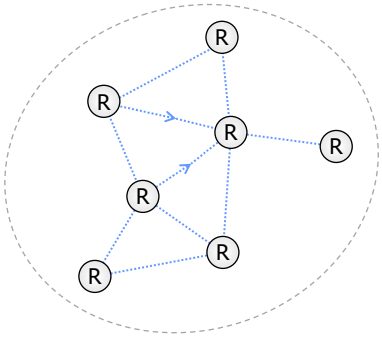
Mobilne sieci ad-hoc (MANET)

Sieci MANET

- **M**obile **A**d hoc **NET**works.
- Wywodzą się z lat 70-tych, z sieci PRnet (DARPA)
  - przed powstaniem Internetu!
  - protokół IP ma swoje korzenie właśnie w PRnet!
- Obecnie kierunki rozwoju koordynują 2 grupy IETF:
  - MANET i (od 2007) AUTOCONF Working Group,
  - cel ogólny to definicja struktury, protokołów routingu, autokonfiguracji węzłów oraz spójność z istniejącymi sieciami IP (np. z Internetem),
  - celem MANET WG jest standaryzacja protokołów routingu IP dla mobilnych i niemobilnych sieci ad hoc,
  - celem AUTOCONF WG jest standaryzacja mechanizmów autokonfiguracji węzłów sieci MANET.

Sieci MANET

MANET to sieć luźno powiązanych routerów w pojedynczej domenie, które mogą być mobilne, ulotne i dostępne przez zmienny i asymetryczny kanał komunikacji bezprzewodowej [2].



Sieci MANET

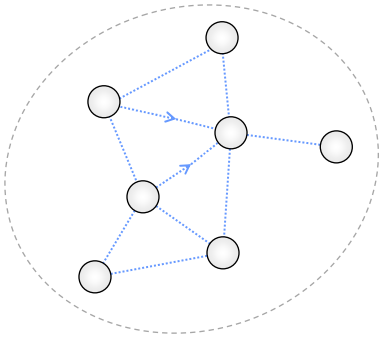
- Autonomiczna (niezależna) grupa mobilnych routerów.
  - może działać w całkowitej izolacji od innych sieci,
  - może posiadać bramki, które łączą ją ze „światem zewnętrznym”
    - wtedy MANET może działać jako sieć końcowa tzw. *stub network*.
- Sieć MANET tworzona jest spontanicznie (*ad hoc*).
- **Sieć warstwy trzeciej**
  - por. IBSS, *piconet*, *scatternet*, 802.15.4.
- Charakteryzuje się zmienną w czasie topologią typu *multi-hop*
  - por. WiFi, ZigBee.
- Działa w środowisku:
  - z ograniczeniami względem zasobów węzła,
  - z ograniczeniami względem jakości transmisji w sieci,
  - podatnym na naruszenie bezpieczeństwa.

Zastosowania

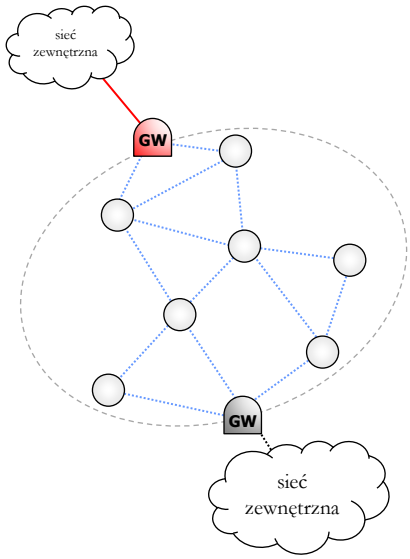
- Militarne (prace na sieciami MANET zapoczątkowane były w opracowaniach wojskowych)
  - zapewnienie łączności na polu walki
- Sytuacje zagrożeń i kataklizmów
  - zapewnienie łączności dla ekip ratunkowych na obszarze pożaru, powodzi, trzęsienia ziemi itp.,
  - w przypadku, gdy tradycyjna łączność zawiedzie.
- Zwiększenie dostępności do sieci komputerowej
  - swobodna łączność w budynkach, kopalniach itp.,
  - sieci PAN.

Scenariusze użycia

- Sieć izolowana
- Wykorzystanie protokołów routingu *ad hoc* do przekazywania pakietów
- Nie ma połączenia z innymi sieciami
  - łatwiejsza adresacja

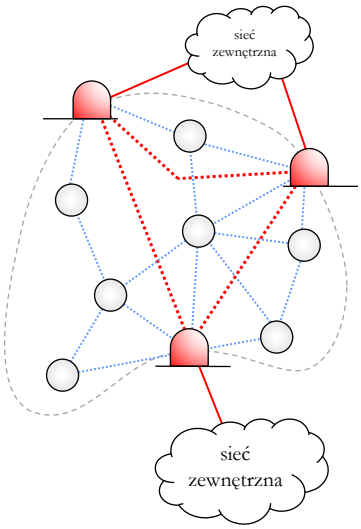


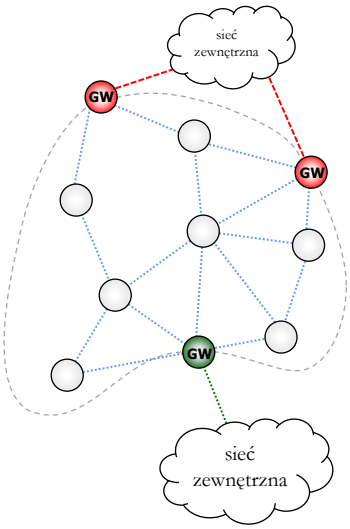
Scenariusze użycia



- MANET dołączony do sieci zewnętrznej
  - dołączenie poprzez bramki
- Bramka może pełnić dodatkowe funkcje
  - informowanie o ścieżkach z wewnątrz
  - kontrola dostępu do sieci zewnętrznej
  - serwisy np. DNS
  - równoważenie obciążenia – jeśli bramek jest więcej
- Bramki mogą
  - tworzyć tzw. *mesh network* lub
  - być uczestnikami MANETu

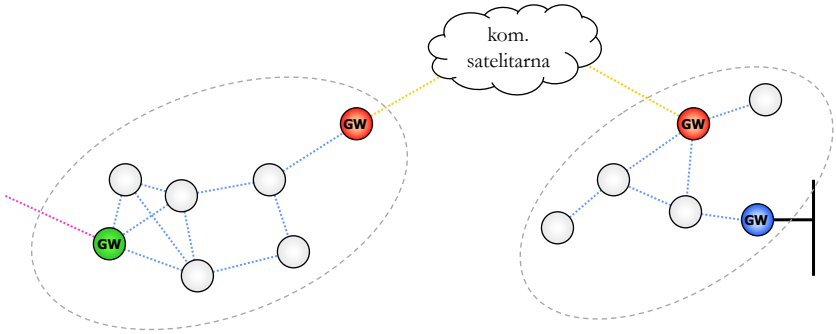
Scenariusze użycia





MANET w sytuacjach zagrożenia

- Sieci MANET są szczególnie przydatne:
  - w sytuacjach zagrożenia/kataklizmów,
  - na polu walki – systemy taktyczne.

