KONCEPCJA DIAGNOZOWANIA BEZPIECZEŃSTWA SIECI TELEINFORMATYCZNEJ

Dariusz LASKOWSKI

Wojskowa Akademia Techniczna, Wydział Elektroniki, Instytut Telekomunikacji
00-908 Warszawa, ul. Gen. S. Kaliskiego 2,
tel.: (+48)(22) 683 73 53, fax: (+48)(22) 683 90 38, email: dlaskowski@wset.edu.pl

Streszczenie

W artykule tym zawarto najważniejsze elementy koncepcji stanowiska do badania bezpieczeństwa sieci teleinformatycznej tj.: protokoły komunikacyjne, oprogramowanie systemowe stanowiące integralną część sieci z realizują usług zabezpieczenia mających na celu przeciwdziałanie szkodliwym oddziaływaniom destruktora. Koncepcja ta umożliwia badanie bezpieczeństwa dla protokołów IPv4 i IPv6 przez zestawienie w warunkach laboratoryjnych zintegrowanego stanowiska badawczego zapewniającego otrzymanie wyników charakteryzujących się wysokim poziomem obiektywności i wiarygodności, dotyczących oceny stosowanych lub projektowanych praktycznych rozwiązań dla systemu bezpieczeństwa.

Słowa kluczowe: system teleinformatyczny, diagnostyka komputerowa, narzędzia diagnostyczne.

DIAGNOSING TEST BED OF NETWORK SECURITY

Summary

In this paper the most important test bed conception elements used for network security tests were shown i.e. communication protocols, system software as an integral part of the network used for counteracting for damaging destructor. This conception makes possible security research for IPv4 and IPv6 by integrated test bed, matched in the laboratory conditions. This test bed guarantees getting high level objectivity and reliable results. Results estimate, used or developed, practical solutions for security system.

Keywords: network, security, computer diagnostic, diagnostic tool.

WSTĘP

Współczesne, eksploatowane sieci teleinformatyczne *STI* są podstawowym medium transmisyjnym zapewniające wiarygodny i terminowy obiegu informacji. Z praktycznych obserwacji wynika, że wiarygodność jest głównym z kryteriów oceny poprawności funkcjonalnej sieci uzyskiwanej przez zapewnienie wymaganego poziomu bezpieczeństwa przekazywanych informacji pomiędzy użytkownikami sieciowymi. Dlatego też, uwzględniając swobodny przepływ informacji i wielokryterialny dostęp do zasobów sieci, adekwatnie do zaistniałej sytuacji reagować należy na oddziaływania destrukcyjne.

Waga tego problemu jest duża, zarówno dla kablowych (*LAN, WAN*, itp.) jak i dla bezprzewodowych (*WLAN*) sieci radiowych wykorzystujących protokół komunikacyjny IP (ang. *Internet Protocol*). Szczególnym wariantem są *WLAN'y*, gdyż zagrożenia dla informacji przekazywanej za pomocą łączy radiowych przyjmują zmienne formy, a ich wynikiem może być np.: utrata prywatności, zniszczenie lub modyfikowanie własnych baz danych, itp. W większości przypadków powoduje to zmniejszenie poziomu efektywności wykorzystania potencjalnych zasobów *STI*, poprzez straty różnych danych w organizacji lub ujawnienia informacji objętych tajemnicą (np. przemysłową).

Dlatego też za celowe uważa się, zamodelowanie koncepcji stanowiska badawczego uwzględniającego zmienność aplikacji systemowych. Stanowisko tego typu może zostać wykonane w oparciu zdefiniowany zbiór stacji sieciowych wzajemnie połączonych relacjami komunikacyjnymi. Przy realizacji przyjętej metodyki diagnozowania, w warunkach laboratoryjnych, można zestawić zintegrowane stanowisko badawcze umożliwiające otrzymanie wyników charakteryzujących się wysokim poziomem obiektywności i wiarygodności, dotyczących oceny stosowanych lub projektowanych praktycznych rozwiązań dla systemu bezpieczeństwa [1].

