Wdrażanie usług korzystających z adresacji anykast – dyskusja problemów i zagrożeń

Agnieszka Chodorek, Robert R. Chodorek, Andrzej R. Pach (e-mail: {a.chodorek@tu.kielce.pl}, {chodorek, pach}@kt.agh.edu.pl)
Samodzielny Zakład Telekomunikacji i Fotoniki, Politechnika Świętokrzyska, Kielce
Katedra Telekomunikacji Akademii Górniczo-Hutniczej, Kraków

STRESZCZENIE

Schemat adresacji anykastowej został wprowadzony w 1993 roku dokumentem RFC 1546. Dwa lata później, adresacja anykastowa została włączona do nowej wersji (szóstej) protokołu IP. Anykast pozwala na transmisję typu 1-do-(1zN), zorientowaną na usługę. Anykastowy datagram IP jest przesyłany do najbliższej stacji należącej do grupy stacji identyfikowanych przez ten sam adres anykastowy. W artykule zostanie przedstawiona dyskusja problemów i zagrożeń związanych z wdrażaniem usług korzystających z adresacji anykast.

ABSTRACT

Challenges of practical application of anycast-based services

The IP anycast address scheme was introduced by RFC 1546 in 1993. Two years later, anycasting became a part of IPv6 networks. Anycast allows the service-oriented, one-to-one-of-many transmission. The IP anycast datagram is delivered to the nearest host, which belongs to the group of hosts identified by common anycast address. In the paper, the main challenges of practical application of anycast-based services will be discussed.

1. Wprowadzenie

Anykast jest schematem adresacji IP, dostarczającym usługi transmisyjnej typu 1-do-(1zN). Anykast jest adresacją zorientowaną na usługę – każda usługa ma swój predefiniowany adres IP, identyczny dla wszystkich serwerów, które świadczą tę usługę, niezależnie od ich lokalizacji geograficznej. Użytkownik podając adres anykastowy, łączy się z jednym z *N* serwerów świadczących daną usługę, a wybór serwera, który będzie tę usługę świadczył, następuje w sposób automatyczny.

Chociaż sama nazwa „anykast" (*anycast*) jest pojęciem stosunkowo nowym (anykast został wprowadzony dokumentem RFC (*Request for Comments*) 1546 z listopada 1993 roku), adresacja o charakterze „anykast" jest znana od dawna. Z punktu widzenia użytkownika usługa taka jest bowiem zbliżona do, znanej na przykład z telefonii, usługi numerów alarmowych. Bez względu na to, w którym miejscu Polski się znajdujemy, zawsze wybierając numer 999, połączymy się z najbliższą stacją Pogotowia Ratunkowego, wybierając 998 połączymy się ze Strażą Pożarną, a 997 – z Policją.

Wdrażanie usług korzystających z adresacji anykastowej może napotkać na swej drodze szereg trudności. Mogą one dotyczyć zarówno wdrażania samej usługi adresacji anykastowej, jak i wynikać ze specyfiki usług na niej bazujących. Artykuł zawiera dyskusję tych problemów i zagrożeń związanych z wdrażaniem usług korzystających z adresacji anykastowej, które – zdaniem Autorów – zasługują na szczególną uwagę.

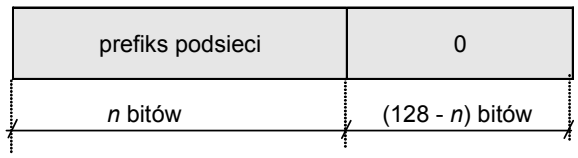
Rozdział 2 niniejszego artykułu zawiera wprowadzenie do adresacji anykastowej IPv6, z uwzględnieniem wybranych problemów wdrażania samej usługi adresacji anykastowej w sieciach IP. Rozdziały od 3 do 6 omawiają najważniejsze, zdaniem Autorów, problemy i zagrożenia związane z wdrażaniem usług korzystających z anykastu. W rozdziale 3 zostanie przedstawiony problem przekierowania zgłoszenia anykastowego do innego serwera usług niż pożądany. Rozdział 4 porusza tematykę współpracy usług połączeniowych korzystających z adresacji anykastowej z bezpołączeniową siecią oferującą usługę adresacji anykastowej. Rozdział 5 omawia kwestie zapewnienia spójności i aktualności zasobów w wieloserwerowych systemach korzystających z adresacji anykastowej. Problematyka bezpieczeństwa takich systemów została poruszona w rozdziale 6. Rozdział 7 stanowi podsumowanie niniejszego artykułu.

2. Adresacja anykastowa i problemy związane z jej wdrażaniem w sieciach IPv6

W przeciwieństwie do adresacji multikastowej, adresacja anykastowa w protokole IPv6 nie posiada odrębnego formatu i wykorzystuje format adresacji unikastowej [8]. Generalnie adresy anykastowe można przydzielać z całej przestrzeni adresowej przeznaczonej dla adresacji unikastowej. Rozróżnienie pomiędzy rodzajami adresów (unikast, anykast) jest dokonywane na podstawie jawnego wskazania podczas konfiguracji interfejsu, iż dany adres jest adresem typu anykast.

W protokole IPv6 istnieją predefiniowane adresy anykastowe, zarezerwowane dla pewnych klas usług. Adresy te, mające w zamyśle ułatwić funkcjonowanie tych usług, zostały jawnie wydzielone z przestrzeni adresowej adresacji unikastowej i nie mogą być wykorzystywane jako adresy typu unikast.

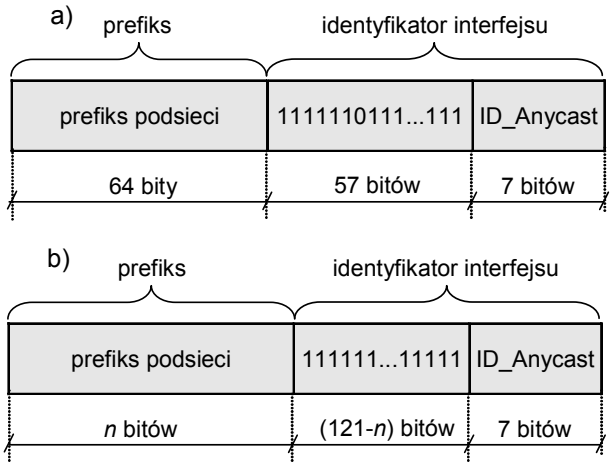
Pierwszym zarezerwowanym adresem typu anykast był adres domyślnego rutera w danej podsieci [8]. Ma on służyć do komunikacji stacji z jednym z ruterów w odległej podsieci. Adres taki składa się z prefiksu podsieci i wyzerowanego identyfikatora interfejsu (rys. 1).



Rys. 1. Adres anykastowy domyślnego rutera danej podsieci

Dla podsieci wydzielono również grupę adresów anykastowych, które mogą być wykorzystywane przez usługi lokalne [13]. Adresy te zajmują końcową część przestrzeni adresowej, dostępnej w danej podsieci. Posiadają one siedmiobitowy identyfikator ID_Anycast (rys. 2), który identyfikuje adres anykastowy usługi w danej podsieci.

Interfejsy w sieciach standardu 802.*x* posiadają adres MAC określany jako tzw. EUI (*Extended Unique Identifier*). Jest on 48-bitowym (EUI-48) lub 64-bitowym (EUI-64) globalnym identyfikatorem interfejsu, którego pierwsze 24 bity są przydzielane przez IEEE Registration Authority zarejestrowanemu użytkownikowi (np. firmie, organizacji), a pozostałe przez zarejestrowanego użytkownika.



Rys. 2. Zarezerwowane adresy anykastowe dla podsieci: a) dla adresów opartych na identyfikatorze interfejsu EUI-64; b) dla pozostałych adresów

W przypadku adresów anykastowych opartych na identyfikatorze interfejsu EUI-64 (rys. 2a), pierwszych 57 bitów pola identyfikatora interfejsu posiada ustawione wszystkie bity (przyjmują one wartość 1) z wyjątkiem bitu będącego negacją znacznika *U*/*L* (*Universal*/*Local*).

