Kraków, 15.12.2016 r.

Raport zawierający wyniki realizacji projektu

Poddziałanie 1.3.2

1. DANE O PROJEKCIE
NR UMOWY O DOFINANSOWANIE: .... WND-POIG.01.03.02-12-010/12.....
TYTUŁ PROJEKTU: . Przygotowanie zgłoszenia patentowego i objęcie ochroną patentową wynalazku FAMTAR.....
DATA ROZPOCZĘCIA REALIZACJI PROJEKTU[1]: …01.10.2012 r……..
DATA ZAKOŃCZENIA REALIZACJI PROJEKTU[2]: …30.09.2015 r…….

W ramach realizacji projektu przeprowadzono szereg prac badawczo-rozwojowych, w wyniku których opracowano dwa zgłoszenia patentowe. Pierwsze zgłoszenie dotyczy mechanizmu FAMTAR (Flow-Aware Multi-Topology Adaptive Routing, zorientowany na przepływy adaptacyjny ruting oparty na wielu topologiach), który pozwala na realizację rutingu wielościeżkowego w sieciach IP. Drugie zgłoszenie dotyczy mechanizmu agregacji przepływów pozwalającego na polepszenie skalowalności mechanizmu FAMTAR.

Prace badawcze dotyczyły głównie analizy opracowanych rozwiązań pozwalających na wielościeżkową transmisję ruchu w sieciach IP oraz agregację przepływów. Dodatkowo analizie zostały poddane istniejące rozwiązania związane z tematyką badaną w trakcie realizacji projektu.

Zorientowany na przepływy adaptacyjny ruting oparty na wielu topologiach

[1] Zgodnie z umową uwzględniającą wszystkie aneksy.
[2] Zgodnie z umową uwzględniającą wszystkie aneksy.

FAMTAR pozwala na ustalenie tras transmisji ruchu w sposób inteligentny w oparciu o aktualne poziomy obciążenia łączy, w wyniku czego możliwe jest efektywne wykorzystanie dostępnych zasobów w sieci.

W sieciach IP podstawowym elementem jest ruter służący m.in. do wyznaczania tras. W obecnie używanych ruterach do wyznaczenia interfejsu wyjściowego dla obsługiwanego pakietu stosowana jest tablica rutingu, która zawiera informacje przechowywane w pamięci rutera, a mianowicie spis wskazujący, przez które sąsiadujące z ruterem węzły sieci prowadzi trasa do sieci docelowych.

W mechanizmie FAMTAR założyliśmy dodanie w ruterze tablicy przekazywania pakietów (ang. Flow Forwarding Table (FFT)). Wpisy w tablicy FFT są ustalane na podstawie tablicy rutingu. Tablica rutingu składa się z wpisów umożliwiających wysyłanie przychodzących do rutera pakietów do każdej sieci lub podsieci docelowej i jest zapisywana i utrzymywana w pamięci fizycznej rutera. Typowy wpis w tablicy rutingu zawiera adres podsieci docelowej, metrykę oraz identyfikator bądź adres interfejsu wyjściowego, przez który dana podsieć jest osiągalna. Regułą jest, że w tablicy rutingu znajduje się tylko jeden, najbardziej korzystny wpis dla każdej z podsieci docelowych.

W mechanizmie FAMTAR przychodzące do rutera pakiety reprezentujące przepływy są analizowane, a następnie kierowane na interfejs wyjściowy zgodnie z wpisami umieszczonymi w Tablicy Przekazywania Przepływów (ang. Flow Forwarding Table, FFT), która jest nowym elementem rutera. W przypadku braku odpowiedniego wpisu dla konkretnego przepływu w tablicy FFT, ruter dodaje przepływ do listy FFT, a interfejs wyjściowy jest pobierany z aktualnej tablicy rutingu.

