



Sieci Ad Hoc (sieci doraźne, sieci spontaniczne)



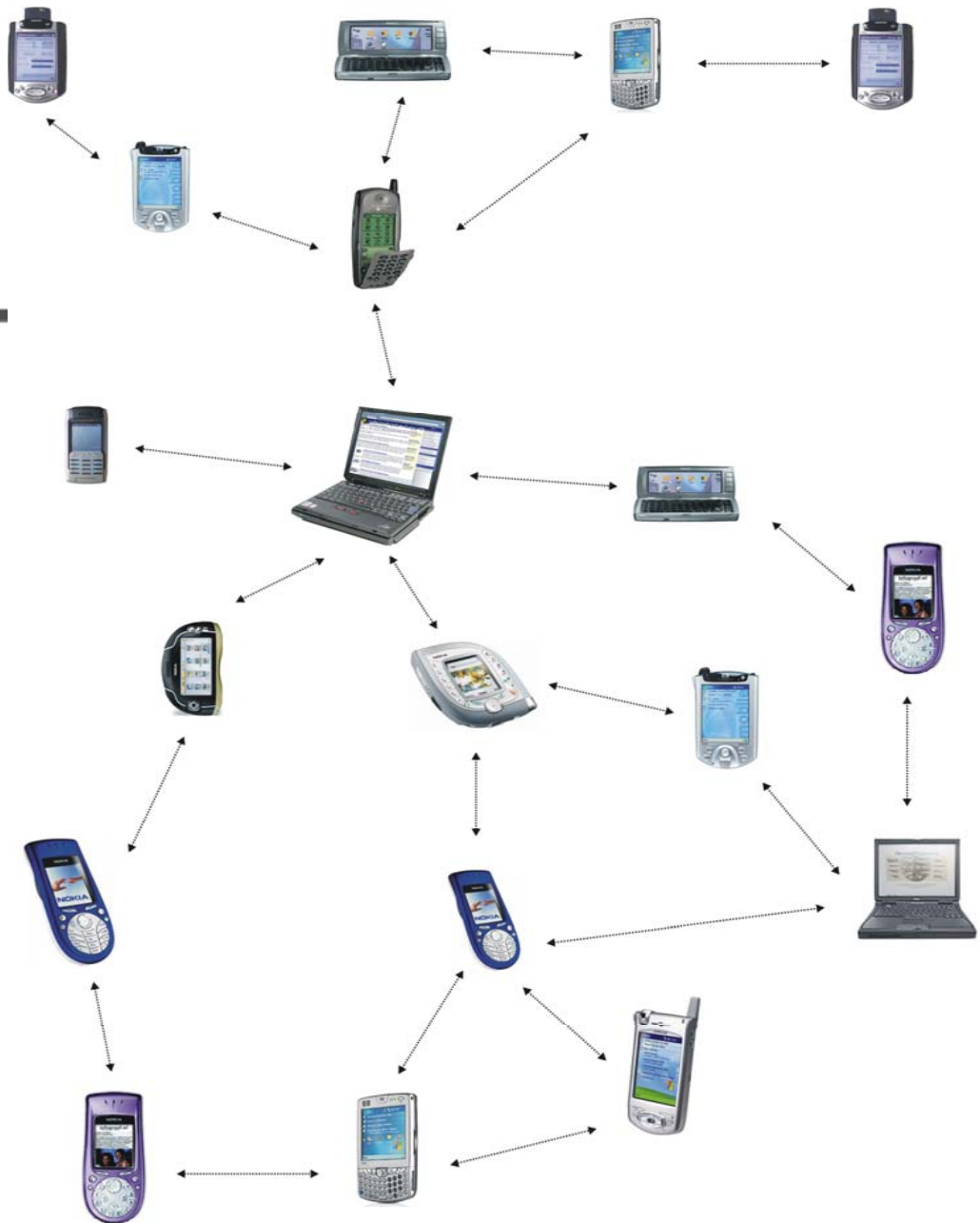
Plan prezentacji

- Wstęp
- Charakterystyka sieci Ad Hoc
- Zastosowania
- Routing
 - Tablicowe protokoły routingu (Table-driven Routing)
 - Routing inicjowany na żądanie źródła sygnału (Source-initiated On-demand Routing)
 - Protokoły hybrydowe

Sieci ad hoc

- Składają się z urządzeń mobilnych wyposażonych w karty do komunikacji bezprzewodowej (w jednym określonym standardzie)

- Każde urządzenie potrafi „rozmawiać” z każdym



Działanie sieci ad hoc



Urządzenie mobilne

+



Karta sieciowa **WLAN** (802.11)



802.11 określa rodzinę specyfikacji dotyczących bezprzewodowych sieci LAN. Zostały one utworzone przez **IEEE** (1997). Określa ona interfejs komunikacji pomiędzy *bezprzewodowym klientem* i *punktem dostępowym*, lub pomiędzy dwoma *bezprzewodowymi klientami*.

Organizacja **Wi-Fi Alliance** zajmuje się certyfikacją produktów zgodnych ze standardami 802.11



