TECHNICAL SCIENCES
Abbrev.: Techn. Sc., No 15(1), Y 2012

MOVING TOWARDS IPV6

Aurel Machalek

University of Luxembourg, Luxembourg

K e y w o r d s: Internet Protocol version 4, Internet Protocol version 6, Seamless communication, TETRA.

A b s t r a c t

This document describes the possibilities for Internet Protocol communications in crisis situations. Its main goal is to show IPv4 and IPv6 solutions developed during the lifetime of the SECRICOM project. Communications technologies in current use are showing their limitations. Whether reacting to a small incident or a great catastrophe, first responders increasingly need to share information such as video, images or other data. Society's evolving expectations concerning safety can be compared with the development of Internet protocols. We examine IP-based communication for crisis management, and show that it is ready to bind together currently fragmented technologies such as TETRA and analogue radios, providing a new dimension of interoperability, including cross-border communication.

ZMIERZAJĄC DO PROTOKOŁU IPV6

Aurel Machalek

University of Luxembourg, Luxembourg

S ł o w a k l u c z o w e: IPv4, IPv6, „bezszwowa" komunikacja, TETRA.

A b s t r a k t

W artykule przedstawiono możliwości wykorzystania protokołu IP (w wersji 4 i 6) w zarządzaniu kryzysowym, ze szczególnym uwzględnieniem rozwiązań wytworzonych w ramach realizacji projektu SECRICOM. Zauważa się, że zbliżamy się do limitów możliwości obecnie wykorzystywanych technologii komunikacyjnych. Podczas akcji ratunkowych – zarówno niewielkich incydentów, jak i wielkich katastrof – u służb ratunkowych w coraz większym stopniu występuje zapotrzebowanie na wymianę informacji pod różnymi postaciami (np. wideo, zdjęcia oraz inne informacje). Zwiększające się oczekiwania społeczeństwa wobec aspektów związanych z bezpieczeństwem mogą być skonfrontowane z możliwościami rozwijającej się technologii. W artykule omówiono łączność w zarządzaniu kryzysowym opartą na protokole IP. Autor zauważa, że podejście takie jest już realizowalne oraz ma potencjał umożliwienia wymiany informacji między różnorodnymi i rozproszonymi sieciami (np. TETRA, systemami analogowymi), wprowadzając nowy wymiar interoperacyjności, także w komunikacji międzygranicznej.

Context and Motivation

The SECRICOM project addresses communication security, interoperability, and connection continuity. Its main deliverable is [...] *a system that ensures end-to-end secure transmission of data and services across heterogeneous infrastructures with real time detection and recovery capabilities against intrusion, malfunctions and failures* [...][1] A major aspect of the project's work was an assessment of the IPv6 protocol, and its advantages and disadvantages in crisis communications. This paper discusses the following topics:

– Research in to crisis management communication and IPv6;
– The exhaustion of the IPv4 address space;
– Motivation for applying an IP-based communication system;
– Solutions to common communications system failure scenarios in crisis situations;
– Benefits for end users.

Related work

Work on this topic started in 2006, with the launch of the U-2010 project: *U-2010 project overall objective is to provide the most capable means of communication and the most effective access to information to everybody required to act in case of accident, incident, catastrophe or crisis, while using existing or future telecommunication infrastructures. The U-2010 project will address the public safety issues by researching new emergency and crisis management solutions investigating on innovative and state-of-the-art communication technologies based on the current and new Internet technologies (i.e. Internet Protocol version 6)*[2]. This work has been continued in the SECRICOM project.

Problem statement

Our research addresses many of the security and interoperability issues that have been highlighted by catastrophes across the world. It must provide answers to these questions:

– Is the Internet ready to be used as an emergency communications channel?

---

[1] Copyright is held by the author/owner(s). D.O.W. SECRICOM Projekt.
[2] Copyright is held by the author/owner(s). D.O.W. U-2010 projekt.

– Can it provide seamless, secure and reliable communications?
– Can first responders use this technology?
– Is IPv6 suitable for use with the latest communications technologies, and can it solve these problems?