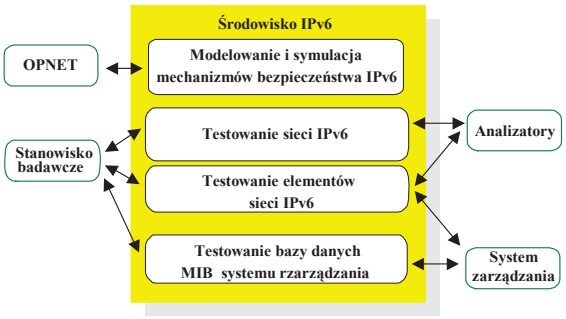
1. ZAŁOŻENIA NA *SDB STI*

Pod pojęciem stanowiska diagnozowania bezpieczeństwa sieci teleinformatycznej (*SDB STI*) są rozumiane zaimplementowane protokoły, oprogramowanie na powszechnego użytku komponentach teleinformatycznych, które stanowiąc integralną część sieci i realizując usługi ochrony mają na celu przeciwdziałanie zagrożeniom. Stanowisko badawcze będzie być wykorzystanie do realizacji następujących zagadnień:

- analizy budowy strukturalnej, zasad działania, stosowanych protokołów komunikacyjnych w oferowanych rozwiązaniach systemów bezpieczeństwa,
- badania możliwości i zakresu współdziałania systemów bezpieczeństwa,
- oceny przydatności rozwiązań mechanizmów bezpieczeństwa w określonych zastosowaniach,
- oceny rozwiązań technicznych, doboru protokołów komunikacyjnych oraz efektywności sieci transmisji danych dla potrzeb systemu bezpieczeństwa,
- weryfikacji architektury fizycznej, funkcjonalnej i informacyjnej projektowanych rozwiązań systemów bezpieczeństwa.

Funkcjonalnie stanowisko badawcze (Rys. 1) będzie obejmowało następujące aspekty badawcze:

- praktyczną ocenę systemów bezpieczeństwa,
- modelowanie i symulację.



Rys. 1. Organizacja funkcjonalna stanowiska badawczego protokołu IP [1]

W koncepcji zamierza się wykorzystać elementy procesu modelowania i symulacji z szeregiem narzędzi do projektowania i analizy systemów łączności. Jako podstawowe narzędzie proponuje się w tym profesjonalne oprogramowanie *OPNET* firmy *Opnet Technologies*. Jest ono wykorzystywane przez światową czołówkę producentów systemów teleinformatycznych, służące do projektowania i modelowania oraz analizy systemowej.

Zadaniem zespołu projektującego stanowisko będzie realizacja prac naukowo-badawczych związanych z oceną bezpieczeństwa funkcjonowania protokołu *IP* (np. wersji 4 lub wersji 6) w oparciu ukompletowanie laboratorium. Wybór wersji to zasadniczy problem ze względu na znaczenie każdego z wymienionych protokołów we współczesnych *STI*. W głównej mierze od niego będzie zależało bezpieczeństwo, przeżywalność oraz terminowość przenoszonych informacji między komponentami sieci.

Ze względu na poziom trudności i liczbę uwarunkowań początkowych oraz protokołów IPv6 proponuje się, aby *SDB STI* obejmowało następujące elementy:

- model sieci rzeczywistej, w której zostanie zaimplementowany protokół *IPv6*,
- aplikacje monitorujące ruch w *STI*;
- aplikacje symulacyjne w środowisku *OPNET* w którym, w miarę potrzeb analizowane będą mechanizmy zabezpieczeń oraz (w miarę możliwości) wykorzystane zostaną dane z systemu zarządzania siecią i z aplikacji monitorujących ruch telekomunikacyjny [1].

2. MODEL RZECZYWISTEJ *STI*

Model rzeczywistej *STI* zrealizowany zostanie w środowisku rozległym z możliwością implementacji tuneli szyfrowych lub szyfratorów IP. Do celów trasowania ruchu zastaną wykorzystane routery, których aplikacje zostały zaimplementowane na bazie komputerów, wyposażonych w odpowiednią liczbę i typ kart komunikacyjnych. W związku z koniecznością optymalizacji kosztów przeznaczonych na badania oraz uniwersalnością rozwiązania proponuje się:

- osadzenie aplikacji trasujących w środowisku systemu operacyjnego *Linux* posiadającego mechanizmy *IPv6*,
- w podsieciach wymieniających wiadomości zainstalowanie urządzeń monitorujących ruchu pakietów i zasadniczych elementów systemu zarządzania.

Powyższe mechanizmy zapewnią zbieranie wiadomości przepływających w sieci oraz możliwość ich wykorzystania w modelach symulacyjnych a także w badaniach mechanizmów bezpieczeństwa *IPv6*.

Lokalne podsieci komputerowe zaimplementowane zostaną z wykorzystaniem rozwiązań przeznaczonych dla stacjonarnych i mobilnych komponentów sieci. Utrudnieniem jest wykorzystanie rozwiązania *WLAN*, które z jednej strony posługują się mechanizmami roamingu firm implementujących daną aplikację a z drugiej mechanizmami *Mobile IP* dostępnych w ramach *IPv6*. Uważa się, że powyższe uwarunkowania umożliwią analizę mechanizmów uwierzytelnienia informacji implementowanych w sieciach mobilnych.