Działanie sieci ad hoc: parametry



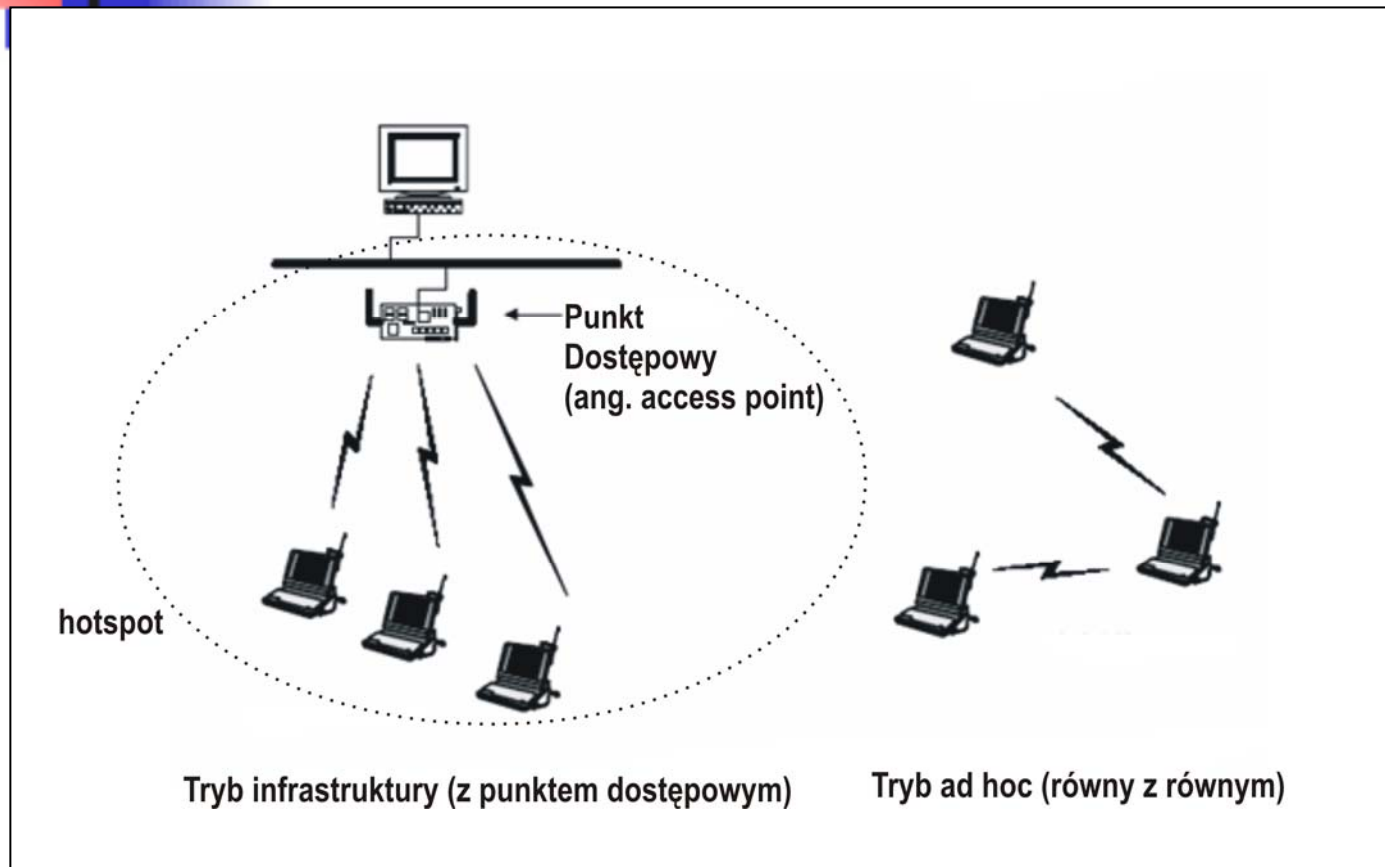
Standardy komunikacji bezprzewodowej



Standard	Prędkość	Modulacja
IEEE 802.11	Do 2 Mbps w paśmie 2.4 GHz	FHSS lub DSSS
IEEE 802.11a (Wi-Fi)	Do 54 Mbps w paśmie 5 GHz	OFDM
IEEE 802.11b (Wi-Fi)	Do 11 Mbps w paśmie 2.4 GHz	DSSS z CCK
IEEE 802.11g (Wi-Fi)	Do 54 Mbps w paśmie 2.4 GHz	OFDM powyżej 20Mbps, DSSS z CCK poniżej 20Mbps
Bluetooth (Personal Area Networks)	Do 2 Mbps w paśmie 2.45 GHz	FHSS
HomeRF	Do 10 Mbps w paśmie 2.4 GHz	FHSS
HiperLAN/1 (Europa)	Do 20 Mbps w paśmie 5 GHz	CSMA/CA
HiperLAN/2 (Europa)	Do 54 Mbps w paśmie 5 GHz	OFDM

Topologia standardu IEEE 802.11

- Dwa tryby: **infrastruktury** i **ad hoc**




Właściwości sieci ad hoc (1 / 2)

- Brak jakiegokolwiek określonej i przewidywalnej struktury sieci, częste zmiany topologii
- Urządzenia mogą dołączać się do sieci i wychodzić z niej dynamicznie w nieprzewidywalny sposób
- Brak centralnego zarządzania strukturą sieci, przepływami, dołączaniem kolejnych urządzeń. Wszystkie urządzenia są równorzędne
- Duży wpływ środowiska, parametrów urządzeń uczestniczących w sieci na zachowanie sieci



Właściwości sieci ad hoc (2/2)

- Informacja jest transmitowana w sposób “zapisz i przekaż” (store and forward) z wykorzystaniem wieloskokowego routingu („multi-hop”). 
- Urządzenie jednocześnie jest terminalem jak i „routerem”
- Ograniczona ochrona fizyczna węzłów
- Ograniczone zasoby: **moc obliczeniowa i pojemność baterii**
- Sporadyczna natura połączeń

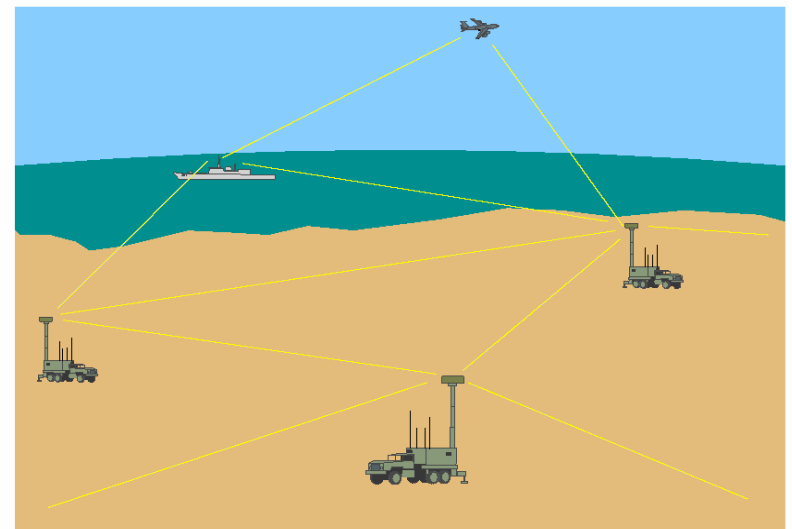
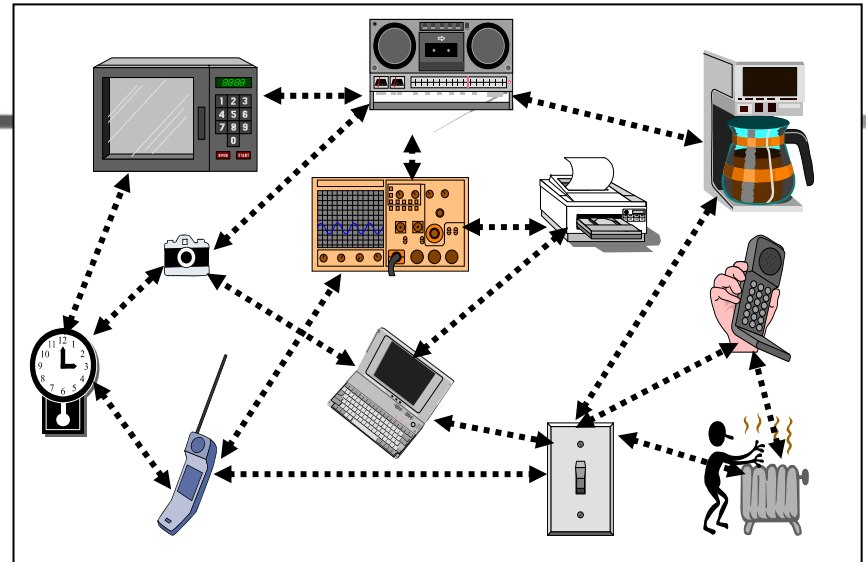
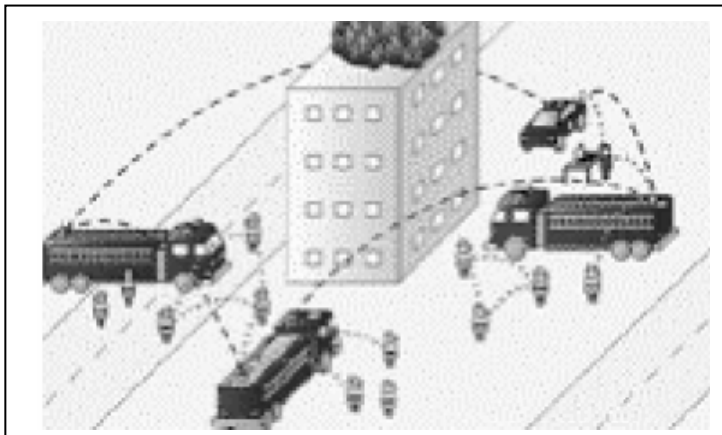


Zastosowania

- *Zastosowania obronne*: Zarządzanie polem bitwy wymaga komunikacji w locie, którą zapewnić mogą sieci ad-hoc i sensorowe.
- *Wirtualna nawigacja*: Dane ze zdalnej bazy danych są transmitowane okresowo w niewielkich, odpowiednich blokach, używając łącz obecnych na drodze pojazdu. Baza danych może zawierać reprezentacje graficzne ulic, budynków, mapy i najświeższe informacje o korkach, informacje te mogą zostać wykorzystane przez kierowcę przy ustalaniu drogi.
- *Tele-medycyna*: Wsparcie konsylium dla chirurga w nagłych, trudnych przypadkach.
- *Przetwarzanie Tele-Geo*: Zapytania zależne od położenia użytkowników.
- *Zarządzanie kryzysowe*: Katastrofy naturalne, w wyniku których cała infrastruktura komunikacyjna uległa zniszczeniu.
- *Edukacja przez internet*: sieci ad-hoc mogą zapewnić możliwość zdalnej edukacji dla ludzi zamieszkałych na terenach słabo zaludnionych oraz ze słabą infrastrukturą sieciową lub komunikacyjną.