Znacznik ten określa, czy dany adres jest administrowany globalnie, tj. przez IEEE Registration Authority (*U*/*L* = 0), czy lokalnie (*U*/*L* = 1). W przypadku adresu anykastowego, znacznik *U*/*L* przyjmuje zawsze wartość 1 (czyli znajdujący się w adresie bit zanegowanego znacznika *U*/*L* przyjmuje wartość 0), co oznacza, że adres jest administrowany lokalnie. Prefiks podsieci w tym typie adresu jest zapisywany zawsze na 64 bitach. Prefiks podsieci identyfikuje podsieć, w której funkcjonuje dana usługa.

W przypadku adresów niebędących adresami opartymi na identyfikatorze EUI-64, prefiks podsieci jest zapisywany na *n* bitach (rys. 2b). Pozostała część adresu anykastowego (tj. 128 – *n* bitów) jest przeznaczona, jak poprzednio, na adres interfejsu, którego ostatnie 7 bitów zajmuje identyfikator ID_Anycast. Pozostałe 121–*n* bitów adresu interfejsu zawsze przyjmuje wartość 1.

Z puli zarezerwowanych adresów anykastowych usług lokalnych obecnie zdefiniowano jedynie adres dla MIP (*Mobile Internet Protocol*). Jest to adres agenta macierzystego będącego wyróżnionym ruterem w sieci macierzystej danej stacji. W adresie tym pole ID_Anycast przyjmuje wartość 7E (heksadecymalnie) [13]. Stacja ruchoma uzyskuje połączenie z agentem macierzystym poprzez podanie adresu anykastowego agenta macierzystego. Dzięki wykorzystaniu adresu anykastowego nie ma potrzeby określania konkretnego adresu agenta macierzystego, co upraszcza konfigurację i zwiększa niezawodność funkcjonowania usługi.

Problemy związane z wdrażaniem adresacji typu anykast w sieciach IP są zbliżone do problemów obserwowanych na wczesnym etapie wdrażania adresacji multikastowej. Problemy funkcjonowania adresacji anykastowej o zasięgu lokalnym (łącza, sieci lokalnej/miejscowej, podsieci) zostały w znacznym stopniu (aczkolwiek nie całkowicie) rozwiązane. Wciąż nie ma jednak w pełni dojrzałych rozwiązań umożliwiających funkcjonowanie adresacji typu anykast w skali globalnej, a istniejące protokoły i algorytmy mają głównie charakter eksperymentalny.

Do tej pory nie zdefiniowano np. puli globalnych adresów anykastowych. Na przeszkodzie stoi m.in. wspólny format adresu typu unikast i anykast, co sprawia z kolei, że adresy anykastowe dezorganizują agregację adresów unikastowych, niezbędną do efektywnego funkcjonowania rutingu. Globalny anykast uniemożliwia agregację, ponieważ ten sam adres anykastowy może występować w wielu różnych podsieciach [17]. Rozwiązanie tego problemu możliwe byłoby np. dzięki zastosowaniu wydzielonej, ciągłej przestrzeni adresowej dla adresów anykastowych, co jednakże wymagałoby rezygnacji z idei wspólnego formatu adresu uni- i anykastowego.

Poważne trudności techniczne napotykane są również podczas prób zbudowania specjalizowanego, global-

nego rutingu anykastowego. Zastosowanie adresacji anykastowej w skali globalnej wymaga opracowania specjalizowanych protokołów rutingu. Obecnie proponowane są m.in. rozwiązania będące modyfikacjami protokołów rutingu multikastowego [6], ruting zintegrowany (jedno- i wielościeżkowy) [12], czy ruting zbudowany z wykorzystaniem sieci aktywnych [17].

Dochodzi do tego kwestia wyboru właściwej metryki trasy. Najprostsza metryka, oparta na liczbie węzłów pośredniczących zlokalizowanych między stacją kliencką a serwerem, może w wielu przypadkach okazać się niewystarczająca. Proponowane rozwiązania obejmują m.in. wykorzystanie pomiarów czasu RTT (*Round Trip Time*) czy obciążenia serwerów usług [19].

Zwróćmy uwagę, że jeżeli adresacja anykastowa jest stosowana (jak obecnie) tylko w skali lokalnej podsieci, problem wyboru trasy z odległych podsieci w praktyce nie występuje. Trasa jest wybierana na podstawie prefiksu określającego daną podsieć, a sam dobór trasy jest realizowany przez typowe procedury rutingu dla transmisji unikastowej.

Pewnych trudności należy się spodziewać także podczas realizacji efektywnych mechanizmów zarządzających adresami anykastowymi. Będą to np. problemy związane z przydziałem adresów anykastowych, rejestracją systemów identyfikowanych takim adresem, zapewnieniem prawidłowej sygnalizacji braku usługi (różnej od braku dostępu do usługi).

3. Problem błędnego przekierowania zgłoszenia

Datagramy wysyłane na adres anykastowy zostają skierowane do jednego z serwerów (najlepiej: najbliższego) świadczących tę usługę. W wyniku błędnego przekierowania, datagramy mogą zostać skierowane do innego serwera usług niż pożądany. W efekcie, użytkownik może zostać podłączony do serwera zawierającego inny zbiór zasobów niż oczekiwany lub też będzie to serwer (z pewnych względów) nieoptymalny.

Podłączenie się do innego zbioru zasobów jest możliwe wówczas, gdy zasoby na poszczególnych serwerach nie są identyczne. Taki brak zgodności zasobów może nastąpić w sposób przypadkowy (np. błąd aktualizacji zasobów, błędny wpis w konfiguracji serwera) lub celowy (np. na lokalnych serwerach znajdują się tylko zasoby najczęściej używane).

Błędne przekierowanie, skutkujące skierowaniem zgłoszenia do nieoptymalnego serwera usług, związane może być np. z błędami funkcjonalnymi rutingu. Błędy te mogą, ale nie muszą wynikać wprost z błędnego funkcjonowania procedur rutingu. Przykładowo, źle skonstruowana metryka, nieuwzględniająca wszystkich uwarunkowań (w tym np. lokalizacji geograficznej) może przynieść podobny skutek jak błędny wpis w konfiguracji rutera/ruterów.

Sytuacje związane z błędnymi przekierowaniami zdarzają się również w przypadku „pierwowzoru" usług anykastowych – numerów alarmowych. Przykładowo, w sierpniu 2005 roku serwis `www.rmf.fm` informował o przypadkach błędnego przekierowania zgłoszeń skierowanych na numer 112. Zdarzało się, że zgłoszenia z okolic Krakowa były kierowane do odległego o 170 km Sandomierza [14]. Dodatkowo, zgłoszenia pochodzące z różnych sieci telefonicznych były kierowane do różnych centrów obsługi, nawet w przypadku tej samej lokalizacji geograficznej abonenta (w przypadku sieci stacjonarnej – do pogotowia ratunkowego, a w przypadku sieci komórkowej – do dyżurnego policji) [16]. Informacja o przypadkach błędnego przekierowania zgłoszeń z telefonów komórkowych do innego miasta pojawiła się również na stronach WWW Internetowego Forum Policyjnego `www.ifp.pl` [3].

Usługi korzystające z adresacji anykastowej powinny móc sobie poradzić z błędnym przekierowaniem zgłoszeń. Jeżeli zasoby na pewnych serwerach zostały ograniczone celowo (tak, jak to miało miejsce w cytowanym przypadku numeru alarmowego 112), błąd przekierowania powinien być naprawiany automatycznie przez system, poprzez dodatkowe przekierowanie. Jeżeli różnice w zawartości zasobów serwerów powstały na skutek działania czynników zewnętrznych (np. błędów oprogramowania, błędów transmisji, itp.), to wykrycie przekierowania do niewłaściwego serwera powinno skutkować uruchomieniem procedur zmierzających do przywrócenia zgodności zasobów.