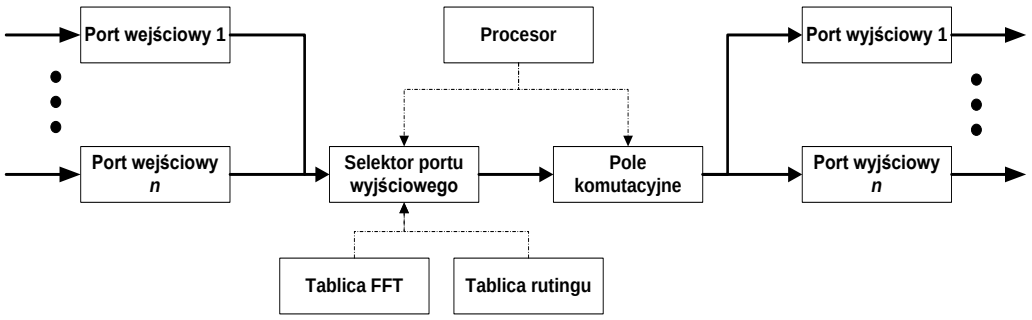
FAMTAR korzysta z popularnego obecnie postrzegania ruchu w sieciach IP za pomocą koncepcji przepływów. Chociaż pojęcie przepływu jest znane i różnie definiowane w literaturze, zawsze jest to strumień danych należących do jednego połączenia pomiędzy dwoma użytkownikami, czy aplikacjami. Identyfikator przepływu może być ustalony zgodnie ze znanymi ze stanu techniki sposobami i nie ma to wpływu na działanie rutera według wynalazku.

Istotą mechanizmu FAMTAR jest sposób sterowania przepływami w sieci, polegający na wyznaczaniu interfejsu wyjściowego dla danego pakietu za pomocą tablicy FFT oraz na tym, że wpisy w tablicy FFT umieszczane są w momencie

pojawienia się nowego przepływu i nie są zmieniane, gdy zmieniają się wpisy w tablicy rutingu.

Ruter to urządzenie sieciowe pracujące w trzeciej warstwie modelu OSI. Ruter służy do łączenia sieci komputerowych – pełni w ten sposób funkcję węzła komutacyjnego.

Sposób implementacji mechanizmu FAMTAR jest przedstawiony na Rys. 1.



Rys. 1. Schemat rutera realizującego koncepcję FAMTAR

Ruter składa się z portów wejściowych, selektora portu wyjściowego, pola komutacyjnego, tablicy rutingu, procesora oraz portów wyjściowych. Każdy pakiet przychodzący do rutera jest analizowany. Selektor portu wyjściowego ustala, na podstawie danych pobranych z tablicy rutingu, na który interfejs wyjściowy należy przesłać dany pakiet i przekazuje tę informację do pola komutacyjnego, które przenosi pakiet na odpowiedni port wyjściowy. Pracą selektora portu wyjściowego oraz pola komutacyjnego steruje procesor.

Elementem każdego rutera jest tablica rutingu, która zawiera informacje o tym, na który interfejs trzeba przesłać pakiet mający konkretny adres docelowy. Tablica rutingu jest więc sprawdzana dla każdego przychodzącego pakietu - dla każdego pakietu odczytywany jest numer interfejsu wyjściowego. Jeżeli w sieci wystąpią jakiekolwiek zmiany (np. awarie, nowe dostępne podsieci, łącza, zmiana polityki rutingu itp.) tablica rutingu zostaje uaktualniona. Uaktualnienie tablicy rutingu ma wpływ tylko na te pakiety, które pojawią się po aktualizacji.

Nowym elementem rutera (w stosunku do tradycyjnie używanych ruterów IP), którego schemat jest przedstawiony na Rys. 1, jest Tablica FFT. Tablica FFT zawiera informację o numerze interfejsu, na który są kierowane pakiety należące do konkretnych przepływów. Tablica ta jest sprawdzana przez selektor portu wyjściowego. Na podstawie identyfikatora przepływu jest odczytywany numer interfejsu z odpowiedniego pola. Jeżeli tablica FFT zawiera informacje o danym

przepływie, tablica rutingu nie jest sprawdzana przez selektor portu wyjściowego. Stanowi to istotną nowość w stosunku do istniejących rozwiązań, bowiem w znanych ruterach tablice rutingu są sprawdzane dla każdego pakietu. Natomiast w opracowanym rozwiązaniu, jeżeli danego przepływu nie ma w tablicy FFT, taki wpis związany z tym przepływem zostaje utworzony w tablicy FFT, a numer interfejsu jest pobierany z aktualnej tablicy rutingu.

