Mariusz BEDNARCZYK, Grzegorz RÓŻAŃSKI

Wojskowa Akademia Techniczna, Wydział Elektroniki

doi:10.15199/48.2015.03.09

Taktyczne sieci ad hoc na współczesnym polu walki

Streszczenie. *W artykule została przedstawiona analiza wymagań dla taktycznych sieci ad hoc oraz aktualna ich realizacja na tle dostępnych na rynku rozwiązań. W świetle tego co oferują aktualnie producenci wydaje się, że jeszcze długa droga do osiągnięcia akceptowalnego stopnia zadowolenia, mimo że znaczenie sieci ad hoc na współczesnym polu walki wydaje się nieocenione.*

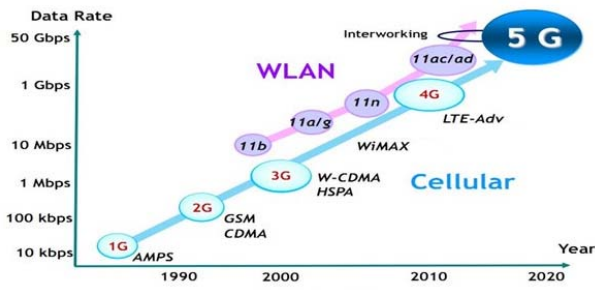
Abstract*. The purpose of this paper is to assess and compare the requirements for tactical ad hoc networks with commercial solutions available on the civilian market. (**Tactical Ad Hoc Battlefield Networking**).*

Słowa kluczowe: sieci ad hoc, zarządzanie zasobami, protokoły routingu, jakość usług, bezpieczeństwo.
Keywords: ad hoc networks, resource management, routing, quality of service, security.

Wstęp

W obserwowanym od wielu lat wyścigu przy wdrażaniu nowych technologii w dziedzinie telekomunikacji szczególnie duży postęp daje się obserwować w obszarze sieci bezprzewodowych. O prymat w dziedzinie bezprzewodowej transmisji danych na dużą odległość walczą dziś trzy technologie: UMTS, LTE i WiFi. Co zaskakuje, w roku 2004 nikt nie miał wątpliwości, że z kolei technologia WiMAX wygra z WiFi. W roku 2006 nie było to już tak pewne, a w 2009 okazało się, że jego rozwój skutecznie został przyhamował przez operatorów telefonii komórkowej, oferujących dostęp do Internetu za pośrednictwem UMTS, HSDPA a obecnie LTE (*Long-Term Evolution*) (rysunek 1). Wydaje się, że technologia jutra w przypadku dużych obszarów, to technologia 4G. W sieciach lokalnych natomiast na dobre przyjmie się standard IEEE 802.11ac/ad, gdzie kolejne wersje sterowników pozwolą na osiągnięcie przepustowości rzędu Gb/s.

Wśród głównych argumentów, decydujących o atrakcyjności technologii bezprzewodowych, w pierwszej kolejności wymienia się: wsparcie dla mobilności użytkowników, elastyczność w konfigurowaniu sieci i skalowalność rozwiązań bezprzewodowych. Istotne są także szybkość i prostota instalacji, zwłaszcza w kontekście częstych rekonfiguracji. Jak widać, rynek cywilny rozwija się w tym kontekście bardzo szybko. Jednak z wojskowego punktu widzenia, nastawionego obecnie na pozyskiwanie i adaptowanie istniejących rozwiązań (tzw. *Commercial Of The Shelf*), wciąż są technologiami wymagającymi dostosowania do szczególnych uwarunkowań potencjalnego wykorzystania, zwłaszcza w odniesieniu do wymagań niezawodnego, bezpiecznego i przede wszystkim terminowego dostarczania informacji.



