모바일 애드 혹 망을 위한 러프 집합을 사용한 교차 특징 분석 기반 비정상 행위 탐지 방법의 설계 및 평가

Design and Evaluation of an Anomaly Detection Method based on Cross-Feature Analysis using Rough Sets for MANETs

배 인 한[*] 이 화 주[**]
Ihn-Han Bae Hwa-Ju Lee

요 약

무선 장치의 확산으로, 무선 애드 혹 망(MANETs, Mobile Ad-hoc NETworks)은 매우 흥미롭고 중요한 기술이 되고 있다. 그러나 MANET은 유선망 보다 더 견고하지 못하다. 유선망을 위하여 설계된 기존의 보안 메커니즘은 새로운 패러다임에서 재설계되어야 한다. 본 논문에서, 우리는 MANET에서 비정상 행위 탐지 문제를 논의한다. 우리의 연구의 초점은 새로운 또는 알려지지 않은 공격을 탐지할 수 있는 비정상 행위 탐지 모델을 자동적으로 구축하는 기법에 있다. 제안하는 방법은 정상 트래픽에서 특징간 상관 관계 패턴을 포착하기 위하여 러프 집합에 기초한 교차 특징 분석을 수행한다. 제안하는 방법의 성능은 시뮬레이션을 통하여 평가되었다. 그 결과, 제안하는 방법의 성능이 특징 속성값의 확률에 기반 하는 교차 특징 분석을 사용하는 Huang의 방법 보다 성능이 우수함을 보였다. 따라서 제안하는 방법이 비정상 행위를 효율적으로 탐지한다는 것을 알 수 있었다.

Abstract

With the proliferation of wireless devices, mobile ad-hoc networking (MANETS) has become a very exciting and important technology. However, MANET is more vulnerable than wired networking. Existing security mechanisms designed for wired networks have to be redesigned in this new environment. In this paper, we discuss the problem of anomaly detection in MANET. The focus of our research is on techniques for automatically constructing anomaly detection models that are capable of detecting new or unseen attacks. We propose a new anomaly detection method for MANETs. The proposed method performs cross-feature analysis on the basis of Rough sets to capture the inter-feature correlation patterns in normal traffic. The performance of the proposed method is evaluated through a simulation. The results show that the performance of the proposed method is superior to the performance of Huang method that uses cross-feature based on the probability of feature attribute value. Accordingly, we know that the proposed method effectively detects anomalies.

☞ Keywords: Anomaly Detection, Rough Sets, Cross-feature Analysis, Inter-feature Correlation Patterns, MANETs.

1. Introduction

In mobile ad hoc networks (MANETs), mobile nodes are not bounded to any centralized control like base stations or access points. This feature offers great flexibility for establishing communications, while at the same time makes MANETs very vulnerable to various attacks. In recent years, with the rapid proliferation of wireless devices, the potentials and importance of mobile ad-hoc networking have become apparent. A mobile ad-hoc network is formed using a group of mobile wireless nodes often without the assistance of fixed or existing network infrastructure. The nodes must cooperate by forwarding packets so

[*] 종신회원 : 대구가톨릭대학교 컴퓨터정보통신공학부 교수
ihbae@cu.ac.kr
[**] 준 회 원 : 대구가톨릭대학교 컴퓨터정보통신공학부 박사과정
hj2380@hanmail.net

[2008/03/25 투고 - 2008/04/14 심사 - 2008/07/10 심사완료]

that nodes beyond radio ranges can be communicate with each other. With a striking similarity of the early days of Internet research, security issues in ad-hoc networking have no yet been adequately investigated in the current stage. MANET is much more vulnerable than wired networking due to its limited physical security, volatile network topologies, power-constrained operations, intrinsic requirement of mutual trust among all nodes in underlying protocol design and lack of centralized monitoring and management point. There are recent research efforts in providing various prevention schemes to secure the ad-hoc routing protocol, i.e., authentication and encryption schemes. However, the history of security research on the wired environments has taught us that we still need to deploy defense-in-depth or layered security mechanisms because security is a process that is as secure as its weakest link.

There are two major analytical techniques in intrusion detection, namely misuse detection and anomaly detection. Misuse detection uses the "signatures" of known attacks, and anomaly detection uses established normal profiles only to identify any unreasonable deviation from them as the result of some attack. Since MANET is still under heavy development and not many MANET-specific attacks have emerged, we believe that anomaly detection is the preferred technique in the current stage [1].

