Applying Basic-Elements and the Extension Theory to Alert-centric Event Correlation for Unified Network Security Management

Hui Xu, Chunzhi Wang, Hongwei Chen and Zhiwei Ye

School of Computer Science, Hubei University of Technology, Wuhan, China
xuhui_1004@hotmail.com

Abstract

With increasing requirements of network users for intelligent security management, unified network security management has become a fashion, and a remarkable development trend is the adoption of an alert-centric event correlation manner. This paper then introduces Extenics into the study on alert-centric event correlation for unified network security management and proposes a formalized approach using basic-elements based on the extension theory. The proposed approach utilizes the basic-elements to formalize the representations of alerts, events, and also correlation policies for network security in a unified manner, and then makes full use of the extension theory to formalize basic operators for extension expressions and extension functions in order to realize alert-centric event correlation. Validation scenarios of timing constraints show that, the proposed approach provides a prospective way to alert-centric event correlation for unified network security management by introducing basic-elements and utilizing extension expressions and extension functions with the use of containing analysis, sequencing analysis and extension transformations based on the extension theory.

Keywords: *Unified Network Security Management, Alert-centric Event Correlation, Extenics, Basic-Element, Extension Theory*

1. Introduction

In the field of network security, two techniques namely collaboration and correlation are adopted by more and more researchers and engineers, while the source information is various alerts and events from network security solutions such as Intrusion Detection Systems (IDSs), firewalls, anti-virus tools, and so on. Thus a remarkable development trend of unified network security management is the adoption of an alert-centric event correlation manner.

As for unified network security management, a unified framework of information and knowledge is of great significance. Since ontology-based security management [1] has been possible, this unified framework in the field of network security may be presented by existing ontology description languages. But from the intelligent management point of view, a more formalized approach is required for this unification.

The thinking of Extenics [2, 3] prospects a promising way by means of a higher formalization for the study on alert-centric event correlation. The logic cell of Extenics is basic-elements [4], and its fundamental theory is the extension theory [5]. The aim of this paper is then to introduce Extenics into the research on unified network security management and apply basic-elements and the extension theory to alert-centric event correlation from the viewpoint of collaboration.

The remainder of this paper is organized as follows. Section 2 introduces basic elements and discusses formal representations of security information and knowledge for alert-centric event correlation using affair-elements, relation-elements and composite-elements. Section 3 then applies the extension theory, including containing analysis, sequencing analysis and extension transformations, to formalize basic operators for extension expressions and extension functions, in order to realize alert-centric event correlation. Section 4 presents two scenarios of timing constraints to validate the feasibility of the proposed formalized approach for alert-centric event correlation. Section 5 concludes this paper.

2. Formal Representations of Security Information and Knowledge using Basic-elements

As for alert-centric event correlation, this section will apply basic elements for formal representations of security information and knowledge in a unified manner.

2.1. Application of basic-elements

Basic-elements include matter-elements, affair-elements and relation-elements, and formalization by their composition formats named as composite-elements. Formula 1 demonstrates a common definition of basic-elements, in which $Object$ means the object for the research, with its characteristics $c_1, c_2, ..., c_n$ and corresponding values $v_1, v_2, ..., v_n$.

$$B = \begin{bmatrix} Object, c_1, v_1 \\ c_2, v_2 \\ ..... \\ c_n, v_n \end{bmatrix} \quad \ldots (1)$$

Base on Formula 1, the class for a type of basic-elements can be defined as Formula 2, in which $V_1, V_2, ..., V_n$ describe the value domains of characteristics $c_1, c_2, ..., c_n$ for the set of objects that is $\{Object\}$.

$$\{B\} = \begin{bmatrix} \{Object\}, c_1, V_1 \\ c_2, V_2 \\ ..... \\ c_n, V_n \end{bmatrix} \quad \ldots (2)$$

When considering issues related to unified network security management, the proposed approach utilizes basic-elements for formal representations of security information and knowledge, including alerts, events and correlation policies by means of affair-elements, relation-elements and composite-elements.