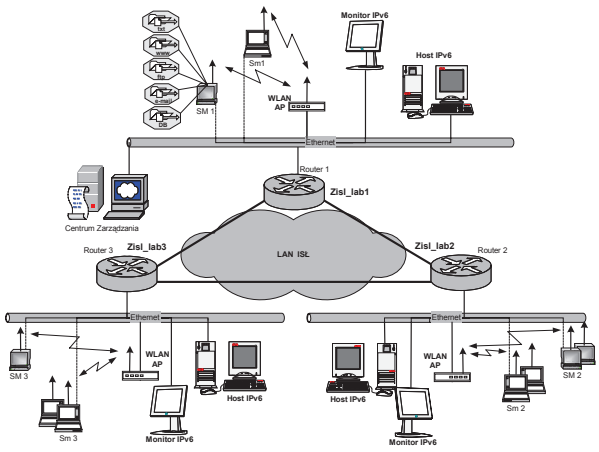
Wiadomości wymieniane w ruchu telekomunikacyjnym zbierane będą w sieci przez osadzone monitory sieci IP oraz będą przechowywane w celu dalszej ich analizy. Aplikacje zarządzania sieciami *IP* będą zbierać i przechowywać informacje zarządzania, które zapewnią analizę mechanizmów bezpieczeństwa

wykorzystanych w sieci *IPv6*. Przykładowe wykorzystanie dostępnych urządzeń zostało przedstawione na poniższym rysunku (Rys. 2.).

Element symulacyjny stanowiska do badania bezpieczeństwa protokołu *IPv6* wykorzystany zostanie w celu implementacji mechanizmów bezpieczeństwa w środowisku symulacyjnym. W aplikacji *OPNET* zaimplementowane zostaną elementy bezpieczeństwa wymagające dodatkowych badań.

SDB STI badawcze systemów zarządzania będzie miało za zadanie praktyczną ocenę implementacji systemów bezpieczeństwa w *IPv6*. Realizacja tego procesu będzie możliwa poprzez wykorzystanie modelu sieci złożonej z następujących komponentów:

- lokalnej sieci komputerowej zbudowanej ze stanowisk umożliwiających implementację badanych systemów bezpieczeństwa i zarządzania lub jej elementów,
- dodatkowych stanowisk do monitorowania i analizy komunikacji między elementami sieci oraz do zbierania i analizy danych pochodzących od zarządzanych elementów.



Rys. 2. Wykorzystanie zasobów laboratoryjnych

Istotnymi elementami będą stanowiska do monitorowania i analizy komunikacji między elementami sieci. Będą je stanowić komputery wyposażone w aplikacje realizujące proces gromadzenia i analizy wymiany danych pomiędzy elementami sieci *IPv6*. Praca stanowiska będzie odbywać się w dwóch trybach:

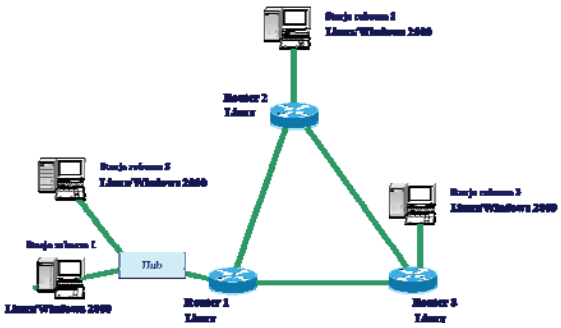
- „*on-line*" z kontrola komunikacji między aplikacjami bezpieczeństwa,
- „*off-line*" z gromadzeniem wymienianych danych i późniejsza ich analiza.

3. OPRACOWANIE I REALIZACJA MODUŁU DOŚWIADCZALNEGO *STI IPv6*

Aby możliwe było badanie bezpieczeństwa sieci w warunkach rzeczywistych, koniecznym staje się zbudowanie miarodajnego i wiarygodnego fragmentu sieci, w którym znajdowałyby się zarówno elementy wykorzystywane przez użytkowników końcowych, jak również urządzenia sieciowe realizujące kierowanie ruchu w sieci. Z punktu widzenia bezpieczeństwa protokołu komunikacyjnego *IPv6* nie są ważne rozmiary geograficzne sieć, lecz realizacja zdefiniowanych usług sieciowych oferowanych uprawnionym użytkownikom sieciowym z wykorzystaniem *IPv6*. Sieć taka powinna również zawierać fragment sieci rozległej *IPv6* z mechanizmami routin'gu dynamicznego lub statycznego. Wobec powyższego powstała koncepcja budowy takiej sieci wygląda następująco (Rys. 3.) [1].

