http://www.icact.org/journal.asp

ICACT-TACT JOURNAL

Transactions on Advanced Communications Technology

Volume 8 Issue 4, July. 2019, ISSN: 2288-0003

Editor-in-Chief
Prof. Thomas Byeongnam YOON, PhD.

GIRI
Global IT Research Institute

Journal Editorial Board

■ Editor-in-Chief

■ Editors

Dr. Youssef SAID, Tunisie Telecom, Tunisia
Dr. Noor Zaman, King Faisal University, Al Ahsa Hofuf, Saudi Arabia
Dr. Srinivas Mantha, SASTRA University, Thanjavur, India
Dr. Shahriar Mohammadi, KNTU University, Iran
Prof. Beonsku An, Hongik University, korea
Dr. Guanbo Zheng, University of Houston, USA
Prof. Sangho Choe, The Catholic University of Korea, korea
Dr. Gyanendra Prasad Joshi, Yeungnam University, korea
Dr. Tae-Gyu Lee, Korea Institue of Industrial Technology(KITECH), korea
Prof. Ilkyeun Ra, University of Colorado Denver, USA
Dr. Yong Sun, Beijing University of Posts and Telecommunications, China
Dr. Yulei Wu, Chinese Academy of Sciences, China
Mr. Anup Thapa, Chosun University, korea
Dr. Vo Nguyen Quoc Bao, Posts and Telecommunications Institute of Technology, Vietnam
Dr. Harish Kumar, Bhagwant institute of technology, India
Dr. Jin REN, North china university of technology, China
Dr. Joseph Kandath, Electronics & Commn Engg, India
Dr. Mohamed M. A. Moustafa, Arab Information Union (AIU), Egypt
Dr. Mostafa Zaman Chowdhury, Kookmin University, Korea
Prof. Francis C.M. Lau, Hong Kong Polytechnic University, Hong Kong
Prof. Ju Bin Song, Kyung Hee University, korea
Prof. KyungHi Chang, Inha University, Korea
Prof. Sherif Welsen Shaker, Kuang-Chi Institute of Advanced Technology, China
Prof. Seung-Hoon Hwang, Dongguk University, Korea
Prof. Dal-Hwan Yoon, Semyung University, korea
Prof. Chongyang ZHANG, Shanghai Jiao Tong University, China
Dr. H K Lau, The Open University of Hong Kong, Honh Kong
Prof. Ying-Ren Chien, Department of Electrical Engineering, National Ilan University, Taiwan
Prof. Mai Yi-Ting, Hsiuping University of Science and Technology, Taiwan
Dr. Sang-Hwan Ryu, Korea Railroad Research Institute, Korea
Dr. Yung-Chien Shih, MediaTek Inc., Taiwan
Dr. Kuan Hoong Poo, Multimedia University, Malaysia
Dr. Michael Leung, CEng MIET SMIEEE, Hong Kong
Dr. Abu sahman Bin mohd Supa'at, Universiti Teknologi Malaysia, Malaysia
Prof. Amit Kumar Garg, Deenbandhu Chhotu Ram University of Science & Technology, India
Dr. Jens Myrup Pedersen, Aalborg University, Denmark
Dr. Augustine Ikechi Ukaegbu, KAIST, Korea
Dr. Jamshid Sangirov, KAIST, Korea
Prof. Ahmed Dooguy KORA, Ecole Sup. Multinationale des Telecommunications, Senegal
Dr. Se-Jin Oh, Korea Astronomy & Space Science Institute, Korea
Dr. Rajendra Prasad Mahajan, RGPV Bhopal, India
Dr. Woo-Jin Byun, ETRI, Korea
Dr. Mohammed M. Kadhum, School of Computing, Goodwin Hall, Queen's University , Canada
Prof. Seong Gon Choi, Chungbuk National University, Korea
Prof. Yao-Chung Chang, National Taitung University, Taiwan
Dr. Abdallah Handoura, Engineering school of Gabes - Tunisia, Tunisia
Dr. Gopal Chandra Manna, BSNL, India