2.2. Formal representations of security information for alerts and events

As for the unified representation of alerts for network security, Formula 3 presents the formal representation of network security alerts using the class of affair-elements labeled as A_A, in which $\{Alert_x\}$ means a particular kind of alert objects, with its characteristics $c_{x1}, c_{x2}, ..., c_{xn}$ and corresponding value domains $V_{x1}, V_{x2}, ..., V_{xn}$.

$$\{A_A\} = \begin{bmatrix} \{Alert_x\}, c_{x1}, V_{x1} \\ c_{x2}, V_{x2} \\ ..... \\ c_{xn}, V_{xn} \end{bmatrix} \quad \ldots (3)$$
$$= (\{Alert_x\}, c_x, V_x)$$

In addition to alerts, events are also valuable for unified network security management. Formula 4 indicates the formal representation of network security events using the class of affair-elements labeled as A_E, in which $\{Event_y\}$ means a particular type of event objects, with its characteristics $c_{y1}, c_{y2}, ..., c_{yn}$ and corresponding value domains $V_{y1}, V_{y2}, ..., V_{yn}$.

$$\{A_E\} = \begin{bmatrix} \{Event_y\}, c_{y1}, V_{y1} \\ c_{y2}, V_{y2} \\ ..... \\ c_{yn}, V_{yn} \end{bmatrix} \quad \ldots (4)$$
$$= (\{Event_y\}, c_y, V_y)$$

2.3. Formal representations of security knowledge for correlation policies

In the same way as formal representations of security information, basic-elements realize formal representations of security knowledge for correlation policies by means of relation-elements and composite-elements.

Formula 5 provides the formal representation of correlation policies for unified network secu rity management using the class of relation-elements labeled as R_C, in which $\{Correlation_z\}$ means a particular kind of correlation objects, with its characteristics $c_{z1}, c_{z2}, ..., c_{zn}$ and corresponding values $V_{z1}, V_{z2}, ..., V_{zn}$.

$$\{R_C\} = \begin{bmatrix} \{Correlation_z\}, c_{z1}, V_{z1} \\ c_{z2}, V_{z2} \\ ..... \\ c_{zn}, V_{zn} \end{bmatrix} \quad \ldots (5)$$
$$= (\{Correlation_z\}, c_z, V_z)$$

According to Formula 5, the Condition-Action paradigm [6] for correlation policies in the field of network security is formalized as the relation-element shown in Formula 6.

$$R_C = \begin{bmatrix} Correlation_z, Condition, v_{z1} \\ Action, v_{z2} \end{bmatrix} \quad \ldots (6)$$

Note that, the formalization of correlation policies shown above is usually in the form of composite-elements. Thus the correlation policies can be described by composite-elements for alert-centric event correlation, which correlates alerts with related events. In this case,

Formula 7 proposes the formalization for alert-centric event correlation by composite-elements based on Formula 6.

$$C_C = \begin{bmatrix} Correlation_z, Condition, Exp(A_A, A_E) \\ Action, Func(A_A, A_E) \end{bmatrix} \quad \ldots (7)$$

As is indicated in Formula 7, the extension expression $Exp(A_A, A_E)$ is introduced for formalization of correlation conditions and the extension function $Func(A_A, A_E)$ is used for formalization of correlation actions.

3. Application of the Extension Theory for Alert-centric Event Correlation

Since the formalization of security information and knowledge has been realized by basic-elements in a unified manner, this section will utilize extension expressions with the support of basic operators and extension functions based on the extension theory [4, 5, 7] for the purpose of alert-centric event correlations.

3.1. Basic operators for extension expressions

As demonstrated in Formula 7, the extension expression $Exp(A_A, A_E)$ is used for the formalization of conditions in the case of alert-centric event correlation, and its key elements are the basic operators, which are used to organize related basic-elements and extension functions. In order to introduce the basic operators for alert-centric event correlation, the definition of basic-element containing and its core principle are first presented in Definition 1 and Principle 1.

