Developments in Fuzzy Sets, Intuitionistic Fuzzy Sets, Generalized Nets and Related Topics. Volume I: Foundations

Developments in Fuzzy Sets, Intuitionistic Fuzzy Sets, Generalized Nets and Related Topics Volume II: Applications

Editors

Krassimir T. Atanassov
Michał Baczyński
Józef Drewniak
Janusz Kacprzyk
Maciej Krawczak
Eulalia Szmidt
Marcin Wygralak
Sławomir Zadrożny

Editors

Krassimir T. Atanassov
Władysław Homenda
Olgierd Hryniewicz
Janusz Kacprzyk
Maciej Krawczak
Zbigniew Nahorski
Eulalia Szmidt
Sławomir Zadrożny

SRI PAS IBS PAN

Developments in Fuzzy Sets, Intuitionistic Fuzzy Sets, Generalized Nets and Related Topics
Volume II: Applications

Systems Research Institute
Polish Academy of Sciences

Developments in Fuzzy Sets, Intuitionistic Fuzzy Sets, Generalized Nets and Related Topics
Volume II: Applications

Editors

Krassimir T. Atanassov
Władysław Homenda
Olgierd Hryniewicz
Janusz Kacprzyk
Maciej Krawczak
Zbigniew Nahorski
Eulalia Szmidt
Sławomir Zadrożny

IBS PAN  **SRI PAS**

© **Copyright by Systems Research Institute**
Polish Academy of Sciences
Warsaw 2010

All rights reserved. No part of this publication may be reproduced, stored in retrieval system or transmitted in any form, or by any means, electronic, mechanical, photocopying, recording or otherwise, without permission in writing from publisher.

Systems Research Institute
Polish Academy of Sciences
Newelska 6, 01-447 Warsaw, Poland
www.ibspan.waw.pl

ISBN 9788389475305

Generalized net model for creating virtual private network using point-to-point protocol over secure shell2 for building passwordless vpn connection

Ivelina Vardeva
Asen Zlatarov University
"Yakimov"1, Burgas, Bulgaria
iveto@btu.bg

Abstract

Constructing virtual tunnel is a logical connection between two end points in which is supported authentication and crypting the data from one point to another. Tunneling is a term used for description of the capsulation which is the process of routing and decapsulation of the packages. It is developed generalized net model reflecting the work of building and transmitting confidential information between a vpn client and vpn server by RSA cryptic tunnel.

Keywords: cryptography, generalized nets, point-to-point potocol, ssh2, virtual private network.

1 Introduction

In VPN is constructed a tunnel through a public net Internet. Data is sent through the public net in a way, which recreates connection of type „from point to point" - Point-to-Point (PPP). This is achieved by enclosing in capsules of data and in that way is created logical independent net from the location of the end points, in which is supported authentication. Data is crypted – they remain private – this is of the important significance to be well protected otherwise everyone can catch them in any time of the transferring through the public Internet network between delivering and accepting end point of the tunnel. VPN allows to be created a logical network, which is independent from the location of the personnel or clients and gives a possibility for establishment of direct

Developments in Fuzzy Sets, Intuitionistic Fuzzy Sets, Generalized Nets and Related Topics. Volume II: Applications *(K.T.Atanassow, W.Homenda, O. Hryniewicz, J. Kacprzyk, M.Krawczak, Z.Nahorski, E. Szmidt, S. Zadrożny, Eds.), IBS PAN - SRI PAS, Warsaw, 2009.*

physical connection. At the article is introduced a model describing the processes of transmitting confidential information. About its development are used Generalized nets [1, 3]. They have powerful apparatus for modeling and analyzing such parallel flowing in time real processes.

VPN networks are used to ensure distant access to the mobile personnel, to ensure extranet network with access to its clients or to ensure the connection between two offices in different locations. VPN is secured tunnel using Internet for connection between two nets and transferring data between them [9].

Enclosing in capsules is hiding of the original package into a new package, which is used to be done the routing through the tunnel i.e. in the header of the new package is assigned the address of the end point of the tunnel, in the header of the original package is the address of the last location, which remains crypted until its arriving at the end point.

