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**

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

ISBN 9788389475305

Generalized net model with intuitionistic fuzzy scale for evaluating the degree of attacked messages sent over the public network

Krassimir Atanassov* and Ivelina Vardeva**

* CLBME – BAN, Sofia, Bulgaria
** Asen Zlatarov University,"Yakimov"1, Burgas, Bulgaria
*krat@bas.bg, **iveto@btu.bg

Abstract

A generalized net is presented in which sending, receiving and intercepting processes between fixed points are described. For achieving higher accuracy, the model uses intuitionistic fuzzy estimates of the messages that are sent, attacked and received. An "independent observer" is defined, collecting information about the running processes in the network between the corresponding users, exchanging confidential messages, and an intruder.

Keywords: cryptanalysis, cryptography, generalized nets, intuitionistic fuzzy sets.

1 Introduction

The presented generalized net model (GN) [2,3,8] considers the degree of the attacked encrypted messages transmitted over the public network.

The expansion of the Internet during the last decade has reached such a degree, that it is considered a basic user technology. The increase of the attacks and the threats with "dark" purposes against the computer systems often raise the problems about computer security, which become increasingly serious [4,5,9] with the development of information technologies.

The general structure of a cryptographic system is considered, whose processes are estimated by intuitionistic fuzzy estimates (IFE) [1]. Those IFEs

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.*

help in finding optimal ways for running the actual processes of estimating the attacked messages between two end points [5,6,7].

A given event running in a real-world system is reflected in the public network by meeting the required conditions for activating the transition. The information that can be read without special efforts is termed plain text. The method of converting the plain text in a way to hide its content is termed encryption. The encryption is aims at information hiding from those who are not the intended recipients. The process of conversion from encrypted text into its plain appearance is termed decryption.

2 Generalized net model

Initially, the following tokens included in the GN are given:

- In the initial moment of the GN in position L_{71A} there are tokens with initial characteristic <0>, and the next characteristics are aggregated through the GN – estimates for messages that have come immediately;
- In the initial moment of the GN in position L_{72A} there are tokens with initial characteristic <0>, and the next characteristics are aggregated through the GN – estimates for messages that have not come at all;
- In the initial moment of the GN in position L_{73A} there are tokens with initial characteristic <0>, and the next characteristics are aggregated through the GN – estimates for messages that have come delayed;
- In the initial moment of the GN in position L_{74A} there are tokens with initial characteristic <0>, and the next characteristics are aggregated through the GN – accumulation estimates for messages that have come delayed;
- In position l_{11} enters the α_1-token with initial characteristic “plain text”;
- In position L_{2A} there is the γ_1-token with initial characteristic “a pair – public and private key of A and a public key for B” – encryption;
- In position L_{4A} enters the δ_2-token c with initial characteristic „received encrypted text”;
- In position L_{5A} enters the γ_2-token with initial characteristic „a pair – public and private key of B and a public key for A” – decryption;
- In position L_{6A} enters the β-token with initial characteristic „received plain text”;
- In position L_{8A} resides the γ_3-token c with initial characteristic „a pair – public and private key of A and a public key for B for deciphering the messages”;