Tablica FFT, w odróżnieniu od tablicy rutingu, jest tworem statycznym. Raz wpisany identyfikator przepływu nie ulega zmianie - aktualizowane jest jedynie pole: "Czas ostatniego pakietu" z każdym nadchodzącym pakietem. Na podstawie tego pola można ustalić czas, który upłynął od przyjścia ostatniego pakietu należącego do danego przepływu.

Gdy w sieci wystąpi przeciążenie jakiegoś łącza, wykonywane jest podwyższenie kosztu tego łącza w protokole rutingu na jego wartość maksymalną, lub inną symbolizującą przeciążenie. W efekcie, zastosowany protokół rutingu rozpropaguje tę informację oraz wykona przeliczenie nowych tras wg zmienionych kosztów. Tablice rutingu na ruterach mogą więc ulegać zmianie, ale przewidziane w ruterze zgodnie z wynalazkiem tablice FFT pozostaną niezmienione. Oznacza to, że tylko nowe przepływy, czyli takie, których identyfikatory nie były wpisane na listę FFT w momencie aktualizacji, odczują zmianę w tablicy rutingu. Przepływy aktywne, wpisane na listę FFT, w momencie aktualizacji nie odczują zmian. Dzięki temu, w momencie wykrycia przeciążenia, nowe przepływy kierowane są na alternatywne ścieżki, natomiast cały istniejący ruch jest przenoszony starymi ścieżkami bez żadnych zmian.

ID przepływu	Port wyjściowy rutera	Czas ostatniego pakietu

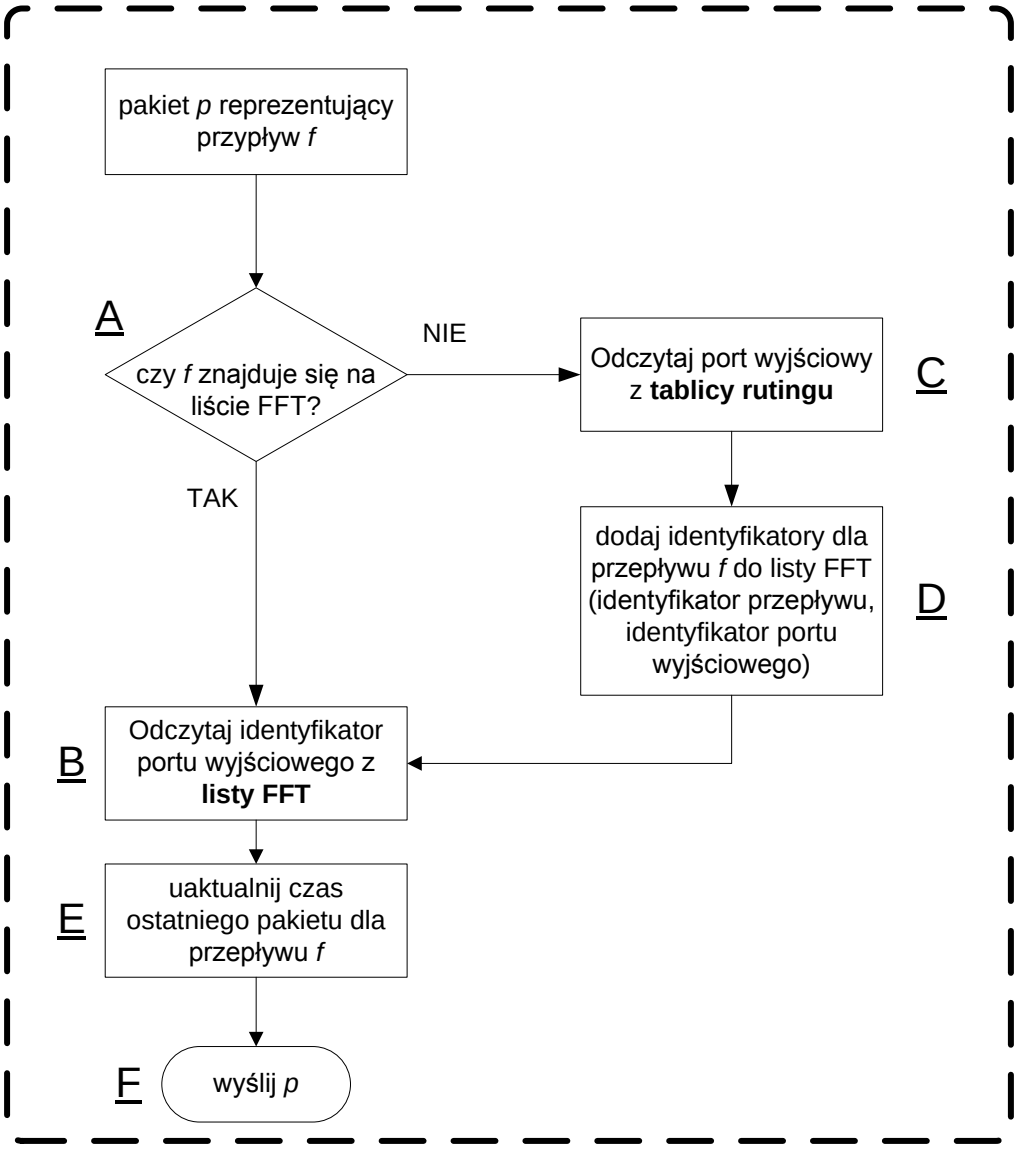
Rys. 2 - Struktura Tablicy Przekazywania Przepływów (FFT)

