DSiP Distributed Systems intercommunication Protocol - A Traffic Engineering Solution for Secure Multichannel Communication

JOHN HOLMSTRÖM*, JYRI RAJAMÄKI** & TAINA HULT**
*Ajeco Ltd.
Arinatie 10, FI-00370 Helsinki
FINLAND
**Laurea University of Applied Sciences
Vanha Maantie 9, FI-02650 Espoo
FINLAND
john.holmstrom@ajeco.fi http://www.ajeco.fi/index.php?language=eng

Abstract: - The importance of reliable telecommunication is constantly increasing. The DSiP-solution makes it possible to distribute all telecommunication among several operators and methods, resulting in a true multichannel communication system. The DSiP-multichannel routing solution increases reliability, security and integrity in telecommunication and allows regular communication methods to be used in mission critical telemetry systems. This is achieved by splitting risks between operators and communication channels; better routing capabilities; taking security and intrusion risks into account; and adding modularity.

Key-Words: - Data communications, Data security, Data traffic engineering, IP, IP networks, Public safety, Security, Security communications

1 Introduction

The two persons who contributed big time to the existence of the Internet are Robert E. Kahn and Vinton Cerf. The Internet was developed in the early 70's. The Internet Protocol (IP) is a good protocol, but no one could foresee the need and amount of communication we have today. Some email applications came in the 80's. Tim Berners Lee specified HTML and wrote a browser in 1990.

Today, the most cost-efficient way to globally transport data is achieved by using networks based on the IP-protocol. Also, multi-path routing for IP networks has been explored for many years in order to mitigate the effect of congestion in the network. Today, many IP-based solutions have been developed for business critical applications. They are used around the world to help companies to make sure that their business critical Internet connections and VPN-tunnels are always online. Sophisticated multichannel systems are constantly monitoring critical traffic having capabilities for using alternative routes if data traffic problems are encountered in the network.

2 Problem Formulation

Fig. 1 shows how a typical multi-modem remote application works. All modems will get their own IP-address from their operators and the control room application will see connection attempts from multiple IP-addresses. This kind of a multi-modem system cannot share communication between different physical media without rewriting the application software to do so, because IP does not support multichannel communications by maintaining simultaneous socket connections over multiple physical media. The rewriting an application software to support multichannel communications is a very challenging task.

A typical security problem many times preventing Virtual Private Networks (VPN) from being used in a multi-modem data communication environment, is that VPN solutions typically allow for creating a secure link over only one physical media at a time. If the media encounters problems, the VPN must be re-established over another media. These limitations are related to IP-addressing issues and how the IP-stack handles socket connections.

2.1 Research Question

The IP-protocol is a great protocol for transporting data but it is not enough when considering mission critical or highly important systems. For that reason, the research question (RQ) of this study is formulated:

ISBN: 978-960-474-286-8

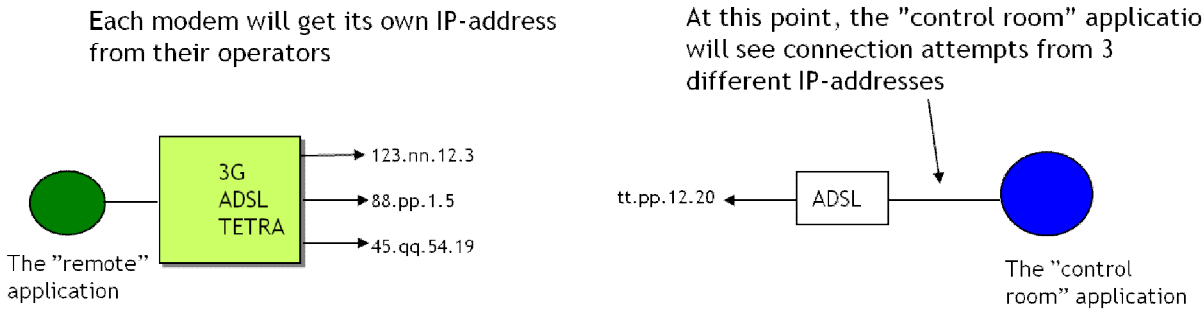

Fig. 1 Typical Multi-modem System

RQ: Is there any solution that allows also regular communication methods to be used in mission critical telemetry systems?