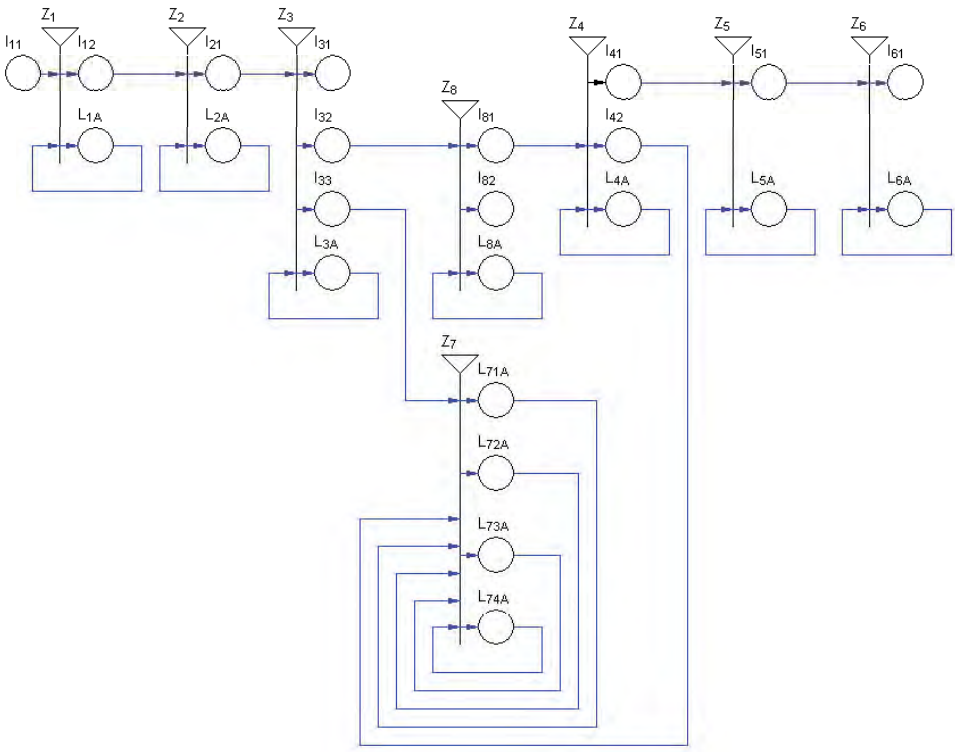

Figure 1: Scale for evaluating the degree of attacked messages

The set A of transitions of the GN is

$$A = \{ Z_1, Z_2, Z_3, Z_4, Z_5, Z_6, Z_7, Z_8 \},$$

where the transitions describe the following processes:

Z_1 – processes performed by the source A,
Z_2 – processes performed by a cryptographic algorithm for encryption,
Z_3 – encrypted messages sending processes,
Z_4 – encrypted messages receiving processes,
Z_5 – processes performed by a cryptographic algorithm for decryption,
Z_6 – processes performed by the source B,
Z_7 – estimates for attacked messages,
Z_8 – attacks performed by C.

Also, initially at location L_{71A} there is a token θ_1 with initial characteristic "<0 ,0>" for the independent observer

$$< \mu^I{}_{k+1}, \nu^I{}_{k+1} > = < \frac{\mu^I{}_k . k + m^I}{k+1}, \frac{\nu^I{}_k . k + n^I}{k+1} > .$$

The current (*k+1*)-th event (for $k \geq 0$) is estimated based on of the previous events from the formula mentioned above, where $<\mu^I_k, \nu^I_k>$ is the previous evaluation, and $<m^I, n^I>$ is the estimation of the latest message, for $m^I, n^I \in [0, 1]$ and $m^I + n^I \leq 1$. The final estimation of the correctness of the information exchanged on the basis of the previous and the latest events is

$$\mu^I = \frac{S_{AB}}{S}, \quad \nu^I = \frac{S_{AC}}{S}, \quad \pi^I = \frac{S''_{ACB}}{S}$$

where

$$S = S_{AB} + S'_{ACB} + S''_{ACB} + S_{AC}$$

S is the number of all messages sent by A;
S_{AB} is the number of sent messages by A that have come to B without a delay for time $\leq t$ that is, those are messages that are not intercepted by C;
S_{AC} is the number of messages sent by A that are intercepted and interrupted by C;
S''_{ACB} is the number of messages sent by A that are intercepted by C and received by B, but modified by C for time $>t$;
t – a time constant determining delays

- If the value of t is ≤ than the input constant, the received message is declared unattacked;
- If the value of t is > than the input constant, the received message is declared attacked.

Also initially at place L_{72A} there is a token θ_2 with initial characteristic "<0 ,0>" for the user B.

$$< \mu^B{}_{k+1}, \nu^B{}_{k+1} > = < \frac{\mu^B{}_k . k + m^B}{k+1}, \frac{\nu^B{}_k . k + n^B}{k+1} > .$$

The current (*k+1*)-th event (for $k \geq 0$) is estimated based on of the previous events from the formula mentioned above. Where $<\mu^B_k, \nu^B_k>$ is the previous evaluation, and $<m^B, n^B>$ is the estimation of the latest message, for $m^B, n^B \in$

[*0,1*] and $m^B + n^B \le 1$. The final estimation of the correctness of the information exchanged on the basis of the previous and the latest events

$$\mu^B = \frac{S_{AB}}{S_1}, \quad \nu^B = \frac{S''_{ACB}}{S_1}, \quad \pi^B = \frac{S'_{ACB}}{S_1}$$

where

$$S_1 = S_{AB} + S'_{ACB} + S''_{ACB}$$

S is the number of all messages sent by A;
S_1 is the number of all sent messages excluding those that have been interrupted, that is, that have not come to B;
S_{AB} is the number of the messages sent by A and received by B without delay for time $\le t$, that is, those are messages that have not been intercepted by C;
S'_{ACB} is the number of the messages sent by A, intercepted by C and received by B, but those are messages for which C has had no time to modify for time $\le t$;
S''_{ACB} is the number of the messages sent by A, intercepted by C and received by B, but modified by C for time $> t$;
t – a time constant determining delays

- If the value of t is ≤ than the input constant, the received message is declared unattacked;
- If the value of t is > than the input constant, the received message is declared attacked.