VPN allows to the local nets placed on different locations to be physically connected to the network of the organization through VPN server.

The developed GN-model at the current article could be used independently or like additional module to others GN-models introducing the work of systems in which are transmit confidential data [2, 7, 8, 6], describing different processes in Internet.

2 VPN work

- The mobile user dials a local Internet Server Provider (ISP) supplier and enters in by the user account and password to construct Internet connection but if the client uses hired or fixed Internet connection връзка, this is not necessary.
- After locating the Internet connection, the client sends for the server for distant access configurated to accept VPN connections using IP address of the distant server.
- The user has to authenticate itself in the private net to receive authorization – definite access and rights. Authentication of the user – checking identity of the VPN client, limiting the VPN access only to the authorized users.
- Addresses control – appointing VPN clients on address in Intranet and to secure used in Internet addresses to be preserved like private.
- Data crypting – data have to be transferred like crypted through Internet.

- Key control – generating and renovating of decrypting keys about the crypted data [9, 4].

PPP – is a protocol for communication between two computers using serial interface typical for the personal computers connections by the phone line to a server. PPP connection is secured on second layer of the OSI model. The protocol PPP includes in itself authentications by the help of Password Authentication Protocol (PAP) – authentication of the password and Challenge Handshake Authentication Protocol (CHAP) – protocol about authentication by using coordination of the both end points [5, 4].

SSH – is Unix based control interface and protocol for receiving certain access of distant computer. This technology is wide used by the net administrators for web distant control. SSH actually has several uses: slogin, ssh, и scp. SSH commands are crypted and they are secured several times. The both points of client-server connection are authentic, they use digital certificate and the passwords are secured. SSH uses RSA crypting algorithm for the both connections and authentications. The others crypting algorithms, which can be used are: DES, Blowfish, IDEA [4].

All definitions related to the concept "GN" are taken from [1]. The GN, describing the work of the SSL, is shown on Figure.1.

Initially the following tokens enter the generalized net:

- in place S_{cd} - α-token with characteristic:
  x_0^{α} = "user name, user password, crypted data, VPN username, SSH public key client, SSH private key client, IP address vpn server";
- in place S_{comp} – β-token with characteristic:
  x_0^{β} = "version of SSH2, PPP";
- stay in place S_{A2} γ-token with characteristic
  x_0^{γ} = "user name, user passwords";
- stay in place S_{A3} δ-token with characteristic
  x_0^{δ} = "IP address vpn server";
- stay in place S_{A3} ε-token with characteristic
  x_0^{ε} = "VPN username, SSH public key client, SSH public server key, SSH private server key".

