torzítást eredményez. Azonban megfelelő mérőjel esetén ezek a torzítások nem jelentősek, és a keresendő jel elég ideig történő küldése a jel teljesítmény spektrumát is kiemeli a háttérzajéból.

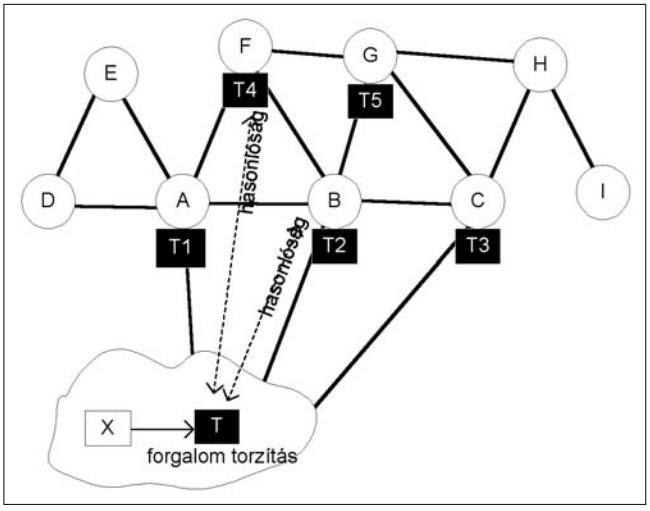
Mérőjelként szinuszos jelet használtunk, ennek egy vonalból áll a spektruma. Ezt a mérőjelet TCP alapú kommunikáció esetén úgy értük el, hogy egy közbeékelődő router segítségével módosítottuk a forgalom alakját, oly módon, hogy a kiküldött csomagok által lét-

2. ábra A Tor anonymizer hálózat



rehozott hálózati forgalom sávszélessége egy szinuszjelet közelítsen az időtartományban. Ezt úgy valósítottuk meg, hogy a TCP kommunikáció felfutási szakaszát (slow start) követően buffereltük a csomagokat. A buffernél a hálózat sávszélességét leszűkítettük úgy, hogy a bufferben összegyűljenek a csomagok. Ezután a bufferből az adott csomagméret és az ennek megfelelő szinuszos sávszélesség érték hányadosa által meghatározott időközönként olvastuk ki és küldtük el a csomagokat.

A támadás elvét a *3. ábra* segítségével mutatjuk be. A támadó célja, hogy egy adott felhasználó forgalmának végpontjait meghatározza, annak ellenére, hogy a felhasználó éppen ezt kívánta eltitkolni. Feltételezzük, hogy a felhasználó el akar érni egy meghatározott szervert (X). Az ebből a szerverből kiinduló forgalmakat a T támadó módosítja. Első lépésben a támadó a szervertől közvetlenül elérhető hálózatok forgalmának spektrumát figyeli, keresve bennük az általa módosított, szinuszos sávszélesség forgalom-mintáit (az ábrán ezek az *A, B, C* hálózatokban a T1,T2, T3 támadók). A támadó az első lépésben megfigyelt hálózatok közül az egyikben talál egyezést az általa keresett mintával (az ábrán a T2 a *B* hálózatban), ezért következő lépésként az innen közvetlenül elérhető hálózatokban hasonlítja össze a forgalmat *T* forgalmi alakjával (az ábrán az *F* és *G* hálózatokban T4,T5 által). A megfigyelést egészen addig folytatja, amíg az éppen megfigyelt hálózatból már nem érhető el közvetlenül egyetlen hálózat sem, és a keresett minta megtalálható a vizsgált hálózat forgalmának spektrumában. Az ábrán ez a hálózat az *F* jelű, vagyis a felhasználó forgalmának végpontja itt található.