Also, initially at place L_{A73} there is a token θ_3 with initial characteristic "$<0, 0>$" for the C.

$$<\mu^C{}_{k+1}, \nu^C{}_{k+1}> = <\frac{\mu^C{}_k .k + m^C}{k+1}, \frac{\nu^C{}_k .k + n^C}{k+1}> .$$

The current set $(k+1)$-st for $k \ge 0$ is estimated on the basis of the previous sets from the formula mentioned above. Where $<\mu^C_k, \nu^C_k>$ is the previous evaluation, and $<m^C, n^C>$ is the estimation of the latest message, for $m^C, n^C \in [0, 1]$ and $m^C + n^C \le 1$. The final estimation of the correctness of the information exchanged on the basis of the previous and the latest events is

$$\mu^C = \frac{S''_{ACB} + S_{AC}}{S}, \quad \nu^C = \frac{S_{AB}}{S}, \quad \pi^C = \frac{S'_{ACB}}{S}$$

where

S is the number of all messages sent by A;

S_{AB} is the number of the messages sent by *A* and received by *B* without delay for time ≤ *t*, that is, those are messages that have not been intercepted by *C*;
S'_{ACB} is the number of the messages sent by *A*, intercepted by *C* and received by *B*, but those are messages for which *C* has had no time to modify for time ≤ *t*;
S''_{ACB} is the number of the messages sent by *A*, intercepted by *C* and received by *B*, but modified by *C* for time > *t*;
S_{AC} is the number of messages sent by *A* that are intercepted and interrupted by *C*;
t – a time constant determining delays

- If the value of *t* is ≤ than the input constant, the received message is declared unattacked;
- If the value of *t* is > than the input constant, the received message is declared attacked.

Also initially at place L_{A74} there is a token θ_4 with initial characteristic "<*0*, *0*>" for the user A.

$$< \mu^{A}{}_{k+1}, \nu^{A}{}_{k+1} > = < \frac{\mu^{A}{}_{k}.k + m^{A}}{k+1}, \frac{\nu^{A}{}_{k}.k + n^{A}}{k+1} > .$$

The current (*k+1*)-st event (for *k≥0*) is estimated based on of the previous events from the formula mentioned above. Where $<\mu^{A}_{k}, \nu^{A}_{k}>$ is the previous evaluation, and $<m^{A}, n^{A}>$ is the estimation of the latest message, for $m^{A}, n^{A} \in [0, 1]$ and $m^{A} + n^{A} \le 1$. The final estimation of the correctness of the information exchanged on the basis of the previous and the latest events.

$$\mu^{A} = \frac{S_{AB} + S_{BA}}{2S} + \frac{S'_{ACB} + S'_{BCA}}{2S}, \quad \nu^{A} = 1 - \mu^{A} - \pi^{A},$$

$$\pi^{A} = \frac{S''_{ACB} + S''_{BCA}}{2S} \text{ with time} > 2t$$

where
S is the number of all messages sent by *A*;
S_{AB} is the number of the messages sent by *A* and received by *B* without delay for time ≤ *t*, that is, those are messages that have not been intercepted by *C*;
S_{BA} is the number of the messages sent by *B* and received by *A* without delay for time ≤ *t*, that is, those are messages that have not been intercepted by *C*;
S'_{ACB} is the number of the messages sent by *A*, intercepted by *C* and received by *B*, but those are messages for which *C* has had no time to modify for time ≤ *t*;

S'_{BCA} is the number of the messages sent by B, intercepted by C and received by A, but those are messages for which C has had no time to modify for time $\leq t$;
S''_{ACB} is the number of the messages sent by A, intercepted by C and received by B, but modified by C for time $> t$;
S''_{BCA} is the number of the messages sent by B, intercepted by C and received by A, but modified by C for time $> t$.