3.1. Moduł doświadczalny STI IPv6

Routery sieci rozległej zbudowane zostaną z wykorzystaniem platformy sprzętowej klasy *PC* oraz systemu operacyjnego *Linux* i *Windows XP*. Tego typu wybór podyktowany został zarówno kosztami budowy sieci (ekonomiczność) oraz rosnącą popularnością systemu *Linux*, a przede wszystkim dostępnością kodu źródłowego całego systemu.



Rys. 3. Koncepcja budowy modułu doświadczalnego sieci opartej na stosie protokołów IPv6

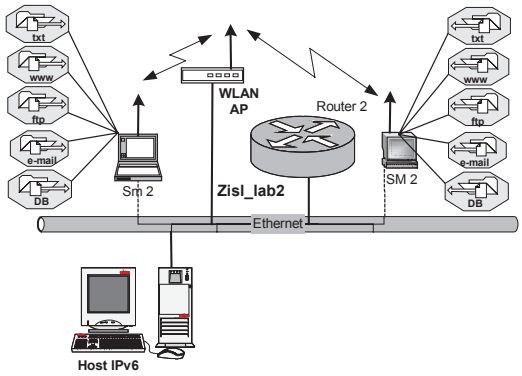
W jednej z podsieci zainstalowany zostanie serwer podstawowych usług sieciowych, które będą głównym źródłem ruchu w sieci.

Przykładowe pojedyncze stanowisko badawcze (Rys. 4, rys. 5) składa się z:

- routera (*Zisl_lab2*),
- punktu dostępowego (*WLAN AP*),
- dwóch stacji roboczych.

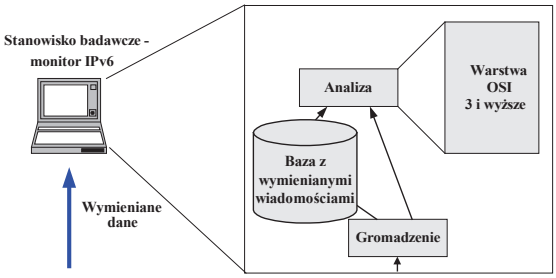
Dla potrzeb realizacji postawionego zadania wszystkie stacje robocze zostały podzielone na dwa zbiory:

- stacji roboczych (*SM X*) na bazie stacjonarnego komputera klasy *PC*,
- stacji roboczych (*Sm X*) na bazie mobilnego komputera (*laptopa*).



Rys. 4. Stanowisko badawcze – analizator

Aby nie wprowadzać zbędnych liczby obiektów przedstawiono tylko po jednej jednostce stacji dla dwóch typów. Zasadniczy dostęp do zasobów sieci odbędzie się poprzez łącze radiowe z wykorzystaniem punktu dostępowego[1]. Jako dodatkowa możliwość (opcjonalnie) będzie możliwe zastosowanie łącza kablowego. Jest to pewnego rodzaju wariantowość rozwiązania, która może być wykorzystana do analizy otrzymanych wyników i ewentualnie dla porównawczych celów statystycznych.



Rys. 5. Schemat blokowy analizatora

3.2. Bezpieczeństwo *STI IPv6*

Do podstawowych wymagań dotyczących bezpieczeństwa w sieci z wykorzystaniem *IPv6* należy zaliczyć:

- w zakresie elementów sieci:
  - określenie wyboru platformy sprzętowej, budowy i rozwoju aplikacji bezpieczeństwa w modelu sieci (dotyczy to systemu operacyjnego i oprogramowania elementów sieci, na którym aplikacje *IPv6* będą osadzane),
  - elementy powinny zostać wyposażone w aplikacje z zaimplementowanymi funkcjonalnościami bezpieczeństwa,
  - elementy sieciowe powinny zostać wyposażone w odpowiednie aplikacje zarządzania;
  - routery sieci powinny zostać wyposażone w dostępne aplikacje i oprogramowanie bezpieczeństwa zaimplementowane na protokole *IPv6*,
- w zakresie aplikacji monitorowania:
  - określenie wyboru aplikacji monitorowania (lub języka programowania, który zostanie wykorzystany do budowy aplikacji stanowiska badawczego bezpieczeństwa),
  - stanowisko badawcze powinno być zbudowane warstwowo zgodnie z modelem definiowanym przez *IETF*,
- w zakresie aplikacji zarządzania:
  - elementy sieci powinny zostać wyposażone w dostępne aplikacje i oprogramowanie zarządzania, które zaimplementowano z wykorzystaniem protokołu *IPv6*;
  - aplikacja centrum zarządzania powinna być wyposażona w mechanizmy umożliwiające współpracę z sieciami *IPv6*.