In this paper, we propose a new anomaly detection method for MANETs. The proposed method detects effectively anomalies through cross-feature analysis on the basis of Rough sets. Our method uses percentage of change in number of hops, percentage of significant traffic change and percentage of route change as the feature value. When an intrusion occurs, the attacker masquerading the legitimate user trends to have a different used pattern. Therefore, we can detect anomaly by comparing the used patterns.

The rest of this paper is organized as follows. Section 2 gives a brief description of related works for intrusion detection techniques in mobile ad hoc networks. Section 3 describes rough sets. Section 4 presents the anomaly detection method on the basis of cross-feature analysis using rough sets. Section 5 presents the simulation study of our proposed method. In Section 6, we conclude this paper and point out future work.

2. Related Works

The number of intrusions into computer system is growing because new automated intrusion tools are appearing every day. The research in securing wireless MANETs has attracted increasing attentions recently, but it is still in its early stage. A few papers have suggested using intrusion detection to enhance the security of MANETs.

Y. Zhang et al [2, 3] proposed new model for intrusion detection system (IDS) and response in mobile ad hoc wireless networks. Each IDS agent runs independently and monitors local activities. It detects intrusion from local traces and initiates response. If anomaly is detected in the local data, or if the evidence is inconclusive and a broader search is warranted, neighboring IDS agents will cooperatively participate in global intrusion detection actions. O. Kachirski and R. Guha [4] proposed multi-sensor intrusion detection system employing cooperative detection algorithm. By efficiently merging audit data from packet level, user level and system level sensors, the entire ad hoc wireless network for intrusion is analyzed. Y. Huang et al [1] presented an anomaly detection approach using cross-feature analysis. They observed that a strong inter-feature correlation exists in normal network traffic and demonstrated that the approach of cross-feature analysis is very efficient to capture this between-feature relationship, thus a good anomaly detection performance has been obtained. In [5], Y. Huang and W. Lee extended the previous idea and further built a rule-based intrusion identification mechanism. They addressed the resource constraints of mobile nodes and investigated the possibility of using cooperative detection to reduce the energy consumption. H. Deng et al [6] proposed a two-step intrusion detection procedure that had been developed to effectively detect anomalies and identify attack types using distributed intrusion detection agents. In the first step, an unsupervised anomaly detection model, learned only from normal network behavior, is applied to detect anomalies. In the second step, the intrusions are classified based on their behavior pattern. I-H Bae [8] proposed the anomaly detection scheme for mobile networks. Bae's scheme uses the trace data of wireless application layer by a user as feature value. Based on this, the user pattern of a mobile's user can be captured by rough sets, and the abnormal behavior of the mobile can be also detected by applying a roughness membership function considering weighted feature values.

3. Rough Sets

The rough set is the approximation of a vague concept by a pair of precise concept, called lower and upper approximation, which are classification of domain of interest into disjoint categories. The rough set approach to processing of incomplete data is based on these approximations [7].

Let U be a finite set of objects called Universe, and R⊆U×U be an equivalence relation on U. The pair A=(U, R) is called approximation space, and equivalence classes of the relation R are called elementary sets in A.

For x∈U, let $[x]_R$ denote the equivalence class of R, containing x. For each X∈U, X is characterized in A by a pair of sets - its lower and upper approximation in A, defined as:

$$\underline{A}X = \{x \in U \mid [x]_R \subseteq X\},$$
$$\overline{A}X = \{x \in U \mid [x]_R \cap X \neq \emptyset\}.$$

The objects in $\underline{A}X$ can be with certainty classified as members of X on the basis of knowledge in R, while the objects in $\overline{A}X$ can be only classified as possible members of X on the basis of knowledge in R. The set $BN_A X = \overline{A}X - \underline{A}X$ is called the A-boundary region of X, and thus consists of those objects that we cannot decisively classify into X on the basis of knowledge in A.

Rough set can be also characterized numerically by the following coefficient called the accuracy of approximation, where *Card* denotes the cardinality.

$$\alpha_A(X) = \frac{Card\ \underline{A}X}{Card\ \overline{A}X}.$$

Obviously $0 \leq \alpha_A(X) \leq 1$. If $\alpha_A(X) = 1$, X is crisp with respect to A, and otherwise, if $\alpha_A(X) < 1$, X is rough with respect to A.