Rys. 1. Przewidywany rozwój technologii bezprzewodowych [1]

Dzisiejsze sieci taktyczne ewoluują w stronę złożonych sieci heterogenicznych, w których przynajmniej kilka węzłów może równocześnie wykorzystywać różne technologie do komunikacji z innymi węzłami. Dostępne na rynku rozwiązania nie pozwalają jeszcze na tworzenie takich złożonych, dynamicznie konfigurowalnych i zarządzanych systemów sieciowych, funkcjonujących przy braku stałej infrastruktury oraz wysokiej mobilności węzłów. Dodatkowo czasowa natura łączy radiowych, a przy okazji wysoki wymóg dotyczący niezawodności wciąż stwarzają wiele problemów, z których najważniejsze to:

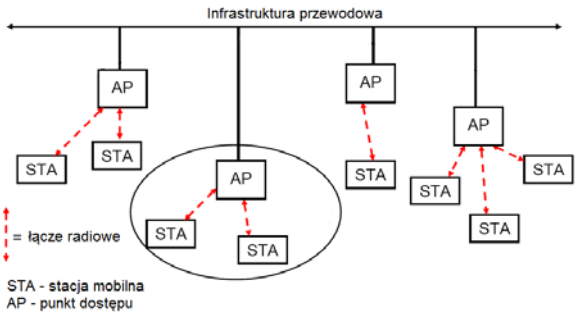
- ograniczenie wzajemnego oddziaływania współzawodniczących między sobą technologii przez dobór odpowiednich protokołów warstwy fizycznej,
- utrzymanie łączności przy dynamicznie zmieniającej się topologii sieci (także w sieci zdegradowanej) poprzez wykorzystanie efektywnych protokołów routingu, uwzględniających także zasoby energetyczne węzłów,
- zachowanie równowagi pomiędzy parametrami sieci, takimi jak: opóźnienia, straty pakietów itd.,
- zagwarantowanie wysokiego poziomu bezpieczeństwa pracy w sieci.

Celem artykułu jest analiza dostępnych na rynku rozwiązań i możliwości ich wykorzystania na współczesnym polu walki biorąc pod uwagę specyfikę oraz charakter prowadzonych operacji. Istotnym bowiem w tym obszarze jest kompleksowe zabezpieczanie działających wojsk w informacje, a możliwość łączenia poszczególnych sieci (domen) w złożone struktury heterogeniczne jest w stanie to zagwarantować [2]. Problem jednak w tym, że oferowane rozwiązania nie mogą być łatwo przeniesione na grunt wojskowy. Przede wszystkim dlatego, że bazują na wykorzystaniu infrastruktury stacjonarnej.

Podstawowe założenia dla systemów cywilnych

Technologie bezprzewodowe sektora cywilnego, zarówno telefonii komórkowej jak i transmisji danych nie są rozwiązaniami opartymi wyłącznie na medium radiowym. W dużej mierze opierają się na wykorzystaniu stacjonarnej infrastrukturze przewodowej jako sieci szkieletowej, do której dostęp jest oferowany poprzez specjalizowane urządzenia wyposażone w dwa interfejsy sieciowe: przewodowy i bezprzewodowy (rysunek 2). Przyjęcie założenia bazującego na infrastrukturze stacjonarnej zaowocowało powstaniem wielu dojrzałych rozwiązań oferujących użytkownikom zaawansowane usługi teleinformatyczne nawet w trakcie przemieszczania się. Są to jednak sieci o charakterze stacjonarnym. Bezprzewodowość jest tu rozpatrywana jedynie na odcinku pojedynczego skoku, umożliwiającego połączenie ze stacją bazową czy punktem dostępowym. Pozostałą trasę stanowią łącza przewodowe zazwyczaj o wysokiej przepustowości. Są one w stanie zagwarantować określoną jakość usług, a łącza radiowe w wielu przypadkach nie stanowią już tzw. „wąskiego gardła”, czego przykładem jest chociażby nowy standard dla WiFi IEEE 802.11ac oferujący przepustowość rzędu 1,7 Gb/s.

Tymczasem takie podejście nie jest akceptowalne z wojskowego punktu widzenia, gdyż użytkownicy nie tylko mogą się przemieszczać i wychodzić poza zasięg oddziaływania stacji bazowej, ale także mogą pracować w warunkach występowania silnych zakłóceń celowych. Co więcej, taki rodzaj struktury zawsze wprowadza „słabe punkty" do sieci w postaci tzw. „pojedynczych punktów uszkodzeń", których neutralizacja skutecznie utrudnia, a nawet uniemożliwia realizację komunikacji między użytkownikami.