Uwzględniając ewolucję mechanizmów związanych z *IPv6*, praktyczne implementacje tego protokołu określane są mianem implementacji testowych. Najchętniej wykorzystuje się aplikacje funkcjonujące pod *Linux'em*, choć protokół ten zaimplementowany został również w *Windows XP* oraz jako dodatek w systemie *Windows NT* oraz *Windows 2000*.

Analiza przeprowadzona w ramach niniejszej pracy wskazuje na to, że istnieje kilka odmian implementacji protokołu *IPv6* dla *Linux'a* zależnych od ośrodek badawczego zajmującego się testowaniem i implementacją *IPv6*.

Podstawowym celem jest koncepcja projektu stanowiska do badania bezpieczeństwa protokołu *IPv6* oraz identyfikacja potencjalnych wad tego protokołu w zakresie bezpieczeństwa przesyłanych informacji. Dlatego też należy w jak największym stopniu wykorzystać istniejące implementacje do praktycznej weryfikacji. Również badanie bezpieczeństwa protokołu z wykorzystaniem fizycznej infrastruktury jest bardziej wiarygodne niż teoretyczne rozważania, czy też eksperymenty symulacyjne przeprowadzone na modelach symulacyjnych.

Dlatego też proponuje się, nie powielanie badań symulacyjnych i wykorzystanie aplikacji testowych. Celowym jest także uzupełnienie stanowiska badawczego o modele symulacyjne elementów, które nie zostały zaimplementowane w fizycznych systemach operacyjnych. Przykładem takich elementów są aplikacje stanowiące rozszerzenie protokołu *IPv6* o część mobilną (tzw. *Mobile IPv6*), lecz ogólnie dostępne oprogramowanie nie funkcjonuje stabilnie. Uwzględniając powyższe sugeruje się konieczność zbudowania modeli symulacyjnych sieci z protokołem *Mobile IPv6* będących uzupełnieniem biblioteki standardowych

[1] Dostęp do sieci *Ethernet* jest możliwy poprzez dowolny *WLAN AP*.

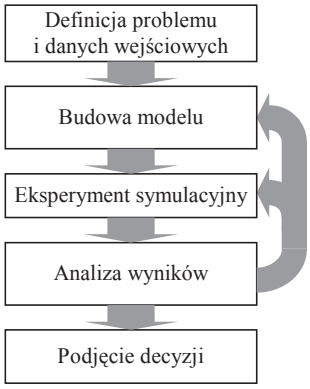
modeli *OPNET'a*. Zbudowane modele oparte będą na powszechnie dostępnych zaleceniach *IETF* oraz dokumentach tymczasowych *IETF* (*IETF drafts*) [8], a także na publikacjach z zakresu bezpieczeństwa protokołu *IPv6* oraz *Mobile IPv6* [11].

3.3. Pakiet symulacyjny OPNET

Optimized Network Engineering Tool to zoptymalizowane narzędzie inżynierii sieci, obecnie wykorzystywane w około 500 firmach branży: telekomunikacyjnej, lotniczej, komputerowej, łączności, multimedialnej i innych. (ALCATEL Network Systems, Aerospace Corporation, Boeing, DEC, Ericsson, General Electric, NASA, Motorola). Dziedziny zastosowań pakietu obejmują między innymi:

- modelowanie standaryzowanych sieci *LAN*, *MAN*, *WAN* i ich analizę pod względem wydajności,
- planowanie połączeń międzysieciowych (ang. *internetworking*),
- badania nad nowymi architekturami i protokołami komunikacyjnymi,
- analizę wydajności nowych technologii łączy,
- badania systemów czasu rzeczywistego np. systemy sterowania i pokładowe,
- zarządzanie zasobami (np. sieci, systemu komputerowego),
- badania systemów radiokomunikacji ruchomej,
- projektowanie sieci satelitarnych,
- projektowanie systemów łączności specjalnej np. służb celnych, wojskowych (rys. 6).

Bardzo obszerne i rozbudowane środowisko programowe pakietu szczególnie predysponuje go do modelowania, symulacji i analizy wydajności dużych i bardzo dużych sieci telekomunikacyjnych, systemów komputerowych oraz systemów rozproszonych.