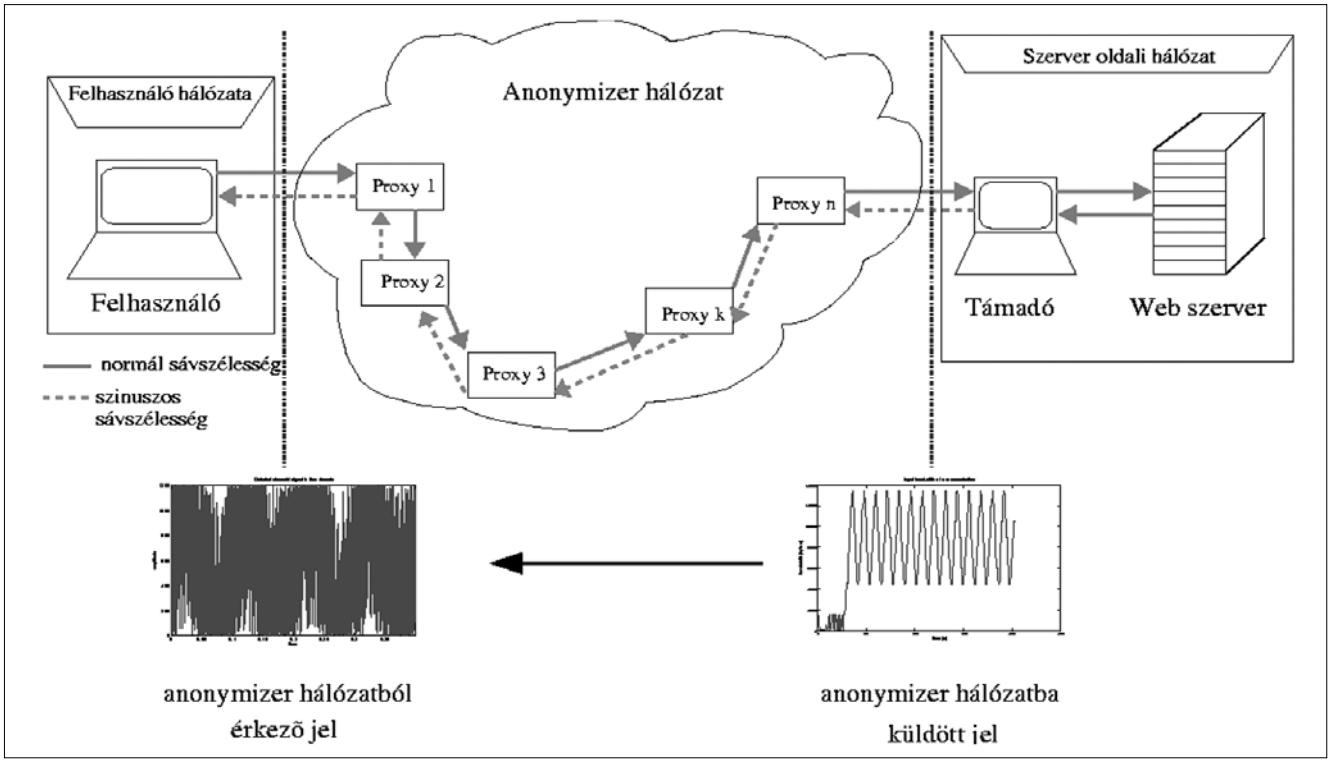
3. ábra A támadás elvének vázlata

3. A támadás megvalósítása

A támadást egy HTTP szerverről történő fájl letöltésén keresztül mutatjuk be. Abban a hálózatban torzítjuk a forgalmat, ahol a szerver elhelyezkedik, így a HTTP kérést küldő felhasználóhoz már a módosított sávszélességgel fog megérkezni a válasz *(4. ábra)*.

A támadás sikeres végrehajtásához az anonymizer hálózat mindkét végpontján, tehát a szerver és a felhasználó hálózatában is szükséges a forgalom vizsgálata. Ezután a két oldal forgalmának frekvenciatartománybeli alakját összehasonlítjuk, és elemezzük az eredményt. Amennyiben a két minta egyezik, akkor fény derült a felhasználó kilétére. Ha a minták nem egyez-

4. ábra A támadás megvalósítása



nek, akkor a felhasználó valószínűleg nem abban a helyi hálózatban tartózkodik, ezért más hálózatokat is vizsgálni kell, egészen addig, amíg valamelyikben a forgalom spektruma hasonlóságot nem mutat a szerver oldali forgalom spektrumával. Ezzel a módszerrel kideríthetjük, hogy merre haladnak a szervertől jövő csomagok, akkor is, ha azok egy anonymizer hálózaton is áthaladnak, mielőtt a felhasználóhoz érnének.