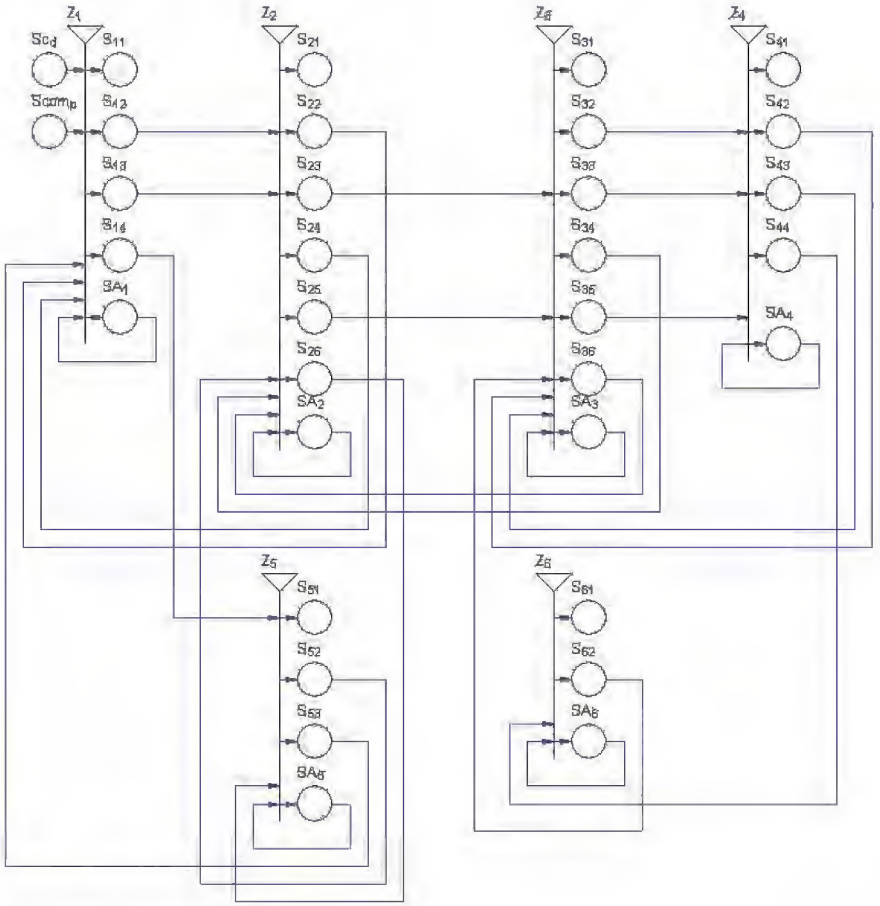

Figure1: GN model for creating virtual private network using point-to-point protocol over secure shell2

The generalized nets is introduced by the set of transitions:

A= { Z_1, Z_2, Z_3, Z_4, Z_5, Z_6}, where the transitions describe the following processes:

Z_1 = "Tasks maked of the client",

Z_2 = "Tasks maked of Internet Server Provider",

Z_3 = "Tasks maked of the LAN server",

Z_4 = "Tasks maked of the VPN server",

Z_5 = "Crypting connection from the client",

Z_6 = "Crypting connection from server".

The transitions with the following description:

$Z_1 = <\{S_{cd}, S_{comp}, S_{22}, S_{24}, S_{53}, S_{A1}\}, \{S_{11}, S_{12}, S_{13}, S_{14}, S_{A1}\}, R_1, \vee (\wedge (S_{cd}, S_{comp}), S_{22}, S_{24}, S_{53}, S_{A1}) >$

$$R_1 = \begin{array}{c|ccccc} & S_{11} & S_{12} & S_{13} & S_{14} & S_{A1} \\ \hline S_{cd} & false & false & false & false & true \\ S_{comp} & false & false & false & false & true \\ S_{22} & false & false & false & false & true \\ S_{24} & false & false & false & false & true \\ S_{53} & false & false & false & false & true \\ S_{A1} & W_{A1,11} & W_{A1,12} & W_{A1,13} & W_{A1,14} & true \end{array}$$

where:

$W_{A1, 11}$ = "It is impossible to establish the connection",

$W_{A1, 12}$ = "There is a request for establishing the connection to ISP",

$W_{A1, 13}$ = "There is an answer from the VPN server for the establishing the VPN tunnel",

$W_{A1, 14}$ = "Send crypted data".

The token x_{cu}^{α} that enters in place S_{12} obtain characteristic

$$x_{cu}^{\alpha'} = " \left\langle pr_1 x_0^{\alpha}, pr_2 x_0^{\alpha} \right\rangle " .$$

The α and β-token are united and enters in place S_{13} with characteristic

$$x_{cu}^{\alpha''} = " \left\langle pr_4 x_0^{\alpha}, pr_5 x_0^{\alpha}, pr_7 x_0^{\alpha}, pr_1 x_0^{\beta}, pr_2 x_0^{\beta} \right\rangle " .$$

The token x_{cu}^{α} that enters in place S_{14} obtain characteristic

$$x_{cu}^{\alpha'''} = " \left\langle pr_3 x_0^{\alpha}, pr_7 x_0^{\alpha} \right\rangle " .$$