Zastosowanie sieci ad hoc (1 / 2)

- **Private Area Networks**, projekt cybernetycznego domu – brak kabli, samokonfigurowalne, wymiana dokumentów i gier, „sterowanie mikserem”
- Akcje ratunkowe
- Konferencje
- Operacje militarne




Zastosowanie sieci ad hoc (2/2)

- Global Information Grid



- Przemysł samochodowy



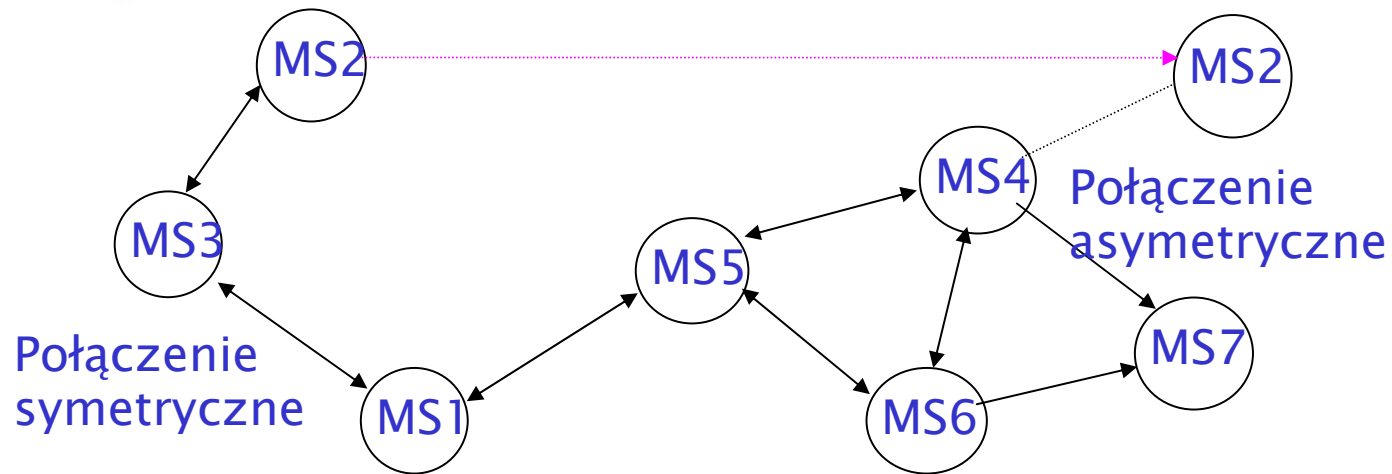


Klasyfikacja sieci ad hoc

- **Sieci ze wstępną inicjalizacją:** węzły mogą być wstępnie zainicjowane/skonfigurowane różnego rodzaju informacjami -
- oferują potencjalnie większy poziom bezpieczeństwa

- **Sieci nieinicjalizowane:** sieć jest tworzona **spontanicznie**, nie ma żadnej wstępnej inicjalizacji węzłów – zapewnienie bezpiecznej komunikacji bardzo trudne

Mobilna sieć Ad hoc



Mobilna sieć Ad-Hoc



Charakterystyka sieci Ad Hoc

- ***Topologie dynamiczne:*** Topologia sieci może ulegać zmianie dynamicznie wraz z przemieszczaniem się węzłów. W przypadku gdy moc transmisyjna dwóch nadajników jest różna, może istnieć połączenie jednokierunkowe.
- ***Łąca o zmiennej pojemności wymuszonej przez przepustowość:*** Rzeczywista przepustowość komunikacji bezprzewodowej jest mniejsza niż maksymalny współczynnik transmisji fal radiowych. Często występują kolizje.
- ***Działanie wymuszone przez źródło energii:*** Niektóre węzły w sieci ad hoc mogą być zasilane bateriami lub innymi wyczerpywalnymi źródłami energii. Dla tych węzłów istotna jest optymalizacja konsumpcji energii.
- ***Ograniczone bezpieczeństwo fizyczne:*** Sieci ad hoc są bardziej podatne na zagrożenia bezpieczeństwa fizycznego niż sieci przewodowe. Należy się liczyć z dużym prawdopodobieństwem ataków typu DoS lub spoofing.



Routing w MANET – Cele

- Udostępniać możliwie maksymalną niezawodność – wykorzystywanie alternatywnych tras w przypadku uszkodzenia węzłów pośrednich.
- Wybierać trasę o najmniejszym koszcie.
- Dawać węzłom najkrótszy możliwy czas odpowiedzi i największą możliwą przepustowość.
- Obliczenia związane z wyznaczaniem trasy muszą być rozproszone. Zcentralizowany routing dynamicznych sieci jest zazwyczaj bardzo kosztowny.
- Obliczenia związane z routingiem nie powinny wymagać utrzymania statycznego stanu sieci
- Każdy węzeł sieci musi mieć szybki dostęp do ścieżek na żądanie.
- Każdy węzeł musi interesować się tylko ścieżkami do swojego punktu docelowego.
- Powinno się unikać transmisji strumieniowej (wysoce zawodne)
- Pożądane jest posiadanie zapasowej trasy, na wypadek gdy pierwotna stanie się nieaktualna.



Klasyfikacja Routingu

Istniejące protokoły routingu można sklasyfikować jako:

- **Proaktywne**: trasa jest znana zanim nadejdzie pakiet do przekazania (trasa cały czas określana).
- **Reaktywne**: tworzy trasę tylko gdy posiada dane do przesłania

Protokoły routingu mogą być również sklasyfikowane jako:

- Protokoły tablicowe (Table Driven)
- Protokoły inicjowane na żądanie źródła (Source Initiated on-demand)



Tablicowe protokoły routingu

- Każdy węzeł przechowuje informacje o routingu dla wszystkich pozostałych węzłów w sieci
- Węzły są proaktywne, więc informacje o routingu są zawsze aktualne
- Gdy topologia sieci ulega zmianie, aktualizacja jest propagowana w całej sieci.
- Przykłady:
 - *Destination Sequenced Distance Vector routing (DSDV)*
 - *Cluster-head Gateway Switch routing (CGSR)*
 - *Wireless Routing Protocol (WRP)*

Destination Sequenced Distance Vector Routing (DSDV)

