STUDIA INFORMATICA 2001
Volume 22 Number 2 (44)

Radosław RUCHAŁA
Wyższa Szkoła Biznesu – National-Louis University, Katedra Informatyki
Krzysztof ZIELIŃSKI
Akademia Górniczo-Hutnicza, Katedra Informatyki

IPv6 IN THE CONTEXT OF MOBILE APPLICATIONS

Summary. Massive deployment of mobile access devices with exiting IPv4 protocol is impossible because of very limited address space, lack of QoS, and proper security support. This increases demand on IPv6 protocol deployment for mobile applications. We present analysis of IPv6 advantages and required extensions to the standard mobility and routing schemas and also give two examples of applications, which would benefit from it.

PROTOKÓŁ IPv6 W KONTEKŚCIE APLIKACJI MOBILNYCH

Streszczenie. Intensywny rozwój urządzeń mobilnych wykorzystujących protokół IPv4 jest ograniczony przez niedostateczną przestrzeń adresową, brak standardowych mechanizmów QoS i odpowiedniego bezpieczeństwa. Skłania to do wykorzystywania protokołu IPv6. Artykuł ten prezentuje zalety samego IPv6, jak też niektóre jego rozszerzenia istotne z punktu widzenia tworzonych aplikacji mobilnych. Dwie takie aplikacje zostały również krótko opisane w niniejszej pracy.

1. Introduction

Mobility is going to be the most demanding feature of access system to information in the 21st century. The access to information should be provided 7x24 a week anywhere, anytime, on anything. This very well known phrase corresponds to forecasts of the most prestige companies on IT technology market. According to this in a year 2004 most information from Internet will be accessible by mobile devices such as PDA and Internet enable cellular phones. IP is a solid, widely accepted by industry standard, which has created foundations of

the currently observed phenomena – rapid grow of networking application. It is a cornerstone of the success of new emerging net-economy. It does not leave any doubt the modern mobile network access devices should support IP protocol. Unfortunately the massive deployment of mobile access devices with exiting IPv4 protocol is impossible because of very limited address space, lack of QoS, and proper security support. This increases demand on IPv6 protocol deployment for mobile applications.

This paper discusses mobility model defined mainly for IP protocol. Next, in this context, the analysis of IPv6 advantages and required extensions of the standard mobility protocol and routing schemas is presented. Finally, examples of some applications using mobile access over IPv6 are shortly described. The paper is ended with summary presenting the objectives of 6WINIT project under which the presented work has been started.

2. Mobility – basic model, refinements

Mobile computing is a very large concept. There are three different forms of mobility [1] in the Internet, we can observe today:

- portable computers, which are transported and re-connected from remote locations;
- mobile computers, which stay connected most of the time during the movement;
- mobile networks, the whole networks connected during their movement.

Portable computing is only the first step toward full mobility – which takes the form of mobile computing, sometimes called also 'ubiquitous computing'.

2.1. IETF mobility model

This mobility is the subject of IETF mobileip charter works [3,4]. It is based on two hard requirements, which assume that the mobile host should be capable of:

- continuing to communicate, using the same IP address, after it has been disconnected from the Internet and reconnected at a different point – to preserve TCP connections,
- interoperating with existing hosts, routers and services – to provide gradual deployment.

Additionally, mobility should provide so-called soft requirements:

- no weakening of IP security,
- multicast capability,
- location privacy.

Normally one wouldn't be able to continue its communication until he re-configures the system with new IP address, the correct netmask and default router address. The problem is based in routing mechanisms currently used in the Internet.

Today's version of Internet protocol – IPv4 assumes that any node has always the same point of attachment. Additionally the node's IP address identifies the link on which the node is available. Existing routing protocols are not able to handle mobility without additional enhancement, because they require the network address to change when a host moves to the new location.

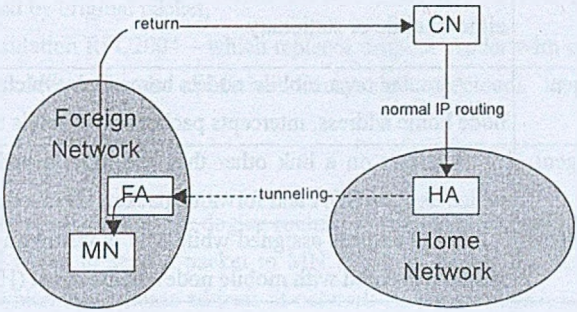

Fig. 1. Mobility – basic model scheme
Rys. 1. Mobilność - schemat modelu podstawowego

The basic model of mobility, worked out by IETF [3], is presented in Fig.1. Mobile Node (MN) is the node, which moves from its Home Network to the Foreign Network. To provide continuous communication he has registered Home Address in the Home Network and obtains a care-of-address (COA) when it visits Foreign Network. Home Agent (HA) belongs to the Home Network and serves the Home Address for the Mobile Node, which is registered. Adequately Foreign Agent (FA) serves visiting Mobile Nodes in the Foreign Network. Correspondent Node (CN) exchanges data with the MN – it may be either mobile or stationary host – sometimes even not aware that it uses mobility for communication.