Definition 1 Suppose B_p, B_q are two basic-elements, if the implementation of B_p must lead to the implementation of B_q, then it means that B_p contains B_q, marked as $B_p \Rightarrow B_q$.

Principle 1 If $B_p \Rightarrow B_r$ and $B_r \Rightarrow B_q$, then $B_p \Rightarrow B_q$, or marked as $B_p \Rightarrow B_r \Rightarrow B_q$.

And then Definition 2-5 respectively describes four general situations of basic-element containing.

Definition 2 If all the implementations of basic-element $B_i(i = 1...n)$ lead to the implementation of basic-element B, then it means that $B_i(i = 1...n)$ by the AND operation contain B, marked as $\underset{i=1}{\overset{n}{\wedge}} B_i \Rightarrow B$.

Definition 3 If at least one of the implementations of basic-element $B_i(i = 1...n)$ lead to the implementation of basic-element B, then it means that $B_i(i = 1...n)$ by the OR operation contain B, marked as $\underset{i=1}{\overset{n}{\vee}} B_i \Rightarrow B$.

Definition 4 If the implementation of basic-element B leads to all the implementations of basic-element $B_i(i = 1...n)$, then it means that B contains $B_i(i = 1...n)$ by the AND operation, marked as $B \Rightarrow \underset{i=1}{\overset{n}{\wedge}} B_i$.

Definition 5 If the implementation of basic-element B leads to at least one of the implementations of basic-element $B_i(i=1...n)$, then it means that B contains $B_i(i=1...n)$ by the OR operation, marked as $B \Rightarrow \underset{i=1}{\overset{n}{\vee}} B_i$.

Using the containing analysis based on the extension theory, Definition 6 formalizes the AND operator for correlation conditions, as is also explained in Figure 1.

Definition 6 If $B_i \in \{\{A_A\},\{A_E\}\}, 1 \le i \le n$, $\underset{i=1}{\overset{n}{\wedge}} B_i \Rightarrow Condition$ and $Condition \Rightarrow \underset{i=1}{\overset{n}{\wedge}} B_i$, then $Condition$ can be defined by the AND operator, marked as $AND(B_i)$.

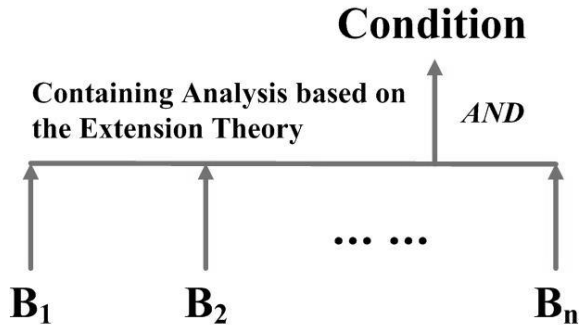

Figure 1. The AND operator using the containing analysis based on the extension theory

Still using the containing analysis based on the extension theory, Definition 7 formalizes the OR operator for correlation conditions, as is also depicted in Figure 2.

Definition 7 If $B_i \in \{\{A_A\},\{A_E\}\}, 1 \le i \le n$, $\underset{i=1}{\overset{n}{\vee}} B_i \Rightarrow Condition$ and $Condition \Rightarrow \underset{i=1}{\overset{n}{\vee}} B_i$, then $Condition$ can be defined by the OR operator, marked as $OR(B_i)$.

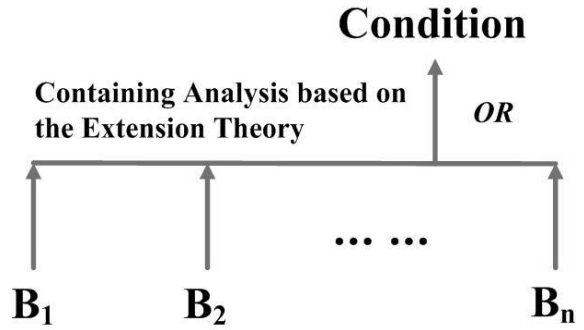

Figure 2. The OR operator using the containing analysis based on the extension theory

In the field of network security, the attacks are possibly implemented step-by-step. The definition of basic-element sequencing is then given in Definition 8 for the case of serialization of basic-elements.