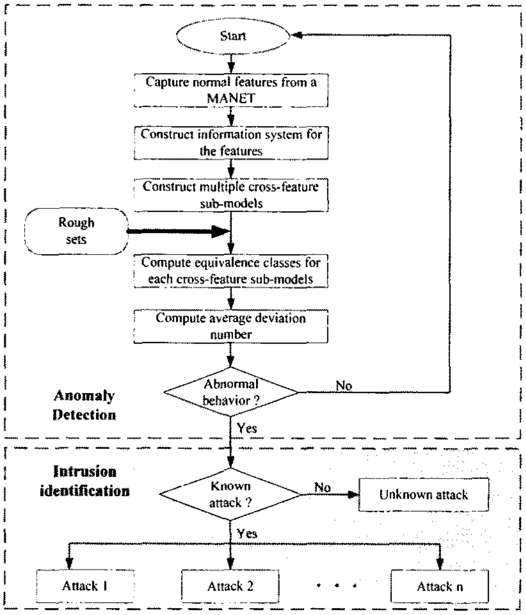
Of course some other measures can also be defined in order to express the degree of exactness of the set X. It is possible to use a variety of $\alpha_A(X)$ defined as:

$$\rho_A(X) = 1 - \alpha_A(X),$$

and referred to as a A-roughness of X. Roughness as opposed to accuracy represents the degree of incompleteness to knowledge A about the set X.

4. Anomaly Detection Method based on Cross-Feature Analysis

In this section, we propose an anomaly detection method based on cross-feature analysis using rough sets. The whole structure of the proposed method is illustrated in Figure 1.


Start
Capture normal features from a MANET
Construct information system for the features
Construct multiple cross-feature sub-models
Rough sets
Compute equivalence classes for each cross-feature sub-models
Compute average deviation number
Abnormal behavior ?
No
Yes
Anomaly Detection
Intrusion identification
Known attack ?
No
Unknown attack
Yes
Attack 1
Attack 2
. . .
Attack n

(Figure 1) The whole structure of the proposed anomaly detection method.

In the first step, the anomaly detection method captures the features of the normal behaviors from a MANET, and constructs an information system from the normal features. The decision to pick up features relay on several factors. It should reflect information from traffic, non-traffic and other sources. Accordingly, our method captures information from traffic pattern, from routing change, and from topological movement in a normal MANET, and an information system is constructed by the feature information. We construct multiple sub-models with respect to each feature, and compute the equivalence classes from each sub-model using rough sets. When a network behavior occurs, based on both the network behavior information and the equivalence class information of sub-models, the deviation number for each sub-model is computed by a roughness membership function, where the deviation number represents the degree that the network behavior is deviated from the normal behavior. We then compute the average deviation number from the deviation numbers of sub-models. If the deviation number is greater than the deviation threshold that is a system parameter, the feature set will be labeled as an UNKNOWN type and go through second step - intrusion identification, otherwise the network activity identified as normal.

To identify each known attack type and recognize the unknown attacks, several identification models are applied, and each of them corresponds to an individual attack type. After the second step, all the identified anomalies are relabeled with the corresponding attack type, and all the unidentified anomalies remain to be of an UNKNOWN type of further investigation.

The main purpose of the two-step intrusion detection method is to detect various attacks (known/unknown) and separate them from normal network behavior, such that the security response can be conducted whenever an attack occurs.

In this paper, we construct the information system for features that reflects traffic pattern, route change and topology movement from normal behaviors of a MANET. Table 1 shows the constructed information system for normal features, where PSTC (Percentage of Significant Traffic Change) and PRC (Percentage of Route Change) as the feature of traffic pattern, and PCH (Percentage of Change in number of Hops) as the feature of route change are chosen, respectively.

Suppose for a given node, at time t1, there are N1 routing entries, the routing entry set is S1, the amount of traffic of all routing entries is T1, and the sum of hops of all routing entries is H1; at time t2, there are N2 routing entries, the routing entry set is S2, the amount of traffic of all routing entries is T2, and the sum of hops of all routing entries is H2. We define PRC, PSTC and PCH as following:

- PRC: PRC is calculated as (|S2-S1|+|S1-S2|)/|S1|. |S| indicates the number of elements in S. (S2-S1) means the newly increased routing entries during the time interval (t2-t1), and (S1-S2) means the deleted routing entries during (t2-t1). They together represent the changes of resulting entries in (t2-t1).
- PSTC: PSTC is calculated as (T2-T1)/T1. (T2-T1) indicates the changes of the amount of traffic of all routing entries during the time interval (t2-t1).
- PCH: PCH is calculated as (H2-H1)/H1. (H2-H1) indicates the changes of the sum of hops of all routing entries during the time interval (t2-t1).