A szerver oldali hosztok megvalósításának blokkvázlata az *5. ábrán* látható. A hardver eszközök számának minimalizálása érdekében a Xen virtualizációs technológiát [7] alkalmaztuk, így emulálva egy hálózatot és hosztokat egyetlen fizikai számítógépen. A Xen technológia lehetővé teszi virtuális gépek, hosztok létrehozását egy számítógépen belül, ahol mindegyik virtuális gép a saját operációs rendszerét használja.

A mérések során a fizikai hoszt *(domain 0)* és a web szerver két különböző hálózatban volt, tehát egymással csak a router hoszton keresztül tudtak kommunikálni. Mindegyik hoszton Debian GNU/Linux operációs rendszer futott. A sávszélesség módosítást a router hoszt végezte, az NTMF (Network Traffic Manipulation Framework) [8] hálózati forgalommódosító keretrendszer alkalmazásával.

Az NTMF C++ nyelven íródott, alapvetően hálózati protokollok tesztelésére szánt keretrendszer. Alacsony szintű hozzáférést enged a linux kernel által továbbított csomagokhoz, moduláris jellege miatt kiválóan alkalmas továbbfejlesztésre, ezért remekül meg tudtuk valósítani vele a kimenő forgalom sávszélesség módosítását.

A router hoszt változtatás nélkül továbbította a szerver felé haladó forgalmat, vagyis a router hoszton *eth0*-tól *eth1*-ig nem történt sávszélesség módosítás (az 5. ábrán, a router hoszton belül folytonos vonallal jelölve). A másik irányban viszont a csomagok kibocsátási ideje módosítva lett, oly módon, hogy a sávszélesség időben szinuszosan változzon (szaggatott vonallal jelölve).

A sávszélesség-idő függvény a következő alakú volt:

$$A + C \cdot \sin((2\pi/N) \cdot f \cdot n),$$

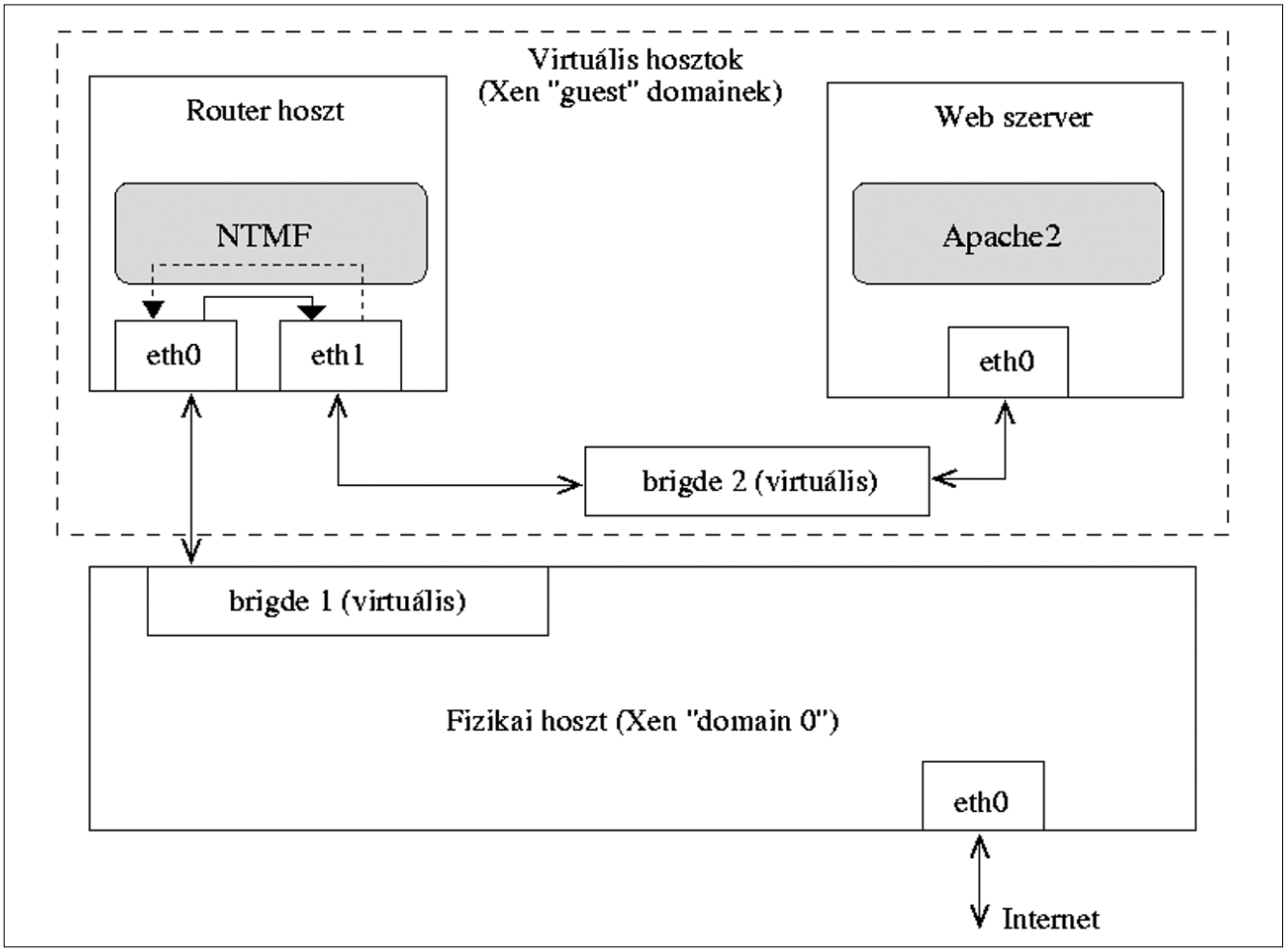
ahol

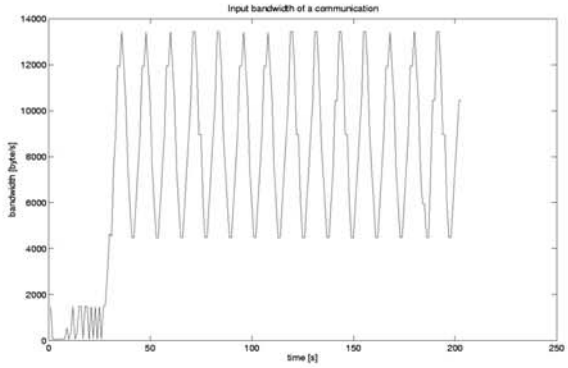
A a sávszélesség DC komponense,
C a szinusz amplitudója (Kbyte/s),
$1/N$ az időkvantum,
f a szinuszos jel frekvenciája (Hz) és
n/N az előző csomag kiküldése óta eltelt idő (sec).

4. Eredmények

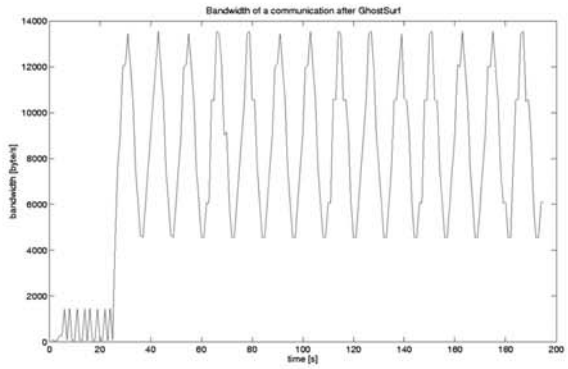
Mindkét anonymizer hálózat esetében a Windows platformra írt kliens szoftvereket teszteltük. A kliens és szerver egymástól fizikailag is távol helyezkedett el, a köztük lévő forgalom az anonymizer hálózaton keresztül haladt.