Dr. Il Kwon Cho, National Information Society Agency, Korea
Prof. Jiann-Liang Chen, National Taiwan University of Science and Technology, Taiwan
Prof. Ruay-Shiung Chang, National Dong Hwa University, Taiwan
Dr. Vasaka Visoottiviseth, Mahidol University, Thailand
Prof. Dae-Ki Kang, Dongseo University, Korea
Dr. Yong-Sik Choi, Research Institute, IDLE co., ltd, Korea
Dr. Xuena Peng, Northeastern University, China
Dr. Ming-Shen Jian, National Formosa University, Taiwan
Dr. Soobin Lee, KAIST Institute for IT Convergence, Korea
Prof. Yongpan Liu, Tsinghua University, China
Prof. Chih-Lin HU, National Central University, Taiwan
Prof. Chen-Shie Ho, Oriental Institute of Technology, Taiwan
Dr. Hyoung-Jun Kim, ETRI, Korea
Prof. Bernard Cousin, IRISA/Universite de Rennes 1, France
Prof. Eun-young Lee, Dongduk Woman s University, Korea
Dr. Porkumaran K, NGP institute of technology India, India
Dr. Feng CHENG, Hasso Plattner Institute at University of Potsdam, Germany
Prof. El-Sayed M. El-Alfy, King Fahd University of Petroleum and Minerals, Saudi Arabia
Prof. Lin You, Hangzhou Dianzi Univ, China
Mr. Nicolai Kuntze, Fraunhofer Institute for Secure Information Technology, Germany
Dr. Min-Hong Yun, ETRI, Korea
Dr. Seong Joon Lee, Korea Electrotechnology Research Institute, korea
Dr. Kwihoon Kim, ETRI, Korea
Dr. Jin Woo HONG, Electronics and Telecommunications Research Inst., Korea
Dr. Heeseok Choi, KISTI(Korea Institute of Science and Technology Information), korea
Dr. Somkiat Kitjongthawonkul, Australian Catholic University, St Patrick's Campus, Australia
Dr. Dae Won Kim, ETRI, Korea
Dr. Ho-Jin CHOI, KAIST(Univ), Korea
Dr. Su-Cheng HAW, Multimedia University, Faculty of Information Technology, Malaysia
Dr. Myoung-Jin Kim, Soongsil University, Korea
Dr. Gyu Myoung Lee, Institut Mines-Telecom, Telecom SudParis, France
Dr. Dongkyun Kim, KISTI(Korea Institute of Science and Technology Information), Korea
Prof. Yoonhee Kim, Sookmyung Women s University, Korea
Prof. Li-Der Chou, National Central University, Taiwan
Prof. Young Woong Ko, Hallym University, Korea
Prof. Dimiter G. Velev, UNWE(University of National and World Economy), Bulgaria
Dr. Tadasuke Minagawa, Meiji University, Japan
Prof. Jun-Kyun Choi, KAIST (Univ.), Korea
Dr. Brownson ObaridoaObele, Hyundai Mobis Multimedia R&D Lab , Korea
Prof. Anisha Lal, VIT university, India
Dr. kyeong kang, University of technology sydney, faculty of engineering and IT , Australia
Prof. Chwen-Yea Lin, Tatung Institute of Commerce and Technology, Taiwan
Dr. Ting Peng, Chang'an University, China
Prof. ChaeSoo Kim, Donga University in Korea, Korea
Prof. kirankumar M. joshi, m.s.uni.of baroda, India
Dr. Chin-Feng Lin, National Taiwan Ocean University, Taiwan
Dr. Chang-shin Chung, TTA(Telecommunications Technology Association), Korea

Editor Guide

■ Introduction for Editor or Reviewer

All the editor group members are to be assigned as a evaluator(editor or reviewer) to submitted journal papers at the discretion of the Editor-in-Chief. It will be informed by eMail with a Member Login ID and Password.