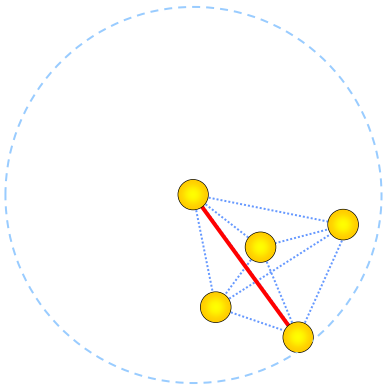


Charakterystyka sieci MANET

- Zalety:
  - zwiększają efektywność komunikacji bezprzewodowej (pojemność sieci),
  - wprowadzają możliwość spontanicznej komunikacji,
  - pozwalają na działanie w trudnych warunkach tj. bez infrastruktury.
- Wyzwania:
  - ograniczone możliwości łącza bezprzewodowego,
  - mobilność węzła,
  - spontaniczna natura sieci.
- Skutki:
  - efektywność komunikacji,
  - powstaje możliwość fragmentacji sieci,
  - kłopoty z ustaleniem adresacji,
  - trudno o dobór uniwersalnego protokołu routingu,
  - zwiększona podatność na naruszenie bezpieczeństwa komunikacji
    - w szczególności *man-in-the-middle*.

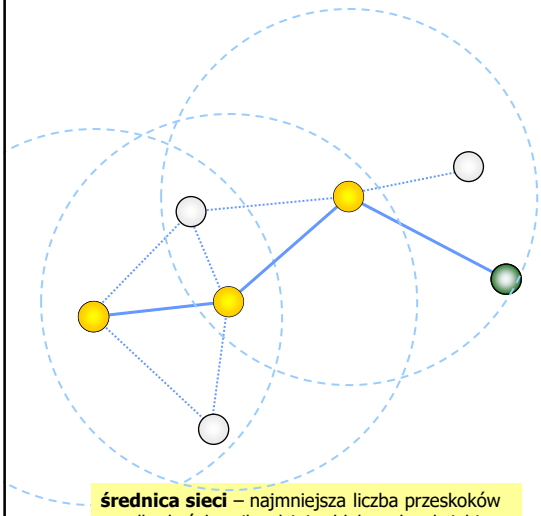
Single-hop

- graf pełny
  - wszystkie węzły w swoim zasięgu
  - zasięg ograniczony technologią komunikacji,
- współdzielenie przestrzeni
  - pojedyncza domena kolizyjna i rozgłoszeniowa,
  - większa interferencja,
  - mniejsza dopuszczalna liczba węzłów,
- nie ma konieczności stosowania routingu
  - por. IBSS, *piconet*, *scatternet*,



zasięg komunikacji

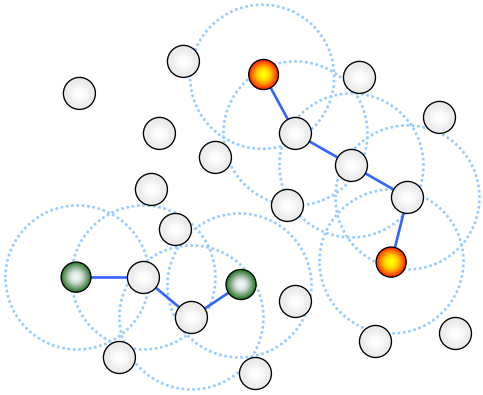
Multi-hop



średnica sieci – najmniejsza liczba przeskoków dla dwóch najbardziej oddalonych od siebie węzłów

- nie wszystkie węzły są w bezpośrednim zasięgu
  - uwaga sieci Bluetooth,
  - uwaga rozgłaszanie,
  - zasięg poszerzony.
- każda stacja uczestniczy w przekazywaniu ruchu
  - większe zapotrzebowanie na zasoby,
  - konieczność stosowania routingu lub przełączania.
- większe rozproszenie – mniejsza interferencja
  - większa dopuszczalna liczba węzłów w sieci,
  - zwiększona pojemność sieci.
- wiele segmentów sieci połączonych przełącznicą/routerem.

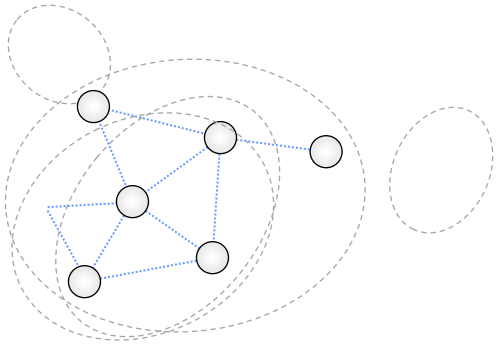
Pojemność sieci



Jaki to rodzaj multipleksacji?

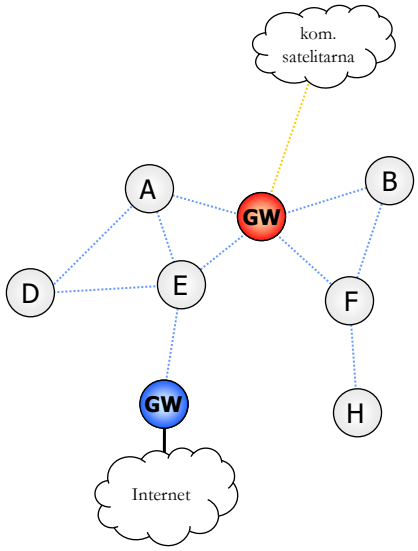
Problem fragmentacji sieci

- Pełna swoboda w poruszaniu się węzłów może doprowadzić do chwilowej bądź długotrwałej fragmentacji
  - rozmycie stanu sieci.
- W sieciach mobilnych jest to istotny problem
  - powoduje wiele kłopotów w warstwach wyższych (4+).



Adresacja

- Jak zapewnić łączność węzłów w obrębie sieci MANET?
  - unikalność adresów
- Jak zapewnić łączność węzłów w Internetem?
- Ustalenie adresów w sieci MANET:
  - statyczne...
    - nieefektywne,
    - sprzeczne z ideą *ad hoc*,
  - dynamicznie
    - potrzebne mechanizmy autokonfiguracji.