Tablica FFT, której struktura pokazana jest na Rys. 2, przechowywana w fizycznej pamięci rutera, zawiera przynajmniej następujące pola:

- identyfikator przepływu,

- port wyjściowy rutera, na który są wysyłane pakiety należące do danego przepływu,
- wpis pozwalający zidentyfikować dokładny czas, który upłynął od przyjścia ostatniego pakietu związanego z tym przepływem.

Gdy pakiet nowego przepływu zostanie przyjęty do obsługi na danym ruterze, identyfikator przepływu reprezentowanego przez ten pakiet jest dodawany do tablicy FFT. Jeżeli przez pewien z góry ustalony czas *t* nie pojawi się żaden nowy pakiet danego przepływu, to wpis w tablicy FFT dotyczący tego przepływu jest usuwany. Jeżeli po upływie czasu *t* pojawi się pakiet należący do usuniętego przepływu, będzie on potraktowany jako nowy przepływ.



Rys. 3 - Schemat działania selektora portu wyjściowego rutera

Schemat działania selektora portu wyjściowego, czyli sposób wyboru portu wyjściowego w ruterze, został przedstawiony na Rys. 3. Na podstawie odpowiednich pól z nagłówka pakietu IP wyliczany jest identyfikator przepływu. Następnie sprawdzane jest, czy identyfikator ten znajduje się w tablicy FFT (**A**). Jeśli przepływ znajduje się w tablicy FFT, odczytywany jest numer interfejsu wyjściowego rutera (**B**), na który ma zostać przesłany pakiet. Następnie aktualizowana jest wartość "Czas ostatniego pakietu" (**E**) (może on być reprezentowany przez aktualny czas), a pakiet jest przesyłany na odczytany interfejs za pomocą pola komutacyjnego rutera (**F**). Jeśli przepływ nie zostanie odnaleziony w tablicy FFT, to odpowiedni port wyjściowy jest odczytywany z tablicy rutingu rutera (**C**). Następnie identyfikator tego przepływu jest dodawany do tablicy FFT (**D**) wraz z numerem portu, na który należy kierować pakiety należące do tego przepływu. Dalsza część jest analogiczna do poprzedniego przypadku, tj., aktualizowana jest wartość "Czas ostatniego pakietu" (**E**) (wpisywany jest tam aktualny czas), a pakiet jest przesyłany na odczytany interfejs za pomocą pola komutacyjnego rutera (**F**).

Kolejność przesyłania informacji i umieszczenie wpisu w tablicy FFT jest obojętne, chociaż korzystnie jest najpierw wysłać pakiet, a potem dokonać wpisu w tablicy FFT, bowiem minimalizuje to opóźnienia związane z przesłaniem pakietu.