The transitions have the following description:

$$Z_1 = < \{l_{11}, L_{1A}\}, \{l_{12}, L_{1A}\}, R_1, \vee (l_{11}, L_{1A}) >$$

$$R_1 = \begin{array}{c|cc} & l_{12} & L_{1A} \\ \hline l_{11} & false & true \\ L_{1A} & W_{1A,12} & true \end{array}$$

where
$W_{1A,12}$ = "a text for encryption is received".

The entering token α_1 from position l_{11} unites with the token α_2, residing in position L_{1A}. The token α_2 from position L_{1A} splits into two identical tokens α_2' and α_2'', that enter the position L_{1A} and l_{12}, respectively. After the transition the token α_2'' from position l_{12} leaves out with the following current characteristic "plain text for encryption".

$$Z_2 = < \{l_{12}, L_{2A}\}, \{l_{21}, L_{2A}\}, R_2, \vee (l_{12}, L_{2A}) >$$

$$R_2 = \begin{array}{c|cc} & l_{21} & L_{2A} \\ \hline l_{12} & false & true \\ L_{2A} & W_{2A,21} & true \end{array}$$

where
$W_{2A,21}$ = "the text is encrypted".

The token α_2'' from position l_{12} enters the position L_{2A}, where it unites with the token γ_1 from the current position in token ε_1 and obtains its new characteristic "encrypted text" based on a cryptographic algorithm for encrypting. The token ε from position L_{2A} splits into two same tokens ε_1' and ε_1'', that enter positions L_{2A} и l_{21}, respectively. After the transition, the token from position l_{21} does not obtain any new characteristic.

$$Z_3 = < \{l_{21}, L_{3A}\}, \{l_{31}, l_{32}, l_{33}, L_{3A}\}, R_3, \vee (l_{21}, L_{3A}) >$$

$R_3 =$

	l_{31}	l_{32}	l_{33}	L_{3A}
l_{21}	*false*	*false*	*false*	*true*
L_{3A}	$W_{3A,31}$	$W_{3A,32}$	$W_{3A,33}$	*true*

where

$W_{3A,31}$ = "the sent message has not been attacked",

$W_{3A,32}$ = „the sent message has been attacked",

$W_{3A,33} = W_{3A,31} \vee W_{3A,32}$.

The token α_2*"* from position l_{21}, upon entering the position L_{3A} unites with the token δ_1 and obtains its new characteristic "encrypted text for sending". The token δ_1 splits into two same tokens δ_1*'* and δ_1*"*. One of them remains in the current position, and the other one enters the position l_{31} or l_{32}. The token l_{33} obtains a characteristic "the message is sent".

$$Z_4 = < \{l_{31}, l_{81}, L_{4A}\}, \{l_{41}, l_{42}, L_{4A}\}, R_4, \vee (l_{31}, l_{81}, L_{4A}) >$$

$R_4 =$

	l_{41}	l_{42}	L_{4A}
l_{31}	*false*	*false*	*true*
l_{81}	*false*	*false*	*true*
L_{4A}	$W_{4A,41}$	$W_{4A,42}$	*true*

where

$W_{4A,41}$ = "an encrypted message is received",

$W_{4A,42}$ = "information about a received message is sent" .

The entering tokens from the positions l_{31} and l_{81} are added to the token δ_2 residing in position L_{4A}, and get their new characteristic "received encrypted text". The token δ_2 splits into two same tokens δ_2' and δ_2". One of them remains in the current position, and the other one enters the position l_{41}. The token from position l_{42} obtains a characteristic "a message is received".

$$Z_5 = < \{l_{41}, L_{5A}\}, \{L_{5A}, l_{51}\}, R_5, \vee (l_{41}, L_{5A}) >$$

$R_5 =$

	L_{5A}
l_{41}	*true*
L_{5A}	*true*

The token δ_2" from position l_{41} enters the position L_{5A}, where it unites with the token γ_2 from the current position into the token ε_2 and obtains its new characteristic "plain text" based on a cryptographic algorithm for decrypting. The token ε_2 from position L_{5A}, splits into two same tokens ε_2' and ε_2", that enter the positions L_{5A} и l_{51}, respectively. After the transition the token from position l_{51} does not get new characteristic.

$$Z_6 = < \{l_{51}, L_{6A}\}, \{ l_{6A}, L_{61} \}, R_6, M_6, \vee (l_{51}, L_{6A}) >$$

$R_6 =$

	l_{61}	L_{6A}
l_{51}	*false*	*true*
L_{6A}	$W_{6A,61}$	*true*

where
$W_{6A,61}$ = "the message text is received" .