3 Problem Solution

The new multichannel data communication concept provides a uniform way to communicate over virtually any type of communications media in such a way that multiple, sometimes parallel communication paths appear as a single robust, secure and reliable communication link between communicating peers.

Our proposed solution is based on the Distributed Systems intercommunication Protocol® (DSiP) [1] which handles communication channel selection and hides link establishment issues from devices and/or software that wish to communicate with each other using the DSiP solution. DSiP is simultaneously a protocol-level and routing-level traffic engineering software solution for intelligently handling data routing, using all kinds of physical media, including IP and non-IP communication. It increases dramatically the reliability, security and controllability of communication systems being completely independent from operators. DSiP can be regarded as a traffic engineering layer above the regular IP-layer – "the missing OSI layer".

DSiP allows for:

1. Combining and using telecommunication methods in parallel so that multiple connections appear like a single reliable connection. DSiP can route data over both IP- and non-IP connections.
2. DSiP is independent from operators. It allows the user to shop and combine telecommunication from any operator.
3. DSiP contains protocol translation methods making equipment, systems and software compatible.
4. DSiP implements security mechanisms as well as reduces risk for DOS attacks and virus-infusion.
5. DSiP has better control over data routing, priorities and services.

3.1 System Overview

Fig. 2 shows an overview of the DSiP telemetry system, which is capable of routing data over any kind of connection, IP and non-IP, and works in multi-operator environments applying satellites, 3G, GPRS, UMTS, HDSPA, IP-network, TETRA, serial connections and radio modems.

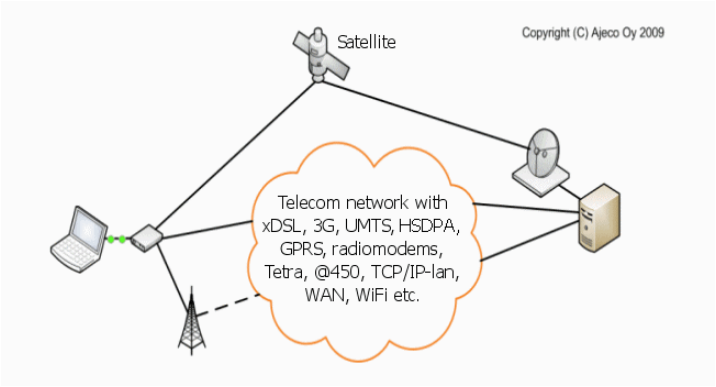

Fig. 2 DSiP Telemetry System

3.2 Robust and Secure Data Communications

The DSiP-protocol supports splitting a VPN tunnel over several physical media without the aforementioned constraints, as shown in Fig. 3. In addition, it solves incompatibility issues on both physical and logical levels in addition to providing modularity, data integrity, security and versatility to data communications systems ranging from small to very large size. By following a set of logical rules within the DSiP and by using IP as means for transport, applications, equipment and software from different vendors may intercommunicate transparently i.e. applications may respond to and ask for services without needing to know about

ISBN: 978-960-474-286-8

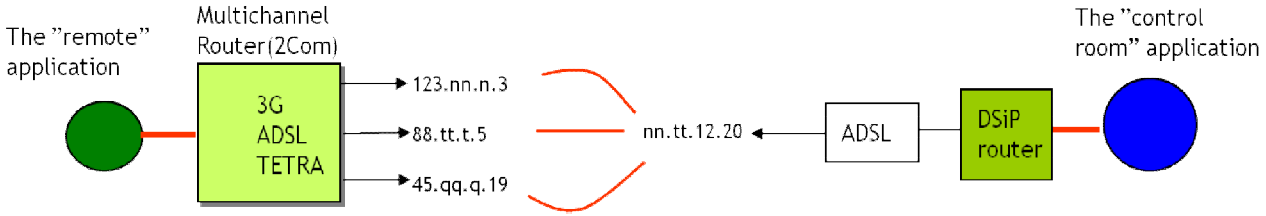

Fig. 3 DSiP Multichannel System

physical implementations [1]. The DSiP protocol enables an unbroken VPN link should traffic move to an alternative route with alternative physical media.