$Z_2 = <\{S_{12}, S_{13}, S_{34}, S_{36}, S_{52}, S_{A2}\}, \{S_{21}, S_{22}, S_{23}, S_{24}, S_{25}, S_{26}, S_{A2}\}, R_2, \vee (S_{12}, S_{13}, S_{34}, S_{36}, S_{52}, S_{A2})>$

$R_2 =$

	S_{21}	S_{22}	S_{23}	S_{24}	S_{25}	S_{26}	S_{A2}
S_{12}	*false*	*false*	*false*	*false*	*false*	*false*	*true*
S_{13}	*false*	*false*	*false*	*false*	*false*	*false*	*true*
S_{34}	*false*	*false*	*false*	*false*	*false*	*false*	*true*
S_{36}	*false*	*false*	*false*	*false*	*false*	*false*	*true*
S_{52}	*false*	*false*	*false*	*false*	*false*	*false*	*true*
S_{A2}	$W_{A2,21}$	$W_{A2,22}$	$W_{A2,23}$	$W_{A2,24}$	$W_{A2,25}$	$W_{A2,26}$	*true*

where:
$W_{A2,\,21}$ = "It is impossible to establish the connection",
$W_{A2,\,22}$ = "The username and password are correct",
$W_{A2,\,23}$ = "Send information by VPN username, SSH public client key, PPP",
$W_{A2,\,24}$ = "The response of the server for correct data for establishing the VPN tunnel",
$W_{A2,\,25}$ = "Send crypted data",
$W_{A2,\,26}$ = "The response of the server for receive data".

The token x_{cu}^{α} that enters in place S_{22} obtain characteristic

$$x_{cu}^{\theta} = \text{"Acknowledge for correct data".}$$

The α and β-token are united and enters in place S_{23} with characteristic

$$x_{cu}^{\alpha''} = \text{"} \left\langle pr_4 x_0^{\alpha},\ pr_5 x_0^{\alpha},\ pr_7 x_0^{\alpha},\ pr_1 x_0^{\beta},\ pr_2 x_0^{\beta} \right\rangle \text{"} .$$

The token x_{cu}^{α} that enters in place S_{24} obtain characteristic

$$x_{cu}^{\theta'} = \text{"Acknowledge for correct data".}$$

The token x_{cu}^{α} , x_{cu}^{β} that enters in place S_{25} obtain characteristic

$$x_{cu}^{\alpha'''} = \text{"} \left\langle pr_3 x_0^{\alpha},\ pr_7 x_0^{\alpha} \right\rangle \text{"} .$$

The token x_{cu}^{α} that enters in place S_{26} obtain characteristic

$$x_{cu}^{\theta''} = \text{"Acknowledge for receive data".}$$

$Z_3 = <\{S_{23}, S_{25}, S_{42}, S_{43}, S_{62}, S_{A3}\}, \{S_{31}, S_{32}, S_{33}, S_{34}, S_{35}, S_{36}, S_{A3}\}, R_3, \vee (S_{23}, S_{25}, S_{42}, S_{43}, S_{62}, S_{A3})>$

$R_3 =$

	S_{31}	S_{32}	S_{33}	S_{34}	S_{35}	S_{36}	S_{A3}
S_{23}	*false*	*false*	*false*	*false*	*false*	*false*	*true*
S_{25}	*false*	*false*	*false*	*false*	*false*	*false*	*true*
S_{42}	*false*	*false*	*false*	*false*	*false*	*false*	*true*
S_{43}	*false*	*false*	*false*	*false*	*false*	*false*	*true*
S_{62}	*false*	*false*	*false*	*false*	*false*	*false*	*true*
S_{A3}	$W_{A3,31}$	$W_{A3,32}$	$W_{A3,33}$	$W_{A3,34}$	$W_{A3,35}$	$W_{A3,36}$	*true*

where:
$W_{A3,\,31}$ = "It is impossible to establish the connection",
$W_{A3,\,32}$ = "Sending information for establishing the VPN tunnel",
$W_{A3,\,33}$ = "Sending information by permission access",
$W_{A3,\,34}$ = "Sending information by permission for establishing the VPN tunnel",
$W_{A3,\,35}$ = "Sending crypted data for server",
$W_{A3,\,36}$ = "Sending crypted data for client".