(Table 1) The information system of normal features for a MANET (Cross-Feature sub-model for PRC)

U	PCH	PSTC	PRC
1	a	a	a
2	b	c	c
3	c	a	d
4	a	c	d
5	a	a	a
6	c	a	b
7	a	c	c
8	b	c	c

Table 1 is the cross-feature sub-model for PRC because attribute PRC is decision attribute, where U is set of object, PCH, PSTC are set of condition attribute, PRC is set of decision attribute (have only one decision attribute), and *n* symbols (a, b, c, d) are used *n* classes to represent the attribute (PCH, PSTC, PRC) values in n ranges. From Table 1, we have the following four equivalence classes, called decision classes.

DE1={1, 5},
DE2={6},
DE3={2, 7, 8},
DE4={3, 4}.

For the conditional attributes (PCH, PSTC), we have the following four equivalence classes, called condition classes.

CE1={1, 5},
CE2={2, 8},
CE3={3, 6},
CE4={4, 7}.

Comparing condition and decision classes, we get the following inclusions.

CE1⊆DE1,
CE2⊆DE3.

(Table 2) The cross-feature sub-models from the information system of normal features

(a) The cross-feature sub-model for PCH

U	PSTC	PRC	PCH
1	a	a	a
2	c	c	b
3	a	d	c
4	c	d	a
5	a	a	a
6	a	b	c
7	c	c	a
8	c	c	b

(b) The cross-feature sub-model for PSTC

U	PRC	PCH	PSTC
1	a	a	a
2	c	b	c
3	d	c	a
4	d	a	c
5	a	a	a
6	b	c	a
7	c	a	c
8	c	b	c

Table 2(a) is the cross-feature sub-model for PCH because attribute PCH is decision attribute. From Table 2(a), we have the following three decision classes.

DE1={1, 4, 5, 7},
DE2={2, 8},
DE3={3, 6}.

For the conditional attributes (PSTC, PRC), we have the following five condition classes.

CE1={1, 5},
CE2={2, 7, 8},
CE3={3},
CE4={4},
CE5={6}.

Comparing condition and decision classes, we get the following inclusions.

CE1⊆DE1,
CE3⊆DE3,
CE4⊆DE1,
CE5⊆DE3.

Table 2(b) is the cross-feature sub-model for PSTC because attribute PSTC is decision attribute. From Table 2(b), we have the following two decision classes.

DE1={1, 3, 5, 6},
DE2={2, 4, 7, 8}.

For the conditional attributes (PRC, PCH), we have the following six condition classes.

CE1={1, 5},
CE2={2, 8},
CE3={3},
CE4={4},
CE5={6},
DE6={7}

Comparing condition and decision classes, we get the following inclusions.

CE1⊆DE1,
CE2⊆DE2,
CE3⊆DE1,
CE4⊆DE2,
CE5⊆DE1,
CE6⊆DE2.

The relation between two classes those are not inclusion relation can be represented by a fuzzy inclusion. The fuzzy inclusion is represented by the inequalities of membership functions. Further, we will allow certain errors as long as they are within the radius ε of tolerance. The fuzzy inclusion is computed by equation (1), roughness membership function.

$$\mu_{sub\text{-}model}(X,Y)=1-\frac{Card\,(\overline{R}X\cap\overline{R}Y)}{Card\,(\overline{R}X\cup\overline{R}Y)}\quad(1),$$

where X and Y represent condition attribute and decision attribute, respectively.

When a network activity (c, a, a) for (PCH, PSTC, PRC) occurs, X={c, a}=CE3 and Y={c}=DE1 are not inclusion relations in cross-feature sub-model for PRC. $\overline{R}X=\{1,3,5,6\}$, $\overline{R}Y=\{1,5\}$. The (X, Y)-roughness of the cross-feature sub-model for PRC is computed by equations (1). $\mu_{prc}(X,Y)=1-(2/4)=0.5$, CE3 and DE1 are in 0.5-fuzzy inclusion.

For the network activity (a, a, c) in the cross-feature sub-model for PCH, X={a, a}=CE1 and Y={c}=DE3 are not inclusion relations. $\overline{R}X=\{1,3,5,6\}$, $\overline{R}Y=\{3,6\}$. Accordingly, the (X, Y)-roughness of the cross-feature sub-model for PCH is computed by equations (1). $\mu_{pch}(X,Y)=1-(2/4)=0.5$, CE1 and DE3 are in 0.5-fuzzy inclusion.

