博士学位論文

Doctoral Thesis

内容の要旨
及び
審査結果の要旨

Thesis Abstracts
and
Summaries of the Thesis Review Results

第18号

The Eighteenth Issue

平成23年9月

September, 2011

The University of Aizu

はしがき

博士の学位を授与したので、学位規則（昭和28年4月1日文部省令第9号）第8条の規定に基づき、その論文の内容の要旨及び論文審査の結果の要旨をここに公表する。

学位記番号に付した「甲」は学位規則第4条第1項（いわゆる課程博士）によるものであることを示す。

Preface

On granting the Doctoral Degree to the individuals mentioned below, abstracts of their theses and the theses review results are herewith publicly announced, in according to the provisions provided for in Article 8 of the Ruling of Degrees (Ministry Of Education Ordinance No.9, enacted on April 1, 1953)

The Chinese character, “甲”, at the beginning of the diploma number represents that an individual has been granted the degree in accordance with the provisions provided for in Paragraph 4-1 of the Ruling Of Degrees (what in called “Katei Hakase,” or the Doctoral Degree granted by the University at which the grantee was enrolled.)

目　次

Contents

4	甲CI博第22号	博士（コンピュータ理工学）	季　節 季　节	Fast Document Analysis Algorithms Based on the Comparative Advantage Theory 比較優位理論に基づく高速文章解析アルゴリズム	9
5	甲CI博第23号	博士（コンピュータ理工学）	沈　安妮 沈　安妮	Lightweight Secure and Privacy-Preserving Protocols in Wireless Network ワイヤレスネットワークにおける軽量かつ安全なプライバシー保護プロトコル	11

Name 氏名	Dmitry Aleksandrovich Vazhenin ディミトリー アレクサンドロビッチ ヴァジェニン
The relevant degree 学位の種類	Doctoral degree (in Computer Science and Engineering) 博士(コンピュータ理工学)
Number of the diploma of the Doctoral Degree 学位記番号	甲 CI 博第 19 号
The Date of Conferment 学位授与日	September 30, 2011 平成 23 年 9 月 30 日
Requirements for Degree Conferment 学位授与の要件	Please refer to the article five of “University Regulation on University Degrees” 会津大学学位規程　第5条該当
Thesis Title 論文題目	Visual language and environment for specification of computational expressions 計算式を明示するための可視化言語環境の研究
Thesis Review Committee Members 論文審査委員	University of Aizu, Prof. Nikolay Mirenkov (Chief Referee) Former University of Aizu Prof. Minetada Osano University of Aizu, Prof. Shigaku Tei University of Aizu, Associate Prof. Vitary Klyuev 会津大学教授　ニコライ ミレンコフ（主査） 前会津大学教授　小佐野　峰忠 会津大学教授　程　子学 会津大学上級准教授　ヴィタリー　クリュエフ

Abstract

This work is a part of the filmification of methods technology research and development, which is based on the visual algorithm representation using an algorithmic CyberFilm concept. Accordingly, each frame of this film/movie should visualize/animate a corresponding step of a program/algorithm execution. Within this technology, to specify a film-based algorithm it is necessary to define space structures and traversal schemes for visiting nodes of those structures. In this dissertation, the main features of the filmification paradigm are also shown, however the focus is on the multiple-view of the algorithmic film components and the extension of a set of these components, on the automatic creation of template programs and the introduction of special data structures, as well as on formula representations and executable code generation.

A special multimedia formula language with high-level constructions and operators is developed in order to make the programming process more efficient and comfortable. This language allows the specification of formulas based on distinguishing the control-flow formulas and computational formulas, their syntax and semantics. Another important feature of the proposed language is multimedia representations of the arithmetical and logical expressions including enhanced text-based terms, tables, images and stencils. This language is supported by a special environment with GUI components for the structure definition and variable declaration, control-flow formulas specification and computational formulas attachment involved. Four stages in the movie-based program design are proposed: 1) creating the algorithmic movie; 2) attaching computational formulas with design-time debugging; 3) generating and running the executable code of movie-based program on a target machine with run-time debugging and 4) exporting algorithmic films to the algorithmic film library. An important feature of the proposed debugging process is that debugging operations can be implemented at any stage of the movie/program design. Examples of movie-based algorithms and their practical testing, as well as results of corresponding numerical experiments are discussed.