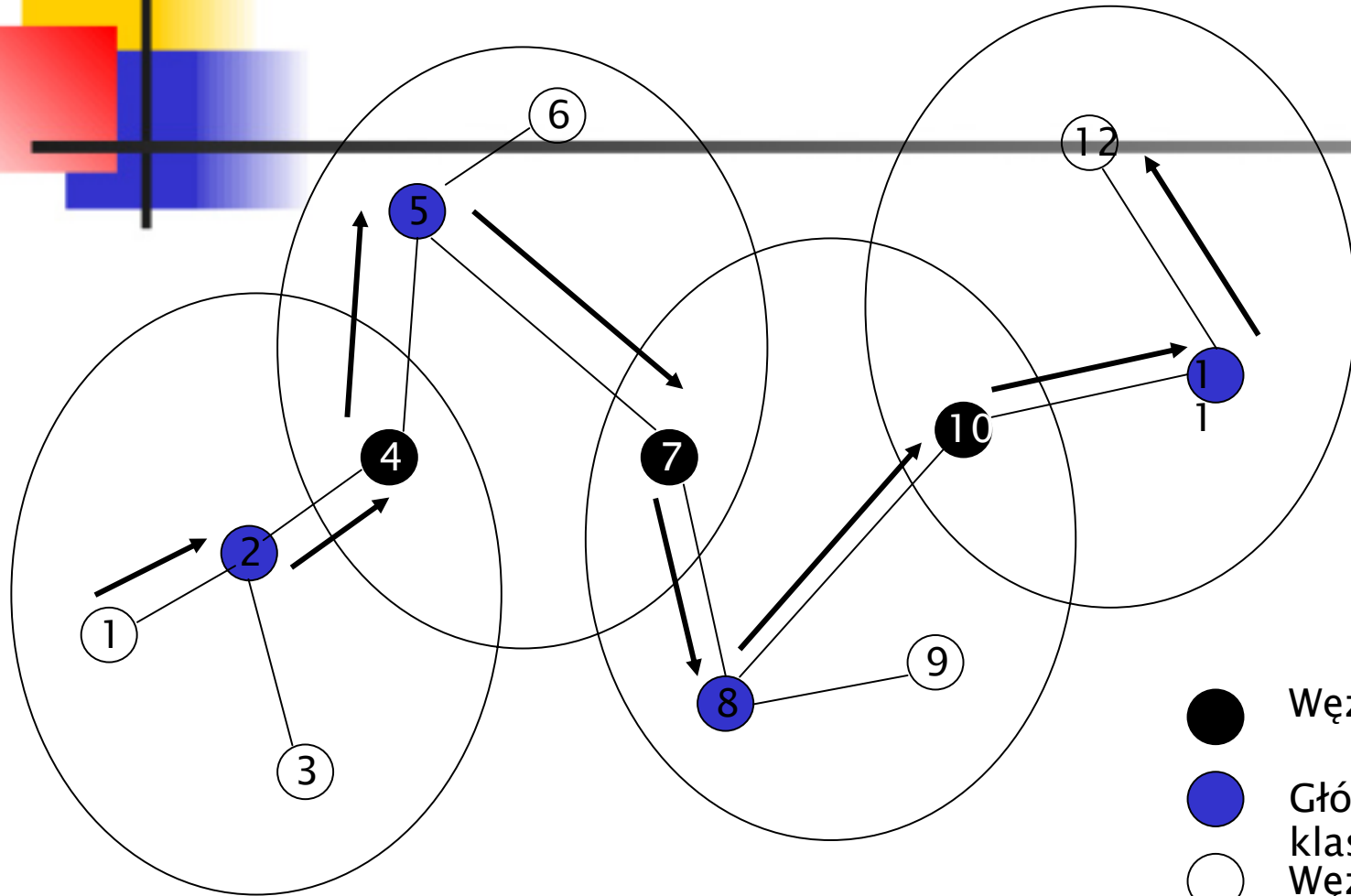
- Opiera się na algorytmie Bellmana–Forda.
- Każdy węzeł mobilny przechowuje tablicę routingu zawierającą liczby skoków do każdego możliwego celu.
- Uaktualnienia tablic routingu są rozgłaszane cyklicznie.
- Każdy wpis w tablicy jest oznaczany przez sekwencję liczb, która pozwala rozróżnić nieaktualne trasy od nowych i tym samym unikać pętli.
- Rozgłoszenie routingu zawiera adres docelowy, liczbę skoków wymaganych do osiągnięcia celu, numer oznaczający cel oraz nowy unikalny numer rozgłaszania.
- Jeśli do celu prowadzi wiele dróg, używana jest ta, z najświeższym numerem.
- Celem minimalizacji liczby uaktualnień, pakiety aktualizacji posiadają zmienne rozmiary zależne od liczby zmian w topologii.



Cluster-head Gateway Switch Routing (CGSR)

- CGSR jest zgrupowaną, wieloskokową, mobilną, bezprzewodową siecią z kilkoma heurystycznymi schematami routingu.
- Rozproszony algorytm wyboru węzła głównego klastra (Cluster Head – CH) jest wykorzystywany do wyboru węzła, który ma stanowić główny węzeł klastra.
- Modyfikuje DSDV poprzez użycie hierarchicznego CH do routowania ruchu w sieci.
- Węzły pełniące rolę bramy służą jako pomosty między dwoma lub więcej klastrami.
- Pakiet wysłany przez węzeł jest najpierw routowany do CH i następnie z CH do bramy kolejnego klastra, następnie do jego CH itd. dopóki pakiet nie osiągnie głównego węzła docelowego klastra.
- Częste zmiany w CH mogą wpływać na wydajność protokołu routingu, gdyż węzły wykorzystują więcej czasu na wybranie nowego CH niż na przekazywanie pakietów

CGSR c.d.



- Węzeł – brama
- Główny węzeł klastra
- Węzeł wewnętrzny

Routing w CGSR z węzła 1. do 12.



Wireless Routing Protocol (WRP)

- Każdy węzeł przechowuje 4 tablice:
 - Tablicę odległości (Distance table)
 - Tablicę routingu (Routing table)
 - Tablicę kosztów połączenia (Link cost table)
 - Tablicę list retransmisji wiadomości (Message Retransmission List – MRL)

Każdy zapis w MRL zawiera numer seryjny wiadomości uaktualniającej, licznik retransmisji oraz listę uaktualnień wysłanych w wiadomości uaktualniającej.



Wireless Routing Protocol c.d.

- Węzły informują się wzajemnie o zmianach połączeń przy pomocy wiadomości uaktualniających.
- Węzły zawierają listę odpowiedzi wskazujących na węzły, które mają być powiadomione o aktualizacji.
- Węzły wysyłają wiadomości uaktualniające po wykonaniu modyfikacji ze strony swoich sąsiadów lub po wykryciu zmian w połączeniu.
- Jeśli węzeł nie wysłał wiadomości, musi wysłać wiadomość kontrolną (HELLO message) w określonym czasie celem potwierdzenia łączności.
- Jeśli węzeł odbiera wiadomość kontrolną (HELLO message) od nowego węzła, węzeł ten zostaje dodany do tablicy.
- Zapobiega problemowi odliczania do nieskończoności (“count to infinity”).



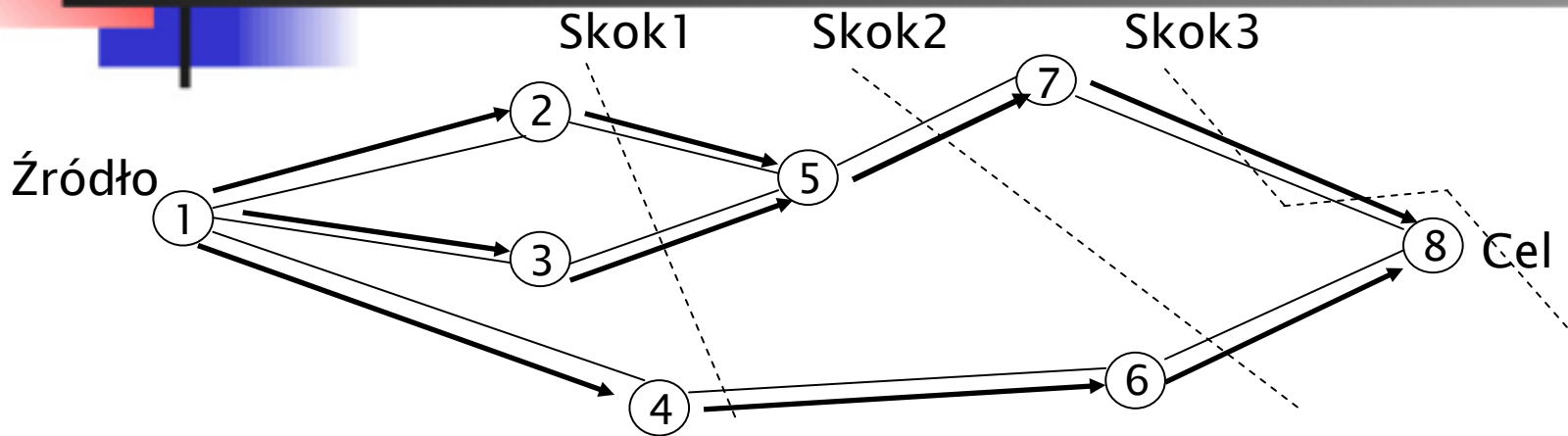
Routing inicjowany na żądanie źródła

- Ad hoc On-Demand Distance Vector (AODV).
- Dynamic Source Routing (DSR)
- Temporary Ordered Routing Algorithm (TORA)
- Associativity Based Routing (ABR)
- Signal Stability Routing (SSR)