The α and β-token are united and enters in place S_{32} with characteristic

$$x_{cu}^{\alpha'} = " \left\langle pr_4 x_0^{\alpha},\ pr_5 x_0^{\alpha},\ pr_7 x_0^{\alpha},\ pr_1 x_0^{\beta},\ pr_2 x_0^{\beta} \right\rangle " .$$

The token x_{cu}^{α} that enters in place S_{33} obtain characteristic

$$x_{cu}^{\theta'''} = \text{"Acknowledge for receive data".}$$

The token x_{cu}^{α} that enters in place S_{34} obtain characteristic

$$x_{cu}^{\theta''''} = \text{"Acknowledge for receive data".}$$

The token x_{cu}^{α} that enters in place S_{35} obtain characteristic

$$x_{cu}^{\alpha'''''} = " \left\langle pr_3 x_0^{\alpha},\ pr_7 x_0^{\alpha} \right\rangle " .$$

The token x_{cu}^{α} that enters in place S_{36} obtain characteristic

$$x_{cu}^{\theta''''''} = \text{"Acknowledge for receive data".}$$

$Z_4 = <\{S_{32}, S_{33}, S_{35}, S_{A4}\}, \{S_{41}, S_{42}, S_{43}, S_{44}, S_{A4}\}, R_4, \vee (S_{32}, S_{33}, S_{35}, S_{A4})>$

$$R_4 = \begin{array}{c|ccccc} & S_{41} & S_{42} & S_{43} & S_{44} & S_{A4} \\ \hline S_{32} & false & false & false & false & true \\ S_{33} & false & false & false & false & true \\ S_{35} & false & false & false & false & true \\ S_{A4} & W_{A4,41} & W_{A4,42} & W_{A4,43} & W_{A4,44} & true \end{array}$$

where:
$W_{A4,\,41}$ = "It is impossible to establish the connection",
$W_{A4,\,42}$ = "Sending request for LAN server by Internet access",
$W_{A4,\,43}$ = "Sending information by VPN username, SSH public client key, PPP are correct",
$W_{A4,\,44}$ = "Sending crypted data for client".

The token x_0^{δ} that enters in place S_{42} obtain characteristic

$$x_{cu}^{\alpha'} = "\left\langle pr_1 x_0^{\delta} \right\rangle" .$$

The token x_{cu}^{α} that enters in place S_{43} obtain characteristic

$x_{cu}^{\theta''''}$ = "Acknowledge for correct data".

The token x_{cu}^{α} that enters in place S_{44} obtain characteristic

$x_{cu}^{\theta''''''}$ = "Acknowledge for receive data".

$Z_5 = <\{S_{41}, S_{26}, S_{A5}\}, \{S_{51}, S_{52}, S_{53}, S_{A5}\}, R_5, \vee (S_{41}, S_{26}, S_{A5})>$

$$R_5 = \begin{array}{c|cccc} & S_{51} & S_{52} & S_{53} & S_{A5} \\ \hline S_{14} & false & false & false & true \\ S_{26} & false & false & false & true \\ S_{A5} & W_{A5,51} & W_{A5,52} & W_{A5,53} & true \end{array}$$

where:
$W_{A5,\,51}$ = "It is impossible to establish the connection",
$W_{A5,\,52}$ = "Send encrypted data",
$W_{A5,\,53}$ = "Send confirming for receive data".