W przypadku protokołu IPv4, pole czasu życia zawiera liczbę przeskoków, które może wykonać pakiet na swojej trasie. Każdy kolejny ruter na trasie zmniejsza wartość w polu TTL przekazywanego pakietu o jeden. Jeśli router otrzyma pakiet z TTL równym 0, odrzuca go i usuwa z sieci. Procedura ta pomaga w unikaniu przeciążeń w przypadku źle skonfigurowanych tras rutingu na ruterach lub w przypadku powstania awarii. W przypadku protokołu IPv6, pole Hop Limit ma identyczne zadanie i działa w taki sam sposób.

Korzystnie jest by podczas dodawania nowego przepływu do tablicy FFT, zapisać w rekordzie również wartość pola Time to Live (TTL, czas życia) z nagłówka protokołu IPv4 lub pola Hop Limit (limit przeskoków) z nagłówka protokołu IPv6 (w zależności od tego, która wersja protokołu IP jest używana). Następnie, dla każdego pakietu wykonywane jest sprawdzenie, czy wartość pola TTL, lub Hop Limit odpowiada wartości zapisanej w tablicy FFT. Jeżeli wystąpi zgodność, pakiet jest

przesyłany wg procedury opisanej wcześniej. Jeżeli wystąpi niezgodność, dany przepływ należy usunąć z listy FFT, a następnie obsłużyć pakiet ponownie od początku. W ten sposób, po wystąpieniu niezgodności, może zmienić się trasa pakietów należących do danego przepływu, ponieważ zostanie usunięty wpis z tablicy FFT (był tam zapamiętany interfejs wyjściowy), a następnie utworzony na nowo (według obecnej tablicy rutingu).

Wyżej opisane rozwiązanie jest korzystne dla sieci z mechanizmem FAMTAR, ponieważ eliminuje problem wystąpienia pętli.

Sposób agregacji przepływów w sieciach IP

Opracowany sposób agregacji przepływów w sieciach IP (ang. Internet Protocol) pozwala na stabilną obsługę ruchu sieciowego identyfikowanego za pomocą przepływów.

Zaproponowany sposób agregacji przepływów może być stosowany w ruterach, w których ruch sieciowy jest identyfikowany za pomocą przepływów.

Jednym z podstawowych problemów obsługi ruchu bazującej na przepływach jest liczba przepływów. W rozległych sieciach przepływów może być bardzo dużo. W efekcie jest konieczne zapewnienie odpowiednio dużej pamięci w ruterze na potrzeby listy przepływów. Jeszcze większym problemem może być przeszukiwanie tej listy z każdym nadchodzącym pakietem. Takie działanie może znacząco obciążać urządzenie i wydłużać czas jego odpowiedzi.

W mechanizmie odpowiedzialnym za agregację przepływów w ruterze brzegowym systemu autonomicznego wyznacza się identyfikator całej trasy dla przepływu w tym systemie autonomicznym. Ten identyfikator jest zapisywany na dodatkowej liście w ruterze wraz z identyfikatorem wyjściowym. Wszystkie rutery na danej trasie postępują identycznie. Dzięki temu, na podstawie tej nowej listy, ruter zawsze wie gdzie wysłać pakiet. Dodatkowo liczba wpisów na liście jest ograniczona do liczby możliwych tras w sieci, gdyż różne przepływy transmitujące ruch tą samą trasą są agregowane do jednego wpisu w tablicy. Liczba wpisów w tablicy jest znacząco mniejsza od liczby obsługiwanych przez ruter przepływów. W efekcie problem skalowalności związany z obsługą przepływów jest rozwiązany. Zastosowanie tego rozwiązania może być szczególnie korzystne w sieciach z

wielodrogową transmisją danych, w których ruch jest identyfikowany za pomocą przepływów.

Mechanizm agregacji może być stosowany wewnątrz sieci kontrolowanej i administrowanej przez danego operatora, nazywanej dalej domeną. Istotą mechanizmu agregacji jest dodanie do każdego pakietu w domenie identyfikatora trasy. Identyfikator trasy jest przenoszony w nagłówku pakietu IP. W protokole IP w wersji 4, może być do tego wykorzystane np. pole Type of Service (Differentiated Services Field wg specyfikacji RFC 2474). W protokole IP w wersji 6 można wykorzystać np. pola Traffic Class lub 20-bitowe pole Flow Label. Wykorzystanie przedstawionych pól nagłówka jest zaledwie przykładem. Z punktu widzenia działania mechanizmu agregacji, wykorzystanie konkretnego pola nie jest istotne.