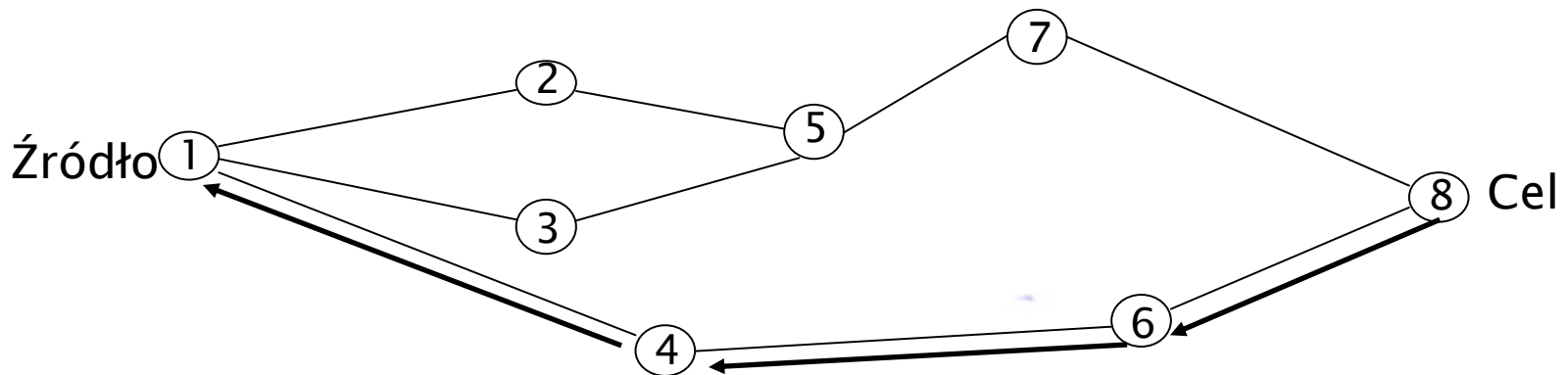
Ad hoc On-Demand Distance vector

- AODV jest udoskonaleniem DSDV, które minimalizuje liczbę wymaganych transmisji poprzez tworzenie tras na żądanie
- Węzły, które nie znajdują się na wybranej trasie nie przechowują informacji o routingu ani nie uczestniczą w wymianie tablic routingu.
- Źródłowy węzeł inicjuje proces odkrywania trasy celem zlokalizowania innych pośrednich węzłów (i w efekcie węzła docelowego). Inicjalizacja ta polega na transmitowaniu pakietów z żądaniem trasy (Route Request – RREQ) do swoich sąsiadów.
- RREQ zawiera własny numer, ID rozgłaszania oraz najświeższą sekwencję dla połączenia źródło–cel.
- Podobnie jak w DSDV używane są sekwencje liczb, zapewniające niezapętlanie się tras oraz zawierające informacje o najaktualniejszej trasie
- Pośrednie węzły odpowiadają tylko wtedy, gdy istnieje trasa do celu z numerem większym lub równym niż ten zawarty w RREQ

Odkrywanie trasy w protokole AODV



(a) Propagacja pakietów z żądaniem trasy (RREQ)



(b) Trasa obrona przez pakiet odpowiedzi (Route Reply – RREP)



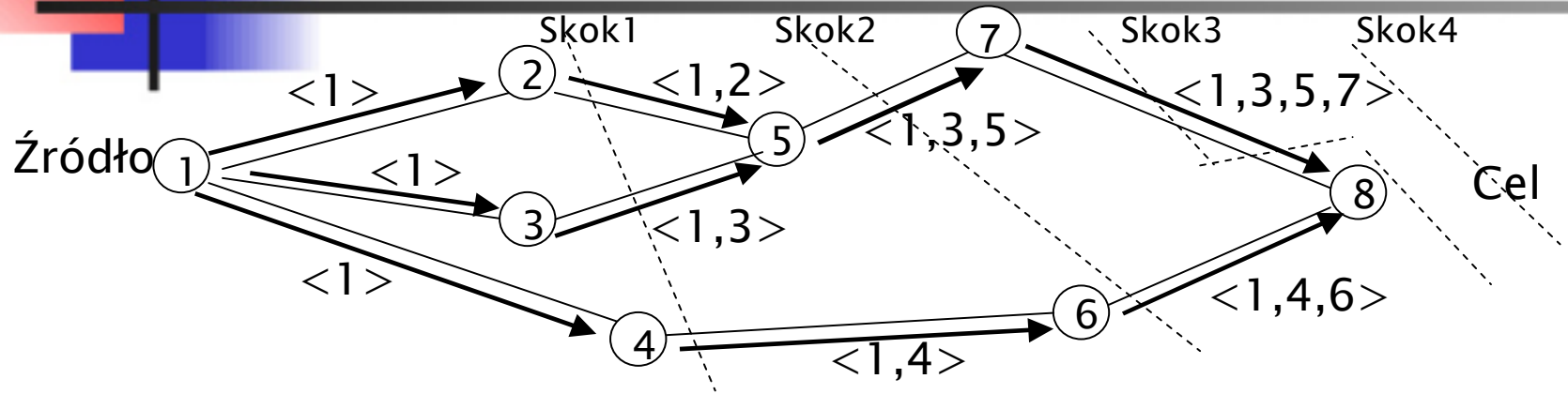
Dynamic Source Routing

- Protokół składa się z dwóch głównych faz:
 - Odkrywania trasy oraz zachowania trasy
- Gdy węzeł mobilny ma pakiet do wysłania do jakiegoś celu, wpieryw sprawdza swoją podręczną pamięć routingu, aby określić czy nie zawiera ona trasy do tego celu.
- Jeśli posiada trasę, która nie wygasła, użyje jej.
- Jeśli węzeł nie posiada trasy w pamięci podręcznej, inicjalizuje odkrywanie jej transmitując pakiety żądania trasy (RREQ).
- Żądanie to zawiera adres celu oraz źródła.

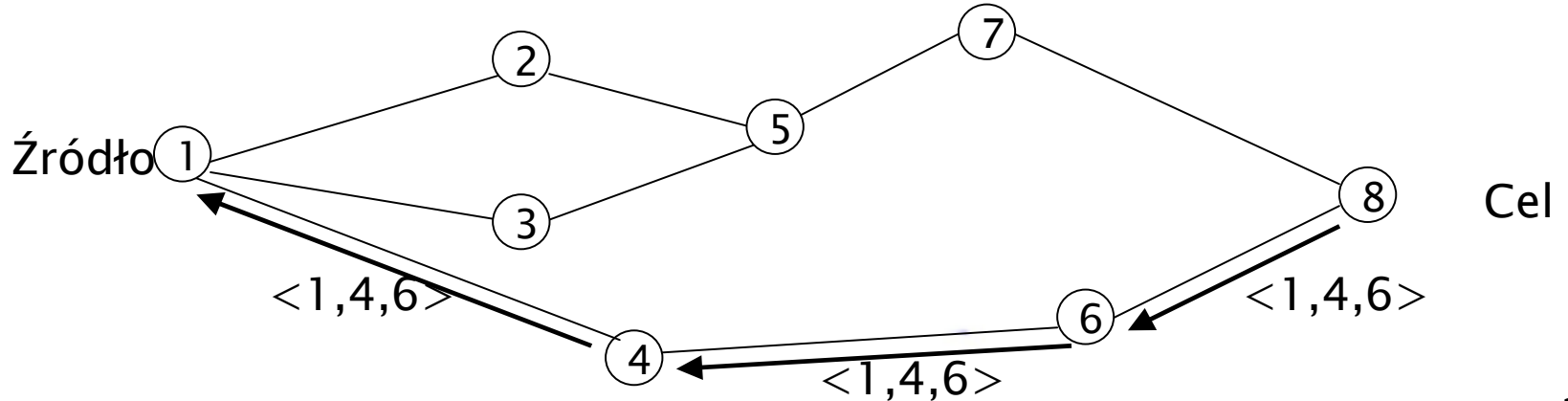
Dynamic Source Request c.d.