Skierowanie zgłoszenia do niewłaściwego (nieoptymalnego) serwera usług jest trudniejsze do wykrycia, niż podłączenie się do innego zbioru zasobów. Naprawa tego błędu często będzie się wiązać ze zmianą sposobu konstruowania metryki trasy. Zwróćmy uwagę, że skierowanie zgłoszenia do innego serwera usług niż optymalny, może (w pewnych warunkach) być również działaniem celowym. Serwer optymalny z punktu widzenia pracy sieci (pracy serwera) może bowiem być serwerem suboptymalnym z punktu widzenia użytkownika. Przykładowo, jeżeli serwer optymalny jest zbyt przeciążony (np. serwer VoD[1)] oferujący atrakcyjny materiał filmowy, czy – o czym rzadziej się pamięta – nowouruchomiony serwer atrakcyjnej usługi[2)]), niekiedy korzystne może być skierowanie części ruchu do serwera pomocniczego (zapasowego).

[1)] VoD – ang. *Video on Demand* – dosł. wideo na żądanie – usługa zdalnego magnetowidu / wypożyczalni wideo.

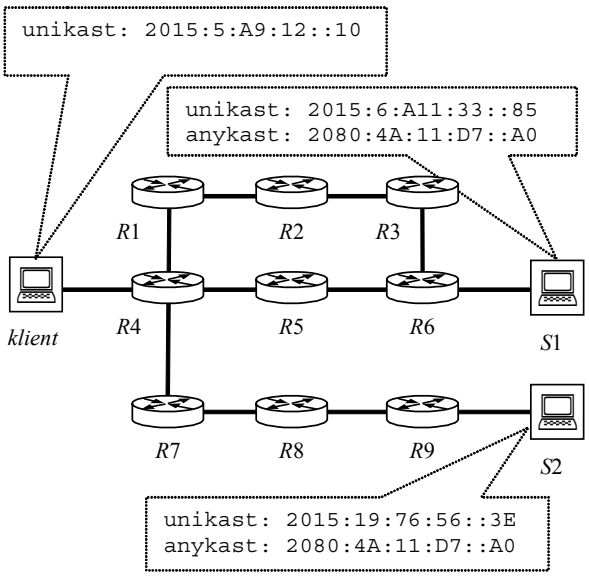
[2)] Nowości, wchodzące właśnie na rynek, zawsze budzą zainteresowanie potencjalnych nabywców, a nowa usługa sieciowa nie jest żadnym wyjątkiem. Jako ciekawostkę dodajmy, że reguła ta odnosi się również do telefonicznych numerów alarmowych. 7 sierpnia 2005 RMF informował: „*gdy w Tarnowie uruchomiono linię ratunkową 112, numer był przez wiele dni zablokowany, bo setki osób dzwoniło tylko po to, by sprawdzić czy rzeczywiście działa*" [14].

4. Usługi połączeniowe korzystające z adresacji anykastowej w sieci bezpołączeniowej

Wiele usług, korzystających z adresacji anykastowej, do transmisji zasobów wykorzystuje (w warstwie transportowej) protokół TCP (*Transmission Control Protocol*) lub inny niezawodny protokół połączeniowy. Protokół taki wymaga, aby przez cały czas trwania połączenia obydwa systemy końcowe (klient i serwer) utrzymywały stan połączenia. A zatem, transmisja zawsze musi być realizowana pomiędzy tymi samymi węzłami sieci.

Protokół IP, dostarczający usługi adresacji anykastowej, jest protokołem bezpołączeniowym i nie wymaga utrzymywania stanu połączenia. W protokole IP każdy datagram może być przesyłany pomiędzy systemami końcowymi (teoretycznie) inną trasą. Zmiany trasy mogą wynikać chociażby ze zmian topologii sieci (np. na skutek przemieszczania się stacji ruchomych, czy w wyniku uszkodzenia się któregoś z węzłów pośredniczących), zadziałania systemu równoważenia obciążeń, specyfiki rutingu (np. ruting QoS – *Quality of Service routing*).

W trakcie transmisji może zatem, w sposób naturalny, nastąpić zmiana trasy datagramu na trasę o innej metryce. Nie powoduje to większych problemów w przypadku transmisji punkt-punkt realizowanej z wykorzystaniem adresacji unikastowej, gdzie adresy IP są jednoznacznie przypisane do systemów końcowych. Jeżeli jednak transmisja punkt-punkt realizowana jest z wykorzystaniem adresacji anykastowej, gdzie wybór systemu końcowego (zwykle serwera usługi) odbywa się na podstawie metryk tras, po każdej aktualizacji tablic rutingu może nastąpić zmiana systemu końcowego. Zmiana taka może nastąpić w trakcie trwania połączenia.



Rys. 3. Przykładowa sieć z adresacją anykastową

Na rysunku 3 została przedstawiona przykładowa sieć IPv6. Stacja kliencka jest identyfikowana tylko swoim adresem unikastowym (2015:5:A9:12::10), natomiast serwery usług *S*1 i *S*2 identyfikowane są zarówno indywidualnymi adresami unikastowymi (*S*1 adresem 2015:6:A11:33::85, natomiast *S*2 adresem 2015:19:76:56::3E), jak i wspólnym adresem anykastowym (2080:4A:11:D7::A0). Adres anykastowy jest adresem globalnym, a zatem nie podlega regułom tworzenia anykastowej adresacji lokalnej (patrz rys. 1 i rys. 2), jest natomiast zgodny z ogólnym formatem globalnego adresu IPv6 typu unikast (patrz [8]).

Trasa pomiędzy stacją kliencką a serwerem *S*1 może prowadzić poprzez węzły pośredniczące (rutery) *R*4, *R*5 i *R*6 lub, alternatywnie, poprzez węzły *R*4, *R*1, *R*2, *R*3 i *R*6. Trasa pomiędzy klientem usług a serwerem *S*2 prowadzi tylko przez węzły *R*4, *R*7, *R*8 i *R*9.

Połączenie anykastowe zostanie nawiązane pomiędzy stacją kliencką a tym serwerem usług, do którego prowadzi trasa optymalna. Jeżeli zastosujemy najprostszą metrykę – liczbę węzłów pośredniczących pomiędzy stacją kliencką a serwerem – to trasą optymalną będzie ta spośród tras (*R*4, *R*5, *R*6), (*R*4, *R*1, *R*2, *R*3, *R*6), (*R*4, *R*7, *R*8 i *R*9), która charakteryzuje się najkrótszą ścieżką (w sensie zastosowanej metryki). Połączenie anykastowe zostanie zatem nawiązane pomiędzy stacją *klient* a *S*1, a trasa datagramów przesyłanych pomiędzy tymi stacjami będzie prowadziła przez węzły *R*4, *R*5 i *R*6.

Załóżmy teraz, że w trakcie transmisji został uszkodzony ruter *R*5, przez co dotychczasowa trasa optymalna (*R*4, *R*5, *R*6) stała się niedostępna. Ponieważ istnieje trasa alternatywna do dotychczas używanej, z punktu widzenia warstwy transportowej uszkodzenie takie nie oznacza uszkodzenia sieci jako całości – w wyniku zadziałania odpowiednich procedur rutingu zostaną zaktualizowane trasy pomiędzy sieciami. Droga datagramów przesyłanych pomiędzy stacją *klient* a stacją *S*1 będzie teraz wiodła przez węzły *R*4, *R*1, *R*2, *R*3 i *R*6. Gdyby transmisja pomiędzy tymi stacjami była transmisją unikastową, odbywałaby się normalnie. Ponieważ warstwa sieciowa ukrywa przed warstwą transportową szczegóły budowy sieci (w tym i wybraną trasę), uszkodzenie nie wpłynęłoby w sposób destrukcyjny na pracę protokołu transportowego.