Name 氏名	袁　世忠（袁　世忠） Yuan Shizong
The relevant degree 学位の種類	Doctoral degree (in Computer Science and Engineering) 博士（コンピュータ理工学）
Number of the diploma of the Doctoral Degree 学位記番号	甲 CI 博第 20 号
The Date of Conferment 学位授与日	September 30, 2011 平成 23 年 9 月 30 日
Requirements for Degree Conferment 学位授与の要件	Please refer to the article five of “University Regulation on University Degrees” 会津大学学位規程　第5条該当
Thesis Title 論文題目	Web-based information sharing for electrocardiograms ウェブにおける心電図の情報共有化に関する研究
Thesis Review Committee Members 論文審査委員	University of Aizu, Associate Prof. Wenxi Chen (Chief Referee) University of Aizu, Associate Prof. Incheon Paik University of Aizu, Associate Prof. Alexander Vazhenin Former University of Aizu Prof. Daming Wei Shanghai University,　Prof. Xu Weiming 会津大学上級准教授　陳　文西（主査） 会津大学上級准教授　白　寅天 会津大学上級准教授　アレキサンダー　ヴァジェニン 前会津大学教授　魏　大名 上海大学教授　Xu Weiming

Abstract

Owing to the lack of ease of access to ECG data located in geographically distributed hospitals, medical practice using serial electrocardiogram (ECG) analysis has not so far been extensively used. Motivated to address this problem, we develop an architecture for cross-hospital access to ECG data. This architecture is aimed at enabling the discovery and retrieval of a particular patient’s ECGs distributed across a number of ECG data sources through a common Web portal.

The architecture adopts a metadata-based approach to facilitate the discovery and retrieval of a particular patient’s ECG data across multiple disparate ECG data sources. We present a metadata model for ECG data discovery and retrieval, and the ECG registry that provides ebXML-based Web services for publishing and discovering ECG data using the metadata model.

The architecture also proposes a framework for publishing the ECG data with the ECG registry from an ECG data source. In order to achieve interoperability with disparate ECG data sources, the framework introduces the concept of Generic ECG Source Layer (GESL), which is the Web-services-based interface to an ECG data source to hide data-source-specific characteristics in data access mechanisms and provide adequate access capability for ECG data query and retrieval. Moreover, the framework has an access control mechanism based on XACML and SAML to address the privacy and security issues related to the access to an ECG source. The access control mechanism can protect ECG data in an ECG data source from disclosure to both the individuals who have no job-related need to access them and those who have been denied the privilege to access them by a patient’s privacy consent.

The architecture is evaluated through the implementation of an experimental scenario. It is shown that the architecture provides an effective and efficient registry-based approach to support access to disparate ECG data sources.

Then we make a further study on federated search and retrieval of a particular patient’s ECG data in the context of multiple ECG registries. We present an efficient federated search model that treats the common patient identity service as a central index to direct a user query to a set of candidate ECG registries.

Our study demonstrates a significant effort to improve ease of cross-hospital access to ECG data.

Name 氏名	Lu Weija 陸　唯佳（陆　唯佳）
The relevant degree 学位の種類	Doctoral degree (in Computer Science and Engineering) 博士(コンピュータ理工学)
Number of the diploma of the Doctoral Degree 学位記番号	甲 CI 博第 21 号
The Date of Conferment 学位授与日	September 30, 2011 平成 23 年 9 月 30 日
Requirements for Degree Conferment 学位授与の要件	Please refer to the article five of “University Regulation on University Degrees” 会津大学学位規程　第5条該当
Thesis Title 論文題目	Studies on Atrial Fibrillation - Algorithms for epicardial mapping and computer modeling 心房細動に関する研究:心外膜マッピングのためのアルゴリズム開発と心臓のコンピュータモデリング
Thesis Review Committee Members 論文審査委員	University of Aizu, Associate Prof. Wenxi Chen (Chief Referee) University of Aizu, Prof. Qiangfu Zhao University of Aizu, Assistant Prof. Xin Zhu Former University of Aizu Prof. Daming Wei Fudan University, Prof. Fang Zuxiang 会津大学上級准教授　陳　文西（主査） 会津大学教授　趙　強福 会津大学准教授　朱　欣 前会津大学教授　魏　大名 復旦大学教授　Prof. Fang Zuxiang

Abstract

Atrial Fibrillation (AF), a common and complicated superventricular tachyarrhythmia, is becoming prevalent and its complications such as stroke may cause a substantial mortality. Feasible drug and non-drug therapies can effectively ameliorate the prognosis of AF, but neither interventional nor surgical therapies are satisfatorily effective to cure AF, because of the depolaziation activies of the atria during AF are chaotic. Therefore it is important to understand the mechanism of AF's trigger and substance from clinical and theoretical points of view by medical professionals and engineers.