The token x_{cu}^{α} that enters in place S_{52} obtain characteristic

$$x_{cu}^{\alpha'} = " \left\langle pr_3 x_0^{\alpha}, pr_7 x_0^{\alpha} \right\rangle " .$$

The token x_{cu}^{α} that enters in place S_{53} obtain characteristic

$$x_{cu}^{\theta''''''} = \text{“Acknowledge for receive data”}.$$

$Z_6 = <\{S_{44}, S_{A6}\}, \{S_{61}, S_{62}, S_{A6}\}, R_6, \vee (S_{44}, S_{A6})$

$$R_6 = \begin{array}{c|ccc} & S_{61} & S_{62} & S_{A6} \\ \hline S_{44} & false & false & true \\ S_{A6} & W_{A6,61} & W_{A6,62} & true \end{array}$$

where:
$W_{A6,61}$ = “It is impossible to establish the connection”,
$W_{A6,62}$ = “Sending confirming for receive data”.

The token x_{cu}^{α} that enters in place S_{62} obtain characteristic

$$x_{cu}^{\theta''''''} = \text{“Acknowledge for receive data”}.$$

4 Conclusions

VPN technologies offer controlled services, which exceed the notion about the traditional services. The virtual private networks ensure protected high speed access to the common information resources of the all personnel of one company or organization. But in their usage is very important to be given protections for crypting, authorization, authenticity of the data. This technology guaranties access to the information of the people, connected in VPN, from any place, in any time.

References

[1] Atanassov, K., Generalized nets, World Scientific, Singapore, New Jersey, London 1991

[2] Atanassov, K., S. Sotirov, V. Kodogiannis, Intuitionistic fuzzy estimations of the Wi-Fi connections, First Int. Workshop on IFSs, GNs, KE, London, 6-7 Sept. 2006,75-80

[3] Atanassov, K.,Introduction in generalized nets, Pontica print, Bourgas (in Bulgarian), 1992

[4] Bronson, S., VPN PPP−SSH Mini−HOWTO, 2002

[5] Light−Williams, C., Drake, J., LINUX PPP HOWTO, 2000

[6] Sotirov, S., V. Kodogiannis, R. Elijah Blessing, Intuitionistic fuzzy estimations for connections with Low Rate Wireless personal area networks, First Int. Workshop on IFSs, GNs, KE, London, 6-7 Sept. 2006, 81-87

[7] Vardeva, I., Sotirov, S., Generalized Net model of SSL with intuitionistic fuzzy estimations, Eleventh Int. Conf. on IFSs, Sofia, 28-30 April 2007, 48-53

[8] Vardeva, I., SSL modeling by the apparatus of Generalized Net, Sixth Int. Workshop on GNs, Sofia, 17 Dec. 2005, 29-33

[9] Wilson, M., VPN HOWTO, 2002

The papers presented in this Volume 2 constitute a collection of contributions, both of a foundational and applied type, by both well-known experts and young researchers in various fields of broadly perceived intelligent systems.
It may be viewed as a result of fruitful discussions held during the Eighth International Workshop on Intuitionistic Fuzzy Sets and Generalized Nets (IWIFSGN-2009) organized in Warsaw on October 16, 2009 by the Systems Research Institute, Polish Academy of Sciences, in Warsaw, Poland, Centre for Biomedical Engineering, Bulgarian Academy of Sciences in Sofia, Bulgaria, and WIT – Warsaw School of Information Technology in Warsaw, Poland, and co-organized by: the Matej Bel University, Banska Bistrica, Slovakia, Universidad Publica de Navarra, Pamplona, Spain, Universidade de Tras-Os-Montes e Alto Douro, Vila Real, Portugal, and the University of Westminster, Harrow, UK:

http://www.ibspan.waw.pl/ifs2009

The Eighth International Workshop on Intuitionistic Fuzzy Sets and Generalized Nets (IWIFSGN-2009) has been meant to commence a new series of scientific events primarily focused on new developments in foundations and applications of intuitionistic fuzzy sets and generalized nets pioneered by Professor Krassimir T. Atanassov. Moreover, other topics related to broadly perceived representation and processing of uncertain and imprecise information and intelligent systems are discussed.

We hope that a collection of main contributions presented at the Workshop, completed with many papers by leading experts who have not been able to participate, will provide a source of much needed information on recent trends in the topics considered.

ISBN-13 9788389475305
ISBN 838947530-8