Definition 8 If all the implementations of basic-element $B_i(i=1...n)$ in a sequential way lead to the implementation of basic-element B, then it means that $B_i(i=1...n)$ serializes B, marked as $\overset{n}{\underset{i=1}{\forall}} B_i \mapsto B$.

Based on Definition 8, Definition 9 formalizes the SEQ operator for correlation conditions, as is also demonstrated in Figure 3.

Definition 9 If $B_i \in \{\{A_A\},\{A_E\}\}, 1 \le i \le n$, and $\overset{n}{\underset{i=1}{\forall}} B_i \mapsto Condition$, then $Condition$ can be defined by the SEQ operator, marked as $SEQ(B_i)$.

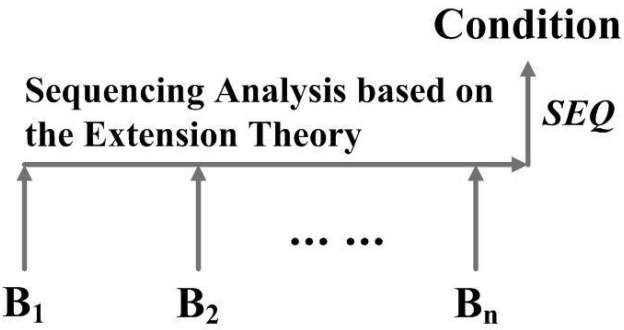

Figure 3. The SEQ operator using the sequencing analysis based on the extension theory

3.2. Formalization of extension functions

When expressing correlation conditions or describing correlation actions, extension functions are introduced to formalize the methods to realize correlation policies for unified network security management.

Definition 10 If the source-object for transformation is $S \in \{\{A_A\},\{A_E\},\{Alert_x\},\{Event_y\},c_x,c_y,V_x,V_y\}$, the extension functions of transformation from S to the target-object S' can be defined by $S' = Func(S)$.

As is indicated in Definition 10, the extension function $S' = Func(S)$ essentially reflects the implementation of an extension transformation that is $T: S \to S'$, which can be formalized as the class of composite-elements labeled as C_F. Thus, Formula 8 presents the description of C_F, in which $\{Object_t\}$ means a particular type of either alert or event objects, with its characteristics $c_{t1}, c_{t2}, ..., c_{tn}$ and corresponding value domains $V_{t1}, V_{t2}, ..., V_{tn}$.

$$S^{'} = Func(S)$$
$$\Leftrightarrow T : S \rightarrow S^{'} \quad \ldots (8)$$
$$\Leftrightarrow \{C_F\} = \begin{bmatrix} \{Object_t\}, c_{t1}, V_{t1} \\ c_{t2}, V_{t2} \\ ..... \\ c_{tn}, V_{tn} \end{bmatrix}$$

4. Validation Scenarios

In order to validate the feasibility of the proposed formalized approach for alert-centric event correlation, this section will discuss two scenarios of timing constraints for unified network security management.

4.1. Extension functions for validation

Several extension functions will be defined for the scenarios of timing constraints [8].

First of all, Formula 9 introduces the extension function OT to record the i th occurrence time for a particular alert or event.

$$A_{AorE}, i \rightarrow OT(A_{AorE}, i)$$
$$\Leftrightarrow \{C_{OT}\} = \begin{bmatrix} \{Object_o\}, AlertorEvent, A_{AorE} \\ SequenceNumber, i \\ OccurrenceTime, ot \end{bmatrix} \quad \ldots (9)$$

Based on the extension function OT, Formula 10 presents the extension function CN to count the occurrence number of a particular alert or event during a specified time slot sts.

$$A_{AorE}, sts \rightarrow CN(A_{AorE}, sts)$$
$$\Leftrightarrow \{C_{CN}\} = \begin{bmatrix} \{Object_c\}, AlertorEvent, A_{AorE} \\ Sepecified\ TimeSlot, sts \\ OccurrenceCount, oc \end{bmatrix} \quad \ldots (10)$$