Rys. 2. Sieci bezprzewodowe są de facto przewodowe

To co jest również charakterystyczne, to możliwość wyboru dogodnych miejsc instalacji stacji bazowych gwarantujących dostęp do sieci w każdym miejscu. Ułatwia to zarówno pokrycie zasięgiem sieci określonego obszaru, jak i zarządzanie samą siecią. Dodatkowo, decydując się na jednego producenta urządzeń, administrator ma pewność, że nie wystąpią problemy z ich współpracą. W odróżnieniu od wymagań stawianych przez sieci taktyczne, urządzenia radiowe nie muszą implementować mechanizmów utrudniających stwierdzenie ich pracy LPI/LPD (*Lower Probability of Intercept/Lower Probability of Detection*), czy posiadać zwiększoną odporność na zakłócenia celowe AJ (*Anty Jamming*) ograniczające ich zdolności transmisyjne.

Taktyczne sieci ad hoc

Bezprzewodowe sieci taktyczne cechują się wysoką dynamiką zmian w strukturze oraz ograniczonymi zasobami sieciowymi. Sieci te często mają strukturę heterogeniczną, zróżnicowaną politykę bezpieczeństwa, charakteryzują się niskimi zdolnościami przepustowymi i są szczególnie narażone na degradację wskutek zakłóceń oraz uszkodzeń (zniszczeń). Ich użytkownicy natomiast oczekują, że usługi będą realizowane bez zakłóceń, także w czasie przemieszczania urządzeń ze znaczną szybkością i to zarówno wewnątrz pojedynczej domeny, jak i pomiędzy różnymi domenami. Wymagania takie implikują dodatkowe mechanizmy, które w odróżnieniu od rozwiązań cywilnych, umożliwią:

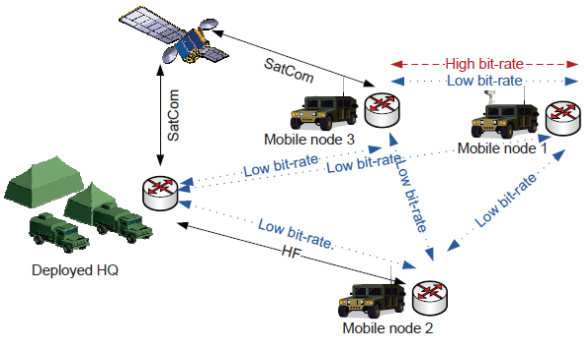
- zmianę struktury sieci przez rezygnację ze zbędnych lub aktywację dodatkowych łączy pomiędzy węzłami,
- wykorzystanie odpowiednich metryk i algorytmów doboru tras wraz ze wskazaniem sposobu modyfikacji struktury sieci zgodnie z przyjętą polityką bezpieczeństwa oraz jakości usług (QoS),
- wykrywanie charakterystyk ruchu w sieci pozwalających na równoważenie wykorzystania zasobów,
- zabezpieczenie sieci przed nieuprawnionym dostępem oraz zapewnienie poufności danych,
- eliminowanie zagrożeń związanych z celowymi atakami na bezpieczeństwo w sieci.

Jak widać z powyższego, wyzwaniem jest nie tylko realizacja usług z wymaganą jakością, ale również transfer danych poprzez różne domeny wykorzystujące niekiedy inne technologie radiowe i charakteryzujące się różnym stopniem zaufania z naszej strony.

Prowadzone przez Europejską Agencję Obrony (EDA) projekty skupiają się na opracowaniu wydajnych mechanizmów w zakresie warstwy fizycznej (tzw. radio kognitywne). W warstwach łącza danych i wyższych proponuje się przeważnie standardowe mechanizmy Internetowe oparte na stosie protokołów TCP/IP. Dotyczy to również architektury jakości usług. Prezentowane rozwiązania koncentrują się na modyfikacji mechanizmu dostępu do medium poprzez wprowadzenie kontroli przyjmowania usług gwarantujący QoS dla różnych klas aplikacji. Coraz częściej podkreślana jest jednak konieczność wykorzystywania informacji dostarczanych przez różne warstwy modelu odniesienia (*cross-layer engineering*), tak aby uzyskać jak najpełniejszy obraz funkcjonowania sieci radiowej. Ideą współpracy międzywarstwowej jest bowiem przekazanie informacji o stanie medium transmisyjnego do warstw wyższych, w celu uruchomienia procedur zapewniających jego optymalne wykorzystanie w trakcie realizacji usług. W przypadku sieci bezprzewodowych, większość informacji, które mogłyby być wykorzystane do efektywnego sterowania ruchem, jest dostępna w warstwie MAC odpowiedzialnej za sterowanie dostępem do medium. Są to informacje o poziomach odbieranych sygnałów, ustawionych parametrach transmisyjnych, przy jednoczesnym umożliwieniu zbierania różnego rodzaju statystyk dotyczących aktywności stacji. Aktualne badania potwierdzają jednak, że proces projektowania międzywarstwowego nie zawsze prowadzi do uzyskania korzystnych rezultatów i z tego względu powinien być realizowany z dużą ostrożnością [3][4].