Istotną różnicą rutera z mechanizmem agregacji przepływów w stosunku do klasycznego rutera, jest fakt, że klasyczny ruter wybiera interfejs/łącze wyjściowe przy pomocy adresu internetowego adresata wiadomości, natomiast urządzenie do przesyłania pakietów na podstawie identyfikatora trasy korzysta z identyfikatora trasy. Takie podejście zapewnia szybsze działanie. Identyfikator trasy to wynik działania jednokierunkowej funkcji hashującej na listę węzłów, które zawiera trasa. Funkcja hashująca musi być dobrana odpowiednio, tzn. musi generować skrót, który zmieści się w konkretnym polu nagłówka protokołu IP, gdyż będzie przenoszony przez każdy pakiet. Dodatkowo, nie może generować takich samych skrótów dla różnych tras. Jednocześnie algorytm powinien generować skrót bardzo szybko, ze względu na znaczną liczbę operacji, które każdy ruter będzie musiał wykonać.

Kolejną charakterystyczną cechą każdego rutera jest utrzymywanie dwóch tablic. Tablica przepływów wiąże dany przepływ z identyfikatorem trasy (Rys. 4). Tablica tras zawiera identyfikatory tras wraz z informacjami na ich temat (Rys. 5).
Do obsługi każdego pakietu, wykorzystywana jest jedna z tablic. Tablica przepływów jest potrzebna do obsługi pakietów, które nie zawierają jeszcze identyfikatora trasy. Są to więc pakiety przychodzące do domeny. Tablica tras jest potrzebna do obsługi pakietów, które posiadają już identyfikator trasy.

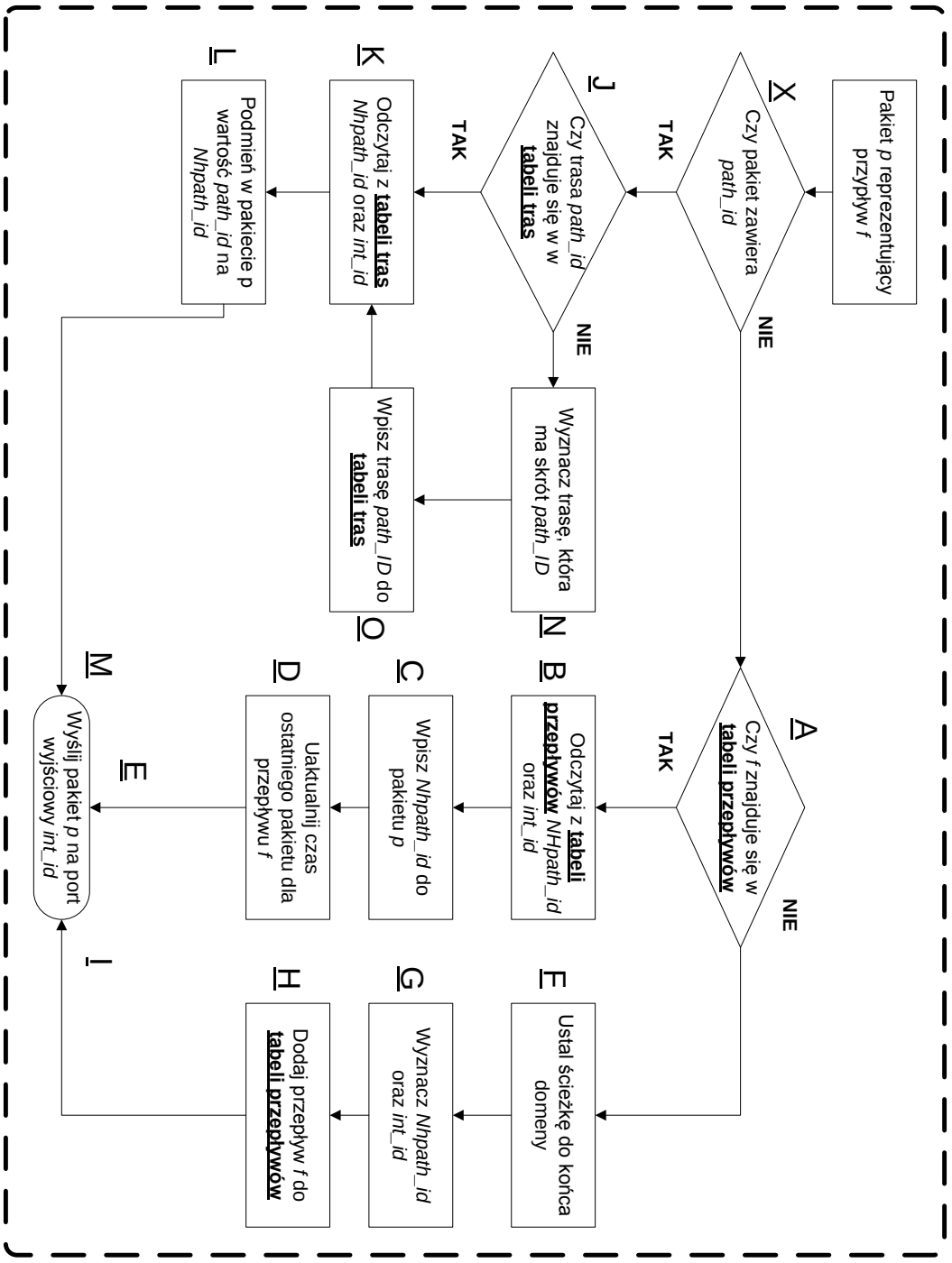
ID przepływu *(flow_id)*	ID trasy widziane z perspektywy następnego węzła *(NHpath_id)*	Interfejs wyjściowy *(int_id)*	Czas ostatniego pakietu *(timestamp)*