When CN wants to send data to an MN it simply formats a regular IP packet using CN's address as the source address and the MN's home address as destination. These packets will arrive, using normal IP routing, to the Home Network. If the MN is currently attached to its Home it will receive packets, if MN is away packets will be intercepted by Home Agent. As the HA keeps track of the current location of the MN it serves, he will encapsulate received packet and will send it to the COA – normally the address of the foreign agent that serves the MN in the foreign domain. The FA will recognise the COA it serves and will know to decapsulate packet carried and forward the packet on the foreign networks using, for example, a local radio or infrared channel. In the other direction MN simply formats a normal IP packet with its own source address and CN's address as destination.

Table 1

Special mobility terms definition

Mobile Node MN	A node that can change its point of attachment from one network to another, while still being reachable via its home address
Correspondent Node CN	A node that is communicating with mobile node – may be either mobile or stationary
Home Agent HA	A router on a mobile node's home link which knows mobile node home address, intercepts packets and tunnels them to CoA
Foreign Agent FA	A router on a link other then the mobile node's home link, which assigns COA and forwards packets received from HA
Care-of-address COA	An IP address assigned while MN is visiting a foreign link. It is also registered with mobile node's home agent (HA).

The basic mobility model has several issues and limitations, which have serious impact on efficiency, and scalability of the whole system. In this paper we will present only a few of them – focusing on those, which are important from IPv6 point of view.

2.2. Encapsulation method

One of such a feature is encapsulation method. It is used to forward IP packets from HA to current mobile node's FA and has direct impact on system efficiency and also on security level of the communication.

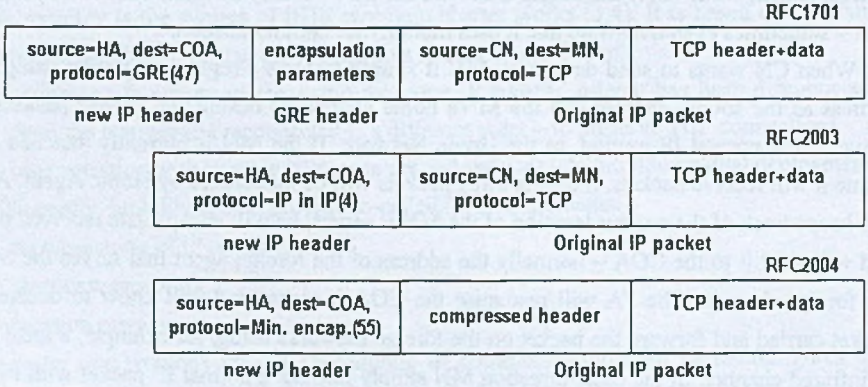

Fig. 2. IP packets encapsulation standards
Rys. 2. Standardy enkapsulacji pakietów IP

There are currently three standardised solutions in that matter, worked by IETF working groups:

- Generic Routing Encapsulation RFC1701 – which has delivery header followed by special GRE header (containing parameters like additional checksum, flags or authentication keys) and then original packet,
- Basic encapsulation procedure RFC2003 – which has new delivery header of IP-in-IP protocol followed by original packet,
- Minimal Encapsulation RFC2004 – which replaces original header with compressed header and wraps it with delivery header of Minimal Encapsulation protocol.

2.3. Dogleg routing elimination

One of the most important issues is dogleg routing elimination, also called 'triangle routing'. Every time the CN wants to send a packet to MN it has to send it via HA. One can easily imagine that MN, which has a home address at network A, is communicating computer from network B while visiting that network. According to the basic mobility model all the traffic must be forwarded via HA which is at network A. This is a very inconvenient situation, especially in case when both networks are geographically far away from each other.