Protokoły sieciowe

Zgodnie z tendencją „all-IP", technologią warstwy trzeciej, która zapewni współpracę sieci heterogenicznych będzie rodzina protokołów IP. Wymaga to jednak dopasowania stosu IP do ograniczeń charakterystycznych dla taktycznych sieci ad-hoc, w której mogą być wykorzystywane różne środki łączności (rysunek 3).



Rys. 3. Przykładowa sieci ad hoc wykorzystująca różne środki łączności [10]

Podstawowym wymogiem jest tu dostosowanie protokołu IP do łączy o niskiej przepustowości. Wymaga to zastosowania kompresji i fragmentacji oraz autokonfiguracji adresów z możliwością ich zastępowania odpowiednio krótkimi identyfikatorami (np. zgodnie z EUI-64 w przypadku IPv6). Pojawiające się w literaturze rozwiązania nie uwzględniają wszystkich czynników w sposób kompleksowy i dotyczą w zasadzie sieci o relatywnie dużych zdolnościach przepustowych. Tymczasem należy zdawać sobie sprawę, że taktyczne sieci ad hoc należy traktować jako zbiór systemów autonomicznych, w których węzły mogą wykorzystywać różnego rodzaju interfejsy radiowe. Przekazanie informacji może wymagać wykorzystanie różnych technologii, w tym także oferujących niskie

przepustowości, zależnie od aktualnie będących w dyspozycji.

Problematyka dotycząca sterowania ruchem i zapewnienia jakości usług w sieciach o małej przepustowości poruszana jest jedynie w ramach grupy roboczej IETF o nazwie „*Routing Over Low power and Lossy networks*" [11]. W dokumencie RFC 4944 [12] przedstawiła ona założenia do sposobu funkcjonowania stosu IPv6 w sieciach opartych na standardzie IEEE 802.15.4 oferujących szybkość transmisji danych do 250 kb/s. Pojawiły się również praktyczne aspekty wykorzystania nowego rozwiązania w odniesieniu do urządzeń o niewielkich mocach obliczeniowych i ograniczonym poziomie energii zasilania [13]. Wpisuje się to jak najbardziej w naturę taktycznych sieci ad hoc. Samo rozwiązanie wprawdzie wymaga dalszego rozwoju, np. związanego z routingiem, ale jest już na tyle stabilne, że można założyć iż jest to tylko kwestia czasu.

Routing

Szczególnie istotne z punktu widzenia taktycznych sieci ad hoc są mechanizmy zarządzania topologią oraz dostępnymi zasobami sieci w celu efektywnego reagowania na dynamiczne zmiany w strukturze sieci. Chodzi tu o szybką reakcję na zmiany w konfiguracji sieci i połączeń pomiędzy węzłami, przy stosunkowo niedużym dodatkowym obciążeniu zasobów [14].

W sieciach radiowych funkcje te są de facto wbudowane w protokół routingu. Dzięki niemu można zapewnić monitorowanie stanu sieci, węzłów i łączy oraz dokonywać wyboru ścieżek transmisyjnych w zależności od przyjętych kryteriów i wymagań stawianych przez usługi. Obecnie istnieje wiele propozycji protokołów routingu dla bezprzewodowych sieci ad-hoc, z czego najliczniejszą grupę stanowią propozycje grupy IETF MANET (*Mobile Ad hoc Network*) [5]. W zależności od przyjętego kryterium można je podzielić na kilka grup. Powszechnie stosowany jest podział na protokoły proaktywne i reaktywne.