Research goals and methods

In order to deal with the increasing frequency and complexity of disasters, whether natural or man-made, forward-looking emergency agencies are developing IP-based architectures able to integrate innovative solutions for their evolving operational requirements. The end user adopting the SECRICOM framework will benefit from:

– Improved Situational Awareness: Real-time communications allow officers to make better decisions more quickly, resulting in safer communities and a more efficient public safety workforce.
– Network Reliability: Redundant wireless network connections ensure reliable communications while on the scene or in motion.
– Office network extended to the incident: Provides real-time access to remote broadband applications for first responders in the field.
– Confidentiality of Information: Ensures information shared between an Emergency Operations Centre and first responders is secure and available only for public safety use.
– Interoperability: Provides a standards-based network platform which enables communications interoperability.

Future network growth requires that Internet-enabled devices can be assigned, used and – most importantly – be reachable anywhere via a globally unique IP address. Without sufficient global IP address space, applications are forced to work with mechanisms that provide local addressing for local internal communications and workaround "fixes" to communicate externally across the Internet. While waiting for a permanent address space solution, there have been numerous optional fixes to try to overcome the address space limitations. These include Network Address Translation (NAT), Classless Inter-domain Routing (CIDR) and extensions to IPv4.

Network Address Translation (NAT) allows multiple devices to be hidden behind one or more real IPv4 addresses. Such mechanisms restrict the end-to-end transparency of the Internet. While NAT has to some extent delayed the pressure on IPv4 address space for the short term, it places severe restrictions on capabilities for bi-directional communication between application endpoints. While a client behind a NAT device can communicate out to servers on the Internet (the client-server communication model), that same

Table 1

IPv6 Feature	Advantage (Compared to IPv4)
128-bit Addressing [RFC 2460]	Scalability from 2^{32} potential addresses to 2^{128} addresses, vastly expanding usable unicast and multicast address space
End-to-End Addressing [RFC 2460]	Reintroduces the end-to-end model to greatly lower the cost and complexity of peer-to-peer communications by eliminating the need for Network Address Translation (NAT)
Network Layer IPsec [RFC 2460, 4301, others]	Improved security support via IP layer security (IPsec) making it cheaper to deploy VPN-like security for all applications
New QOS Support [RFC 2460]	Potential new QOS capability through use of IPv6 flow labels
Auto configuration [RFC 2461, 2462, others]	Improved "plug and play" support using IPv6 link-local addressing, scoped multicasting & anycast support to automatically self-configure and discover neighbour nodes, routers, and servers
New Address Types [RFC 4291, 4193]	New addressing options for link local, anycast, intra-domain3, and globally unique Internet communications.
Security Addressing [RFC 3041, 3972]	New security addressing options for randomly-generated addresses to protect privacy, and cryptographically-generated addresses used to sign and authenticate messages
Enhanced Multicast Features [RFC 3306, 3956, 4291]	Enhanced local and global multicasting support scoped multicasting, and a tremendous expansion of usable multicast address space. Each site receiving an IPv6 prefix can generate 2^{32} globally routable multicast groups[1]. IPv6 multicasting can support creation of new geospatial and community-of-interest information distribution paradigms. Embedded-RP removes the need for IPv4 MSDP, simplifying deployment. Multicasting is a key feature used extensively for IPv6 autoconfiguration features
Multihoming Features [RFC 4291]	Multiple addresses can be assigned to IPv6 network interfaces. Use of different addresses can be used to differentiate link-local, intra-domain, and global messages. Addresses can be assigned and utilized for specific security, reliability, load-balancing, and QOS policies.
Simplified Header [RFC 2460]	Improved header structure that retains only the absolutely necessary header fields and eliminates IPv4's unnecessary CRC checksum fields. Speeds up packet processing in routers and makes basic IPv6 header more compressible than IPv4 for low data rate wireless and dial-up connections.
Extensible Headers [RFC 2460]	Extension headers are an extremely powerful feature that allows additional protocol-level information to be added to the basic IPv6 header. This allows additional protocols and services such as IPsec and mobile IPv6 to easily be integrated on top of the basic IPv6 protocol
Advanced Network Services [RFC 2460, 3775]	Basic IPv6 features and extension headers can be leveraged to build more powerful network services for mobility, security, QOS, peer-to-peer applications, etc. Mobile IPv6 improves on IP mobility for IPv4.