- Każdy węzeł odbierający pakiet sprawdza czy posiada w pamięci trasę do celu tego pakietu. Jeśli nie – dodaje swój adres do zapisu trasy pakietu i przekazuje go dalej.
- Odpowiedź (RREP) jest generowana, gdy żądanie osiąga cel lub węzeł pośredni, który posiada w pamięci podręcznej aktualną trasę do tego celu.
- Jeśli węzeł generujący odpowiedź jest celem pakietu, to w odpowiedzi umieszcza on zapis trasy zawarty w żądaniu.
- Utrzymanie trasy odbywa się za pomocą specjalnych pakietów błędów (route-error packets) generowanych w węzle, kiedy warstwa łącza danych napotka krytyczny błąd transmisji. W takim wypadku dany skok jest usuwany z pamięci podręcznej routingu.

Tworzenie zapisu trasy w DSR



(a) Budowanie zapisu trasy w trakcie jej odkrywania



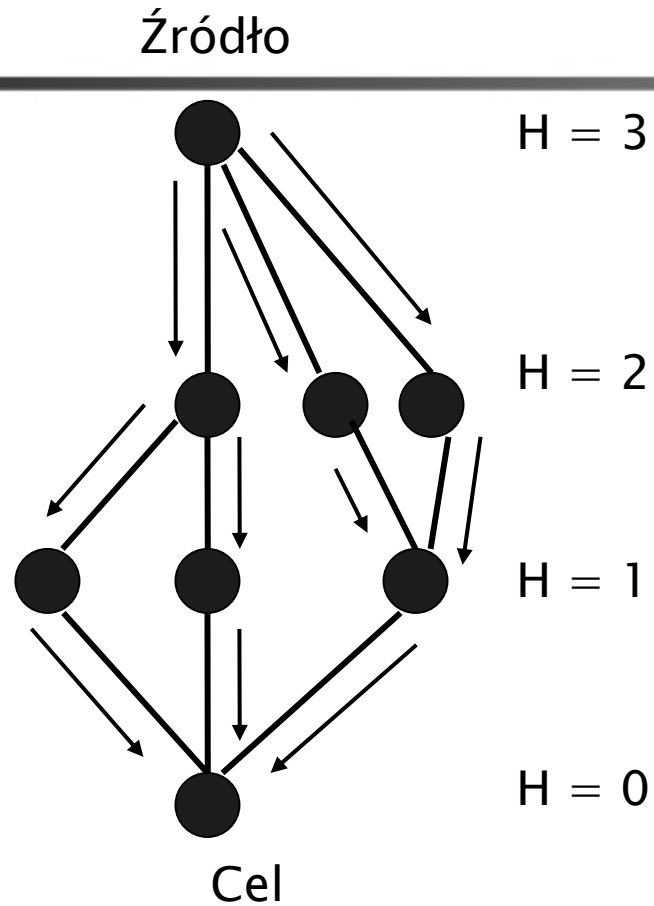
(b) Propagacja odpowiedzi zawierającej zapis trasy



Temporarily Ordered Routing Algorithm (TORA)

- TORA jest wysoce adaptacyjnym, rozproszonym algorytmem routingu, nie tworzącym zapętleń i bazującym na koncepcji inwersji połączenia oraz nie wykorzystującym dynamicznych mechanizmów routingu
- Minimalizuje ona reakcję na zmiany topologii, co jest osiągnięte przez to, że TORA rozdziela tworzenie potencjalnych dalekosiężnych wiadomości kontrolnych od stopnia zmian topologicznych.
- Miara wysokości jest wykorzystywana do modelowania stanu routingu w sieci.

TORA c.d.



Ilustracja miary wysokości w TORA



TORA c.d.

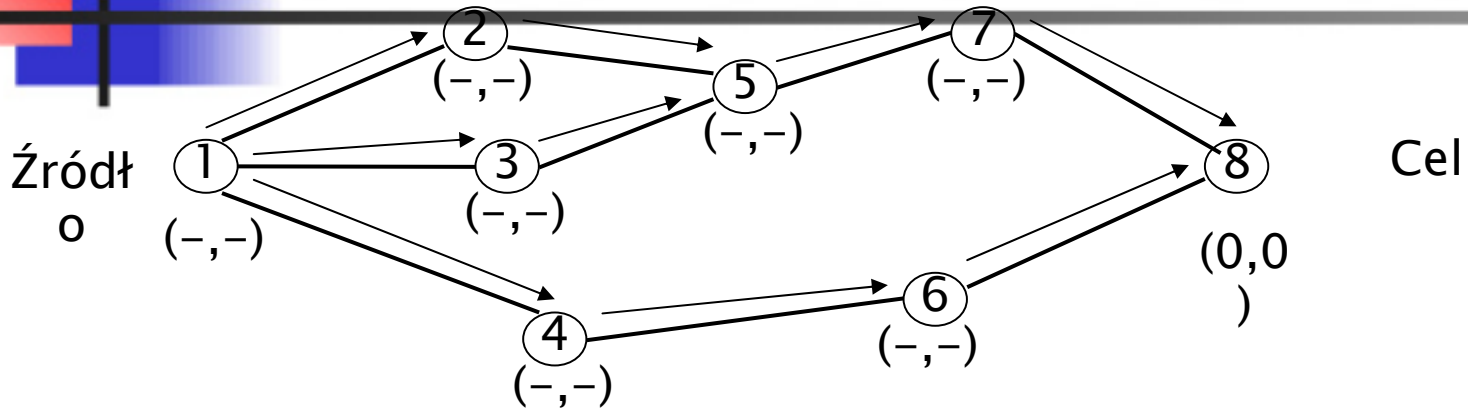
- Protokół udostępnia trzy podstawowe funkcje: tworzenie trasy, utrzymanie trasy oraz usuwanie trasy.
- W trakcie trwania fazy tworzenia i utrzymania trasy, węzły używają miary wysokości celem zbudowania skierowanego, acyklicznego grafu (DAG) o korzeniu w celu trasy.
- Odtąd połączenia mają przypisane kierunki oparte na względnych wysokościach
- Jeśli węzeł wykryje, że trasa do celu nie jest dłużej ważna, zwiększa jej wysokość by była najwyższa w swym sąsiedztwie (maksimum lokalne) i rozgłasza pakiet uaktualnienia (UPDATE packet)
- W przypadku gdy żaden z sąsiadów nie ma skończonej wysokości ze względu na cel, węzeł źródłowy inicjuje nowe poszukiwanie trasy



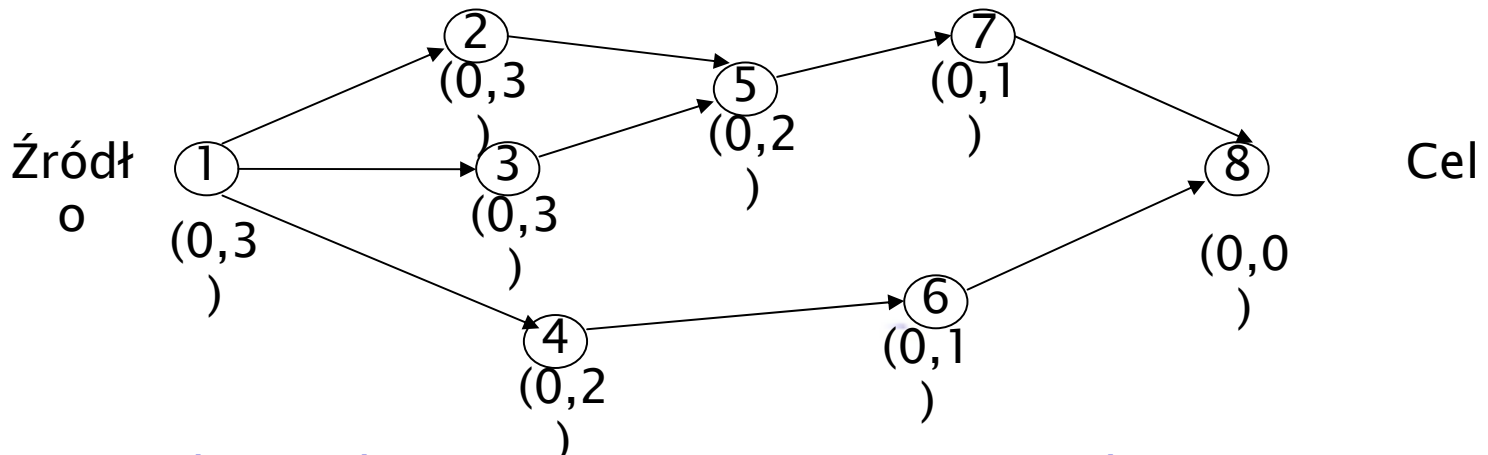
TORA c.d.