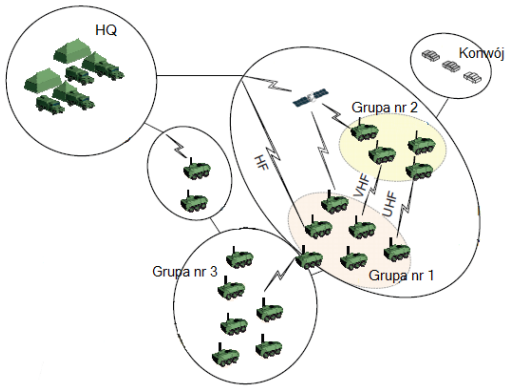
Protokoły proaktywne przechowują informacje o struturze sieci oraz trasach do wszystkich węzłów bez względu na to, czy zmieniają one swoje położenie, czy nie. Informacje o ścieżkach są cyklicznie odnawiane w celu dostosowania się do zmieniających się warunków w sieci (przeciążenie medium lub utrata połączenia). Częste uaktualnianie tras powoduje dodatkowe obciążenia związane z ruchem kontrolnym w sieci oraz zwiększeniem zużycia energii.

Protokoły reaktywne z kolei, wyszukują trasy tylko wtedy, kiedy jest to konieczne. Cechuje je mniejsze obciążenie łącza oraz zużycie energii. Wadą tych protokołów jest zwiększenie opóźnienia dostarczenia komunikatu do odbiorcy spowodowane koniecznością najpierw wyznaczenia trasy.

Istnieje ok. 50 różnych rozwiązań, przy czym tylko dwa są aktywnie rozwijane: protokół reaktywny - AODV (*Ad hoc On demand Distance Vector*) [6] i proaktywny - OLSR (*Optimized Link State Routing*) [7]. Grupa MANET pracuje nad 2. generacją tych protokołów, tj. OLSRv2 [9] oraz DYMO (*Dynamic MANET On-demand*) [8] jako sukcesor protokołu AODV.

Nie spełniają one jednak wymagań stawianych przez taktycznych sieci ad-hoc. W szczególności nie są w stanie, w odpowiednio krótkim czasie, reagować na zmiany konfiguracji sieci i połączeń pomiędzy węzłami. Ponadto ich działanie wymaga zazwyczaj zużycia znacznych zasobów energetycznych, które są znacznie ograniczone w przypadku urządzeń korzystających z niewielkich baterii. Istotnym problemem, na który jest zwracana uwaga, to zapewnienie stacjom klienckim informacji o równoległych ścieżkach przepływu danych. Istnienie tras zabezpieczających pozwoli zapewnić ciągłość realizowanych usług, także w przypadku umyślnego działania czynników zewnętrznych. Ponieważ czas niezbędny na przeprowadzenie odpowiednich działań i retransmisję danych, które nie zostały dostarczone do węzłów docelowych w okresie pomiędzy wystąpieniem zakłócenia (lub ataku), a aktywacją ścieżki zabezpieczającej może być długi, konieczne są odpowiednie metryki i algorytmy doboru tras, które uwzględniać będą nie tylko właściwość łącz radiowych oraz warstwy dostępu do medium, ale także rodzaj usługi przenoszonej w sieci oraz jej wymagania jakościowe.

Ponadto, ze względu na możliwość wykorzystywania przez węzły różnych rodzajów interfejsów radiowych, jak i hierarchiczność wzajemnych relacji informacyjnych w sieci taktycznej, należy ją traktować jako zbiór systemów autonomicznych. Routing w takim przypadku musi uwzględniać możliwość transferu danych zarówno wewnątrz jak i pomiędzy domenami. O ile w pierwszym przypadku sytuacja jest korzystniejsza ze względu na homogeniczność rozwiązań sieciowych (interfejsów, stosowanych standardów, wykorzystywanych protokołów), o tyle w drugim jest już bardziej skomplikowana. Wynika to przede wszystkim z braku rozwiązań dla protokołów routingu międzysystemowego uwzględniających mobilność całych domen. Zazwyczaj wybór drogi między takimi systemami realizowany jest z wykorzystaniem protokołów routingu międzydomenowego, które zazwyczaj bazują na rozszerzeniach bądź modyfikacjach protokołu BGP (*Border Gateway Protocol*) [15]. Wolna zbieżność tego protokołu i jego statyczna konfiguracja wymagają stałej topologii sieci. W przeciwnym wypadku następuje znaczna utrata transmitowanych danych. Statyczna struktura sieci nie jest możliwa do utrzymania w sieciach taktycznych, gdzie poszczególne systemy autonomiczne mogą się przemieszczać i tracić, bądź zyskiwać nowe dowiązania do innych systemów autonomicznych. Sytuacja może się zmieniać w czasie i struktura sieci może być zupełnie inna niż w momencie uruchamiania.