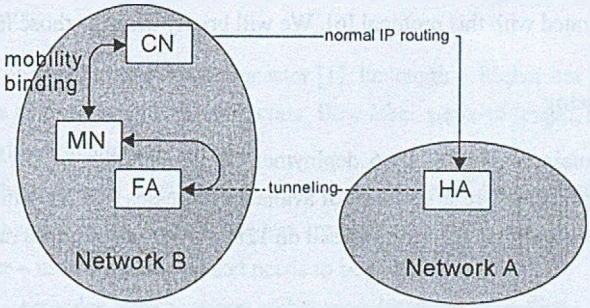

Fig. 3. Dogleg routing – sample architecture
Rys. 3. Dogleg routing – przykładowa architektura

It would be better if CN, that is aware of communicating with MN, has the ability to send packets directly to FA if he knows its location. The solution is based on 'mobility binding' between MN and CN. CN stores MN's home address and current COA. On the other side MN has to send 'update binding' to all CN it communicates when it changes the COA. Of course in case CN is not aware of that solution, then traditional, old-fashioned method is used – sending to the home address.

2.4. Mobility enhancement

There are several enhancements to the mobility model described above. Let's point just a few of them, giving a brief explanation about their field of activity:

- Multiple HAs – as HA is a 'single point of failure' of the whole system there could be several HA in the same network,
- Hierarchical Mobile IP – an extension which separates mobility into micro and macro level having several FA (one for each level), which form a hierarchy and use 'Regional Registration' mechanism,
- Mobile ad-hoc networking – organising mobile stations into a routing domain using different routing algorithms like 'hot potato routing' or 'flood and trace',
- All IP-solutions in cellular architectures – implementation of mobility in cellular telephony 2G (GSM, CDMA) and also 3G.

3. IPv6 and its conformance to mobility guidelines

IP mobility support described in previous section is possible and standardised for both IPv4 and IPv6 [5]. Due to the enhanced functionality and later design of IPv6 some mobility features are already integrated with this protocol [6]. We will briefly describe those IPv6 advantages.

3.1. Addressing

One of the main reasons of IPv6 deployment is the shortage of IPv4 addressees. Every mobile network must have reserved a set of available addresses (COA), which FA can assign to visiting MNs. IPv6 addressing scheme, based on 128 bit address, provides much grater space for host addressing.

Additionally, scope of validity – global, local or link-local and separation between interface ID and network prefix have meaningful impact when the host is moving between networks. Anycast addresses, which were not available in IPv4, are used for example in Dynamic Home Agent Discovery, when sending binding update to the home agent anycast address.

Stateless address autoconfiguration and neighbour discovery mechanisms are integral part of 'normal' IPv6 but they also feel great serving mobile nodes present in the network. Neighbour discovery mechanism is a set of ICMPv6 messages, which are used i.e. to advertise or solicit all necessary router or host parameters. Stateless autoconfiguration enables host to achieve its IPv6 address by combining 'interface token' with routers advertised prefixes. The MN that is visiting foreign network does not need any special treatment in that matter – any IPv6 router can serve

as foreign agent in its network – so there is no need for such an entity as Foreign Agent. Additionally router advertisements can be also used for movement detection procedures.

The Home Agent Registration procedure needs sending 'Binding Update' from MN to its HA and returning 'Binding Acknowledgement' information to the MN, similarly as it was in IPv4. The only difference is that those data are sent using destination option header and not separate packets.

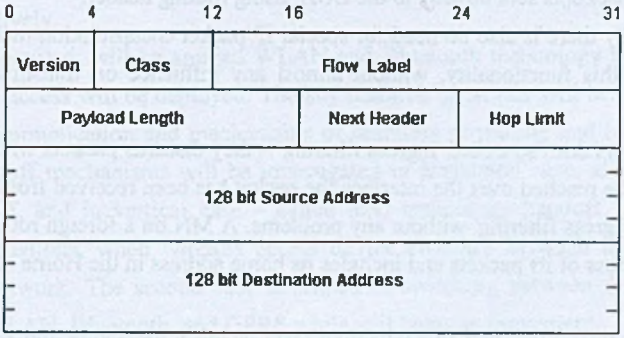

Fig. 4. IPv6 packet structure
Rys. 4. Struktura pakietu IPv6

3.2. IPv6 packets

IPv6 packet has changed a lot from its ancestor [1]. Its length is higher but fixed (40 octets) and contains 8 fields of fixed length: version, class, flow label, payload length, next header, hop limit, source and destination address.

There are no options, like in IPv4. Instead IPv6 uses extensions headers, which are chained together using 'next header' fields. Several headers are already defined:

- Fragment Header – used when the packet needs to be fragmented,
- Routing Header – provides source routing and encapsulation functionality,
- Security Header – contains authentication header or encrypted security payload,
- Destination Option Header – generic construction for defining new headers.

All those headers should be placed within IPv6 packet in a proper sequence.