For the network activity (c, a, a) in the cross-feature sub-model for PSTC, X={c, a}=CE6 and Y={a}=DE1 are not inclusion relations.

$\overline{R}X = \{1, 3, 5, 6\}$, $\overline{R}Y = \{1, 3, 5, 6\}$. Accordingly, the (X, Y)-roughness of the cross-feature sub-model for PSTC is computed by equations (1). $\mu_{pstc}(X, Y) = 1 - (4/4) = 0.0$, CE6 and DE1 are in 0.0-fuzzy inclusion. The roughness value from equation (1) is depended on decision attribute (Y), considerably. Accordingly, we compute the average roughness value from the roughness values of sub-models to get more correct roughness value. The average (X, Y)-roughness of the network activity (c, a, a) for (PCH, PSTC, PRC) is computed by equation (2).

$$\mu_{ave}(X, Y) = ave(\mu_{prc}(X, Y), \mu_{pch}(X, Y), \mu_{pstc}(X, Y)) \quad (2),$$

where *ave*() is the average function returns the average value of input parameter values. Finally,

$$\mu_{ave}(X, Y) = ave(0.5, 0.5, 0.0) \approx 0.33.$$

If the deviation threshold (ε) is 0.4, the network activity is identified as normal because $\mu_{ave}(X, Y) \leq \varepsilon$. While, we assume that ε is 0.3. The network activity is identified as abnormal because $\mu_{ave}(X, Y) > \epsilon$, go to intrusion identification step.

5. Performance Evaluation

We use the following two metrics to evaluate the performance of our proposed anomaly detection scheme:

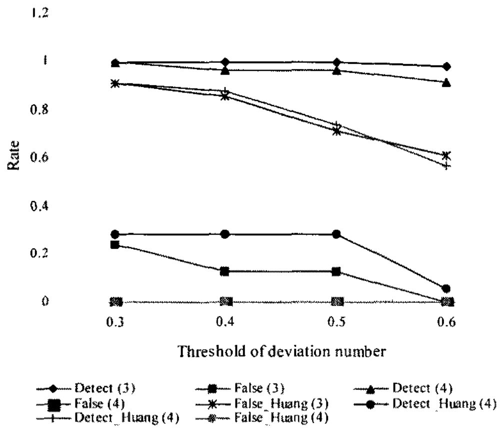
- Detection Rate: It is measured over abnormal itineraries. Suppose *m* abnormal itineraries are measured, and *n* of them are detected, detection rate is defined as *n/m*.
- False Alarm Rate: It is measured over normal itineraries. Suppose *m* normal itineraries are measured, and *n* of them are identified as abnormal, false alarm rate is defined as *n/m*.

We present and analyze the simulation results at different deviation threshold. The simulation program is developed with Visual C++ 6.0 on the Intel Pentium 4. In the simulation, we define the number of feature data that two features among three features match with the features of the information system, is called *similarity number*. If the similarity number of the network activity is larger than the input value, the network activity is defined as normal behavior. Otherwise, the network activity is anomalous. Table 3 shows the parameter and values for the simulation.

(Table 3) Parameters for anomaly detection simulation

Parameters	Values
The number of network activities	*300*
Similarity number	*3, 4*
The type of PCH values	*random(1, 3)*
The type of PSTC values	*random(1, 3)*
The type of PRC values	*random(1, 4)*

Simulation results of the detection rate and the false alarm rate over deviation threshold are illustrated in Figure 2. The performance of the proposed method is compared with the performance of Huang method [1] that uses cross-feature analysis based on the probability of feature attribute value. As a result, we identify that the performance of the proposed method is superior to the performance of Huang method as a whole. In Huang method, the determination of the probability for feature attribute values is very difficult because that the deviation number of an event depends on the probability, highly. Additionally, we know that the proposed method detects effectively abnormal behaviors of network activities. When the similarity number is 3, the best performance is got in the case that the deviation threshold is 0.6, and when the similarity number is 4, the best performance is got in the case that the deviation threshold to 0.3. Also, we find out that false detections those actual normal network activities are estimated as abnormal network activities by our method are occurred in the case that the similarity number is 3 and the deviation threshold is 0.5, and detection misses those actual abnormal network activities are estimated as normal network activities by our method are occurred in the case that the similarity number is 3 and the deviation threshold is 0.6. Table 4 reports on numerical data for the performance of the proposed method over deviation thresholds.