W przypadku transmisji anykastowej, problem jest nieco bardziej złożony. Należy bowiem zastanowić się, czy różnica metryk „starej" i „nowej" trasy pomiędzy stacjami *klient* i *S*1 (odpowiednio: 3 i 5) ma wpływ na optymalność połączenia (tu: w sensie minimalizacji metryki). Biorąc pod uwagę, że trasa pomiędzy stacjami *klient* i *S*2 ma metrykę 4, po wymuszonej przez uszkodzenie rutera *R*5 zmianie trasy, *S*1 stał się nieoptymalnym (z punktu widzenia metryki) serwerem usług. Nie można zatem kontynuować połączenia anykastowego stacji klienckiej *klient* z serwerem *S*1.

Od tej chwili, datagramy anykastowe będą przesyłane pomiędzy stacją *klient* a stacją *S*2.

Z punktu widzenia protokołu IP – protokołu bezpołączeniowego, który nie wymaga utrzymywania stanu połączenia – tego typu zmiana serwera usług jest zarówno dopuszczalna, jak i możliwa. Inaczej rzecz się ma z punktu widzenia połączeniowego protokołu transportowego. Jeżeli transmisja jest realizowana z wykorzystaniem protokołu TCP, „nowy" system końcowy (tu: *S*2) odrzuci przychodzące pakiety TCP. Z kolei „stary" system końcowy (tu: *S*1) będzie czekać na wznowienie transmisji lub zakończenie połączenia.

Problem usług połączeniowych korzystających z adresacji anykastowej IPv6 nadal jest otwartym tematem badawczym. Proponowane rozwiązania obejmują m.in. [17]: pięcioetapowe porozumienie, identyfikację źródła oraz odwzorowanie adresu. Wszystkie one opierają się na wykorzystaniu adresu unikastowego tego serwera usług, który w chwili rozpoczęcia transmisji datagramów anykastowych był serwerem optymalnym.

W pięcioetapowym porozumieniu (*Five-Way Handshake*) [17] dokonano rozszerzenia mechanizmu nawiązywania połączenia protokołu TCP o dodatkowe dwa etapy. W odpowiedzi na pakiet inicjujący połączenie, system identyfikowany adresem anykastowym przesyła do drugiego systemu końcowego swój adres typu unikast. Następnie obydwa systemy kontynuują nawiązywanie połączenia TCP klasyczną metodą trójetapowego porozumienia (*Three-Way Handshake*), używając swoich adresów unikastowych.

Metoda identyfikacji źródła (*Source Identification Option*) [17] pozwala na nawiązanie połączenia TCP metodą trójetapowego porozumienia. Jest to możliwe dzięki wprowadzeniu do wersji 6 protokołu IP obsługi dodatkowego nagłówka opcjonalnego. W odpowiedzi na pakiet inicjujący połączenie, wysłany na adres anykastowy, system identyfikowany tym adresem przesyła do drugiego systemu końcowego pakiet z ustawionymi znacznikami SYN i ACK. Pakiet ten przenoszony jest w datagramie IP, którego pole *adres_źródłowy* zawiera adres typu unikast, natomiast adres anykastowy jest przesyłany w polu nagłówka opcjonalnego. Po otrzymaniu takiego pakietu, dalsza transmisja (wraz z dokończeniem fazy nawiązywania połączenia TCP) będzie odbywała się z wykorzystaniem adresów typu unikast.

W przeciwieństwie do obu opisywanych powyżej rozwiązań, odwzorowanie adresu anykastowego w adres unikastowy (*Anycast Address Mapper*) [17] nie wymaga modyfikacji ani protokołu TCP, ani IP. System inicjujący połączenie wysyła komunikat ICMP ECHO Request na adres anykastowy. W odpowiedzi, system identyfikowany tym adresem wysyła do systemu inicjującego komunikat ICMP ECHO Replay wpisując w polu nadawcy swój adres unikastowy. Po otrzymaniu tego komunikatu, system inicjujący rozpoczyna nawiązywanie połączenia TCP, wykorzystując adresację unikastową.

5. Spójność danych i aktualizacja zasobów

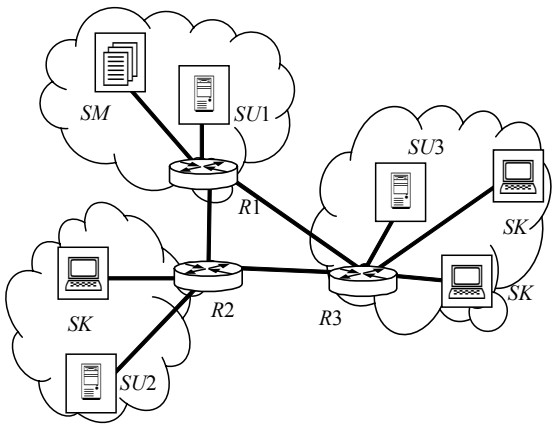
W sieciach IPv6, transmisja anykastowa wykorzystywana może być w przypadku współpracy klienta z grupą serwerów udostępniających zasoby wielu klientom. Każdy z serwerów powinien posiadać identyczny (z punktu widzenia klienta) zbiór zasobów. Klient usługi połączy się z dowolnym serwerem, podając adres anykastowy grupy serwerów. Zostaje wówczas połączony z najbliższym serwerem, przy czym miarą „bliskości" serwera jest metryka danej trasy, znajdująca się w tablicy rutingu. W efekcie, użytkownik jest łączony z optymalnym (z punktu widzenia metryki) z grupy serwerów, nie mając przy tym świadomości, który fizycznie serwer go obsługuje.

Aby usługa taka mogła efektywnie funkcjonować, dane na wszystkich serwerach informacyjnych, z którymi może połączyć się użytkownik, muszą być spójne i muszą być aktualizowane jednocześnie. Zbudowanie takiej efektywnej aktualizacji jest możliwe na bazie *M* połączeń punkt-punkt wykorzystujących niezawodny protokół transportowy lub na bazie niezawodnej transmisji multikastowej pomiędzy wszystkimi serwerami usług.

Jednym z możliwych rozwiązań tego problemu jest zaproponowana w pracy [1] koncepcja systemu aktualizacji zasobów serwerów usług korzystających z adresacji anykastowej. Koncepcja ta zakłada istnienie następujących elementów (rys. 4):

- serwera matki *SM*, zawierającego dane pierwotne, rozsyłane multikastowo do serwerów usług;
- serwerów usług *SU*, zawierających kopie danych pierwotnych, które podlegają redystrybucji do stacji klienckich;
- stacji klienckich *SK*,

połączonych infrastrukturą sieciową IPv6.



Rys. 4. Przykładowa sieć dystrybucyjna

Stacja kliencka, która zamierza korzystać z usługi świadczonej przez system, podłącza się do najbliższego (w sensie metryki) serwera usług, wykorzystując właściwości adresacji anykastowej. Każdy serwer usług posiada globalny adres anykastowy, wspólny dla wszystkich serwerów danej usługi.

Aby zapobiec ewentualnym problemom, jakie mogłyby wystąpić podczas nieoczekiwanej zmiany serwera usług (wynikającej z zadziałania procedur rutingu anykastowego – patrz rozdział 4), transmisja danych pomiędzy stacją kliencką a serwerem usług jest realizowana z wykorzystaniem transmisji unikastowej lub multikastowej. Stacja kliencka otrzymuje odpowiedni adres unikastowy lub multikastowy podczas rejestracji w serwerze usług. Unika się w ten sposób stosowania protokołów bądź architektur wymagających ingerencji w sieć IPv6.