Once logined the Website via the Member Login menu in left as a evaluator, you can find out the paper assigned to you. You can evaluate it there. All the results of the evaluation are supposed to be shown in the Author Homepage in the real time manner. You can also enter the Author Homepage assigned to you by the Paper ID and the author's eMail address shown in your Evaluation Webpage. In the Author Homepage, you can communicate each other efficiently under the peer review policy. Please don't miss it!

All the editor group members are supposed to be candidates of a part of the editorial board, depending on their contribution which comes from history of ICACT TACT as an active evaluator. Because the main contribution comes from sincere paper reviewing role.

■ Role of the Editor

The editor's primary responsibilities are to conduct the peer review process, and check the final camera-ready manuscripts for any technical, grammatical or typographical errors.

As a member of the editorial board of the publication, the editor is responsible for ensuring that the publication maintains the highest quality while adhering to the publication policies and procedures of the ICACT TACT(Transactions on the Advanced Communications Technology).

For each paper that the editor-in-chief gets assigned, the Secretariat of ICACT Journal will send the editor an eMail requesting the review process of the paper.

The editor is responsible to make a decision on an "accept", "reject", or "revision" to the Editor-in-Chief via the Evaluation Webpage that can be shown in the Author Homepage also.

■ Deadlines for Regular Review

Editor-in-Chief will assign a evalaution group(a Editor and 2 reviewers) in a week upon receiving a completed Journal paper submission. Evaluators are given 2 weeks to review the paper. Editors are given a week to submit a recommendation to the Editor-in-Chief via the evaluation Webpage, once all or enough of the reviews have come in. In revision case, authors have a maximum of a month to submit their revised manuscripts. The deadlines for the regular review process are as follows:

Evalution Procedure	Deadline
Selection of Evaluation Group	1 week
Review processing	2 weeks
Editor's recommendation	1 week
Final Decision Noticing	1 week

■ Making Decisions on Manuscript

Editor will make a decision on the disposition of the manuscript, based on remarks of the reviewers. The editor's recommendation must be well justified and explained in detail. In cases where the revision is requested, these should be clearly indicated and explained. The editor must then promptly convey this decision to the author. The author may contact the editor if instructions regarding amendments to the manuscript are unclear. All these actions could be done via the evaluation system in this Website. The guidelines of decisions for publication are as follows:

Decision	Description
Accept	An accept decision means that an editor is accepting the paper with no further modifications. The paper will not be seen again by the editor or by the reviewers.
Reject	The manuscript is not suitable for the ICACT TACT publication.
Revision	The paper is conditionally accepted with some requirements. A revision means that the paper should go back to the original reviewers for a second round of reviews. We strongly discourage editors from making a decision based on their own review of the manuscript if a revision had been previously required.

■ Role of the Reviewer

Reviewer Webpage:

Once logined the Member Login menu in left, you can find out papers assigned to you. You can also login the Author Homepage assigned to you with the paper ID and author's eMail address. In there you can communicate each other via a Communication Channel Box.

Quick Review Required:

You are given 2 weeks for the first round of review and 1 week for the second round of review. You must agree that time is so important for the rapidly changing IT technologies and applications trend. Please respect the deadline. Authors undoubtedly appreciate your quick review.

Anonymity:

Do not identify yourself or your organization within the review text.

Review:

Reviewer will perform the paper review based on the main criteria provided below. Please provide detailed public comments for each criterion, also available to the author.

- How this manuscript advances this field of research and/or contributes something new to the literature?
- Relevance of this manuscript to the readers of TACT?
- Is the manuscript technically sound?
- Is the paper clearly written and well organized?
- Are all figures and tables appropriately provided and are their resolution good quality?
- Does the introduction state the objectives of the manuscript encouraging the reader to read on?
- Are the references relevant and complete?