Furthermore, combined with the extension functions OT and CN, Formula 11 demonstrates the extension function RT, which aims to record the i th relative occurrence time during a relative time slot rts for a particular alert or event.

$$A_{AorE}, rts, i \rightarrow RT(A_{AorE}, rts, i)$$
$$\Leftrightarrow \{C_{RT}\} = \begin{bmatrix} \{Object_r\}, AlertorEvent, A_{AorE} \\ \text{Re}lativeTimeSlot, rts \\ SequenceNumber, i \\ \text{Re}lativeOccurrenceTime, rot \end{bmatrix} \quad \ldots (11)$$

Formula 12 then provides an equivalence relation of two extension functions OT and RT when $CN(A_{AorE},t)+i\rangle 0$.

$$\begin{aligned} & A_{AorE},t,i \rightarrow RT(A_{AorE},t,i) \\ \Leftrightarrow \{C_{RT}\} &= \begin{bmatrix} \{Object_r\}, AlertorEvent, A_{AorE} \\ \quad RelativeTimeSlot, t \\ \quad SequenceNumber, i \\ \quad RelativeOccurrenceTime, rot \end{bmatrix} \\ \Leftrightarrow \{C_{OT}\} &= \begin{bmatrix} \{Object_o\}, AlertorEvent, A_{AorE} \\ \quad SequenceNumber, CN(A_{AorE},t)+i \\ \quad OccurrenceTime, ot \end{bmatrix} \\ \Leftrightarrow & A_{AorE}, CN(A_{AorE},t)+i \rightarrow OT(A_{AorE}, CN(A_{AorE},t)+i) \end{aligned} \quad \ldots (12)$$

4.2. Scenario analysis

Using the definition of extension functions above, two scenarios of timing constraints for alert-centric event correlation in view of unified network security management will be analyzed as follows.

Scenario 1 Suppose that a particular alert or event A_{AorE} occurs frequently during a specified unit of time slot t. In this case $CN(A_{AorE},t)\rangle cv$, where cv expresses the critical value for occurrence frequency of A_{AorE} specified by the security managers. Thus a reminding event should then be notified to related security managers using the event subscription mechanism, which can be realized by the extension function NE.

Formula 13 shows a general formalization of NE for notification events, in which A_{NE} is an instance of network security events using the class of affair-elements labeled as $\{A_E\}$.

$$\begin{aligned} & A_{AorE},t,cv \rightarrow NE(A_{AorE},t,cv) \\ \Leftrightarrow \{C_{NE}\} &= \begin{bmatrix} \{Object_n\}, AlertorEvent, A_{AorE} \\ \quad Trigger, CN(A_{AorE},t)\rangle cv \\ \quad EventforNotification, A_{NE} \end{bmatrix} \end{aligned} \quad \ldots (13)$$

Scenario 2 The scenario above is a relatively simpler one for the case of timing constraints, and this scenario will take more complex timing constraints into consideration. As for the Distributed Denial of Service (DDoS) attacks simulated by 2000 DARPA Intrusion Detection Evaluation Data Sets from MIT Lincoln Laboratory [9], they are comprehensive attacks, in which many alerts and events should be correlated for the sake of unified network security management.

As is presented in Definition 9 with the use of the sequencing analysis based on the extension theory, the SEQ operator formalizes this sequential relationship of related alerts and events for correlation conditions. However, there are usually timing constraints between adjacent alerts and events, which can be described by TC.