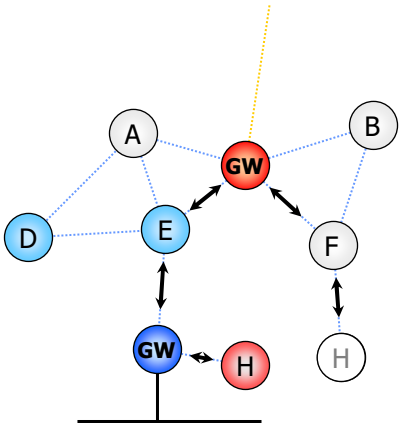
Adresacja

- Mechanizmy autokonfiguracji:
  - m.in. bezstanowa i stanowa autokonfiguracja IPv6

  niewystarczające
  - projektowane dla sieci *single-hop* i pojedynczej domeny rozgłoszeniowej,
  - niedostosowane do sieci *multi-hop*, dynamicznej topologii i częstej fragmentacji i scalania sieci,
- Bramki do sieci publicznej mogą też być węzłami MANET
  - co, jeśli bramka zniknie z sieci?
    - wszystkie węzły, które wykorzystywały do komunikacji prefiks ogłaszany przez tą bramkę muszą poszukać nowej.
- Zmiana adresu może stanowić problem dla protokołu routingu:
  - np. w OLSR zmiana adresu węzła równoznaczna jest z uszkodzeniem węzła
    - potrzebny jest czas na propagację informacji o „nowym" węźle lub
    - modyfikacja protokołu.

Adresacja

- Wybór prefiksu wymusza przekazywanie ruchu przez bramkę, która ten prefiks ogłasza.
- Każda bramka ogłasza inny prefiks
  - w przeciwnym razie utrudniłoby to komunikację z siecią publiczną.
- Wybór prefiksu dla adresu globalnego może mieć istotny wpływ na efektywność komunikacji.



Adresacja

- Bardzo wiele propozycji rozwiązań:
  - dla sieci autonomicznych
  - dla sieci podłączonych
- Przykładowe rozwiązanie [9] polega na:
  - przydzieleniu węzłowi jednego niezmiennego adresu tzw. *Primary Address* (PADD) poprawnego w obrębie sieci MANET
    - np. adresu *Unique Local IPv6 Unicast Address*,
  - przydzieleniu węzłowi zero lub więcej adresów publicznych z prefiksami bramek tzw. *Secondary Addresses* (SADD)
    - węzeł wybiera (na podstawie routingu) domyślny adres SADD, który będzie wykorzystywać w komunikacji (DSADD),
    - informacja o pozostałych adresach SADD jest (w zależności od protokołu) rozgłaszana w sieci.

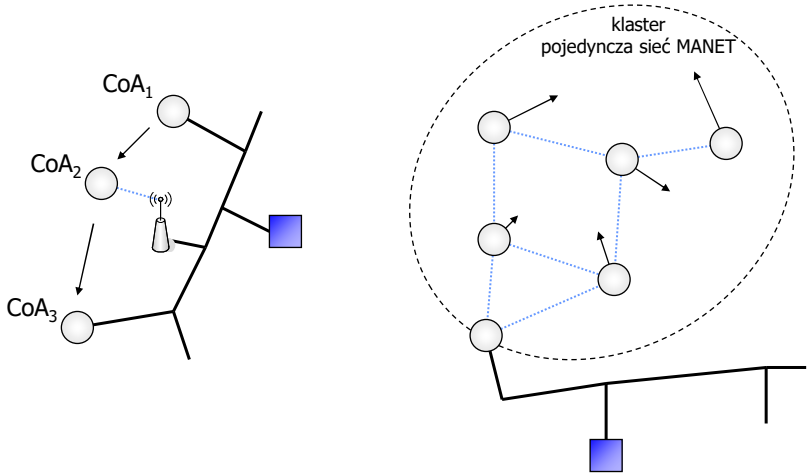
Adresacja

- Inne propozycje – bramka pracująca jako NAT:
  - Założenie 1: sieć MANET to sieć ad-hoc więc ma charakter sieci prywatnej,
  - Założenie 2: każdy węzeł ustala unikalny adres prywatny w sieci
  - węzeł komunikujący się z siecią zewnętrzną wybiera (najlepszą, osiągalną) bramkę, z której chce korzystać w danym momencie,
  - zadaniem bramki jest dokonywać translacji adresów z puli MANET na pulę zgodną z jej prefixem,
  - węzeł zawsze jest osiągalny pod adresem PADD.
  - wezeł może poprosić wybraną bramkę (jeśli jest zadowolony z jej usług, bo np. jest trwała i szybka) o publiczny adres z puli z jej prefixem.
- Prace nad autokonfiguracją węzłów w sieci MANET trwają
  - protokoły routingu powstawały wcześniej zakładając istnienie w sieci poprawnej adresacji,
  - problem adresacji pozostawiony był „na później”.

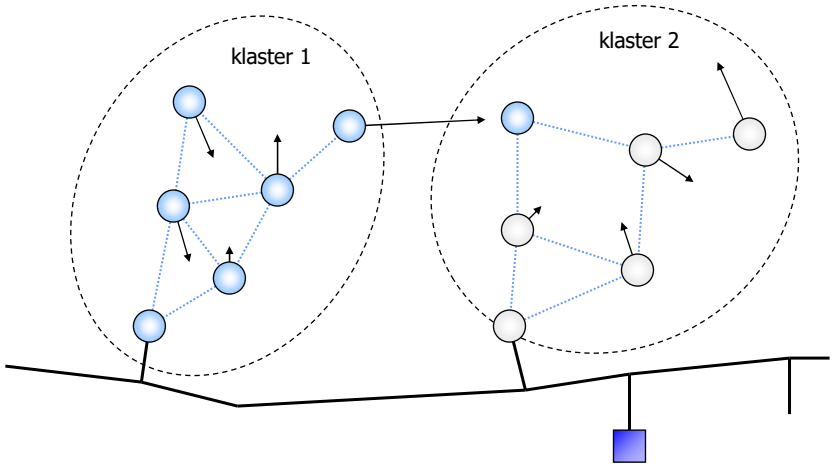
MobileIP vs MANET

- MobileIP
  - wymaga istnienia infrastruktury
  - niewielka liczba węzłów wędrujących pomiędzy potencjalnie dużą liczbą sieci
  - do komunikacji wykorzystuje istniejące mechanizmy routingu i tunelowania
- MANET
  - sieci tworzone w sposób spontaniczny
  - mogą pozostawać całkowicie autonomiczne; bez konieczności istnienia infrastruktury,
  - zakładają mobilność wszystkich węzłów,
  - wymagają dostosowania mechniazmów komunikacyjnych do nowego środowiska.

MobileIP vs MANET



MobileIP i MANET



Kierowanie ruchem

- W jaki sposób można zrealizować komunikację w bezprzewodowej sieci *ad hoc multi-hop*?
  - przełączanie/bridging – warstwa 2
    - ESS w WiFi, *piconet*/*scatternet* w Bluetooth.
  - routing – warstwa 3
    - jedna sieć IP/czy wiele sieci IP?
- MANET ⇒ routing L3, ale...