5. ábra A szerver oldali hosztok megvalósításának blokkvázlata

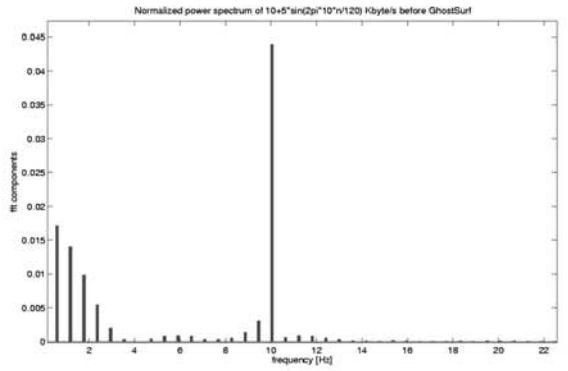




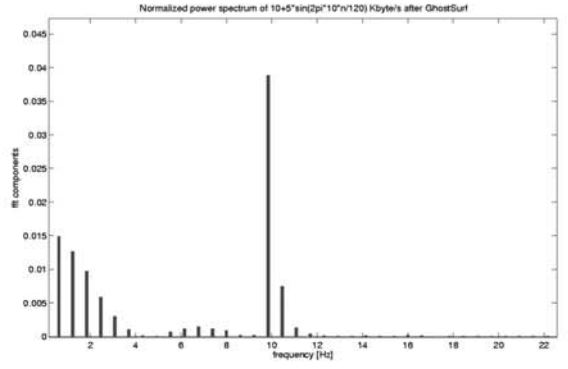
A bemeneti sávszélesség



A sávszélesség a GhostSurf hálózat után

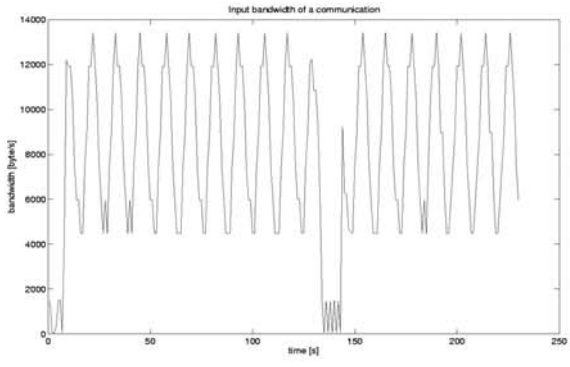


A bemeneti sávszélesség spektruma

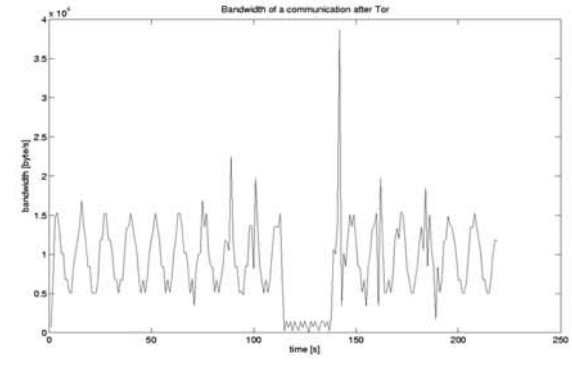


A sávszélesség spektruma a GhostSurf hálózat után

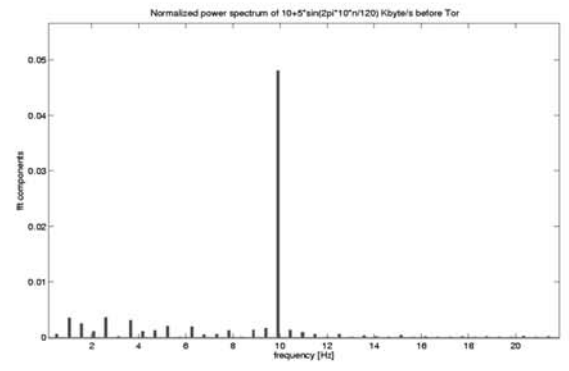
6. ábra



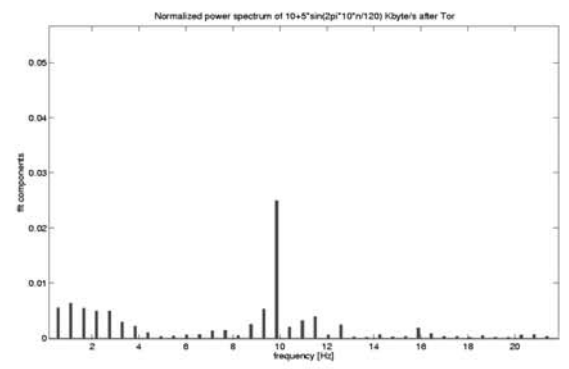
A bemeneti sávszélesség



A sávszélesség a Tor hálózat után



A bemeneti sávszélesség spektruma



A sávszélesség spektruma a Tor hálózat után

7. ábra

A mérések eredményeit bemutató ábrákon az anonymizer hálózat bemeneti sávszélesség-idő függvénye, ennek spektruma a frekvenciatartományban, az anonymizer hálózat utáni ismeretlen kimeneti forgalom sávszélesség-idő függvénye és ennek spektruma a frekvenciatartományban látható.

A bufferből a csomagokat mindkét vizsgálat során

$$8.5 + 4.5 \cdot \sin((2\pi/120) \cdot 10\ [Hz] \cdot n)\ \text{[Kbyte/s]}$$

változó sávszélességgel engedtük ki.

Tehát a spektrumokban 10 Hz-nél csúcs várható.

4.1. GhostSurf 2005 Platinum

A GhostSurf anonymizer hálózatban végzett vizsgálat eredményei a *6. ábrán* találhatók.

A mérés alapján megállapítható, hogy a bemeneti forgalom spektruma jól illeszkedik a GhostSurf hálózat utáni ismeretlen forgalom spektrumához. Ez azt jelenti, hogy a GhostSurf anonymizer hálózat csak csekély mértékben módosította a forgalom sávszélességét, és megmaradt annak szinuszos jellege.

A támadás tehát sikeresnek bizonyult, a felhasználó azonossága nem maradt rejtve.

4.2. Tor

A *7. ábrán* a Tor anonymizer hálózatban mért eredményeket ismertetjük.