Formula 14 provides the general formalization of timing constraints applied to $SEQ(B_i)$ in an ascending order, where $B_i \in \{\{A_A\},\{A_E\}\}, 1 \le i \le n$.

$$OT(B_j, m) + TC_j \ge OT(B_{j+1}, m), 1 \le j \le n-1, TC_j \rangle 0 \quad \ldots (14)$$

Formula 15 shows the general formalization of timing constraints applied to $SEQ(B_i)$ in a descending order, where $B_i \in \{\{A_A\},\{A_E\}\}, 1 \le i \le n$.

$$OT(B_j, m) + TC_j \le OT(B_{j+1}, m), 1 \le j \le n-1, TC_j \langle 0 \quad \ldots (15)$$

Formula 16 demonstrates a general description of *Condition* for the specified case of sequential correlation with timing constraints to promote the formalization of alert-centric event correlation based on basic-elements.

$$\begin{aligned} &SEQ(B_i) \wedge TC_j \\ &(B_i \in \{\{A_A\},\{A_E\}\}, 1 \le i \le n, 1 \le j \le n-1) \end{aligned} \quad \ldots (16)$$

Figure 4 then presents the formalization of conditions for the case of sequential correlation with timing constraints based on the extension theory.

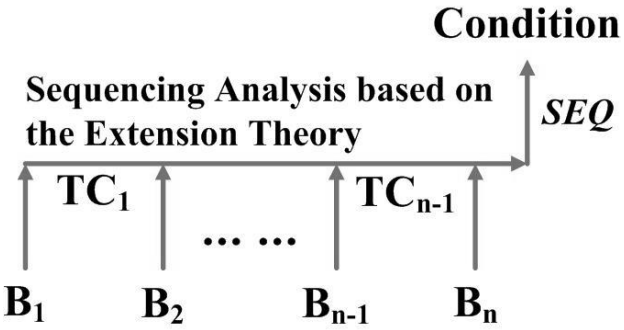

Figure 4. The formalization of conditions for the case of sequential correlation with timing constraints based on the extension theory

Thus a root alert should be generated to related security managers, which can be realized by the extension function *GR*. Formula 17 shows a general formalization of *GR* for generating the root alert, in which A_{GR} is an instance of network security alerts using the class of affair-elements labeled as $\{A_A\}$.

$$\begin{aligned} &SEQ(B_i), TC_j \rightarrow GR(SEQ(B_i), TC_j) \\ &\Leftrightarrow \{C_{GR}\} = \begin{bmatrix} \{Object_g\}, Sequence, SEQ(B_i) \\ Ti\min gConstra\text{int}, TC_j \\ RootAlert, A_{GR} \end{bmatrix} \\ &(B_i \in \{\{A_A\},\{A_E\}\}, 1 \le i \le n, 1 \le j \le n-1) \end{aligned} \quad \ldots (17)$$

The evaluation result of these validation scenarios above shows that, the proposed approach provides a prospective way to alert-centric event correlation for unified

network security management by introducing basic-elements and utilizing extension expressions and extension functions with the use of containing analysis, sequencing analysis and extension transformations based on the extension theory.

5. Conclusions

The main contribution of this paper is to consider alert-centric event correlation for unified network security management from the thinking of Extenics and prospect a formalized approach using basic-elements based on the extension theory.

The proposed approach makes use of the basic-elements to formalize the representations of alerts, events and correlation policies for network security in a unified manner, and then utilizes the extension theory to formalize not only extension expressions with the support of basic operators by containing analysis and sequencing analysis, and also extension functions with the use of extension transformations, in order to realize alert-centric event correlation for the purpose of unified network security management.

Acknowledgements

This work has been supported by the General Program for Natural Science Foundation of Hubei Province in China (No. 2012FFB00601), the Key Project for Scientific and Technological Research of Wuhan City in China (No. 201210421134), the Doctoral Scientific Research Fund from Hubei University of Technology (No. BSQD12029), the Provincial Teaching Reform Research Project of Education Department of Hubei Province in China (No. 2012273), the General Program for National Natural Science Foundation of China (No. 61170135), the National Natural Science Foundation of China for Young Scholars (No. 61202287), the Key Project for Natural Science Foundation of Hubei Province in China (No. 2010CDA011), the General Program for Natural Science Foundation of Hubei Province in China (No. 2011CDB075), the Key Project for Scientific and Technological Research of Education Department of Hubei Province in China (No. D20111409, No. D20121409), and the Twilight Plan Project of Wuhan City in China (No. 201050231084). The authors would like to thank all project partners for their valuable contributions and feedbacks.