Rys. 6. Schemat blokowy algorytmu *OPNET'a*

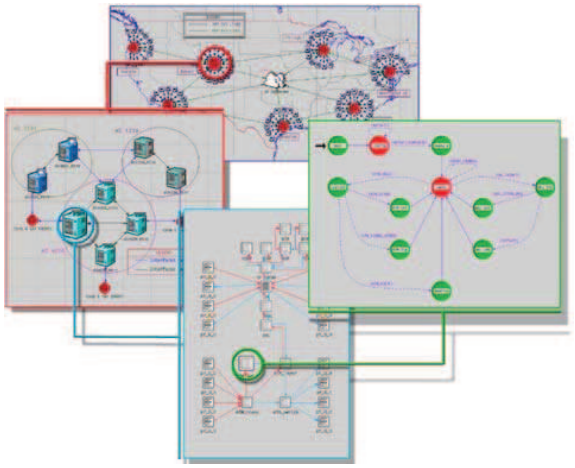
Obecnie na rynku oferowane są dwie wersje pakietu podstawowa i wzbogacona tzw. *Modeler / Radio*. Wersja podstawowa umożliwia symulację systemów stacjonarnych. Bogata biblioteka zawiera standardowe modele wykorzystywane w symulacji. Modele te obejmują m.in.: architektury sieci, topologie, protokoły komunikacyjne, węzły sieci, kolejki, przetwarzanie informacji itd. Jako przykłady sieci i protokołów, których modele zawarto w bibliotece wymieńmy: *ETHERNET, TOKEN RING, FDDI (Fiber Distributed Data Interface), ISDN (Integrated Services Digital Network), B-ISDN (Broadband ISDN), ATM (Asynchronous Transfer Mode), HSSB (High-Speed Serial Bus), LAPB (Link Access Protocol Balanced), X-25, IP (Internet Protocol), TCP (Transmission Control Protocol)*. W miarę pojawiania się nowych technologii producent czuwa nad użytkownikami pakietu i udostępnia nowe modele. Istnieje również model sieci *IPv6*, który niestety wymaga dodatkowych licencji. Ze względu jednak na ograniczenia finansowe niniejszej pracy, nie możliwe jest pozyskanie tego modelu. Dlatego też, dla potrzeb pracy, autorzy zdecydowali się na wykonanie własnych elementów bibliotecznych *IPv6*.

W wersji *Modeler/Radio* dostępne są narzędzia do modelowania łączy radiowych i ruchomych węzłów telekomunikacyjnych. Istotną różnicą w porównaniu do wersji podstawowej jest to, że modele sieci muszą uwzględniać aktualne położenie węzła w przestrzeni trójwymiarowej oraz określenie trajektorii po, której będzie poruszał się dany obiekt. Modele te zawierają szereg parametrów istotnych do modelowania tego typu systemów np. częstotliwość nadajnika, jego pasmo, moc, warunki przestrzenne dla emitowanego sygnału oraz charakterystyki anten. Standardowo zaimplementowane współczynniki np. wykorzystania kanału, sygnał-szum, czułości odbiorników są niezwykle pomocne w analizie otrzymanych wyników metodą symulacji.

OPNET posiada zaawansowany graficzny interfejs użytkownika pracujący w środowisku *X Windows* oraz *NT*, *2000*. Program dostępny jest na większość znanych platform sprzętowych m.in.: SUN, DEC, HP, oraz Silicon Graphics. W skład pakietu wchodzi 8 głównych narzędzi przeznaczonych do:

- modelowania systemów,
- definiowania parametrów symulacji,
- sterowania procesem symulacji,
- analizy otrzymanych wyników.

Podstawowymi narzędziami są edytory graficzne zorientowane obiektowo (*Network Editor, Node Editor oraz Process Editor*) umożliwiające definiowanie topologii oraz architektury systemów (rys. 7).



Rys. 7. Modelowanie w narzędziu *OPNET*

Narzędzie to umożliwiają użytkownikowi intuicyjne przejście od rzeczywistego lub projektowanego systemu do jego modelu symulacyjnego. Edytory są ukierunkowane na definiowanie modelu adekwatnym do odpowiedniego poziomu np.: sieci, węzła i procesu. Użytkownik ma więc możliwość zdefiniowania bardzo ogólnych elementów projektowanego systemu (np. położenia geograficznego sieci), podsieci czy węzła jak również elementów bardzo szczegółowych (np. protokołów komunikacyjnych), procesów i zadań realizowanych na poszczególnych stacjach w ramach określonego węzła. Takie hierarchiczne podejście zaprezentowane w pakiecie ułatwia specyfikację i prezentację dużych i złożonych sieci, ułatwiając projektowanie od ogółu do szczegółu.

Po przygotowaniu wszystkich niezbędnych elementów modelu plan eksperymentu symulacyjnego tworzony jest przy użyciu narzędzia zwanego *Simulation Tool*. Jego interfejs graficzny zbliżony do arkusza kalkulacyjnego, pozwala w wygodny sposób zaplanować m.in.: czasy symulacji, liczbę przebiegów, dane wejściowe oraz wyjściowe, oraz określić nazwy plików dla składowanych wyników.

Program symulacyjny w *OPNE'cie*, jest generowany w języku *C*. Proces kompilacji programu jest prowadzony automatycznie przez program lub wsadowo przez użytkownika pakietu. Ta druga możliwość zapewnia dołączanie własnych bibliotek symulacyjnych do wygenerowanego kodu programu.