Supply missing references:

Please supply any information that you think will be useful to the author in revision for enhancing quality of the paperor for convincing him/her of the mistakes.

Review Comments:

If you find any already known results related to the manuscript, please give references to earlier papers which contain these or similar results. If the reasoning is incorrect or ambiguous, please indicate specifically where and why. If you would like to suggest that the paper be rewritten, give specific suggestions regarding which parts of the paper should be deleted, added or modified, and please indicate how.

Journal Procedure

Dear Author,

- **You can see all your paper information & progress.**

- **Step 1. Journal Full Paper Submission**

Using the Submit button, submit your journal paper through ICACT Website, then you will get new paper ID of your journal, and send your journal Paper ID to the Secretariat@icact.org for the review and editorial processing. Once you got your Journal paper ID, never submit again! Journal Paper/CRF Template

- **Step 2. Full Paper Review**

Using the evaluation system in the ICACT Website, the editor, reviewer and author can communicate each other for the good quality publication. It may take about 1 month.

- **Step 3. Acceptance Notification**

It officially informs acceptance, revision, or reject of submitted full paper after the full paper review process.

Status	Action
Acceptance	Go to next Step.
Revision	Re-submit Full Paper within 1 month after Revision Notification.
Reject	Drop everything.

- **Step 4. Payment Registration**

So far it's free of charge in case of the journal promotion paper from the registered ICACT conference paper! But you have to regist it, because you need your Journal Paper Registration ID for submission of the final CRF manuscripts in the next step's process. Once you get your Registration ID, send it to Secretariat@icact.org for further process.

- **Step 5. Camera Ready Form (CRF) Manuscripts Submission**

After you have received the confirmation notice from secretariat of ICACT, and then you are allowed to submit the final CRF manuscripts in PDF file form, the full paper and the Copyright Transfer Agreement. Journal Paper Template, Copyright Form Template, BioAbstract Template,

Journal Submission Guide

All the Out-Standing ICACT conference papers have been invited to this "ICACT Transactions on the Advanced Communications Technology" Journal, and also welcome all the authors whose conference paper has been accepted by the ICACT Technical Program Committee, if you could extend new contents at least 30% more than pure content of your conference paper. Journal paper must be followed to ensure full compliance with the IEEE Journal Template Form attached on this page.

➢ How to submit your Journal paper and check the progress?

Step 1. Submit	Using the Submit button, submit your journal paper through ICACT Website, then you will get new paper ID of your journal, and send your journal Paper ID to the Secretariat@icact.org for the review and editorial processing. Once you got your Journal paper ID, never submit again! Using the Update button, you can change any information of journal paper related or upload new full journal paper.
Step 2. Confirm	Secretariat is supposed to confirm all the necessary conditions of your journal paper to make it ready to review. In case of promotion from the conference paper to Journal paper, send us all the .DOC(or Latex) files of your ICACT conference paper and journal paper to evaluate the difference of the pure contents in between at least 30% more to avoid the self replication violation under scrutiny. The pure content does not include any reference list, acknowledgement, Appendix and author biography information.
Step 3. Review	Upon completing the confirmation, it gets started the review process thru the Editor & Reviewer Guideline. Whenever you visit the Author Homepage, you can check the progress status of your paper there from start to end like this, " Confirm OK! -> Gets started the review process -> ...", in the Review Status column. Please don't miss it!