Rys. 4. Przykład dynamiki sytuacji w sieci taktycznej (na podstawie [10])

Sytuacja taka jest widoczna na rysunku 4, gdzie do domeny utworzonej przez grupy nr 1 i 2 dowiązał się konwój, a dodatkowo do grupy nr 1 grupa zadaniowa nr 3. W takim przypadku, aby możliwe było wykorzystanie standardowego protokołu BGP konieczne jest opracowanie nowego mechanizmu zarządzania konfiguracją, który zapewni rozszerzenie funkcjonalności protokołu BGP do pracy w sieciach z przemieszczającymi się domenami.

Bezpieczeństwo

Jedną z istotniejszych kwestii w taktycznych sieciach ad hoc jest zapewnienie odpowiedniego poziomu bezpieczeństwa. Problem dodatkowo się komplikuje, jeśli weźmie się pod uwagę różne poziomy wrażliwości transmitowanej informacji oraz różne stopnie zaufania do węzłów pośredniczących w transmisji. W momencie transferu danych poprzez różne domeny szczególnie istotny staje się dobór tras poprzez węzły o stopniu zaufania odpowiednim do poziomu wrażliwości przenoszonych informacji. Konieczne są tu rozbudowane mechanizmy tworzenia wiedzy o stopniu zaufania do współpracujących węzłów, na podstawie której będzie podejmowana decyzja o sposobie sterowania ruchem. Wysyłanie danych o najwyższym poziomie wrażliwości łączami, które nie są bezpieczne, może spowodować wyciek lub przejęcie danych przez osoby nieuprawnione. Brak mechanizmów pozwalających na wybór trasy o odpowiednim poziomie wrażliwości lub umożliwiających dokonania oceny ryzyka, jakie się wiąże z wyborem danej ścieżki może prowadzić do niepowodzenia misji. W związku z tym, ważnym aspektem jest uwierzytelnianie i autoryzacja elementów sieciowych już na etapie formowania sieci oraz w momencie dołączania się nowego użytkownika czy domeny. Wiedza o stopniu zaufania do współpracujących węzłów musi być stale uaktualniana ze względu na zmiany w topologii sieci mobilnej, możliwe ataki na tożsamość węzła, a także działania zmuszające węzły do pracy pod przymusem. W tym ostatnim przypadku konieczne są rozwiązania pozwalające na blokowanie lub izolowanie wybranych węzłów, przy jednoczesnym stałym ich śledzeniu i braku objawów wskazujących na odkrycie skompromitowanego działania. Jest to szczególnie trudne zważywszy na coraz bardziej wyszukane formy prowadzenia ataków na bezpieczeństwo sieci i coraz trudniejsze ich wykrycie.

W efekcie musi być implementowana architektura bezpieczeństwa wielopoziomowego. Wiążą się z tym odpowiednio zdefiniowane reguły i zasady dotyczące uwierzytelniania i autoryzacji komponentów sieci taktycznej w dynamicznych fazach jej aktywności. Dodatkowo niezbędne są mechanizmy obrony ograniczające możliwość wystąpienia ataku na zasoby sieci oraz integralność i poufność danych. Złożoność problemów i konieczność ich ujęcia w sposób kompleksowy powoduje, że wciąż stanowią przedmiot intensywnych badań.

Podsumowanie

Podstawowym wymaganiem stawianym taktycznym sieciom ad hoc, niezależnie od realizowanej koncepcji zapewniania jakości usług, jest optymalne wykorzystanie zasobów sieci. Zadanie to nabiera szczególnego znaczenia, jeśli weźmie się pod uwagę uwarunkowania, w których te sieci funkcjonują:

- duża różnorodność środków teleinformatycznych o różnych, także niskich zdolnościach przepustowych,
- częsta zmienność położenia węzłów,
- wykorzystywanie głównie urządzeń zasilanych przez źródła bateryjne o skończonej pojemności,
- wysoki współczynnik narażenia na degradację wskutek zakłóceń oraz zniszczeń.