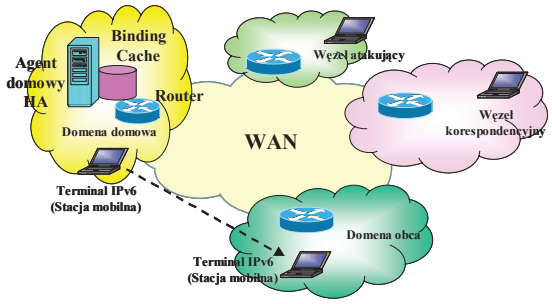
3.4. Założenia modelu symulacyjnego *STI*

Celem symulacji komputerowej jest analiza bezpieczeństwa protokołu *Mobile IPv6* oraz identyfikacja potencjalnych zagrożeń wynikających z możliwości ataków na bezpieczeństwo protokołu *IPv6*. W związku z tym, model symulacyjny systemu wykorzystującego *IPv6* powinien uwzględniać wszystkie te elementy, które mają bezpośredni wpływ na bezpieczeństwo *IPv6*, a symulacja komputerowa powinna pozwalać na badanie tego bezpieczeństwa. W tym celu niezbędne jest przyjęcie szeregu założeń do modelowania.

Załóżmy zatem, że obiektem modelowania jest sieć składająca się z następujących elementów [14], [15]:

- terminala *IPv6*,
- routera *IPv6*,
- węzła korespondencyjnego *IPv6*,
- sieci rozległej *WAN*,
- węzła atakującego.

Powyżej wymienione elementy tworzą szkielet struktury sieci wykorzystany do wykonania modeli symulacyjnych (rys. 8).



Rys. 8. Sieć IPv6 – założenia

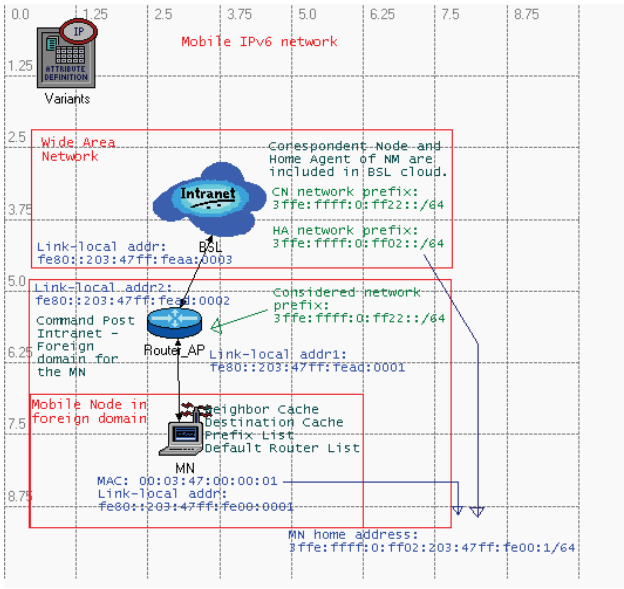
Ze względu na cel pracy i wieloaspektowość, zdecydowano się na uproszczenia, które pozwoliły na zmniejszenie modelu, do których zaliczono:

- brak dokładnego odwzorowania sieci rozległej *WAN*,
- wartości opóźnienia pakietów przechodzących przez sieć *WAN* określono z uwzględnieniem rozkładów ich prawdopodobieństw wystąpienia,
- nie odwzorowuje się trajektorii ruchu terminali mobilnych, a tylko moment pojawienia się terminala w domenie obcej,
- przyjmuje się, że terminal korespondencyjny, agent domowy oraz terminal atakujący znajdują się w oddzielnych podsieciach,
- nie rozpatruje się ataków z wnętrza sieci, w której znajduje się rozpatrywany terminal ruchomy *IPv6*.

Przyjmuje się również, że terminale w sieci dokonują konfiguracji adresów globalnych oraz adresów typu „*link-local*" automatycznie, na podstawie wiadomości rozgłoszeniowych wysyłanych przez routery (mechanizm *Neighbor Discovery* [9]) oraz na podstawie zdefiniowanych adresów *MAC* [2] - [4].

Przykładowy model sieci zgodny z przyjętymi założeniami został zaprezentowany na rysunku (rys. 9). Terminal mobilny, oznaczony na rysunku przez „*MN*" zamodelowany jest jako węzeł na stałe dołączony do routera (węzła dostępowego) oznaczonego na rysunku jako „*Router_AP*". Router ten odwzorowuje węzeł znajdujący się w domenie obcej. Router dostępowy dołączony jest do sieci rozległej oznaczonej jako „*BSL*". Agent domowy

(w rzeczywistości implementowany w routerach *IPv6*), węzeł korespondencyjny oraz węzeł atakujący zamodelowany został jako integralna część sieci rozległej BSL.