Volume. 8 Issue. 4

Using the Actionable Intelligence Approach for the DPI of Cybercrime Insider Investigation

Da-Yu KAO

Department of Information Management, Central Police University, Taoyuan 333, Taiwan

dayukao@gmail.com

***Abstract*— Cybercrime threats are often originating from trusted, malicious, or negligent insiders, who have excessive access privileges to an organization's network, system, or data. The sophistication of insider threats has led to cybercrime issues. Even when an incident is detected, the follow-up countermeasures are required to analyze the results. The analysis of cybercrime insider investigation presents many opportunities for actionable intelligence on improving the quality and value of digital evidence. There are several advantages of applying Deep Packet Inspection (DPI) methods in cybercrime insider investigation. This study discusses the importance of actionable intelligence to conduct investigations and addresses the countermeasure of a cybercrime insider investigation with DPI to detect anomalies in network packets.**

Keywords—Deep Packet Inspection, Digital Evidence, Insider Investigation, Actionable Intelligence, Network Forensics

I. INTRODUCTION

Every organization must be vigilant when it comes to sensitive data protection. When cybercrime is causing significant economic damage, insider threats of increasing cyberattacks are often exposed to unauthorized access to data. Insider threats are challenging cybersecurity issues. They involve a variety of motivations and are very difficult to identify ahead of time [6]. Routine monitoring allows cybersecurity experts to decrease their risk exposure by quickly detecting unusual activities, undue work outside regular work hours, or excessive missing work [13]. Investigators should make specific observations and interpretations of the digital data, supply sufficient evidence in crime reconstruction, and prove the suspect's illegal access to the computer itself. When the thorough protection of network activities is essential to protect sensitive and individual data, continuous monitoring is highly recommended as part of information security controls in insider risk management. Digital evidence has become an essential part of crime scene investigation to collect live/volatile network information in cybersecurity breaches. Deep packet inspection (DPI) methods can be used to investigate and detect cybercrime attacks [5].

The purpose of forensic examination for a cybercrime investigation lies in the following various processes [15]: identification, individualization/classification, association, and reconstruction. While these processes were initially developed to examine and analyze evidence in terms of physical forensics, they are equally applicable to the digital forensics discipline. The cybercrime investigation focuses on (1) identifying the digital evidence from computer logs (identification), (2) finding the suspect ID/account and determining a typical class from evidence process (individualization/classification), (3) inferring interactions between the evidence and the suspect from copied data (association), and ordering the associations in time and space from necessary information (reconstruction). This study will develop new analysis technology to drill down into digital evidence based on the examination of insider threat incidents.

This study tries to recognize cybercrime insider issues from vast collections of computer logs and network packets in order to discover criminal activities more effectively from vague connections. The structure of this study is organized as follows. Section 2 provides a review of global trends in cybercrimes and insider threat detection. The sample case of Taiwan ATM heist is described in Section 3. Section 4 demonstrates the proposed actionable intelligence approach for the DPI of insider threat investigation. Finally, the last section concludes the study and makes some suggestions for future work.

II. LITERATURE REVIEWS

Insiders are authorized users that have legitimate access to business operations. Some are the result of a casual mistake or careless employee behavior. They will continue to seek to challenge security countermeasures, exploit potential vulnerabilities, and increase their knowledge of security procedures for nefarious purposes. Not all insider threats are malicious.

A. Global Trends in Cybercrimes

Cybercriminals are using more advanced malware to target computers, smartphones, and network devices. Illegal acquisition of data breaches is a prominent threat. Some hackers

Manuscript received Jan. 1, 2019. This work was a follow-up of the invited journal to the accepted & presented paper of the 21st Conference on Advanced Communication Technology (ICACT2019), and this research was partially sponsored by the Executive Yuan of the Republic of China under the Grants Forward-looking Infrastructure Development Program (Digital Infrastructure-Information Security Project-109).

Da-Yu Kao is with the Department of Information Management, Central Police University, Taoyuan 333, Taiwan (Corresponding Author phone: +886-3-328-2321; fax: +886-3-328-5189; e-mail: dayukao@gmail.com).

are often involved in large-scale money theft through payment systems or politic espionage operations under the guidance of the government. They may present a hybrid of both forms for profit or their living. Russian crime rings are often suspected of being highly skilled in breaching data systems primarily for organized crime profit. That is shedding renewed light on how vulnerable the online system can be [10].