Dystrybucja danych pierwotnych z serwera matki do serwerów usług będzie realizowana z wykorzystaniem niezawodnej transmisji multikastowej. Zastosowanie transmisji multikastowej zwiększa efektywność aktualizacji danych, a także pozwala na równoczesne dokonywanie aktualizacji we wszystkich serwerach usług.

W warstwie transportowej należy zastosować protokół, który najlepiej odpowiada wymaganiom danej usługi. Przykładowo, może to być protokół PGM (*Pragmatic General Multicast*) – jeden z najnowszych, uniwersalnych protokołów transportowych, przeznaczony do niezawodnej transmisji multikastowej [2]. Protokół PGM nie realizuje zapobiegania przeciążeniom, w tym celu zwykle wykorzystywany jest, współpracujący z PGM, blok funkcjonalny PGMCC. PGMCC należy do klasy tzw. protokołów sprzyjających TCP i, jako taki, emuluje mechanizm zapobiegania przeciążeniom stosowany w protokole TCP.

Jeżeli aktualizacja zawartości serwerów usług musi być realizowana w czasie rzeczywistym (np. gdy serwery usług dokonują redystrybucji danych giełdowych), należy zastosować specjalizowany, niezawodny protokół transportowy czasu rzeczywistego. Przykładem takiego protokołu może być eksperymentalny protokół T-RMP (*Timed Reliable Multicast Protocol*). Umożliwia on dostarczanie danych do wszystkich procesów T-RMP w tym samym czasie, zapewniając pełną synchronizację otrzymywania danych przez wszystkich odbiorców [2].

Jeżeli świadczona usługa tego wymaga, do aktualizacji zasobów można wykorzystać inny typ protokołu transportowego niż niezawodny. Przykładowo, jeśli system świadczy usługę telewizji internetowej, dystrybucja danych pierwotnych (audycji telewizyjnej) z serwera-matki (pełniącego tutaj rolę dostawcy treści przekazu multimedialnego – *content provider*) do serwera usług może być realizowana z wykorzystaniem protokołu RTP (*Real-time Transport Protocol*), zaprojektowanego pod kątem multikastowej transmisji czasu rzeczywistego [2]. Serwer usług spełnia wówczas rolę serwera proxy. Proponowana koncepcja dopuszcza pełnienie przez niego również funkcji dostawcy usługi (*service provider*).

6. Problemy bezpieczeństwa systemów korzystających z usług typu anykast

Bezpieczeństwo systemów korzystających z usług typu anykast jest pojęciem złożonym. Z jednej strony obejmuje ono bowiem problematykę zapewnienia bezpieczeństwa bezpośrednio usłudze adresacji anykastowej. Należy jednak pamiętać, że adresacja anykastowa nie funkcjonuje samotnie, bez innych mechanizmów, zapewniających chociażby aktualizację zasobów serwerów. Dyskusja bezpieczeństwa systemów korzystających z usług typu anykast musi zatem dotykać również problematyki odporności usługi zbudowanej na bazie anykastu na ataki zewnętrzne.

Jak wskazano w poprzednim rozdziale, korzystne jest, by usługa taka do aktualizacji zasobów serwerów wykorzystywała transmisję multikastową. Dlatego integralna częścią analizy problemów bezpieczeństwa systemów korzystających z usług typu anykast jest, zdaniem Autorów, dyskusja zagrożeń występujących podczas multikastowej aktualizacji serwerów anykastowych.

Problemy bezpieczeństwa usługi adresacji anykastowej związane są głównie z możliwością stosunkowo łatwego (w porównaniu z transmisją unikastową) podszywania się „obcego” serwera pod właściwy serwer usługi. Serwer usługi nie jest rozpoznawalny przez stację kliencką (np. poprzez adres indywidualny), zatem sytuacja, gdy „obcy” serwer dołącza się do grupy „swoich” serwerów, może być trudna do zidentyfikowania przez użytkownika lub też będzie mylnie interpretowana jako błąd przekierowania zgłoszenia.

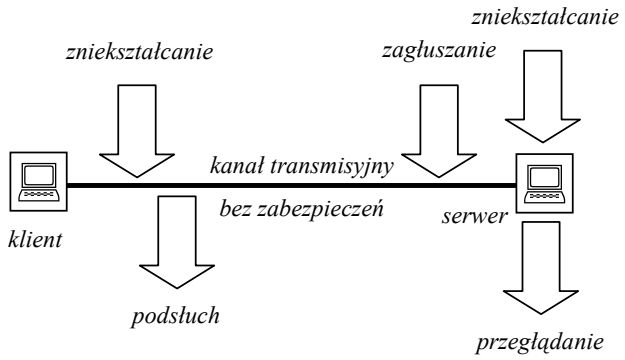
Odporność usługi zbudowanej na bazie anykastu na ataki zewnętrzne dotyczy zarówno bezpieczeństwa danych przechowywanych w serwerach usług, jak i bezpieczeństwa systemu aktualizacji zasobów. Zagrożenie danych przechowywanych w serwerach usług występuje głównie ze strony klienta usługi, nie można jednak wykluczyć próby ataku podczas aktualizacji danych. Zbliżone w skutkach, lecz odmienne pod względem zastosowanych rozwiązań technicznych może być naruszenie bezpieczeństwa transmisji podczas aktualizacji danych.

Zarówno w przypadku samej usługi adresacji anykastowej, jak i innych usług zbudowanych na jej bazie, naruszenie bezpieczeństwa może sprowadzać się do (rys. 5):

- podsłuchu,
- zniekształcania,
- zagłuszania.

lub dowolnej ich kombinacji.

Podsłuch (podsłuch bierny) polega na nieupoważnionym wglądzie do danych [4]. Stosowany jest w celu pozyskania określonych zasobów, np. zasobów serwera usługi, ale również zasobów komputera użytkownika.



Rys. 5. Zagrożenia bezpieczeństwa w systemach informacyjnych

W tym ostatnim przypadku przybiera on formę m.in. nieupoważnionego przeglądania danych.

Usługi bazujące na adresacji anykastowej są narażone na podsłuch oraz na nieupoważnione przeglądanie zawartości baz danych, jak każda inna sieć komputerowa i system baz danych. Dochodzi do tego potencjalna możliwość łatwego podszywania się nieuprawnionego serwera pod legalny serwer usługi. Serwer nieuprawniony działałby wówczas jak przekaźnik, przechwytujący strumień danych i przekierowujący go do właściwego serwera. W ten sposób mogłyby zostać przechwycone zarówno dane użytkownika (np. numer karty kredytowej użytkownika, zapisy transakcji bankowych itd.), jak i dane serwera (np. pozyskiwanie nielegalnych kopii utworów muzycznych lub filmowych).

Jeżeli aktualizacja zasobów serwerów usług realizowana jest z wykorzystaniem transmisji multikastowej, należy liczyć się z możliwością podłączenia się nieautoryzowanego odbiorcy do trwającej sesji multikastowej. Zgodnie z ideą multikastu IP, zakładającej pełną anonimowość odbiorcy, nie istnieją mechanizmy zabraniające odbiornikowi podłączania się ani do grupy multikastowej, ani do trwającej transmisji.

Transmisja multikastowa jest swoistym przeniesieniem do sieci (przewodowej i/lub bezprzewodowej) transmisji o charakterze rozsiewczym. Również zabezpieczenia przed podsłuchem są zbliżone w swej idei do zabezpieczeń tam stosowanych. Są to [7]: szyfrowanie informacji (typowo z wielokrotną zmianą klucza w trakcie trwania pojedynczej sesji multikastowej) oraz ograniczanie dostępu do informacji o prywatnych i lokalnych sesjach multikastowych. Możliwe jest również zapewnienie ochrony z wykorzystaniem specjalizowanego protokołu transportowego i (lub) rozsyłanie datagramów multikastowych z wykorzystaniem wirtualnej sieci prywatnej [7].