Routing w sieciach MANET

- Potrzebne jest inne podejście niż w sieciach przewodowych.
- Istnieją pewne istotne czynniki mające duży wpływ na jakość protokołu:
  - szybkość zmian topologii sieci,
  - pojemność łączy,
  - modele ruchu węzłów,
  - częstość i procent węzłów w stanie uśpienia,
  - rozmiar sieci: średnica, liczba węzłów,
  - *network connectivity* - stopień „wypełnienia” grafu,
  - procent łączy jednokierunkowych.
- Nie ma protokołu routingu, który będzie zachowywał się dobrze dla dowolnych wartości ww. parametrów.

Routing w sieciach mobilnych

- Istnieje wiele sposobów klasyfikacji protokołów routingu:
  - statyczny – dynamiczny,
  - dystans-wektor – stanu przyłączy,
  - źródłowy,
  - wewnętrzny – zewnętrzny.
  - proaktywny – reaktywny,
  - hybrydowe
  - single-hop – multi-hop,
  - z podziałem na strefy rozgłaszania,
  - kontekstowy np.: location aware routing.

Routing reaktywny/proaktywny

- Routing reaktywny działa wyłącznie na żądanie.
- W konsekwencji protokół reaktywny:
  - nie jest aktywny, jeśli wszystkie węzły znają trasę do swoich węzłów docelowych,
  - może generować większe opóźnienia w stosunku do protokołu proaktywnego,
  - dobrze znosi większe szybkości poruszania się terminali,
  - źle znosi bardziej zróżnicowane charakterystyki ruchu (wiele różnych par źródło-odbiorca).
- Routing proaktywny działa cały czas.

reactive – reacting to events or situations rather than acting first to change or prevent something
proactive – taking action by causing change and not only reacting to change when it happens
Cambridge Advanced Learner's Dictionary

Problem zbieżności

- Co to jest zbieżność protokołu routingu?
- Kiedy ten problem występuje w sieciach przewodowych?
- W sieciach mobilnych problem zbieżności ma dużo większe znaczenie
  - im większa szybkość zbieżności tym większa dopuszczalna mobilność węzłów

Mobilność

- Im większa mobilność węzłów tym większy narzut komunikacyjny
  - lepsze zachowanie protokołów reaktywnych przy niskim zróżnicowaniu charakterystyki ruchu,
- Im większa mobilność węzłów tym mniejsza zbieżność protokołu
  - granica zbieżności przesuwa się w nieskończoność w zależności od szybkości poruszania się węzłów w stosunku do szybkości przekazywania pakietów.

Narzut routingu dynamicznego

- W sieciach mobilnych szczególnie istotny problem
  - przepustowości łączy bezprzewodowych są zwykle o 1, 2 rzędy wielkości niższa niż łączy przewodowych,
  - zmienność topologii sieci wymusza
    - czasami częstszą,
    - czasami bardziej intensywną,

    komunikację modułów routingu,

Routing w sieci MANET

- Istnieje bardzo wiele protokołów routingu dla mobilnych sieci ad hoc:
  - reaktywne:
    - *Dynamic Source Routing* (DSR), *Ad hoc On-demand Distance Vector* (AODV), *Dynamic MANET On-demand Routing* (DYMO),
  - proaktywne:
    - *Destination-Sequenced Distance Vector* (DSDV), *Fisheye State Routing* (FSR), *Link State Routing* (LSR), *Optimized Link State Routing* (OLSR), *Topology Dissemination Based on Reverse-Path Forwarding* (TBRPF), *IPv6 Routing Protocol for Low-power and Lossy networks (RPL), Better Approach To Mobile Adhoc Networking (B.A.T.M.A.N.)*
  - mieszane (hybrydowe):
    - *Zone Routing Protocol* (ZRP), *Temporally-Ordered Routing Algorithm* (TORA), *Geographical Routing Algorithm* (GRA).
- Parametry ustandaryzowane
  - porty 269/TCP, 269/UDP
  - wartość pola protokołu w nagłówku IPv4 - 138

Dynamic Source Routing

- Opracowany w 1996 przez D. Johnsona i D. Maltza [6]
- Protokół reaktywny tj. działa na żądanie.
- Przewidziany dla sieci do 200 węzłów o stosunkowo dużym stopniu mobilności
- Przewidziany dla niewielkich sieci o średnicy 5 do 10 skoków, ale często większych niż 1.
- Umożliwia kierowanie ruchu do celu wieloma ścieżkami tzw. *multipath routing*
  - równoważenie obciążenia
  - zwiększenie przepustowości (pojemność)
- Zapewnia routing bez pętli.

Dynamic Source Routing

- Wykorzystuje dwa mechanizmy *route discovery* i *route maintenance*:
  - korzysta z nich „na żądanie”
  - nie generuje żadnych pakietów okresowo np.:
    - stanu przyłączy,
    - wykrywania sąsiadów
  - w szczególności, gdy sieć „zastygnie” i wszystkie potrzebne w sieci ścieżki są znane, DSR nie generuje **żadnego** ruchu,
  - ruch generowany przez DSR wzmaga się w miarę coraz większej mobilności węzłów oraz w przypadku kierowania pakietów do nowych węzłów docelowych

Dynamic Source Routing

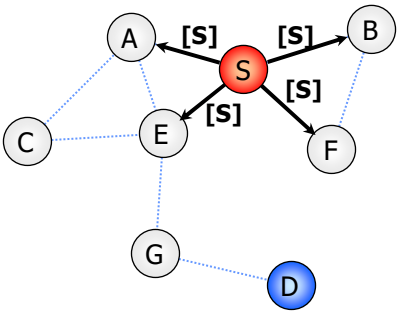
- Wykorzystuje routing źródłowy tj.:
  - w nagłówku każdego pakietu danych zapisana jest ścieżka przez którą powinien on przewędrować do celu.
- Dzięki temu:
  - można zapewnić routing bez pętli – węzeł źródłowy określa odpowiednią ścieżkę,
  - trasa może w łatwy sposób być zapamiętana w pamięci podręcznej przez węzły pośredniczące – optymalizacja,
  - równoważenie obciążenia – optymalizacja.

DSR – ***route discovery***

- Jeśli węzeł źródłowy S chce przesłać dane do węzła docelowego D to musi określić ścieżkę routowania (Dynamic **Source** Routing)
  - poszukując ścieżki w tzw. *Route Cache'u*,
  - wykorzystując mechanizm *route discovery.*
- Wykrywanie ścieżki następuje poprzez zalewanie:
  - inicjator (S) generuje na lokalny *broadcast* zapytanie *Route Request* (RREQ)
- Wezeł S może przechowywać więcej niż jedną ścieżkę do D, dzięki czemu w razie unieważnienia jednej istnieją ścieżki zapasowe
  - nie ma wtedy potrzeby wykonywania kolejnego *route discovery*,
- Może być wykorzystywany na łączach jednokierunkowych oraz asymetrycznych

DSR – *route discovery*

- Węzeł źródłowy S chce przesłać dane do węzła docelowego D.
- S nie ma żadnych informacji nt. D
  - inicjuje więc mechanizm wykrywania ścieżki
- Wysyła zapytanie RREQ na lokalny *broadcast*.