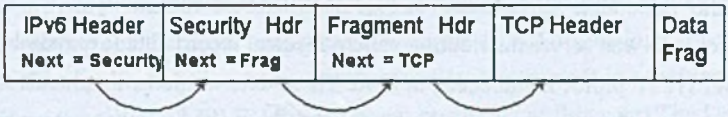

Fig. 5. IPv6 headers chain structure
Rys. 5. Struktura łańcucha nagłówków pakietu IPv6

3.3. Routing mechanisms

To avoid triangle routing a mobile node can send 'Binding Update' to any mobile or stationary Correspondent Node. Every IPv6 node has a Binding Cache, which is used to hold the bindings to other nodes. If a node receives a 'Binding Update' it will add this data to its binding cache. Every time the packet is send the Binding Cache is searched for proper entry. If it is present the packet is sent directly to the COA, using routing header.

Additionally there is also no need for special IP packet encapsulation methods, as 'Routing Header' does this functionality, without almost any influence on transmission security and efficiency.

Many routers does so-called 'ingress filtering' – they discards packets with source addresses which cannot be reached over the interface the packet has been received from. Mobile IPv6 can coexist with 'ingress filtering' without any problems. A MN on a foreign route uses its COA as the source address of its packets and includes its home address in the Home Address destination option.

Security requirements like authentication, data integrity protection and reply protection are developed in IPv6 as a part of the protocol – they are not any more an enhancement. The use of existing protocols (ICMPv6 or IPv6 headers) makes it possible to use implemented security features without the necessity to deploy new solutions.

4. Mobile applications – examples

One of very obvious area of mobile system applications is telemedicine. There may be identified many scenarios where direct voice and video communication may play a crucial role in teleconsultation and telediagnose of urgent cases in the place of accident. There are also many medical disciplines, as for example cardiosurgery, where picture and video data play a fundamental role in identification of cases and further patient treatment.

This is a reason of choosing two following scenarios for further study:

1. Streaming audio and video over IPv6 protocol to mobile devices. As a natural consequence of participation of the authors in the MECCANO project, RAT and VIC audio-video tools implementation over IPv6 has been chosen [7].
2. Access to web server distributing patient medical record data (i.e. radiology database) over HTTP protocol embedded in IPv6. Those data would be invaluable for the doctor in the ambulance or for a family doctor when he visits his patient. Apache web server implementation over Linux operating system will be used for this scenario.

Both applications require QoS, security and are data intensive enough to create problems for the existing wireless access devices. The following types of wireless access systems will be investigated:

- Bluetooth – short distance radio communication up to 30m with speed up to 1Mbps,
- Wireless LAN connectivity – up to few hundred meters with speed up to 11Mbps,
- GPRS and UMTS – long distance communication with speed up to 160Kbps and up to 2Mbps respectively.

Inter hospital network will be applied WLAN and Bluetooth technology but outside the GRPS and UMTS access will be deployed. The key research questions will be related to QoS of the wireless communication and mechanisms of seamless re-routing and handoff of data streams. The handoff mechanisms will be investigated in horizontal case, also called intra-technology handoff, and in vertical case – called inter-technology handoff. The first case corresponds to situations, when wireless access device switches between different access points to wired network. The second case is related to switching between different access technology, e.g. WLAN, Bluetooth, and GPRS while still being in movement.

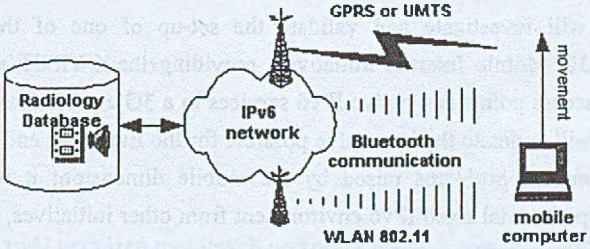

Fig. 6. Sample application scenario
Rys. 6. Przykładowa aplikacja mobilna

5. Conclusions and future work

The paper provides an overview of the existing IPv6 technology in the context of mobile applications pointing out the most important advantages of this technology leverage. The concept of the first applications has been also very briefly described. It is a starting point for 6WINIT Project initiated as 5th FR EU Project in the beginning of this year. The Department of Computer Science at UMM and ACC Cyfronet are the active members of the consortium leading by UC London.

The principal objectives of the 6WINIT project are the following:

1. To validate the introduction of the NEW MOBILE WIRELESS INTERNET in Europe - based on a combination of the new Internet Protocol version 6 (IPv6) and the new wireless protocols (GPRS and UMTS/3GPP);
2. To validate the integration of the protocol suites in (1) into real applications by running complete application test beds;
3. To ensure that the implementations of (1) are generic, and not specific to a particular supplier or operator;
4. To ensure that the validation applications of (2) are not too tied to specific choice of applications;
5. To ensure that the international perspective is maintained.