Zniekształcanie informacji (w przypadku zagrożenia bezpieczeństwa łączności używana jest również nazwa „podsłuch aktywny") polega na nieupoważnionej modyfikacji danych [4]. Modyfikacja taka może polegać zarówno na podmianie czy skasowaniu informacji, jak i na ich dodaniu (np. powielenie informacji sygnalizacyjnej w celu wywołania określonej reakcji systemu). Stosowana jest ona w celu przekazania użytkownikowi (tu: klientowi usługi) określonych (niepożądanych) treści lub niedopuszczenia do pozyskania pewnych zasobów przez użytkownika (np. poprzez zmianę zawartości bazy danych – w tym podmianę lub usunięcie części danych). Podsłuch aktywny, który w swojej najłagodniejszej postaci może sprowadzać się do niewinnych – z pozoru – czynności, jak rozsyłania spamu (np. reklam – niepożądanych, lecz nie naruszających norm społecznych czy obyczajowych), w skrajnym przypadku może mieć charakter nawet ataku terrorystycznego[3)].

Zniekształcanie informacji może dotyczyć zarówno systemu aktualizacji zasobów, jak i bezpośrednio baz danych. W tym ostatnim przypadku, wymagane jest uprzednie uzyskanie (nieautoryzowanego) dostępu do systemu baz danych. Może mieć on charakter włamania do systemu (*hacking*). Należy jednak pamiętać, że znacznie prostsze (choć zdecydowanie mniej spektakularne) jest pozyskanie dostępu od osób uprawnionych do modyfikacji danych. Niejednokrotnie dzieje się tak na skutek zwykłej lekkomyślności – jak chociażby niemal przysłowiowego, ale wciąż spotykanego, przyklejania karteczek z hasłem do monitora.

Podsłuch, zarówno bierny, jak i aktywny, należy do typowych zagrożeń bezpieczeństwa łączności. Zabezpieczenia przed zniekształcaniem informacji podczas aktualizacji zasobów są zbliżone do, omawianych wyżej, zabezpieczeń przed podsłuchem biernym. Będą to zatem: szyfrowanie treści przekazu, ograniczanie dostępu do informacji o sesjach, a opcjonalnie także wykorzystanie wirtualnej sieci prywatnej.

Zniekształcenie może dotyczyć zarówno przesyłanych (bądź przechowywanych) danych użytkownika, jak i informacji sygnalizacyjnej. W tym ostatnim przypadku celem jest wywołania określonej reakcji systemu. Z tego względu ochronie powinny podlegać takie komunikaty, jak potwierdzenia prawidłowego odbioru pakietu danych (zwłaszcza negatywne potwierdzenia, wymuszające retransmisję), komunikaty rutingu, czy inne komunikaty mające wpływ na strukturę drzewa dystrybucji (np. komunikaty SPM (*Source Path Message*) protokołu PGM) [7].

Zniekształcenie informacji przechowywanej w bazach danych może powstawać na etapie transmisji informacji, w wyniku nieupoważnionego dostępu do bazy danych lub podszywania się pod bazę danych (np. udostępnianą anykastowo). Zniekształcenie informacji może przynieść poważne skutki w przypadku usługi DNS (*Domain Name System*) i innych, krytycznych (z punktu widzenia pracy sieci) usług. Równie poważne w skutkach może się okazać zniekształcanie danych przekazywanych użytkownikowi w ramach świadczonej usługi (np. danych giełdowych).

[3)] Należy sobie uświadomić, że sieć teleinformatyczna lub system baz danych jest tak samo atrakcyjnym celem dla terrorystów, jak każdy inny [10].

Zniekształcanie informacji może prowadzić do chaosu w systemach teleinformatycznych. Wymierne straty materialne, będące efektem tego chaosu, mogą wówczas przekroczyć (nawet kilkakrotnie) koszty instalacji takiego systemu. Jeżeli (czego nie można wykluczyć) zniekształcenie informacji będzie miało charakter zamachu terrorystycznego, skutki takiego chaosu mogą być równie znaczące (a czasami większe) jak eksplozja podłożonego ładunku wybuchowego [10]. Zabezpieczeniem przed zniekształceniem informacji podczas transmisji jest mechanizm uwierzytelniania datagramu IP gwarantujący, że adres nadawcy oraz zawartość datagramu nie zostały zmienione.

Potencjalnie bardzo groźnym, aczkolwiek zwykle niedocenianym niebezpieczeństwem, jest możliwość modyfikacji przekazu podczas transmisji mediów strumieniowych (radia internetowego, telewizji internetowej). Niedocenianie roli podsłuchu aktywnego bierze się zapewne stąd, iż zagrożenia bezpieczeństwa w przypadku mediów strumieniowych kojarzą się zwykle z aktami piractwa komputerowego, a zatem z podsłuchem biernym. Zmiana zawartości transmisji (np. w celu przekazywania ukrytych treści, oddziaływania podprogowego, ale również „zwykłej" podmiany jednego przekazu na drugi) wydaje się być obecnie raczej domeną powieści z gatunku *science fiction* lub *political fiction*. Tym niemniej, nie należy zapominać, że takie działania są realizowalne technicznie. Należy pamiętać również o tym, że wraz z rozpowszechnianiem się mediów internetowych, rola tych środków przekazu zacznie rosnąć, a wtedy groźba taka stanie się coraz bardziej realna. Już teraz zdarzają się przypadki podmiany zawartości stron WWW przez hakerów. Jest to realizowane przez podmianę stron na „legalnym" serwerze, podmianę odnośników, przekierowujących użytkownika do strony znajdującej się na „obcym" serwerze, bądź nawet przez podmianę „legalnego" serwera WWW (np. w wyniku nieuprawnionej modyfikacji tablic rutingu).

Zabezpieczenie przed zmianą zawartości transmisji strumieniowej może nabrać szczególnego znaczenia w dobie wojny z terroryzmem. Terroryzm to wojna psychologiczna, zorientowana na oddziaływanie na społeczeństwo [10]. W tym kontekście pojedynczy zamach terrorystyczny lub groźba jego realizacji jest bronią, a media stają się zasobami strategicznymi[4)].

Potencjalna możliwość zmiany treści informacji przekazywanych dużej grupie ludzi[5)], realizowana w celu wywołania w społeczeństwie określonych zachowań, może już niedługo okazać się bardzo atrakcyjna dla różnego rodzaju grup ekstremistycznych. Działalność taka może być szczególnie niebezpieczna w przypadku podszywania się pod media powszechnie uważane za wiarygodne (np. znana agencja informacyjna, znana stacja telewizyjna nadająca w Internecie). Trzeba bowiem mieć świadomość, że nawet najbardziej absurdalne (zdawałoby się) wiadomości, ale podane w odpowiedni sposób i przez uznane źródło, mogą doprowadzić do paniki. Klasycznym przykładem tego typu sytuacji są wydarzenia z 30 października 1938 roku, kiedy to radiowa adaptacja powieści G. Wellsa „Wojna światów" wywołała lawinę masowej histerii w Stanach Zjednoczonych [15].

Podmiana zawartości przekazu telewizyjnego, mająca na celu wywołanie określonych zachowań w społeczeństwie (np. paniki) może być szczególnie niebezpieczna, jeżeli pojawi się jako działanie skojarzone np. z klęską żywiołową, epidemią lub zamachem terrorystycznym. Odpowiednio skonstruowana wiadomość, która w normalnych warunkach przyniosłaby mały efekt (lub nawet żaden), potęguje bowiem istniejące w społeczeństwie lęki i frustracje, a efekt propagandowy takiej dezinformacji jest dodatkowo wzmacniany przez niezbyt odległe w czasie, tragiczne wydarzenia[6)].