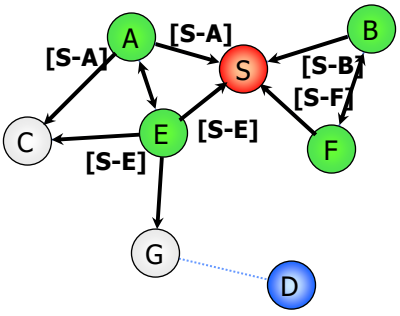


węzły w zasięgu komunikacji

transmisja pakietów RREQ z trasą określoną w [...]

DSR – *route discovery*

- Gdy węzeł pośredni otrzymuje pakiet *Route Request* przekazuje go dalej tak samo tj. na lokalny *broadcast*
- Zapisuje jednocześnie swój adres na liście węzłów pośrednich:
  - o ile już go tam nie ma, bądź ostatnio przetwarzał on RREQ z tym samym identyfikatorem i z tego samego źródła
  - w takim przypadku porzuca pakiet.

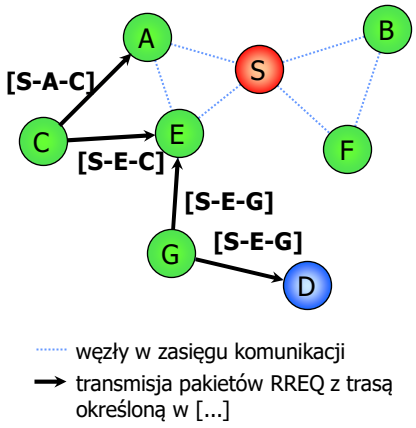


węzły w zasięgu komunikacji

transmisja pakietów RREQ z trasą określoną w [...]

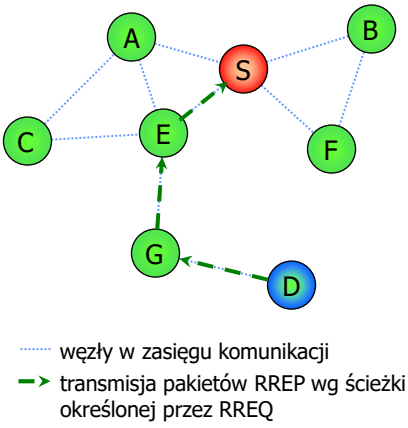
DSR – *route discovery*

- Gdy węzeł pośredni otrzymuje pakiet *Route Request* przekazuje go dalej tak samo tj. na lokalny *broadcast*.
- Zapisuje jednocześnie swój adres na liście węzłów pośrednich:
  - o ile nie już go tam nie ma, bądź ostatnio przetwarzał on RREQ z tym samym identyfikatorem i z tego samego źródła,
  - w takim przypadku porzuca pakiet.



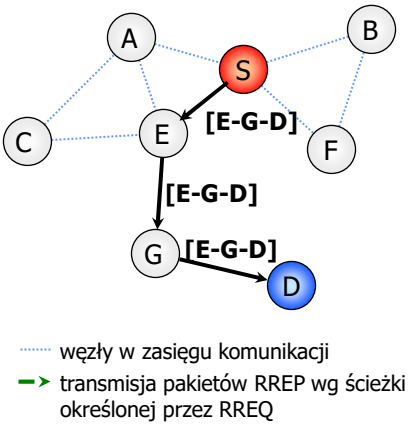
DSR – *route discovery*

- Gdy węzeł docelowy otrzyma pakiet RREQ odpowiada do źródła pakietem *Route Reply*, który zawiera zapamiętaną trasę.
- Odpowiedź wędruje trasą z cache'a bądź wg odwróconej listy węzłów pośredniczących z pakietu RREQ
  - to z kolei wymaga, aby warstwa łącza danych umożliwiała komunikację dwukierunkową,
  - jeśli tak nie jest to D lub inny węzeł pośredni generuje *route discovery*.



DSR – dostarczanie danych

- Węzeł S zapamiętuje trasę w swoim Route Cache'u.
- Dane dostarczane są za pomocą routingu źródłowego (*strict*)
  - tj. do nagłówka pakietu dołączana jest trasa.

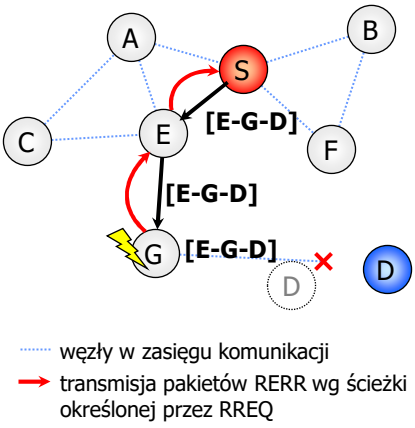


DSR – *route maintenance*

- Utrzymanie aktywnych ścieżek.
- Każdy węzeł odpowiedzialny jest za weryfikację łącza ze swoimi sąsiadami:
  - poprzez potwierdzenia warstwy łącza danych np. w WiFi, Bluetooth
  - poprzez pasywne potwierdzenie np. węzeł słyszy, że jego następnik transmituje dane do swojego następnika,
  - poprzez okresowe wymuszenie potwierdzenia odbioru pakietu.
- Po nieotrzymaniu potwierdzenia przez pewien czas, węzeł wysyłający usuwa wpis ze swojego *Route Cache'a* i wysyła *Route Error* do wszystkich węzłów, które używały tego przejścia
- W przypadku unieważnienia ścieżki, S może zacząć używać innej trasy, może też za pomocą *route discovery* wykryć nową trasę.

DSR – *route error*

- Węzeł G odnotowuje fakt o zerwaniu łącza do D.
- Po otrzymaniu pakietu do D, węzeł G generuje błąd o uszkodzeniu łącza z D (pakiet *Route Error*)
- Wszystkie węzły pośredniczące usuwają ze swojego cache'a wpisy ze ścieżką G-D.



Rozszerzone *route discovery*

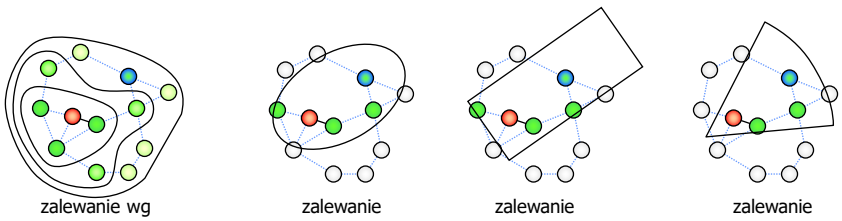
- Węzeł pośredniczący, który wchodzi w posiadanie informacji nt. ścieżki do celu wpisuje ją do swojego cache'a
  - *promiscuous mode*,
  - *packet forwarding*.
- Węzeł pośredniczący, który w swoim Route Cache'u ma zapisaną trasę do celu dokonuje konkatenacji dotychczas przebytej trasy pakietu z trasą zapisaną w cache'u
  - podczas konstrukcji trasy węzeł musi zapewnić, aby powstała ścieżka nie zawierała pętli
  - zwrócona trasa MUSI zawierać węzeł pośredniczący.