- Miara wysokości w TORA zależy od czasu wystąpienia błędu połączenia.
- Algorytm zakłada, że wszystkie węzły są ze sobą zsynchronizowane.
- Miara wysokości składa się z 5 czynników;
 - Czas błędu połączenia
 - Unikalne ID węzła definiującego nowy poziom odwołania
 - Bit-wskaźnik odbicia
 - Parametr kolejności propagacji
 - Unikalne ID węzła
- TORA jest reaktywna (trasa tworzona na żądanie) oraz proaktywna (dostępność wielu tras w przypadku błędu połączenia)

TORA c.d.



(a) Propagacja wiadomości z zapytaniem



(b) Wysokości węzłów uaktualnione w wyniku wiadomości uaktualniającej



Associativity Based Routing (ABR)

- Jest to protokół wolny od zapętleń, zakleszczeń oraz duplikatów pakietów
- Celem jest odkrywanie tras “długo żyjących”
- Występują trzy fazy ABR: odkrywanie trasy, rekonstrukcja trasy, usunięcie trasy.
- W ABR trasa jest wybierana w oparciu o stopień stabilności związanej z węzłami mobilnymi.
- Stabilność związku (Association stability) definiuje się jako stabilność połączenia jednego węzła w odniesieniu do drugiego w czasie i przestrzeni.
- Każdy węzeł generuje boję (beacon) celem zaznaczenia swej obecności.
- Gdy sąsiednie węzły otrzymają boję (beacon), spowoduje to uaktualnienie ich tablic asocjacyjnych.
- Odkrywanie trasy zostaje ukończone w cyklu Transmisji Zapytanie – Odpowiedź (Broadcast Query– Reply /BQ–REPLY/)
- Gdy odkryta trasa nie jest dłużej potrzebna, węzeł źródłowy inicjuje transmisję usuwania trasy (Route Delete), aby wszystkie węzły wzdłuż niej uaktualniły swoje tablice routingu.



Signal Stability Routing (SSR)

- SSR wybiera trasę opierając się na sile sygnału między węzłami oraz stabilności położenia węzła.
- Takie kryteria doboru trasy skutkują wyborem tras, które charakteryzują się lepszą łącznością.
- SSR może być podzielone na dwa współpracujące protokoły DRP (dynamic routing protocol) oraz SRP (static routing protocol).
- DRP jest odpowiedzialne za utrzymywanie tablicy stabilności sygnału (siły sygnałów sąsiednich węzłów) i tablicy routingu; wszystkie transmisje są obsługiwane przez DRP.
- SRP otrzymuje odebrane pakiety po aktualizacji tablicy i przekazuje je dalej



Protokoły hybrydowe

- **Zone Routing Protocol (ZRP):**
 - jest połączeniem proaktywnych i reaktywnych protokołów.
 - Próbuje ograniczać zasięg przeszukiwań proaktywnych do najbliższego otoczenia węzła. W tym samym czasie może być również wykonane przeszukanie globalne poprzez odpytywanie wybranych węzłów. Sąsiedztwo węzła nazywane jest strefą routingu.
 - Węzeł proaktywnie utrzymuje trasy do celu wewnątrz lokalnego sąsiedztwa. Tworzenie strefy routingu (routing zone) wymaga od węzła wiedzy, kto jest jego sąsiadem. Jest to zaimplementowane w warstwie MAC w protokole odkrywania sąsiedztwa (Neighbor Discovery Protocol).
 - ZRP używa proaktywnego protokołu routingu wewnątrzstrefowego (IARP) do utrzymania stref routingu.
 - Do odkrywania i utrzymywania tras do węzłów z poza strefy³⁶ ZRP wykorzystuje międzystrefowy protokół routingu (IERP).



Protokoły hybrydowe

- **Fisheye State Routing (FSR):**
 - Celem redukcji wielkości nagłówków uaktualnienia routingu w wielkich sieciach, stosuje się wielopoziomowe tzw. pola widzenia rybiego oka (fisheye scopes).
 - Zapewnia to zbieranie tych danych o topologii, które mogą być przydatne wkrótce, co pomaga utrzymać skalowalność protokołu routingu.
 - FSR zbiera informacje, o zmianach w topologii zachodzących w niedużej odległości od węzła, z dużą dokładnością i bardzo często.
 - Zmiany w bardziej oddalonych częściach sieci są zbierane rzadziej i z mniejszą dokładnością



Protokoły hybrydowe

- **Landmark Routing (LANMAR):**
 - Wykorzystuje punkty orientacyjne (landmarks) celem śledzenia logicznej podsieci.
 - Tablice routingu LANMAR zawierają jedynie te węzły, które znajdują się w zasięgu punktów orientacyjnych oraz same punkty. (w odróżnieniu od FSR, które przechowuje informacje o wszystkich węzłach w sieci).
 - Węzły wymieniają informacje o stanie łącza tylko ze swoimi sąsiadami (jak w FSR).



Protokoły hybrydowe

- **Location-Aided Routing (LAR):**
 - Wykorzystuje lokalne informacje do ograniczania zasięgu routingu.
 - LAR ogranicza wyszukiwanie w oparciu o spodziewane położenie węzła docelowego. Skutkiem tego ogranicza i kontroluje napływ pakietów żądania trasy (Route Request).
 - Informacje o położeniu węzłów mogą być pozyskiwane z pomocą technologii GPS.
 - Węzeł, który ma do wysłania pakiet, określa potencjalną strefę położenia węzła docelowego (Expected zone) w czasie t_1 na podstawie jego położenia w czasie t_0 oraz średniej prędkości
 - Im więcej informacji historycznych o położeniu i poruszaniu się węzła docelowego, tym mniejsza potencjalna strefa położenia. (w przypadku braku informacji o przeszłości, strefą staje się cała sieć)
 - Ponadto budowana jest jeszcze prostokątna strefa żądania (Request zone) obejmująca obszar zawierający węzeł źródłowy i potencjalną strefę położenia węzła docelowego. W jej obrębie pakiet jest przekazywany do celu



Protokoły hybrydowe

- **Distance Routing Effect Algorithm for Mobility (DREAM):**
 - Działa w oparciu o efekt odległości (distance effect) oraz współczynnik mobilności węzła.
 - Efekt odległości polega na tym, że im dalej znajdują się dwa węzły od siebie tym później ich ruch będzie miał wpływ na routing między nimi.
 - Im dwa węzły znajdują się dalej od siebie, tym mniejsza częstotliwość uaktualnień tablicy routingu jest wymagana.
 - Na podstawie współczynnika mobilności każdy węzeł może optymalizować częstotliwość z jaką wysyła aktualizacje do sieci i dzięki temu redukować zużycie przepustowości i energii.