Warto zauważyć, że nie ma potrzeby, aby autorzy zdarzenia „pierwotnego" i zdarzeń „wtórnych" byli ze sobą w jakikolwiek sposób powiązani. Sugeruje się raczej, że cele, jakie pragną osiągnąć terroryści (bądź ich naśladowcy), są jednakowe bez względu na ich światopoglądową orientację[7)] [11]. Nie należy zatem zakładać, że brak warunków do zaistnienia zdarzeń pierwotnych (np. brak w Polsce „rodzimych" tradycji terrorystycznych) wyklucza możliwość zaistnienia zdarzeń „wtórnych" oraz gwałtownych reakcji społeczeństwa na te zdarzenia.

---

4) Z tego względu coraz częściej mówi się o konieczności zapewnienia (w rozsądnych granicach, rzecz jasna) kontroli nad mediami, w tym również nad Internetem.

5) W chwili składania niniejszego artykułu do publikacji, w mediach pojawiła się wiadomość o incydencie w trakcie transmitowanego na żywo wystąpienia wiceprezydenta USA Dicka Cheneya. Jak podaje serwis internetowy RMF FM, w momencie, gdy polityk potępiał osoby krytykujące wojnę w Iraku, na jego twarzy pojawił się symbol „X" [18]. Stacja CNN, która nadawała wystąpienie, tłumaczy incydent błędem oprogramowania i usterką techniczną. Brak jest informacji o jakimkolwiek podłożu politycznym tego incydentu.

6) Tragicznym przykładem, do czego może doprowadzić dezinformacja skojarzona z wcześniejszymi, realnymi wydarzeniami, są wypadki z 31 sierpnia 2005 roku, gdy plotka o zamachowcu-samobójcy doprowadziła do paniki milionowy tłum pątników. Na moście A'Imma w Bagdadzie śmierć poniosło wtedy około tysiąca osób, a drugie tyle zostało rannych [9] – więcej, niż od początku 2003 roku zginęło w Iraku w jakimkolwiek zamachu z wykorzystaniem materiałów wybuchowych. Zanim doszło do paniki, miejsce pielgrzymki zostało ostrzelane trzema pociskami moździerzowymi, w wyniku czego zginęło 7 osób, a 35 zostało rannych [5].

7) Występowanie zdarzeń „pierwotnych" i „wtórnych" można było zaobserwować np. po zamachach w Nowym Jorku i w Londynie. Po zamachach z 11 września 2001 roku pojawiło się szereg przypadków rozsyłania pocztą przesyłek zawierających bakterie wąglika lub imitujących takie przesyłki. Pomimo że odnotowane wówczas zarażenia wąglikiem były nieliczne i dotyczyły tylko Stanów Zjednoczonych, objawy niepokoju i strachu przed „listami z białym proszkiem" pojawiły się na całym świecie. Po zamachach w Londynie z 7 lipca 2005 roku, niemal natychmiast pojawiły się fałszywe alarmy bombowe w Budapeszcie, a następne dni przyniosły falę fałszywych alarmów w Polsce. Brak jest dowodów, aby w opisywanych przypadkach autorzy zdarzeń „pierwotnego" i „wtórnych" byli ze sobą powiązani.

W przypadku zdarzeń mających charakter podsłuchu aktywnego, na przeszkodzie stoi raczej zbyt mała jeszcze grupa odbiorców serwisów radiowych i telewizyjnych nadających w Internecie (w stosunku do liczby odbiorców „tradycyjnego" radia i telewizji), stosunkowo częste jeszcze wykorzystywanie w tego typu serwisach transmisji punkt-punkt oraz brak łatwo dostępnego oprogramowania umożliwiającego podmianę zawartości przekazu. Jeżeli (choć może raczej należałoby napisać: „kiedy") te warunki ulegną zmianie, należy się spodziewać częstych naruszeń bezpieczeństwa przekazu – mających chociażby formę żartu. Ale nawet najbardziej niewinny żart może, w razie niesprzyjającego zbiegu okoliczności, doprowadzić do nieszczęścia.

Odmianą zniekształcania informacji jest zagłuszanie. Polega ono na takim zniekształceniu przesyłanej informacji, aby jej odbiór był niemożliwy z przyczyn technicznych. Celem zagłuszania jest niedopuszczenie do pozyskania określonych zasobów przez uprawnionego użytkownika (użytkowników). W tym sensie, odpowiednikiem zagłuszania jest naruszanie bezpieczeństwa bazy danych w postaci kasowania informacji.

Zagłuszanie stosowane jest typowo w przypadku mediów rozsiewczych, takich jak radio czy telewizja (starsi Czytelnicy pamiętają zapewne zagłuszanie wiadomości Radia Wolna Europa). W sieci pakietowej, na zagłuszanie najbardziej narażona jest transmisja multikastowa. Wynika to, po pierwsze, z właściwości transmisji multikastowej, stanowiącej swoiste odwzorowanie transmisji rozsiewczej w dowolnym medium transmisyjnym (zarówno rozsiewczym, jak i nierozsiewczym) [2]. A po drugie, z właściwości źródła multikastowego, które (zgodnie z ideą multikastu IP) nie musi nawet należeć do grupy multikastowej, na adres której nadaje.

Zagłuszanie może być realizowane na wiele sposobów. Od skomplikowanego – podszywanie się pod źródło oryginalne tak, by użytkownik otrzymywał przekaz bezużyteczny lub by przekaz oryginalny docierający do użytkownika był zniekształcony w stopniu uniemożliwiającym jego odtworzenie. Po najprostsze – nadawanie w celu wywołania przeciążeń w węzłach pośredniczących, które uniemożliwiłyby poprawną transmisję przekazu oryginalnego. W tym przypadku, zagłuszanie może dotyczyć tylko pewnej gałęzi drzewa dystrybucji multikastowej bądź całego drzewa. Będzie ono najskuteczniejsze, jeśli nieupoważniony nadajnik będzie zlokalizowany możliwie najbliżej korzenia drzewa dystrybucji multikastowej.

Nadawanie w celu sztucznego wywołania przeciążeń jest traktowane jako odmiana ataku DoS (*Denial of Service*), czyli ataku typu „odmowa dostępu do usługi" [7] (tu: usługi transmisyjnej). W przypadku mediów strumieniowych, wymagających dodatkowo zapewnienia gwarantowanej jakości usług sieciowych (żądanej przepustowości, stopy błędów, opóźnienia transmisyjnego, fluktuacji opóźnienia) ten rodzaj zagłuszania nazywany bywa również atakiem DQoS (*Denial of Quality of Service*), czyli atakiem typu „odmowa gwarancji jakości usługi" [7]. W przypadku powodzenia ataku DQoS, brak gwarantowanej jakości usług sieciowych sprawia, że usługa wymagająca transmisji informacji w czasie rzeczywistym staje się nieakceptowalna dla użytkownika.

Samo pojęcie ataku typu DoS jest znacznie szersze i, w przypadku omawianej klasy usług, może dotyczyć również ataku na serwer (serwery) usług lub na serwer matkę. Zwykle jest to związane z nagłym pojawieniem się tak dużej liczby użytkowników (stacji klienckich w przypadku ataku na serwer usług, serwerów usług w przypadku ataku na serwer matkę), że obciążenie serwera (i/lub infrastruktury sieciowej w pobliżu serwera) przekracza możliwości obsługi oferowane przez ten serwer.

Zabezpieczenia przed zagłuszaniem obejmują m.in. autoryzację źródła, filtrację źródeł oraz stosowanie transmisji multikastowej zorientowanej na źródło (typu SSM – *Source-Specific Multicast*).

7. Podsumowanie

Anykast jest stosunkowo nowym rodzajem adresacji w sieciach IP, wprowadzonym dopiero do wersji 6 protokołu. Obecne problemy związane z jego wdrażaniem są zbliżone do problemów obserwowanych na wczesnym etapie wdrażania multikastu IP. Nie zdefiniowano puli globalnych adresów anykastowych (globalne adresy anykastowe należą do puli adresów unikastowych), co dezorganizuje agregację adresów unikastowych. Brak jest zestandaryzowanego rutingu anykastowego oraz mechanizmów zarządzających adresami anykastowymi. Nie opracowano procedur wyboru metryki trasy.