1) *Cybercrime Investigation*

Law Enforcement Agencies (LEAs) initiate an investigation when a crime is suspected. The presence of relevant, reliable, and sufficient evidence can officially open a case in LEAs. The criminal investigation begins with data on crime. The evidence can verify if a crime has been attributed to a specific person, which has a lot to do with the identification, collection, examination, analysis, and presentation of evidence in law [15]. As cybercrime continues to change, investigators must develop a working knowledge of big data approach to discover the truth, combat cybercrimes, and enforce the law.

2) *Network Packets*

The sources of computer logs or network packets can be used for the evidence. Computer logs were used to identify the attacker, including system logs, application logs, network logs, and database logs. Digital forensics provides investigators with evidence that might be traced back to a criminal event. All the information on the Internet is transferred using network packets. Cyber threats leave some traces in the packets. Since the packets make vast volumes of the data, the methods of big data can help to structure this data. Investigators can monitor the behavior and improve the analyses for identifying the root cause. They can reconstruct the series of events associated with the incident over the entire system and the Internet.

B. *Insider Threat Detection*

Insider activities on systems and networks at financial institutions are a significant great threat to sensitive/confidential data. Preventing, detecting, or investigating internal attacks is a troublesome task since insiders have enough knowledge to access sensitive data. There are still great difficulties in identifying insiders who attempt to conceal their activities by changing their behaviors over time [16].

1) *Big Data Analytics*

Pieces of evidence of malicious insider activity are often buried within big computer logs accumulated over months. Multiple classification models to achieve anomaly detection are evolving to determine insider threat over evolving stream activities. The methods of big data can help again in reconstructing high-level events on the base of low-level artifacts to indicate the areas of interest. An integrated platform for big data processing systems is critical to improve overall performance, analyze an incident, automate their processes, and ensure reliable, scalable, and cost-effective findings. The big data analytics can be applied for insider threat detection of cybercrimes, which are dynamic and heterogeneous [16]. Big data analytics can help investigators analyze such data to detect security violations.

2) *Deep Packet Inspection*

DPI enables the cybercrime investigator to analyze network packets in real-time interception according to their payload. Although packet sampling and selective data can improve performance, the risk of missing substantial evidence for relevant, reliable, or sufficient data is too substantial [5]. A complete picture of cybercrime investigation is identifying the suspects as well as the contents of their communications. Performing full-packet capture is excellent to maintain evidence of what happened after an alert is triggered. By performing DPI, investigators can view and analyze the traffic data with the full context. This study will propose a set of tasks to be conducted in an insider threat investigation using DPI.

III. SAMPLE CASE

A. *Taiwan ATM Heist in July 2016*

The threat of cybercrime is becoming increasingly complex and diverse in putting citizen's data or money in danger. The forensic investigation of Taiwan LEAs identified a piece of malware that allows criminals to attack ATMs directly. The ATM heist was committed without inserting cards or touching the ATM in any improper or illegal way, with the machines simply spitting out bills continuously. When the attackers had obtained control of ATM management service, money was withdrawn directly from the ATM by the attacker command. ATM malware is only active in July 2016. That is considered to be a higher-level attack because it requires access to the back end of the ATM and bypasses the need for capturing consumer bank card data [4]. Taiwan's dense network of surveillance cameras plays an essential role in helping investigators crack the ATM heist. Surveillance cameras fed police information about where the suspects located. This case has demonstrated a high level of technological and financial knowledge in conducting their cybercrimes and exploiting new opportunities for gain.

B. *Answering Some Questions*

The sheer amount of information to find relevant data can be overwhelming at the start of an investigation. A significant effort to keep up with the suspect still requires a continually changing effort in every investigation. A crime investigation can focus on identifying supporting materials to support or refute a case. It is a systematic examination to identify facts on who, what, when, where, and how. Investigators increasingly depend on digital data to find the available evidence, produce appropriate documentation, and verify the impact/context of a crime or incident [2]. Special attention is paid to the 4W1H questions to test case studies in the insider threat domain. The objective of this study is to systematize knowledge in the incident analysis of insider threats [6]. Some questions are initiated for answering this sample case [8].