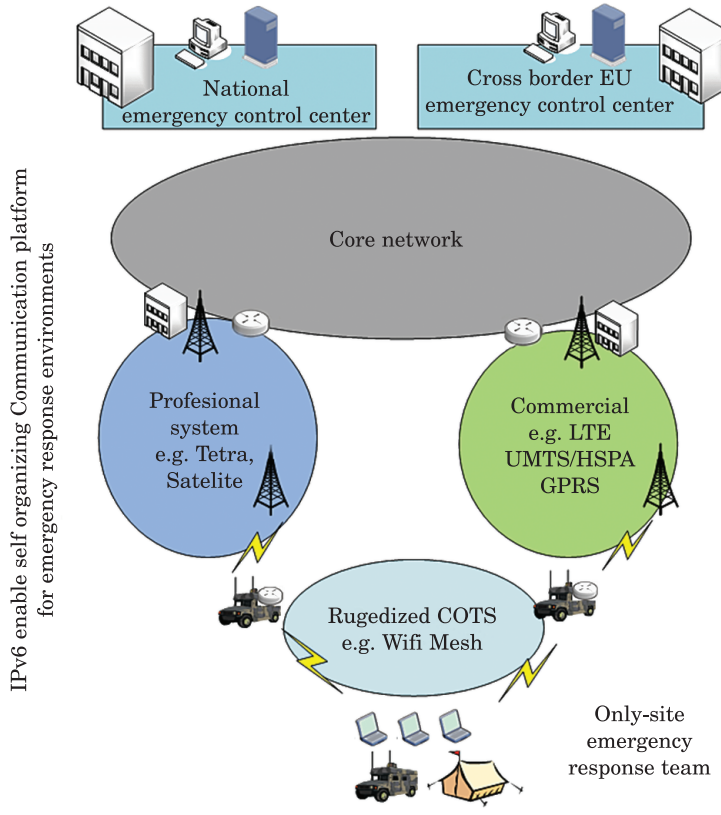

Fig. 1. High-level system overview

client cannot be guaranteed to be accessible when external devices wish to establish a connection to the client (as typified by the peer-to-peer communication model). NAT breaks the end-to-end principle of the Internet, restricting many applications that could be deployed as peer-to-peer to being deployed within a more complicated and expensive modified client-server model that relies on communications gateways and intermediate servers to connect hosts. NAT inhibits the evolution of next-generation applications that demand IP address space and direct remote connectivity into business premises and home networks (e.g. from IP-enabled mobile handsets). IPv6 reintroduces the ability to provide true end-to-end security that is not always readily available through a NAT-based network (Ipv6 Forum Roadmap...).

IPv6 has numerous technical features which, when compared to IPv4, make it a more powerful and flexible framework to deploy next-generation network applications and services (tab. 1).

Some of the operational benefits brought by adopting the SECRICOM system are:

– Extension of emergency mission network to Outdoor & Mobile Environments.

– Seamless mobility & continuous access.

– Network Security, Scalability & Manageability.

– Standards-based interoperable solution with investment protection.

Conclusion

The technical benefits of IP are:

– Redundancy: Redundant network connections across multiple wireless networks using standards based mobile IP.

– Security: Secure connectivity to the vehicle using network encryption, firewall, intrusion detection, FIPS 140-2 compliance.

– Connectivity: Mobile router provides network connectivity for wired or wireless client devices in or around a vehicle Network Management: Use the same network management tools to manage the office network and mobile network.

– Multi-Media Applications: Broadband wireless network for voice, video, and data applications for real-time communications with mobile network.

– Wireless Agnostic: Interfaces with 802.11b/g, licensed 4.9GHz, 3G and future wireless networks.

– Modular Design: Enclosure slots allows module expansion (e.g. video).

Translated by AUTHORS

Accepted for print 30.06.2012

References

U-2010 project: http://www.u2010.eu.

Next Generation Public Safety Communication Networks and Technologies (NgenSafe'09).

SEINHARDT G. *Blackblot Procedural Requirements Management Model*. Rev. 2.1. Available at: http://www.blackblot.com/prm-model/.

Wikipedia, *Emergency management*. Available at: http://en.wikipedia.org/wiki/Emergency_management.

IPv6 Forum Roadmap – http://www.ipv6forum.com/dl/forum/wwc_ipv6forum_roadmap_vision_2010.pd.