Protokoły hybrydowe

- **Relative Distance Microdiscovery Ad Hoc Routing (RDMAR):**
 - Wysoce adaptacyjny, wydajny i skalowalny protokół routingu.
 - Odpowiedni dla wielkich sieci mobilnych o umiarkowanym stopniu zmian topologicznych.
 - Działa w oparciu o obliczaną względną odległość między dwoma terminalami.
 - Napływ zapytań jest zlokalizowany w ograniczonym regionie, którego środek stanowi węzeł źródłowy.
- **Power Aware Routing:**
 - Do tworzenia tras stosuje miary uwzględniające moc.
 - Takie podejście redukuje koszt, zapewnia, że średni czas do awarii węzła zwiększa się nie powodując żadnych opóźnień w dostarczeniu pakietu.

Charakterystyki protokołów (1 / 2)

Protokół	Poznanie trasy	"Zalewanie" przy odkrywaniu trasy	Opóźnienie przy odkrywaniu trasy	Wielościżkowy charakter	Skutek awarii trasy
DSDV	liczona a priori	Nie	Nie	Nie	Uaktualnia tablicę routingu wszystkich węzłów
WRP	liczona a priori	Nie	Nie	Nie	Uaktualnia tablice routingu wszystkich węzłów przez wymianę MRL między sąsiadami
DSR	Na żądanie, tylko gdy potrzebna	Tak. Silne wykorzystanie cache'u może zredukować "zalewanie".	Tak	Nie wyraźnie. Technika ratowania (salvaging) może szybko odtworzyć trasę.	Błąd trasy propagowany do źródła celem usunięcia niepoprawnej ścieżki.

Charakterystyki protokołów (2/2)

Protokół	Poznanie trasy	"Zalewanie" przy odkrywaniu trasy	Opóźnienie przy odkrywaniu trasy	Wielosieczkowy charakter	Skutek awarii trasy
AODV	Na żądanie, tylko gdy potrzebne	Tak. Kontrolowane użycie cache'u ogranicza "zalewanie".	Tak	Nie, jednak ostatnie badania sygnalizują wykonalność	Błąd trasy propagowany do źródła celem usunięcia niepoprawnej ścieżki.
TORA	Na żądanie, tylko gdy potrzebne	Zasadniczo jeden raz - przy inicjacji odkrywania trasy	Tak. Podczas konstruowania DAG znajdowane są wielokrotne ścieżki.	Tak	Błąd jest naprawiany lokalnie
LAR	Na żądanie, tylko gdy potrzebne	Redukowane przez wykorzystanie informacji o lokalizacji	Tak	Nie	Błąd trasy propagowany do źródła
ZRP	Hybrydowe	Tylko poza strefą źródła	Tylko gdy cel jest poza strefą źródła	Nie	Hybryda uaktualniania tablic węzłów wewnątrz strefy i propagacji błędu trasy do źródła ⁴³

On-Demand Multipath Routing w mobilnych sieciach ad hoc

- Jest rozwinięciem DSR (Dynamic Source Routing).
- Wykorzystuje technikę wielościeżkowości dla zmniejszenia częstotliwości rozgłaszania zapytań celem odkrycia nowych tras.
- Zaproponowano dwa rozszerzenia DSR:
 - W pierwszym węzeł docelowy odpowiada na zestaw zapytań. Główną trasę od celu do źródła stanowi trasa zbudowana w odpowiedzi na pierwszy pakiet zapytania, jaki dotarł od celu do źródła. Źródło przechowuje pozostałe trasy w pamięci podręcznej. Jeśli główna trasa zawodzi, wykorzystywana jest najkrótsza z pozostałych tras.
 - Drugie rozszerzenie zapobiega retransmisji pakietu, w trakcie wysyłki którego nastąpiła awaria trasy. Wszystkie pośrednie węzły posiadają alternatywne trasy na wypadek odłączenia od trasy głównej.

Ad Hoc On-Demand Distance Vector - Backup Routing

- Jest wielościeżkowym protokołem routingu, który konstruuje trasy na żądanie i korzysta z alternatywnych ścieżek tylko wtedy gdy główna trasa zostaje przerwana.
- Podobnie jak AODV, składa się z dwóch faz:
 - budowy trasy
 - Mechanizm działa podobnie jak w AODV
 - Węzły podsłuchują pakiety odpowiedzi (RREP) transmitowane przez swoich sąsiadów i zapisują sąsiada, który nie przesyła RREP bezpośrednio do niego, jako kolejny skok do celu w alternatywnej trasie
 - Trasy główna i alternatywne tworzą strukturę sieci (mesh structure)
 - utrzymania trasy
 - Gdy węzeł wykryje awarię połączenia, rozgłasza pakiet do swoich najbliższych sąsiadów, w nagłówku którego umieszcza dane o zerwanym połączeniu. Gdy pakiet trafia do węzła, który posiada węzeł docelowy w swojej alternatywnej tablicy routingu, przekazuje pakiet dalej. W ten sposób tworzy się alternatywną trasę dla pakietu bez jego utraty.

Split Multipath Routing

- Jest protokołem routingu na żądanie.
- Tworzy maksymalnie rozłączoną ścieżkę między danym źródłem i celem
- Tworzonych jest wiele tras, a ruch sieciowy jest rozdzielany między nie celem uniknięcia przeciążenia i ułatwienia efektywnego wykorzystania zasobów sieciowych.
- Podobnie jak inne protokoły routingu na żądanie SMR tworzy wielokrotne trasy wykorzystując cykle żądanie – odpowiedź.
- Składa się zasadniczo z dwóch części: odkrywania trasy oraz utrzymania trasy

Caching and Multipath Routing Protocol



- Każdy węzeł posiada mały bufor na przechowywanie pakietów, które przez niego przeszły.
- Jeśli węzeł dalej na trasie odkrywa błąd w przekazywaniu, węzeł poprzedni na trasie posiadając odpowiednie dane w swoim buforze oraz dane o alternatywnej trasie może retransmitować dane.
- Jest użyteczny tylko w przypadku, gdy węzły przechowują dane o alternatywnej trasie do węzła docelowego.
- Głównymi cechami tego protokołu są: krótsze odkrywanie alternatywnych tras oraz wspólne buforowanie pakietów (cooperative packet caching)



Neighbour-Table-Based Multipath Routing w sieciach Ad Hoc

- Jest odmianą wielościeżkowego protokołu routingu, który radzi sobie ze stałymi zmianami w topologii mobilnych sieci ad hoc.
- Każdy węzeł przechowuje tablicę sąsiadów, która zapisuje jego sąsiadów osiągalnych w k -skokach.
- Protokół ten składa się również z dwóch części: odkrywania trasy oraz utrzymania trasy.
- Główny mechanizm polega na zbudowaniu dla każdego węzła tablicy sąsiadów oraz pamięci podręcznej tras.
- Trasy w tablicy sąsiadów są wykorzystywane w konstrukcji pamięci podręcznej tras jak i do ustalenia czasu życia (lifetime) połączeń bezprzewodowych, celem wspomaganie odkrywania trasy.

Charakterystyki protokołów

Protokół	Typy tras	Liczba tras	Trasy wykorzystywane do transmisji	Alternatywne trasy w węzłach pośrednich?	Caching tras	Skutek pojedynczej awarii trasy
MDSR	Rozdzielanie uwzględniające połączenie	Bez ograniczenia	Wykorzystywana jest najkrótsza trasa, alternatywne trasy są zachowywane jako backup	Tak	Tak	Pakiet błędu jest wysyłany do źródła. Węzeł pośredni z alternatywnymi trasami odpowiada i najkrótsza z tras jest używana.
AODV-BR	Nie konieczne rozłączanie	Bez ograniczenia	Wykorzystywana jest najkrótsza trasa, alternatywne trasy są zachowywane jako backup	Tak	Nie	Pakiet błędu jest rozgłaszany do najbliższych sąsiadów, sąsiad z alternatywną trasą do celu odpowiada i przekazuje dane do celu. Pakiet błędu trasy jest wysyłany do źródła celem zainicjowania odkrywania trasy.
SMR	Maksymalne rozłączanie	Dwie	Wykorzystywana jest najkrótsza trasa, alternatywne trasy są zachowywane jako backup	Nie	Nie	Pakiet błędu jest wysyłany i alternatywna trasa jest wykorzystywana do dalszej wysyłki danych.