Rozszerzone *route discovery*

- Pole TTL może służyć do ograniczenia zasięgu zapytania *route discovery*.
- Może też być wykorzystane w celu zapytania o trasę najpierw tylko sąsiadów (TTL=1) a dopiero potem normalne zapytanie.
- Istnieje też strategia „expanding ring” z powiększaniem TTL o jeden przy każdym niepowodzeniu w wykrywaniu ścieżki
  - zwiększone opóźnienia

Mechanizmy zalewania

- Niekorzystny wpływ na sieć bezprzewodową.
- Istnieją algorytmy ograniczające przestrzeń zalewania:
  - najprostsze – według pola *hop-limit* (TTL) (w DSR),
  - wymagające znajomości położenia geograficznego
    - eliptyczne, wstęgowe, sektorowe, itp.



zalewanie wg pola *hop-limit* | zalewanie eliptyczne | zalewanie wstęgowe | zalewanie sektorowe

Rozszerzone *route maintenance*

- Po uszkodzeniu połączenia i otrzymaniu Route Error węzeł źródłowy przekazuje Route Error w kolejnych zapytaniach Route Request
  - dzięki temu w odpowiedzi węzeł nie otrzyma ponownie ścieżki, w której znajduje się uszkodzone łącze,
  - ponadto węzły będą miały okazję zaktualizować sobie Route Cache

Inne mechanizmy

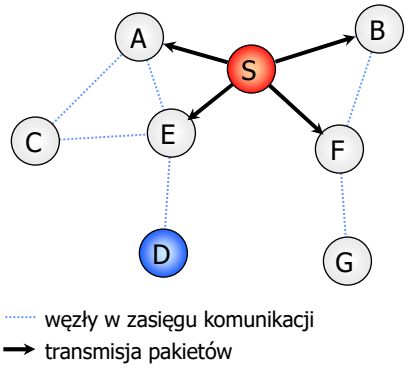
- DSR Flow State – zmniejszenie narzutu związanego z routowaniem źródłowym.
- Skracanie ścieżki – jeśli węzeł pośredniczący podsłucha pakiet nie skierowany bezpośrednio do niego, a węzeł znajduje się dalej na liście węzłów pośredniczących to może wygenerować *Gratuitous Route Reply* do źródła
- Ratowanie pakietów – jeśli w węźle pośredniczącym ścieżka, którą pakiet ma być przekazany okazuje się błędna:
  - węzeł generuje Route Error do źródła oraz
  - jeśli w Route Cache'u posiada dodatkową trasę to wykorzystuje ją do przekazania pakietu dalej (podmienia trasę pakietu). Podmiana jest ograniczana przez pewną wartość progową.

AODV

- *Ad Hoc On-Demand Distance Vector* [7]
- Podobnie jak DSR:
  - protokół routingu dla sieci mobilnych ad hoc multi-hop,
  - protokół reaktywny,
  - gwarantuje ochronę przed pętlami,
  - wykorzystuje zapytania RREQ, odpowiedzi RREP i RERR
    - w zapytaniach wykorzystywane jest zalewanie,
  - informacja o ścieżce przechowywana jest we wszystkich węzłach pośredniczących w ruchu.
- Inaczej niż DSR:
  - informacje o ścieżce przechowywane są w formie wpisów w tablicy routingu
    - w zamian za przechowywanie kompletnych tras w tablicy *Route Cache* [DSR],
  - dostępna jest tylko jedna, najbardziej aktualna, trasa,
  - przeznaczony dla większych sieci: dziesiątki do tysięcy węzłów mobilnych.

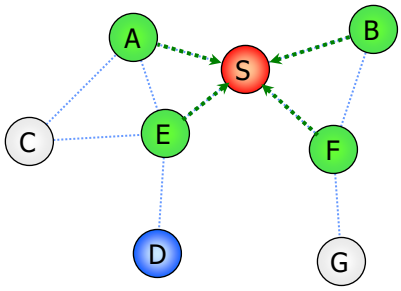
co to znaczy?

AODV - Poszukiwanie węzła docelowego



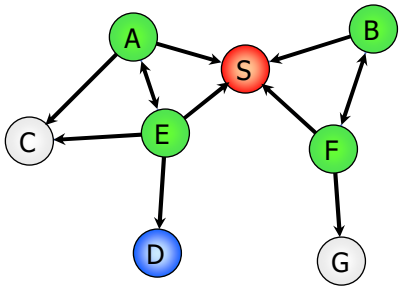
- Węzeł źródłowy S otrzymuje z warstwy wyższej pakiet skierowany do węzła D.
- Protokół routingu AODV nie znając trasy do D generuje zapytanie RREQ (*Route Request*).
- Zapytanie wysyłane jest do wszystkich sąsiadów
  - broadcast – zalewanie.

AODV - Poszukiwanie węzła docelowego



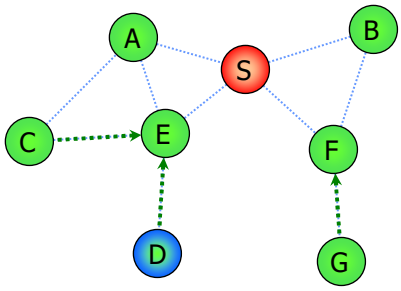
- Sąsiedzi 1-skoku wpisują do tablicy routingu ścieżkę powrotną do S.

AODV - Poszukiwanie węzła docelowego



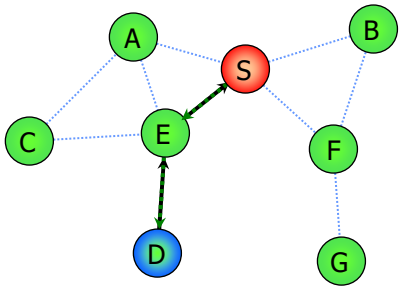
- Sąsiedzi 1-skoku wpisują do tablicy routingu ścieżkę powrotną do S.
- Każdy węzeł przekazuje zapytanie dalej, do wszystkich swoich sąsiadów
  - zalewanie

AODV - Poszukiwanie węzła docelowego



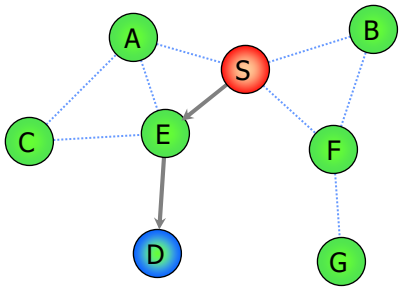
- Sąsiedzi 2-skoku wpisują do tablicy routingu ścieżkę powrotną do S.