In this dissertation, two of our contributions to the study of AF are presented. The first issue is relative to a clinical respect of AF, that is presenting a novel interpolation method to epicardial potential mapping technique for measurement of atrial fibrillation. This method is based on the alignment of the activation time of local myocardium. Through evaluating with the data of animal experiments, our method got a precision 6% higher than the traditional B-spline interpolation method. The second issue is relative to a theoretical aspect of AF study, that is presenting a computer model for simulations of AF. This model is based on the anatomic data from BodyParts3D database (http://lifesciencedb.jp/bp3d/) developed by Research Organization of Information and Systems, Japan National Institute of Genetics.

In the animal experiment, reloaded the new interpolation method, we successfully observe an onset of AF lasting for 25 m and 40 s by delivering electrical stimulation in the vagal ganglia and measured the corresponding epicardial electrograms. The animal experimental results are in accordance with Scherlag et al.'s study, i.e., one or more foci are generated at the beginning of AF, and finally AF changes to the reentry-maintained one. According to the literature retrieving, the electrophysiological remodeling might acts as the substance of the triggering and mantaining of the macro-reentry, but the relationship between them is remained to be testified.

Therefore, we conducted the computer simulation by setting two boost trains of pacing at the opening of the pulmonary vein and the inferior vena cava, thus obtained a foci-triggered AF, one was first driven by foci and changed to the reentry maintained. The simulation result conforms to those of our animal experiments and proves the relationship between electrophysiological remodeling and macro-reentry

Name 氏名	Ji Jie 季　節　（季　节）
The relevant degree 学位の種類	Doctoral degree (in Computer Science and Engineering) 博士（コンピュータ理工学）
Number of the diploma of the Doctoral Degree 学位記番号	甲 CI 博第 22 号
The Date of Conferment 学位授与日	September 30, 2011 平成 23 年 9 月 30 日
Requirements for Degree Conferment 学位授与の要件	Please refer to the article five of “University Regulation on University Degrees” 会津大学学位規程　第5条該当
Thesis Title 論文題目	Fast Document Analysis Algorithms Based on the Comparative Advantage Theory 比較優位理論に基づく高速文章解析アルゴリズム
Thesis Review Committee Members 論文審査委員	University of Aizu, Prof. Qiangfu Zhao (Chief Referee) University of Aizu, Prof. Sugiyama Hosei University, Prof. Ma Jianhua University of Aizu, Associate Prof. Incheon Paik University of Aizu, Associate Prof. Yong Liu 会津大学教授　趙　強福（主査） 会津大学教授　杉山　雅英 法政大学教授　馬　建華 会津大学上級准教授　白　寅天 会津大学上級准教授　劉　勇

Abstract

Nowadays, more and more electronic documents are available on the internet. To deal with such large amount of information, it is natural to classify them into several categories. However, most online documents are unlabeled. Many existing learning algorithms could not be applied directly. Semi-supervised learning is proposed to solve this problem. The method is a combination of unsupervised learning algorithm and supervised learning algorithm. A semi-supervised learning system could start from an unlabeled document set, and learn user's intention step by step.

In this thesis, several learning methods and algorithms are proposed for semi-supervised learning. The most important feature of these proposed algorithms is fast. Since each method has its own relative merits, the key point is to find a balance from them. Experimental results show that the performance of these proposed algorithms are better than existing classic learning algorithms.

I also developed a system which could help user to organize these algorithms. Based on fast learning algorithm, user could analysis document set effectively and efficiently. This is a long term research of our laboratory and is names as "The Cyber- Eye System". Although the system has not been completed yet, necessary components and concepts in the Cyber-Eye system are described. This thesis includes the structure, flow chart, learning algorithms, visualization algorithms and graphic interface of the Cyber-Eye system.

Name 氏名	Shen An-Ni 沈　安妮（沈　安妮）
The relevant degree 学位の種類	Doctoral degree (in Computer Science and Engineering) 博士(コンピュータ理工学)
Number of the diploma of the Doctoral Degree 学位記番号	甲 CI 博第 23 号
The Date of Conferment 学位授与日	September 30, 2011 平成 23 年 9 月 30 日
Requirements for Degree Conferment 学位授与の要件	Please refer to the article five of “University Regulation on University Degrees” 会津大学学位規程　第5条該当
Thesis Title 論文題目	Lightweight Secure and Privacy-Preserving Protocols in Wireless Network ワイヤレスネットワークにおける軽量かつ安全なプライバシー保護プロトコル
Thesis Review Committee Members 論文審査委員	University of Aizu, Associate Prof. Song Guo (Chief Referee) University of Aizu, Prof. Shigaku Tei University of Aizu, Prof. Hirokuni Kurokawa University of Aizu, Prof. Anh T. Pham 会津大学上級准教授 ソン グオ （主査） 会津大学教授　程　子学 会津大学教授　黒川　弘国 会津大学教授　アン　T.　ファム