Do głównych problemów należą zadania związane z zarządzaniem zasobami, w tym zadania wyznaczania optymalnych tras, sterowania przepływem oraz zagadnienia dotyczące bezpiecznego transferu danych. Złożoność proponowanych mechanizmów będzie zależała od złożoności potrzeb różnicowania jakości usług dostarczanych jednocześnie różnym grupom użytkowników przy jednoczesnym uwzględnianiu zmienności i dynamiki zachowań w pracy sieci. Aktualnie prowadzone prace dążą do rozwiązania jednostkowych problemów, bez wglądu na kompleksowość rozwiązania. Stąd niejednokrotnie ciekawe propozycje nie mogą być adoptowane wprost, ale muszą być dopiero adaptowane do wymagań taktycznych sieci ad hoc. Tak jest np. w przypadku silnie promowanych protokołów routingu dla sieci MANET jak OLSR czy AODV, które nie biorą pod uwagę poziomu energii zasilania węzłów, podobnie protokołu BGP, który nie uwzględnia mobilności domen.

Z przedstawionej w artykule problematyki wynika, że jeszcze wiele kwestii musi być rozwiązanych, a od tego jak szybko zostanie to zrobione będzie zależała możliwość wykorzystania taktycznych sieci ad hoc na współczesnym polu walki.

LITERATURA

[1] Osang Kweon, *Mobile Broadband Market Trends and Insight*, ITU Workshop on Bridging the Strd. Gap, July, 2012

[2] *Priorytetowe kierunki badań w resorcie obrony narodowej na lata 2013-2022*, DNiSW MON, 2013

[3] Edirisinghe, R., Zaslavsky A., *Cross-Layer Contextual Interactions in Wireless Networks*, IEEE Communications Surveys & Tutorials, vol. 16, issue: 2, pp. 1114-1134, 2014

[4] Bin Hu, Zhongmin Wang, *A cross-layer congestion control algorithm for underground mine video transmission over wireless networks*, ICNSC'2014

[5] strona: http://www.ietf.org/html.charters/manet-charter.html

[6] Perkins C., et al., *Ad hoc On-Demand Distance Vector (AODV) Routing*, RFC 3561, July 2003

[7] Clausen T., Jaquet P., *Optimized Link State Routing Protocol (OLSR)*, RFC 3626, Oct. 2003,

[8] Perkins C., et al., *Dynamic MANET On-demand (AODVv2) Routing*, draft-ietf-manet-dymo-26, Feb. 2013

[9] Clausen T., et al., *The Optimized Link State Routing Protocol version 2, draft-ietf-manet-olsrv2*, October 2011

[10] Hauge M., et al., *Multi-Topology routing for QoS support in the CoNSIS convoy MANET*, MCC'2012

[11] RFC 4919, *IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals, Network Working Group*, Aug. 2007

[12] RFC 4944, *Transmission of IPv6 Packets over IEEE 802.15.4 Networks, Network Working Group*, Sept. 2007

[13] Pediredla B., Kevin I-Kai Wang, et al., *A 6LoWPAN implementation for memory constrained and power efficient wireless sensor nodes*, IECON 2013

[14] Krygier J., Bednarczyk M., Maślanka K., *Efektywny transfer danych w bezprzewodowych sieciach kratowych i sensorowych*, Przegląd Elektrotechniczny nr 07/2013

[15] Rekhter Y., et al., *A Border Gateway Protocol 4 (BGP-4)*, RFC 4271, January 2006

Autorzy: *dr inż. Mariusz Bednarczyk, Wojskowa Akademia Techniczna, Wydział Elektroniki, ul. Gen S. Kaliskiego 2, 00-908 Warszawa, E-mail:* mbednarczyk@wat.edu.pl*; dr hab. inż. Grzegorz Różański, Wojskowa Akademia Techniczna, Wydział Elektroniki, ul. Gen S. Kaliskiego 2, 00-908 Warszawa, E-mail:* grozanski@wat.edu