The token ε_2" from position l_{51} enters the position L_{6A} with a characteristic "plain text".

$$Z_7 = <\{ l_{33}, l_{42}, L_{71A}, L_{72A}, L_{73A}, L_{74A}\},\{ L_{71A}, L_{72A}, L_{73A}, L_{74A} \}, R_7, \vee (l_{33}, l_{42}, L_{71A}, L_{72A}, L_{73A}, L_{74A})>$$

$R_7 =$

	L_{71A}	L_{72A}	L_{73A}	L_{74A}
l_{33}	*true*	*true*	*true*	*true*
l_{42}	*true*	*true*	*true*	*true*
L_{71A}	*true*	*false*	*false*	*false*
L_{72A}	*false*	*true*	*false*	*false*
L_{73A}	*false*	*false*	*true*	*false*
L_{74A}	*false*	*false*	*false*	*true*

The tokens entering position L_{71A} obtain characteristic "$<m^I, n^I>$", where $<m^I, n^I>$ is the estimation of the established of the communication between the user *A*, user *B* and *C*.

When the message is received successfully, $<m^I, n^I> = <0, 1>$ they obtain those values.

When the message is received unsuccessfully, $<m^I, n^I> = <1, 0>$.

In all other cases $<m^I, n^I> = <0, 0>$.

The tokens entering position L_{72A} obtain characteristic "$<m^B, n^B>$", that is, the estimation of the established of the communication between the user *A*, user *B* and *C*.

When the messages are received at *B* and there is a confirmation by *A*, $<m^B, n^B> = <0, 1>$.

When the messages are not received at *B*, but there is a confirmation by *A*, $<m^B, n^B> = <1,0>$.

In all other cases $<m^B, n^B> = <0, 0>$.

The tokens entering position L_{73A} obtain characteristic "$<m^C, n^C>$", where m^C, n^C is the estimation of the established communication between the user *A*, user *B* and *C*.

When the message is successfully attacked, $<m^C, n^C> = <0, 1>$.

When the messages are passed - unattacked, $<m^C, n^C> = <1, 0>$.

In all other cases $<m^C, n^C> = <0, 0>$.

$$Z_8 = < \{l_{32}, L_{8A}\}, \{l_{81}, l_{82}, L_{8A}\}, R_8, \vee (l_{32}, L_{8A}) >$$

$R_8 =$

	l_{81}	l_{82}	L_{8A}
l_{32}	*false*	*false*	*true*
L_{8A}	$W_{8A,81}$	$W_{8A,82}$	*true*

where

$W_{8A,81}$ = "the attacked message is sent",

$W_{8A,82}$ = "the attacked message is interrupted" .

The tokens received from positions l_{22} with characteristic „intercepted/attacked message" enter the position L_{8A}, where depending on the corresponding performed attack, the message may remain in its current position, may be modified or an entirely new message may be or a copy may be made. The token entering position l_{81} gets a characteristic "sending an attacked message".

3 Conclusions

The model allows for considering different stages of running the process of information exchange, as well as its simulation and behaviour in the future. A general structure for sending and receiving encrypted messages is considered, using an independent party, collecting information about the processes running in the network. This aids the problem solving in building security systems for achieving a higher accuracy in determining the attacked messages, sent and received over the network.

References

[1] Atanassov, K. "Intuitionistic Fuzzy Sets", Springer, Heidelberg, 1999

[2] Atanassov, K., "Introduction to the generalized nets theory", Burgas, 1992 (in Bulgarian).

[3] Atanassov, K., "Generalized nets", World Scientific, Singapore, New Jersey, London1991.

[4] Denning, Dorothy E., "Cryptography and data security", Purdue University, 1983.

[5] Hristov, H., Trifonov, V., "Communication reliability and security", Sofia, 2005 (in Bulgarian).

[6] Menezes, A., Van Orschot, P., Vanstone, S., "Handbook of Applied Cryptography", CRC Press, 1997.

[7] Piper, F., Murphy, S., „Cryptography: A Very Short Introduction", Oxford University Press 2002.

[8] Vardeva, I., "A generalized net model of a cryptographic system using a symmetric key" – Annual of Informatics section of the Union of the Scientists in Bulgaria, vol., 2008 (in Bulgarian).

[9] Vardeva, I., "SSL Modeling by the Apparatus of Generalized Net", Sixth Int. Workshop on GNs, Sofia, 17 Dec. 2005, pp. 29-33.

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