AODV - Poszukiwanie węzła docelowego



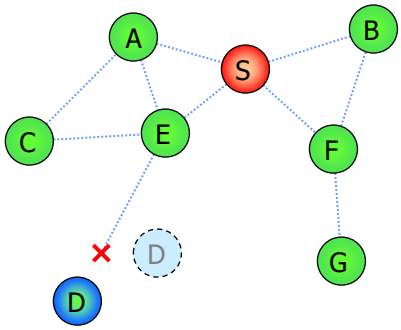
- Sąsiedzi 2-skoku wpisują do tablicy routingu ścieżkę powrotną do S.
- Węzeł docelowy generuje odpowiedź RREP (*Route Reply*) formuując jednocześnie ścieżkę dla pakietów z S tzw. *forward path*

AODV - Transmisja danych



- Po znalezieniu węzła D (otrzymaniu odpowiedzi RREP) węzeł S może kierować do niego zgromadzone pakiety

AODV - Zerwanie łączności



- Z S do D prowadzi aktywna ścieżka, którą wędrują pakiety.
- Jeśli np. D wyjdzie z zasięgu węzła E nastąpi przerwanie ścieżki.
- W takim przypadku E generuje komunikat RERR o nieaktualnej ścieżce.

Utrzymanie aktywnych ścieżek

- Węzeł pośredniczący w ruchu powinien zadbać o utrzymanie aktualnego stanu łączy aktywnych ścieżek:
  - przy użyciu mechanizmów 2 warstwy,
  - na skutek odebrania jakiegokolwiek pakietu od sąsiada,
  - przy użyciu mechanizmu ICMP Echo,
  - przy wykorzystaniu komunikatów AODV Hello.
- Jeśli ścieżka do sąsiada okaże się nieaktywna to:
  - węzeł ją unieważnia oraz
  - przekazuje wszystkim zainteresowanym komunikat RERR.

AODV

- Przeznaczony dla
  - sieci złożonych z dziesiątków a nawet tysięcy bezprzewodowych i mobilnych węzłów,
  - sieci z niską i średnią mobilnością,
- W większości przypadków AODV jest bardziej wydajny od DSR
  - DSR lepszy dla niewielkich sieci o mniej złożonych charakterystykach ruchu.

DYMO

- DYMO - Dynamic MANET On-demand,
- Następca AODV,
- Może działać jako protokół proaktywny i reaktywny,
- Ustalenia trasy:
  - Wysłanie komunikatu rozgłoszeniowego "Route Request" (RREQ) od nadawcy poprzez węzły pośrednie do odbiorcy. Każdy węzeł dodaje informacje o sobie do RREQ.
  - Po otrzymaniu przez odbiorcę docelowego RREQ, wysyłany jest przez niego komunikat "Routing Reply" (RREP) potwierdzający wyznaczenie żądanej ścieżki.

Protokół RPL

- RPL - Routing Protocol for Low Power and Lossy Networks,
- Opis standardu – IETF RFC 6550 (03.2012),
- Przeznaczony dla routingu w sieciach IPv6 złożonych z urządzeń mobilnych (np. sensorów) o ograniczonych zasobach (pamięć, procesor, zasilanie) – sieci Low-power Lossy Networks (LLNs),
- Komunikacja w sieciach LLNs jest realizowana m.in. z wykorzystaniem technologii: IEEE 802.15.4, Bluetooth, Low Power WiFi, przewodowych (w tym PLC - Powerline Communication).

Protokół RPL

- Protokół proaktywny,
- Wykorzystuje optymalne drzewo bez cykli do wyznaczania drogi pakietów,
- Metryka może uwzględniać: opóźnienie, pewność lub stan węzła (wł./wył.),
- Definiuje nowe wiadomości ICMPv6 (DAG Information Object, DAG Information Solicitation, Destination Advertisement Object).
- Wykorzystywany w koncepcji IoT (*Internet of Things*)

Protokół B.A.T.M.A.N.

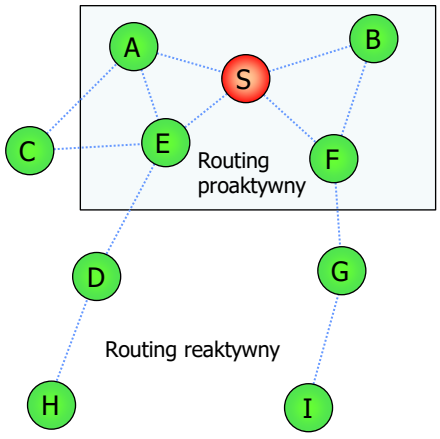
- Better Approach To Mobile Adhoc Networking (B.A.T.M.A.N.)
- Protokół proaktywny,
- Następca protokołu OLSR,
- Możliwość wykorzystania routingu na poziomie warstwy 2 (łącza danych) zamiast na warstwie 3 (sieciowej).
- Zamiast wysyłania pakietów UDP istnieje możliwość udostępnienia wirtualnych interfejsów sieciowych i wykorzystania ich do wyznaczania tras.

Protokół B.A.T.M.A.N.

- B.A.T.M.A.N. eliminuje konieczność rozpowszechnianie informacji dotyczących zmian w sieci do każdego węzła sieci.
- Poszczególny węzeł zapisuje informacje jedynie o "kierunku" z którego otrzymał dane.
- Dane są wysyłane od węzła do węzła i pakiet otrzymuje bezpośrednio dynamicznie stworzoną trasę.

Protokoły hybrydowe

- Łączą w sobie cechy protokołów proaktywnych i reaktywnych
- Routing proaktywny jest zastosowany do utrzymania stałego połączenia z bliskimi węzłami.
- Odległe węzły są objęte routingiem reaktywnym.



Protokół hybrydowy - ZRP

- Zone Routing Protocol (ZRP) – protokół obszarowy gdzie węzły są pogrupowane na obszary.
- Wewnątrz obszaru ścieżki są dostępne natychmiast.
- Dostęp do węzłów spoza obszaru wymaga uruchomienia procedury wyszukania ścieżki.
- Struktura protokołu ZRP jest płaska i nie ma zależności pomiędzy obszarami.

Protokół hybrydowy - TORA

- Temporally-Ordered Routing Algorithm (TORA) – protokół minimalizujący potrzebę licznych reakcji na zmiany w topologii sieci.
- Funkcje - tworzenie, utrzymanie i usunięcie ścieżek.
- Dwa rodzaje komunikatów kontrolnych:
  - Lokalne, wysyłane częściej, o bardzo małym zasięgu, ograniczające się do węzłów w pobliżu nadawcy.
  - Dalekiego zasięgu, wysyłane rzadko, w odległe punkty sieci. Częstość wysyłania komunikatów dalekiego zasięgu jest stała, nie zależy od szybkości zmian topologii.