Rys. 9. Model sieci Mobile IPv6

Zatem, nie będzie symulowane ciągłe przemieszczanie się terminala mobilnego, lecz:

- moment pojawienia się tego terminala w domenie obcej,
- procedury zarządzania mobilnością szczególnie narażone na atak.

Z uwagi na fakt przyjęcia zasady otwartości i uniwersalności, model sieci a także modele poszczególnych jej elementów, zawierają moduły rozszerzeń modelu o dodatkowe, niestandardowe funkcje. Moduły te, aczkolwiek widoczne na rysunkach, nie zostaną uszczegółowione w kolejnych artykułach i nie będą tutaj komentowane.

Proces symulacji powinien być realizowany do momentu, gdy czas symulacyjny osiągnie czas końca symulacji lub zebrana zostanie wymagana liczba próbek zapisanych w statystykach wynikająca z założonego błędu statystycznego. W tym czasie okresowo następuje zmiana domeny obcej przez stację mobilną. Każde przesłanie wiadomości zarządzania mobilnością (*BU*, *BA*) związane jest z uruchomieniem procedur bezpieczeństwa w węzłach pośrednich, tj. obliczanie funkcji skrótu (*Hush Function*) wg *MD5*.

WNIOSKI

Przedstawiony, w ogólnym zarysie, model stanowiska diagnozowania bezpieczeństwa sieci teleinformatycznej, może zostać zastosowany do prowadzenia eksperymentów naukowo-badawczych oszacowujących poziom bezpieczeństwem protokołu komunikacyjnego. Kolejnym etapem działań badawczych będzie:

- identyfikacja możliwych ataków do wystąpienia na sieć *IPv6* na podstawie dostępnych publikacji [11]-[13],
- metodyka wykonania eksperymentów symulacyjnych,
- wykonanie symulacji komputerowych.

Pod uwagę bierze się również możliwość rozbudowy modelu o elementy, które mogą być niezbędne do realizacji specyficznych eksperymentów. Powszechnie jest bowiem wiadomo, że z dnia na dzień powstają nowe, coraz to bardziej wyrafinowane, metody ataku na bezpieczeństwo technologii internetowych, których wcześniej nie można było przewidzieć.

LITERATURA

[1] PBS 643: *Stanowisko do badania bezpieczeństwa protokołu komunikacyjnego IP wersja 6, Sprawozdanie roczne z realizacji pracy badawczej*.
[2] RFC2373, *IP Version 6 Addressing Architecture.*
[3] RFC2374, *An IPv6 Aggregatable Global Unicast Address Format.*
[4] RFC 2462, *IPv6 Stateless Address Autoconfiguration.*
[5] RFC2401, *Security Architecture for the Internet Protocol.*
[6] RFC2402, *IP Authentication Header.*
[7] RFC2406, *IP Encapsulating Security Payload (ESP).*
[8] RFC2460, *Internet Protocol, Version 6 (IPv6).*
[9] RFC2461, *Neighbor Discovery for IP Version 6 (IPv6).*
[10] Draft-ietf-mobileip-ipv6-15, *Mobility Support in IPv6.*
[11] Draft-aura-mipv6-bu-attacks-01, *MIPv6 BU Attacks and Defenses.*
[12] Draft-ietf-mobileip-mipv6-ha-ipsec-01: *Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents*
[13] Tuquerres G., Salvador M. R., Sprenkels R., *Mobile IP: Security & Application.*
[14] Amanowicz M., Krygier J., Jarmakiewicz J., Maslanka K., *Mobility Management In IPv6 Tactical Networks*, Proceedings of MILCOM 2002, Anaheim USA, October 2002.
[15] Bednarczyk M., Jarmakiewicz J., Krygier J., *The Tactical Intranet IPsec Security Concept*, RCMCIS2002, Zegrze, October 2002.

Dr inż. **Dariusz LASKOWSKI** w 1997 roku ukończył Wydział Elektroniki Wojskowej Akademii Technicznej, gdzie obecnie pracuje w Instytucie Telekomunikacji na stanowisku asystenta naukowo - dydaktycznego. Członek *Polish Safety and Reliability Association*, stopień doktora nauk technicznych otrzymał w dyscyplinie telekomunikacja o specjalność sieci teleinformatyczne. Autor publikacji krajowych i zagranicznych, współwykonawca sześciu prac naukowo-badawczych oraz autorskich opracowań *Programu Zapewnienia Niezawodności* dedykowanych urządzeń i systemów łączności.