References

[1] B. Tsoumas and D. Gritzalis, “Towards an Ontology-based Security Management”, Proceeding of 20th International Conference on Advanced Information Networking and Applications, IEEE Press, **(2006)**, pp. 985-992.
[2] W. Cai, “Extension Set and Non-Compatible Problems”, Journal of Scientific Exploration, in Chinese, vol. 1, **(1983),** pp. 83-97.
[3] W. Cai, “Matter-Element Analysis, Simplified Chinese version”, Guangdong Higher Education Press, Guangzhou, **(1987)**.
[4] W. Cai, C. Y. Yang and B. He, “Preliminary Extension Logic”, Simplified Chinese version, Science Press, Beijing, **(2003)**.
[5] C. Y. Yang and W. Cai, “Extension Engineering”, Simplified Chinese version, Science Press, Beijing, **(2007)**.
[6] W. L. Han and C. Lei, “A Survey on Policy Languages in Network and Security Management”, Computer Nerworks, vol. 56, no. 1, **(2012)**, pp. 477-489.
[7] L. X. Li, C. Y. Yang and H. W. Li, “Extension Strategy Generation System”, Simplified Chinese version, Science Press, Beijing, **(2006)**.
[8] A. K. Mok, P. Konana, G. Liu, C. Lee and H. Woo, “Specifying Timing Constraints and Composite Events: An Application in the Design of Electronic Brokerages”, IEEE Transactions on Software Engineering, vol. 30, no. 12, **(2004)**, pp. 841-858.
[9] MIT Lincoln Laboratory, 2000 DARPA Intrusion Detection Evaluation Data Sets, www.ll.mit.edu/mission/communications/cyber/CSTcorpora/ideval/data/2000data.html, **(2013)**.

Authors

Hui Xu received a bachelor's degree in Computer Science and Technology from Huazhong Normal University, Wuhan, China in 2005, a master's degree in Computer Application Technology from Huazhong Normal University, Wuhan, China in 2008, and a doctor's degree in Radio Physics from Huazhong Normal University, Wuhan, China in 2010. Since 2006, she has been a certified computer system analyst in China. Now, she is a Lecturer at the School of Computer Science in Hubei University of Technology, Wuhan, China. Currently, her major field of study is network and service management.

Dr. Xu became a Member of Institute of Electrical and Electronics Engineers (IEEE) in 2007, a Member of Association for Computing Machinery (ACM) in 2007 and a Member of China Computer Federation (CCF) in 2008. She has authored or coauthored 1 book and 2 book chapters in the field of network management, 9 papers published by international journals, 4 papers published by Chinese journals, and more than 20 papers published by international conferences. In April 2008, she was awarded by International Association of Engineers (IAENG) for her first-authored paper presented to 2008 IAENG International Conference on Communication Systems and Applications. In July 2008, her biography was selected for inclusion in the 26th edition (2009) of the Marquis Who's Who in the World, California, USA. Additionally, she was a Session Co-Chair or a Paper Reviewer for 2nd&3rd&7th&8th International Conference on Computer Science and Education (ICCSE 2007&2008&2012&2013), a Session Chair for 1st International Symposium on Electronic Commerce and Security (ISECS 2008), a Paper Reviewer for 4th IEEE Conference on Industrial Electronics and Applications (ICIEA 2009), a Paper Reviewer for 3rd International Conference on Computer and Network Technology (ICCNT 2011), and a Paper Reviewer for Security and Communication Networks, an international journal published by Wiley Press.

Chunzhi Wang is a Professor at the School of Computer Science in Hubei University of Technology, Wuhan, China. She is also the Dean of the School of Computer Science in Hubei University of Technology, Wuhan, China. Currently, her major field of study is cooperative management.

Hongwei Chen is a Associate Professor in the School of Computer Science at Hubei University of Technology, Wuhan, China. Currently, his major field of study is distributed management.

Zhiwei Ye is a Associate Professor in the School of Computer Science at Hubei University of Technology, Wuhan, China. Currently, his major field of study is computational intelligence.