A mérés kimeneti forgalom-mintájának spektrumában az eredeti minta 10 Hz-es komponense a legnagyobb energiájú, a bemeneti forgalom spektruma tehát jól illeszkedik a Tor hálózat utáni forgalom spektrumára.

Ez azt jelenti, hogy a támadás ez esetben is sikeres volt, még a Tor hálózat sem védi felhasználóit az ilyen típusú támadások ellen.

5. Összefoglalás

Cikkünkben egy olyan forgalom analízisen alapuló támadási módszer került bemutatásra, amely a TCP protokollra épülve valósítja meg az anonymizer hálózatok felhasználóinak nyomkövetését. A mérések alapján megállapítható, hogy ezek a támadási módszerek követhetővé teszik a célpontokat, vagyis a bemutatott anonymizer hálózatokban a felhasználók anonimitása nem megfelelően biztosított.

Ez azt jelenti, hogy Internet szolgáltatók, vagy a felett álló kormányzati szervek használhatnak ilyen eljárásokat, hogy az anonymizer hálózatok mögé bújó személyek kilétére fényt derítsenek. A hálózati forgalmak szisztematikus megfigyelésével, és a forgalmakban egy előre definiált minta keresésével meghatározható egy adott felhasználó forgalmának mindkét végpontja, ezzel a felhasználó anonimnak vélt kommunikációja nem marad rejtve.

Irodalom

[1] Steganos Internet Anonym Pro 7, http://www.steganos.com
[2] Bypass Proxy Client, http://www.bypass.cc
[3] Anonymizer 2004, http://www.anonymizer.com
[4] MorphMix, http://www.tik.ee.ethz.ch/~morphmix
[5] GhostSurf 2005 Platinum, http://www.tenebril.com
[6] A Tor anonymizer hálózat, http://tor.eff.org
[7] The Xen virtual machine monitor, http://www.cl.cam.ac.uk/Research/SRG/netos/xen
[8] Real-time Network Traffic Manipulation Framework for Protocol Testing, http://ntmf.sourceforge.net