Rysunek 4 – struktura tablicy przepływów

ID trasy *(path_id)*	ID trasy widziane z perspektywy następnego węzła *(NHpath_id)*	Interfejs wyjściowy *(int_id)*

Rysunek 5 – struktura tablicy tras

Pierwszym krokiem jest sprawdzenie, czy przychodzący pakiet zawiera identyfikator trasy (**X**). Następnie, w zależności od tego, czy pakiet zawiera identyfikator trasy czy nie, ruter postępuje wg opisu poniżej.



Rysunek 6 – schemat blokowy obsługi pakietów w mechanizmie agregacji przepływów.

Schemat obsługi pakietów w opisywanym rozwiązaniu został przedstawiony na Rys. 6. Poniżej znajduje się opis poszczególnych kroków.

Dla każdego pakietu, który nie posiada ID trasy (wchodzący do domeny):

1. Ruter sprawdza, czy ID przepływu skojarzonego z pakietem istnieje w tablicy przepływów (**A**).
2. Jeżeli przepływ istnieje w tablicy przepływów:
    a. Ruter odczytuje z tablicy przepływów ID trasy widziane z perspektywy następnego węzła oraz interfejs wyjściowy (**B**).
    b. Ruter wpisuje do pakietu wartość pola ID trasy widziane z perspektywy następnego węzła (**C**)
    c. Ruter uaktualnia pole Czas ostatniego pakietu wpisując aktualny znacznik czasu (**D**)
    d. Ruter przesyła pakiet na interfejs wyjściowy odczytany z tablicy. W zależności od typu łącza, pakiet jest przesyłany w postaci sygnału elektrycznego, optycznego lub radiowego do następnego węzła sieci. (**E**)
3. Jeżeli przepływ nie istnieje w tablicy przepływów:
    a. Ruter ustala ścieżkę do końca domeny (do węzła docelowego, lub do ostatniego węzła w domenie, w sytuacji gdy węzeł docelowy leży poza domeną). Ścieżka jest przedstawiona w postaci listy węzłów (**F**).
    b. Ruter wyznacza „ID trasy widziane z perspektywy następnego węzła" oraz interfejs wyjściowy dla pakietów (**G**).
    c. Ruter tworzy nowy wpis do tablicy przepływów i wpisuje w odpowiednie pola wyznaczone wartości (**H**)
    d. Ruter przesyła pakiet na wyznaczony interfejs wyjściowy. W zależności od typu łącza, pakiet jest przesyłany w postaci sygnału elektrycznego, optycznego lub radiowego do następnego węzła sieci. (**I**)