3.2 Modularity

A DSiP telemetry system always consists of three elements: the remote site, the telecommunication system and the command and control room. If one of these element changes, it do not affect the others, so DSiP solution is modular as Fig. 4 shows.

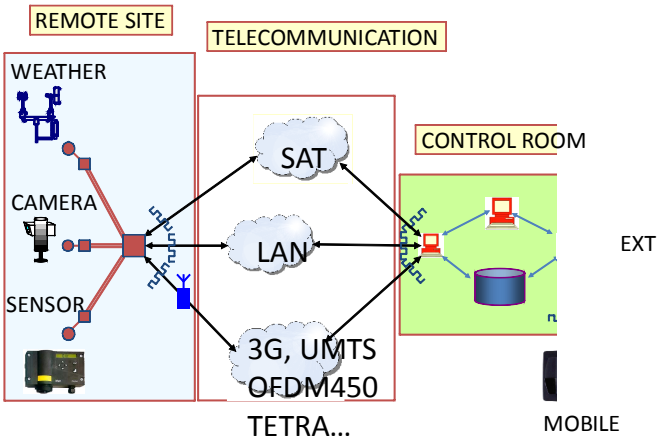

Fig. 4 Modularity of DSiP

4 Applications

4.1 SCADA Systems

DSiP is applied in controlling of Finland's main power grid. Furthermore, a major part of Vattenfalls power distribution network is managed and controlled by DSiP, AM08M RTU's and AM06T communication bridges. Power grid breakers are monitored and controlled by a SCADA-system via the DSiP-system. Fig. 5 shows how an operative system works.

4.2 Coast Guard Surveillance System

The Finnish Frontier & Coast Guard uses coastal surveillance cameras in order to continuously execute control and get telemetry information. The Finnish archipelago with its harsh climatic conditions put a lot of stress upon equipment installed in maritime surveillance systems. The DSiP-system allows for location independent operation i.e. control rooms can be placed at any desired location.

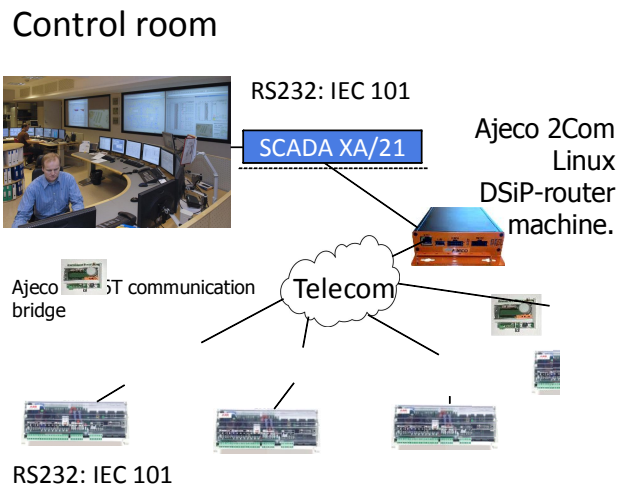

Fig. 5 DSiP-encapsulated IEC-messaging to electrical substations

DSiP is deployed, also, in the Integrated System for Interoperable sensors & Information sources for Common abnormal vessel behaviour detection & Collaborative identification of threat (I2C) integration project [2] and the Protection of European seas and borders through the intelligent use of surveillance (PERSEUS) demonstration project [3] both funded by EU's FP7.