(Figure 2) Detection rate and false rate at different deviation threshold.

(Table 4) Numerical data for the performance of the proposed method over deviation thresholds.

Deviation threshold	Similarity number			
	3		4	
	Detection rate	False alarm rate	Detection rate	False alarm rate
0.3	1.0	0.246	1.0	0.0
0.4	1.0	0.13	0.968	0.0
0.5	1.0	0.13	0.968	0.0
0.6	0.983	0.0	0.915	0.0

6. Conclusions

In this paper, we propose an anomaly detection method based on cross-feature analysis using rough sets. The proposed method captures information from traffic pattern, from routing change, and from topological movement in a normal MANET, and an information system is constructed by the feature information. We construct multiple sub-models with respect to each feature, and compute the equivalence classes from each sub-model using rough sets. When a network behavior occurs, based on both the network behavior information and the equivalence class information of sub-models, the deviation number for each sub-model is computed by a roughness membership function. We then compute the average deviation number from the deviation numbers of sub-models. If the deviation number is greater than the deviation threshold that is a system parameter, the feature set will be labeled as an UNKNOWN type and go through second step - intrusion identification, otherwise the network activity identified as normal. The performance of the proposed anomaly detection method is evaluated through a simulation. From the results, we identify that the performance of the proposed method is superior to the performance of Huang method that uses cross-feature analysis based on the probability of feature attribute value, and we know that the proposed anomaly detection method detects well abnormal behaviors of network activities.

Future works include development of a new roughness membership function that reflects precise deviation number of network activities in MANETs, applying aging to the information system of normal features for network activities, and development of the proposed anomaly detection method for a MANET.

7. References

[1] Yi-an Huang et al., "Cross-Feature Analysis for Detecting Ad-Hoc Routing Anomalies", Proceedings of the 23rd International Conference on Distributed Computing Systems, May 2003.

[2] Y. Zhang, W. Lee, Y-A. Huang, "Intrusion Detection Techniques for Mobile Wireless Networks", *ACM/Kluwer Mobile Networks and Applications*, Vol. 9, No. 3 pp.545-556, 2002.

[3] Y. Zhang, W. Lee, "Intrusion Detection in Wireless Ad-Hoc Networks", MobiCom'2000, 275-283, 2000.

[4] O. Kachirski, R. Guha, "Effective Intrusion Detection Using Multiple Sensors In Wireless Ad Hoc Networks," HICSS'03, 2003

[5] Y. Huang and W. Lee, "A cooperative intrusion detection system for ad hoc networks", In Proc. of the 1stACM workshop on Security of ad hoc and sensor networks, pp. 135-147, 2003.

[6] Hongmei Deng, et al., "Agent-based Distributed Intrusion Detection Methodology for MANETs", Proceedings of the 2006 International Conference on Security &Management, pp. 200-206, 2006.

[7] Z. Pawlak, Rough Sets Theoretical Aspects of Reasoning about Data, Kluwer Academic Pub., 1991.

[8] Ihn-Han Bae et al., "Design and Evaluation of a Rough Set-Based Anomaly Detection Scheme Considering Weighted Feature Values", International Journal of Knowledge-based and Intelligence Engineering Systems, Vol. 11, No.4, pp.201-206, 2007.

◐ 저 자 소 개 ◑

배 인 한(Ihn-Han Bae)

1984년 경남대학교 전자계산학과 졸업(학사)
1986년 중앙대학교 대학원 전자계산학과 졸업(석사)
1990년 중앙대학교 대학원 전자계산학과 졸업(박사)
1996년~1997년: CIS, The Ohio State University(Postdoc)
2002년~2003년: CS, Old Dominion University(Visiting Scholar)
1989~현재 대구가톨릭대학교 컴퓨터정보통신공학부 교수
관심분야 : 모바일 컴퓨팅, 유비쿼터스 멀티미디어, 웹 2.0, etc.
E-mail : ihbae@cu.ac.kr

이 화 주(Hwa-Ju Lee)

2000년 위덕대학교 컴퓨터공학과 졸업(학사)
2004년 대구가톨릭대학교 교육대학원 전자계산교육전공 졸업(석사)
2005~현재 대구가톨릭대학교 컴퓨터정보통신공학부 박사과정
관심분야 : 모바일 컴퓨팅, 모바일 멀티미디어, etc.
E-mail : hj2380@hanmail.net