Abstract

Recently, the micro-electro-mechanical system (MEMS) has applied to a variety applications. And the wireless sensor networks (WSNs) relies on it to work. The WSNs adopt MEMS technology and do not rely on any pre-deployed network architecture. It thus communicates via a self-organization protocol to autonomously aggregate into collaborative, peer-to-peer networks. A wireless sensor networks is composed of a large number of low-cost sensor nodes; each sensor node with limited battery power, limited memory storage, limited data processing capacity and limited short radio transmission range. Now WSNs can be operated to variety application, such as disaster response, factory monitoring, medicine and health care and intelligent house control in civil scenarios. To deploy a WSN, the sensitive data must be protected properly. Therefore, the key management scheme for WSNs is very important.

However, due to the limited resources of sensors, conventional asymmetric key cryptosystem cannot be applied in WSNs. And sensors nodes often are deployed in unattached area; the adversary may be able to easily capture the sensor devices to compromise their stored sensitive data and communication keys. To establish security channel between sensor nodes, many related key management schemes for WSNs have been proposed, but these schemes are either inefficient, insecure or unable to provide full connectivity.

In real applications, new network devices need to be added into an already deployed network from time to time in order to replace the power-exhausted or compromised devices such that the performance of the whole network would not significantly degrade. Moreover, using single pair-wise key between sensor devices in long term may easily incur the brute-force attack. Hence, rekeying issuance is also an important topic to design secure protocols for WSNs.

Many service applications of Vehicular Ad-hoc NETworks (VANETs) require privacy and secure data communications. For improvement driving safety and comfort, each driver will regular broadcast routine traffic-related status information. Without the security and privacy guarantee, attackers could tracking their interested vehicle by collection traffic message. Hence, anonymous message authentication is an essential requirement of VANETs. However, when a driver who is involved in a dispute event of safety message, the certificate authority should able to recover the real identity of vehicle.

To deal with the problem of security wireless networks, several schemes have been proposed in this thesis.

1. Key Agreement: Key agreement problem is fundamental requirement for secure WSNs. Hence, we first propose a key distribution method for establishment of secure key between sensor devices. Compare with other proposal, our method provides full connectivity of network and completely defends against the node capture attack. The simulation results show our scheme reduces the storage and communication overhead.

2. Addition of New Sensor Nodes: A well key management for WSNs needs to achieve robustness against the node capture attack and addition of new sensor devices for the renewable WSNs at same time. Hence, based on our key pre-distribution scheme, we develop a method to support key distribution for renewable WSNs. Performance and security analysis result our proposal is more efficient and secure compare with other existing schemes.

3. Rekeying Problem: When the WSNs run for a long time using a fixed key, it increases the probability for the adversaries to compromise the key by analyzing of adequate messages from eavesdrop or captured nodes. Thus, we propose two rekeying schemes to update the group key and pairwise key, respectively. Compared existing schemes, our rekeying method possesses the following features:(1)robustness to the node capture attack, (2)reactive rekeying capability to malicious nodes, and (3)low communication and storage overhead.

4. Anonymous authentication: To deal with the issue of privacy authentication secure protocol with condition authority traceability in VANET, we proposed a new secure scheme elliptic curve based chameleon hashing. Compare with existing schemes, our approach possesses the following features: (1)mutual and anonymous authentication, (2)unlinkability, (3)authority tracking and (4)efficiency. We demonstrate the merits through extensive analysis in terms of security and performance.

Keyword: Wireless sensor network, Vehicular Ad-hoc networks, Key management, Rekeying, Node addition, Conditional privacy, Chameleon hashing, Security

博士学位論文
Doctoral Thesis

内容の要旨
及び
審査結果の要旨
Thesis Abstracts
and
Summaries of the Thesis Review Results

第18号
The Eighteenth Issue

平成23年9月
September, 2011

発行 会津大学

〒965-8580 福島県会津若松市一箕町鶴賀
TEL: 0242-37-2600
FAX: 0242-37-2526
THE UNIVERSITY OF AIZU
Tsuruga, Ikki-machi Aizu-Wakamatsu City
Fukushima, 965-8580 Japan