Zarządzanie zasilaniem

- Urządzenia mobilne w sieci MANET mają ograniczony czas pracy ze względu na wykorzystywane baterie lub akumulatory.
- Jednym z pomysłów na wydłużenie czasu pracy jest wprowadzenie urządzenia w stan uśpienia w sytuacji kiedy nie jest prowadzona transmisja.
- Innym sposobem na ograniczenie zużycia energii jest dynamiczne sterowanie mocą nadajników czyli zwiększanie lub zmniejszanie mocy nadawania w celu utrzymania odpowiedniej jakości transmisji przy optymalnym zużyciu energii.

Zarządzanie zasilaniem

- Istnieje możliwość monitorowania węzła na poziomie warstwy fizycznej (zajętość medium, poziom błędów itp.) i określania prawdopodobieństwa poprawnej transmisji. W sytuacji kiedy prawdopodobieństwo poprawnej transmisji jest niskie, urządzenia (węzły sieci MANET) mogą w ogóle nie wysyłać danych i tym samym zaoszczędzić energię.
- Także protokoły routingu w sieci MANET powinny uwzględniać aspekty oszczędzania energii przez węzły. Dlatego do wyznaczania drogi przesyłanych danych powinny być uwzględnione (w metryce) informacje o zasilaniu węzła. Metryka w protokołach routingu powinna opierać się na najmniejszym koszcie a nie na najkrótszej ścieżce.

Zarządzanie zasilaniem

- Opracowywane są także mechanizmy oszczędzania energii wbudowane w protokoły warstwy 2 i 3 modelu OSI/ISO.
- Oprócz rozwiązań projektowanych dla sieci MANET oszczędzanie energii jest realizowane na wielu płaszczyznach związanych z urządzeniami mobilnymi (procesory, pamięci, układy transmisji bezprzewodowej itp.)

Bezpieczeństwo

- Sieci MANET wykorzystują technologie radiowe które są trudne do zabezpieczania (między innymi przed podsłuchem).
- Istnieje niebezpieczeństwo wprowadzania niepożądanych węzłów które mogą zakłócać pracę protokołów routingu.
- Pewne mechanizmy wykrywające zagrożenia są zawarte w niektórych specyfikacjach protokołów routingu w sieciach MANET. Przykładowo w protokole AODV każdy z węzłów posiada licznik odpowiedzialny za zapisywanie informacji o nieoczekiwanych zachowaniach sąsiednich węzłów. W przypadku przekroczenia określonej wartości tego licznika informacja ta jest wysyłana do sąsiednich węzłów.

Bezpieczeństwo

- Charakter sieci MANET (brak punkty centralnego) powoduje problemy z centralnym zarządzaniem certyfikatami wykorzystywanymi przy technologiach szyfrowania oraz całościowym monitorowaniem i zarządzaniem siecią.
- Dystrybucja kluczy (potrzebna do szyfrowania danych) nie jest realizowana przez system centralny a zamiast tego każdy węzeł w sieci MANET wykorzystuje swoje lokalne repozytorium. Przy nawiązywaniu połączenia dwa węzły scalają swoje lokalne repozytoria w celu znalezienia odpowiednich łańcuchów certyfikacyjnych (potrzebne dość duże pasmo do stworzenia lokalnego repozytorium, proces wykonywany stosunkowo rzadko).

Podsumowanie

- Małe
  - 2-30 węzłów
- Średnie
  - 30-100 węzłów
- Duże
  - 100-1000 węzłów
- Bardzo duże
  - >1000 węzłów

- Płaska struktura MANET powoduje trudności komunikacji w sieciach dużych i bardzo dużych
  - aktywne pole badań

Podsumowanie

- Sieci MANET – autonomiczny zbiór mobilnych węzłów.
- Szczególnie przydatne w sytuacjach zagrożenia, na polu walki
  - wszędzie tam, gdzie rozproszenie i swoboda dostępu do sieci jest najbardziej istotna,
  - coraz częściej stosowane w sieciach prywatnych.
- Mobilność jest czynnikiem, który stanowi największe wyzwanie dla efektywnej komunikacji.
- Wprowadzenie adresacji w tego typu sieciach nie jest sprawą trywialną
  - pojawiają się problemy z agregacją ruchu z sieci publicznej,
  - w sieciach MANET dużo trudniej o hierarchizację, por. VLSM w sieciach przewodowych.
- Istnieje bardzo wiele protokołów routingu dla sieci MANET
  - niestety nie ma jednego/kilku, które byłyby uniwersalne.
- Obecnie sieci typu MANET
  - z jednej strony tracą nieco na znaczeniu przez coraz wydajniejszą komunikacje w oparciu o infrastrukturę tj. WiFi, WiMAX, LTE, LTA-A i kom. satelitarną ale z drugiej strony szansą dla ich rozwoju jest na przykład koncepcja IoT.
- Ważne zagadnienia – zarządzanie zasilaniem oraz bezpieczeństwo !

Literatura

1. Bacelli E.: *Address Autoconfiguration for MANET: Terminology and Problem Statement*, IETF AUTOCONF Working Group, Internet-Draft, February 2008.
2. Bernardos C., Calderon M., Moustafa H.: *Survey of IP address autoconfiguration mechanisms for MANETs*, IETF AUTOCONF Working Group, Internet-Draft, November 2008.
3. Cała J.: *Mobilne sieci ad-hoc w technologii Bluetooth*. TeleNetforum 06/2002.
4. Chakeres I., Macker J., Clausen T.: *Mobile Ad hoc Network Architecture*. IETF AUTOCONF Working Group, Internet-Draft, November 2007.
5. Corson S., Macker J.: *Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations*. Request for Comments 2501, January 1999.
6. Johnson D.B., Maltz D.A., Hu Y.-C.: *The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks*. IETF MANET Working Group, Internet-Draft, 19 July 2004.
7. Perkins C.E., Belding-Royer E., Das S.: *Ad hoc On-Demand Distance Vector (AODV) Routing*. Request for Comments 3561, July 2003.
8. Perkins C.E., Royer E.M., Das S.R., Marina M.K.: *Performance Comparison of Two On-Demand Routing Protocols for Ad Hoc Networks*. IEEE Personal Communications, February 2001.
9. Ruffino S., Stupar P.: *Automatic configuration of IPv6 addresses for nodes in a MANET with multiple gateways*. IETF MANET Working Group, Internet-Draft, June 2005.
10. Tymofiejewicz A., Witos G.: *Ocena nowych protokołów doboru trasy w sieciach multi-hop ad hoc*. Praca dyplomowa, Katedra Telekomunikacji, Akademia Górniczo-Hutnicza. Kraków, 2006.
11. Suchan B., Fronczyk M.: *Lokalizacja i udostępnianie serwisów w sieciach MANET*. Praca dyplomowa, Katedra Informatyki, Akademia Górniczo-Hutnicza. Kraków, 2011.