4.3 Outdoor Lighting Control

The DVB-Gate-unit replaces ripple control receiver units in the power distribution network. It contains two communication interfaces: A DVB-T/H interface for receiving broadcasted commands and a GPRS interface for sensor- and energy meter feedback. The GPRS also acts as a reserve channel. The DSiP-system provides the data communication infrastructure together with its controller tasks and nodes.

ISBN: 978-960-474-286-8

5 Discussion

With DSiP, customers can use multiple communication channels in parallel in such a way, that ending peers ”think” they are using one channel. DSiP shares communication resources between different hardware equipment and software modules; automatically routes data and uses secondary routes if primary connections are broken. It always knows the correct sender and correct receiver and uses strong encryption and timestamps. So, DSiP makes communications more robust and improves data security.

With DSiP, customers have enhanced controlling possibilities: (1) control priorities – important information is routed first, less important later; (2) control over network timeouts – no undetermined delays or waits; (3) control the usage of communication and bandwidth – DSiP always ”knows” the condition of all routes; and (4) have better control over maintenance and configuration.

DSiP combines IP and non-IP communication into a single controllable system. Transparently communicate through DSiP-connections is reached, because DSiP allows tunneling of other protocols through itself. DSiP makes equipment and software compatible via very intelligent interface mechanisms.

Being independent from every single telecommunication operator, end-user could distribute the operator risk by using multi-operator network topology.

DSiP is not a heavy or difficult protocol to embed into various equipment and platforms. However, DSiP contains features like:

- Solutions for data-integrity and security and authentication
- Automatic re-routing of information via backup channels – redundancy
- A controllable method for multi & broadcasting – bandwidth control
- A standardized interface to software & equipment – solves compatibility issues
- Scalability – the system is very flexible – easily add new and old equipment & swr
- Complete independency of physical communication methods – any means for transmitting a bit is good
- Real-time online knowledge of the network topology – NO unwanted connection delays.

A DSiP testing environment is set up in Laurea University of Applied Sciences, which purpose is to test and demonstrate the functioning of the multichannel routing solution exploiting multiple communication paths in practice. By creating different problem situations, we are able to test the reliability and robustness of the communication system. So far, the results from the testing environment have been encouraging. Multiple connections over all tested types of media appear like a single ultra-robust communications channel. When one connection fails, DSiP easily finds another working route. The way how the new connections are created can be read from log files. However, this is not very illustrative and for that reason, we are developing new visualizing tools. [4]

6 Conclusion

The need for secure multichannel communication is global and exploding. DSiP is a solution that allows also regular communication methods to be used in mission critical telemetry systems. It also enables a combination of all kinds of telecommunication resources: IP traffic and non-IP traffic over TETRA, radio links, satellite communications, serial connections etc. can all co-exist forming a single maintainable system.

References:

[1] M. Nordman, M. Lehtonen, J. Holmström, K. Ramstedt and P. Hämäläinen, ”A TCP/IP communication architecture for distribution network operation and control”, in Proc. of the 17th Internal Conference on Electricity Distribution, Barcelona, Spain, May 12-15, 2003.

[2] M. Morel and S. Claisse, “Integrated System for Interoperable sensors & Information sources for Common abnormal vessel behaviour detection & Collaborative identification of threat (I2C)” in Proc. of the Ocean and Coastal Observation: sensors and observing systems, numerical models and information systems, Brest, France, June 21-23, 2010.

[3] Demonstration project on the Surveillance of the EU Sea Borders, by Europolice on 22. January2011, Available: http://euro-police.noblogs.org/2011/01/demonstration-project-on-the-surveillance-of-the-eu-sea-borders/

[4] J. Rajamäki, J. Holmström and J. Knuuttila, Robust Mobile Multichannel Data Communication for Rescue and Law Enforcement Authorities, Proc. of the 17th Symposium on Communications and Vehicular Technology in the Benelux, ,Twente, The Netherlands Nov. 24-25, 2010.