Dla każdego pakietu, który posiada już ID trasy (obsługiwany w domenie)**:**

1. Ruter sprawdza, czy trasa odczytana z pakietu znajduje się w tablicy tras (**J**)
2. Jeżeli trasa widnieje w tablicy tras:
    a. Ruter odczytuje ID trasy widziane z perspektywy następnego węzła oraz interfejs wyjściowy z tablicy tras (**K**)
    b. Ruter podmienia ID trasy w pakiecie na wartość odczytaną z pola ID trasy widziane z perspektywy następnego węzła (**L**)
    c. Ruter przesyła pakiet do węzła następnego. W zależności od typu łącza, pakiet jest przesyłany w postaci sygnału elektrycznego, optycznego lub radiowego do następnego węzła sieci. (**M**)

3. Jeżeli trasa nie widnieje w tabeli tras:
    a. Ruter wyznacza trasę (listę węzłów), której ID jest równie ID trasy zapisanej w pakiecie (**N**)
    b. Ruter wyznacza ID trasy widziane z perspektywy następnego węzła oraz interfejs wyjściowy, a następnie dodaje trasę do tabeli tras. (**O**)
    c. Obsługa pakietu wraca do punktu 2b.

Dla każdego pakietu wychodzącego z domeny:

1. Ruter kasuje ID trasy z nagłówku pakietu IP.
2. Ruter wysyła pakiet poza domenę zgodnie z zasadą działania tradycyjnej sieci IP. W zależności od typu łącza, pakiet jest przesyłany w postaci sygnału elektrycznego, optycznego lub radiowego do następnego węzła sieci.

Dokonane zgłoszenia patentowe: „Urządzenie do rutingu pakietów wieloma ścieżkami w sieciach teleinformatycznych oraz sposób jego zastosowania” (ang." A device for multipath routing of packets in computer networking and the method for its use").

• zgłoszenie: 2014-08-05, nr KR20140100515 (Korea Południowa),
dostępne na stronie: http://patenty.bg.agh.edu.pl/pelneteksty/KR20150016916A.pdf
• zgłoszenie: 2014-08-05, nr CA20142858449 (Kanada),
dostępne na stronie: http://patenty.bg.agh.edu.pl/pelneteksty/CA2858449A1.pdf
• zgłoszenie: 2014-08-01, nr JP 2015057879 A (Japonia),
dostępne na stronie: http://patenty.bg.agh.edu.pl/pelneteksty/JP2015057879A.pdf
• zgłoszenie: 2014-04-29, nr US201414264880 (USA),
dostępne na stronie: http://patenty.bg.agh.edu.pl/pelneteksty/US20150063118A1.pdf
• zgłoszenie: 2014-08-01, nr CN201410375537 (Chiny),
dostępne na stronie: http://patenty.bg.agh.edu.pl/pelneteksty/EP2905932A1.pdf
• zgłoszenie: 2014-03-29, nr EP20140162518 (kraje Unii Europejskiej),
dostępne na stronie: http://patenty.bg.agh.edu.pl/pelneteksty/EP2905932A1.pdf
• zgłoszenie: 2014-08-01, nr TW 201519603 A (Tajwan),
dostępne na stronie: http://patenty.bg.agh.edu.pl/pelneteksty/TW201519603A.pdf
• zgłoszenie: 2013-08-05, nr P.404986 (Polska),
dostępne na stronie: http://patenty.bg.agh.edu.pl/pelneteksty/PL404986A1.pdf

Uzyskane patenty:
• udzielony: 2016-07-21, nr TW I1543567 B (Tajwan),
dostępny na stronie: http://patenty.bg.agh.edu.pl/pelneteksty/TWI543567B.pdf

Pozostałe zgłoszenia patentowe są w trakcie rozpatrywania.

Planowane jest dokonanie sprzedaży praw do uzyskanych patentów. Oferta jest kierowana do producentów sprzętu sieciowego, m.in. do Cisco czy Huawei. Aktualnie jesteśmy po pierwszych rozmowach z różnymi producentami sprzętu. Jednak szanse powodzenia przedsięwzięcia są dziś trudne do oszacowania.