Offering IPv6 in wireless networks will solve the current problems of the dual scarcity in the IP and wireless world of the following: IP address limitation, quality of service and security from the IP side and lack of spectrum and bandwidth from the wireless side. The 6WINIT project will investigate and validate the set-up of one of the first European operational IPv6-3G Mobile Internet initiatives, providing the 6WINIT project customers with native IPv6 access points and native IPv6 services in a 3G environment. Combining the two technologies will generate the best value possible for the European end-user. The project will concentrate on the problems raised by the mobile dimension; it will build on the existence of an experimental fixed IPv6 environment from other initiatives, and will link into such existing infrastructures.

BIBLIOGRAPHY

1. Huitema Ch.: Routing in the Internet, 2nd edition, Prentice Hall PTR, 2000
2. Deering S., Hinden R.: Internet Protocol, Version 6 (IPv6) Specification, RFC 2460, 1998
3. Johnson D. B., Perkins C.: Mobility Support in IPv6, Internet Draft (work in progress), draft-ietf-mobileip-ipv6-13.txt, November 2000
4. MOBILEIP Working Group, IETF : http://www.ietf.org
5. IPNG Working Group, IETF : http://www.ietf.org
6. Fritsche W., Heissenhuber F.: Mobility support for the Next Generation Internet, IABG, IPv6 Forum Whitepaper, 2000
7. Zieliński K., Ruchała R.: Evaluation of Meccano Tools in Distance Learning Applications, Proceedings of EUNIS Congres, Poznan, 2000

Recenzent: Dr. George P. Kowalczyk

Wpłynęło do Redakcji 7 kwietnia 2001 r.

Streszczenie

Intensywny rozwój urządzeń mobilnych wykorzystujących protokół IPv4 jest ograniczony przez niedostateczną przestrzeń adresową, brak standardowych mechanizmów QoS i odpowiedniego bezpieczeństwa. Podstawowy model aplikacji mobilnych, przedstawiony na rysunku 1, został opracowany zarówno dla IPv4, jak i dla IPv6. W architekturze tej mobilny host (MN) posiada zarejestrowany adres w sieci domowej, gdzie jego agent domowy (HA) jest w stanie przechwytywać pakiety do niego przeznaczone w czasie jego nieobecności. Będąc w obcej sieci, MN uzyskuje tymczasowy adres (CoA) od tamtejszego agenta (FA) i zestawia tunel pomiędzy HA a FA. Tunelem tym HA przesyła enkapsułowane pakiety IP, które wysłał wcześniej inny host (CN) z przeznaczeniem dla MN. Komunikacja powrotna odbywa się bezpośrednio do zainteresowanego CNa.

Ze względu na późniejszy czas powstawania i posiadane już doświadczenie projektantów protokół IPv6 zawiera wiele cech, które faworyzują go w przypadku aplikacji mobilnych. Znacznie zwiększona przestrzeń adresowa wraz z hierarchiczną budową adresu nie jest już dłużej ograniczeniem. Odmienna struktura pakietu (rys. 4) posiada stałe rozmiary pól i nową

łańcuchową budowę rozszerzeń nagłówka (rys. 5). Sposób realizacji routingu oparty na automatycznym przydzielaniu adresu, przesyłaniu odpowiednich rozszerzeń nagłówka IP i przetrzymywaniu na każdym komputerze w pamięci podręcznej danych o tym, w jaki sposób jest osiągalny dany adres IP. Wpisują się więc naturalnie w opracowaną koncepcję mobilności i w znacznym stopniu eliminują problemy związane z enkapsulacją pakietów (rys.2) czy niesymetrycznym routingiem (rys. 3) – występujące w IPv4.

Przekonuje to do wykorzystywania protokołu IPv6 w tworzonych aplikacjach mobilnych. Przykładem takiej aplikacji może być system telemedyczny, w którym dane, np. z bazy radiologicznej, są udostępniane klientom (lekarzom) za pośrednictwem łączy radiowych Bluetooth czy WLAN na obszarze szpitala, a poza nim poprzez sieci GPRS lub UMTS. Podstawowe problemy takiej architektury to: zapewnienie odpowiedniego bezpieczeństwa, poziomu jakości usług oraz ciągłości przekazu w czasie poruszania się klienta.

Wszystko wskazuje na to, iż opracowanie jednolitego rozwiązania do komunikacji w sieciach bezprzewodowych z pewnością będzie bazować na protokole IPv6.