Niemniejsze problemy związane są z wdrażaniem usług korzystających z anykastu. Należy opracować mechanizmy wykrywania i korekcji błędnego przekierowania zgłoszenia, w tym również skierowania zgłoszenia do niewłaściwego (nieoptymalnego) serwera usług.

Projektując system anykastowy, należy uwzględnić możliwość wystąpienia zmiany serwera usług w trakcie trwania połączenia oraz konieczność zbudowania efektywnego systemu aktualizacji danych na wszystkich serwerach informacyjnych, z którymi może połączyć się użytkownik. Jednym z możliwych rozwiązań jest zaproponowana przez Autorów koncepcja systemu aktualizacji zasobów na bazie niezawodnej transmisji multikastowej, realizowanej pomiędzy wszystkimi aktywnymi serwerami usług. Nie mniej ważnym problemem jest bezpieczeństwo systemów korzystających z usług anykastowych. Dotyczy to zarówno bezpieczeństwa danych przechowywanych w serwerach usług, jak i bezpieczeństwa systemu aktualizacji zasobów.

Literatura

[1] Chodorek R.R., Pach A.R., Chodorek A.: *Koncepcja systemu aktualizacji zasobów serwerów korzystających z adresacji anykastowej*. Telekomunikacja Cyfrowa – Technologie i Usługi, tom 7, 2005

[2] Chodorek R.R., Pach A.R.: *Transmisja multikastowa w sieciach IP*. Kraków, Wydawnictwo FPT 2003

[3] *Co słychać w naszych radiostacjach*. Internetowe Forum Policyjne, wiadomość z dnia 16 czerwca 2005, godz. 09:44. URL: http://www.ifp.pl/index.php?name=PNphpBB2&file=viewtopic&p=101013&sid=cdc3b669d8572ab97ffa7fe142ca35da#101013

[4] Denning D.E.: *Kryptografia i ochrona danych*. Warszawa, Wydawnictwa Naukowo-Techniczne, 1992

[5] *Do 1000 osób zginęło w panice w Bagdadzie*. Dziennik internetowy *PAP*, informacja z dnia 31 sierpnia 2005, godz. 19:05, URL: http://dziennik.pap.com.pl/?dzial=IRAK&poddzial=WOJNA&id_depeszy=17222386

[6] Doi S., Ata S., Kitamura H., Murata M.: *IPv6 anycast for simple and effective service-oriented communications*. IEEE Communications Magazine, maj 2004

[7] Hardjono T., Dondeti L.R.: *Multicast and group security*. Boston-London, Artech House, 2003

[8] Hinden R., Deering S.: *Internet Protocol version 6 (IPv6) addressing architecture*. RFC 2373, IETF, lipiec 1998

[9] *Irak w żałobie, pogrzeby ofiar środowej paniki, rząd krytykowany*. Dziennik internetowy PAP, informacja z dnia 1 września 2005, godz. 15:59, URL: http://dziennik.pap.com.pl/?dzial=IRAK&poddzial=WOJNA&id_depeszy=17228290

[10] Jałoszyński K.: *Oblicze współczesnego terroryzmu i walka z nim w kontekście bezpieczeństwa międzynarodowego*. Zeszyty Naukowe Akademii Obrony Narodowej, nr 2(51), 2003

[11] Jałoszyński K.: *Terroryzm XXI wieku – nowe zagrożenie dla bezpieczeństwa*. Zeszyty Naukowe Akademii Obrony Narodowej, nr 1(50), 2003

[12] Jia W., Xuan D., Zhao W., *Integrated routing algoithms for anycast messages*. IEEE Communications Magazine, styczeń 2000

[13] Johnson D., Deering S.: *Reserved IPv6 subnet anycast addresses*. RFC 2526, IETF, marzec 1999

[14] *Nie ma takiego numeru, czyli na ratunek pod 112*. RMF-FM Radio Muzyka Fakty, informacja z dnia 7 sierpnia 2005, godz. 07:11, URL: http://www.rmf.fm/fakty/?id=85406

[15] *Radio listeners in panic, taking war drama as fact*. New York Times, 31 października 1938, (przedruk zamieszczony na stronie WWW: http://members.aol.com/jeff1070/wotw.html)

[16] *Ratunkowe 112 z telefonów stacjonarnych, ale z przeszkodami*. RMF-FM Radio Muzyka Fakty, informacja z dnia 19 sierpnia 2005, godz. 13:41. URL: http://www.rmf.fm/fakty/?id=85894.

[17] Weber S., Cheng L.: *A survey of anycast in IPv6 networks*. IEEE Communications Magazine, styczeń 2004

[18] *X, czyli wirus na twarzy Cheney'a*. RMF-FM Radio Muzyka Fakty, informacja z dnia 23 listopada 2005, godz. 09:58. URL: http://www.rmf.fm/fakty/?id=90408

[19] Yu S., Zhou W., Wu Y.: *Research on network anycast*. Proceedings of the IEEE 5th International Conference on Algorithms and Architectures for Parallel Processing (ICA3PP 2002), Pekin, 23-25 października 2002

Praca naukowa finansowana ze środków Komitetu Badań Naukowych w latach 2003–2005 jako projekt badawczy nr 4 T11D 015 24.

Agnieszka Chodorek ukończyła studia na Wydziale Elektrotechniki, Automatyki i Informatyki Politechniki Świętokrzyskiej w Kielcach w roku 1991. Uzyskała stopień naukowy doktora inżyniera w 2001 roku. Obecnie jest pracownikiem Samodzielnego Zakładu Telekomunikacji i Fotoniki Politechniki Świętokrzyskiej. Zainteresowania zawodowe obejmują: analizę ruchu w sieciach telekomunikacyjnych, sieci teleinformatyczne, multimedia.

Robert Chodorek ukończył studia na Wydziale Elektrotechniki, Automatyki i Informatyki Politechniki Świętokrzyskiej w Kielcach w roku 1990. Stopień doktora nauk technicznych uzyskał na Wydziale Elektrotechniki, Automatyki i Elektroniki Akademii Górniczo-Hutniczej w Krakowie w roku 1996. Obecnie jest pracownikiem Katedry Telekomunikacji AGH. Zainteresowania zawodowe obejmują: sieci teleinformatyczne, protokoły komunikacyjne, badanie wydajności protokołów, specyfikacja protokołów, aplikacje multimedialne.

Andrzej Ryszard Pach ukończył Wydział Elektrotechniki, Automatyki i Elektroniki AGH w roku 1975, w r. 1977 doktoryzował się na AGH, a w roku 1990 uzyskał stopień doktora habilitowanego na Wydziale Elektroniki Politechniki Warszawskiej. Zatrudniony jest obecnie na stanowisku profesora zwyczajnego w Katedrze Telekomunikacji AGH, w której pełni funkcję kierownika. Wcześniej był prodziekanem Wydziału EAiE.

Główne zainteresowania naukowe związane są z sieciami telekomunikacyjnymi oraz systemami informacyjnymi. Autor ponad stu publikacji naukowych z zakresu protokołów komunikacyjnych, modelowania i analizy sieci komputerowych, sieci szerokopasmowych z integracją usług. Aktywnie uczestniczy w projektach europejskich IST, ACTS, COST i COPERNICUS. Członek komitetów programowych konferencji międzynarodowych. Konsultant firm państwowych i prywatnych w zakresie nowoczesnej telekomunikacji.

Współzałożyciel i wiceprezydent Fundacji Postępu Telekomunikacji, przewodniczący IEEE Communications Society Chapter.