1) *Who: Andrejs Peregudovs, Mihail Colibaba, and Nikolay Penkov*

The 19 suspects in the heist came from the following six nations: Russia, Moldova, Estonia, Romania, Latvia, and

Australia. They entered and exited Taiwan at different times to avoid police detection.

2) What: US$2.61 Million Theft in an ATM Looting

NT$83.27 million (US$2.61 million) was illegally withdrawn from 41 compromised ATMs of First Bank in Taiwan. On July 20, the police have recovered NT$17.17 million (US$535,700) in total. There is still NT$ 5.86 million (US$182,800) of the loot still unaccounted for (see Table I). Taiwan is a small island. It is quite natural for people to get together for exchanging intelligence. The police were well trained and highly capable of investigating cybercrime.

3) When: July 9 ~ 10, 2016

The group heist allegedly occurred on July 9 and 10, 2016. On July 17, 2016, Taiwan police arrested three suspects in Taiwan. All other suspects fled Taiwan before the police could get hold of them.

4) Where: Three Suspects Were Sentenced in Taipei, Taiwan

On May 18, 2017, Taiwan High Court upheld prison sentences of more than four years for these three Eastern Europeans. The three men will also have to pay fines between NT$300,000 (US$9,900) and NT$500,000 (US$16,500) for each person [8],

5) How: ATM Attacks Targeting Wincor Nixdorf Model

Attacks follow a similar pattern. Through these direct attacks, criminals can empty the cash cassettes of ATMs produced by a specific manufacturer running Microsoft Windows XP. The malware was triggered automatic cash disbursement and a command file installed into the bank's ATM Wincor Nixdorf model "ProCash 1500." Three different malware programs hacked these ATMs: 'cnginfo.exe' read data from the machine, 'cngdisp.exe' executed the money-delivery process, and 'sdelete.exe' deleted the former two programs.

C. Answering Follow-up Questions: Are there any insiders involved in this case?

Organizations should deal with malicious or accidental insider threats. Malicious insiders purposely cause harm to an organization by stealing, damaging, or disclosing information. Accidental insiders are tricked into causing damage or whose credentials have been stolen. That is always happening [3]. New questions and follow-up questions will arise during the investigation. When LEAs investigated how the bank's network was compromised and how the ATMs had been controlled, they found irregularities in the connections between the voice server in London, the bank's internal network and the ATMs in Taiwan. Because the bank's computer system is a closed network, insider assistance could not be ruled out yet in this case [8]. The compromised victim claimed there was no insider threat attack in this case. However, this may mislead investigators. It is important to note that victims do not have proper or effective ways to detect insider attacks. Preventing internal attacks is much more challenging than external breaches, as insiders with legitimate access unwittingly create vulnerabilities or intend to exploit an organization's cyber devices maliciously. It is necessary to identify high-risk insiders based on their behaviors, indicators, or work patterns [13].

TABLE I
MONEY FLOW IN TAIWAN ATM HEIST

Date	Money	Activity	Location
July 9 and 10, 2016	NT$83.27 million (US$2.61 million)	Seventeen suspects were illegally withdrawn	41 compromised ATMs of First Bank in Taiwan
July 11, 2016	NT$200,000	Two suspects have converted more than NT$200,000 into South Korean won, Australian dollars, and US dollars	Taiwan Taoyuan International Airport
July 17, 2016	NT$60.24 million	Two suspects were arrested. Some money was recovered	Taipei hotel.
July 20, 2016	NT$12.63 million	Police found Andrejs's bag	A hill near Xihu Park in Taipei's Neihu District
July 20, 2016	NT$4.54 million	Mr. Ko handed another bag to the police.	Taipei
Note: On July 11, 2016, two suspects converted more than NT$200,000 into South Korean won, Australian dollars and US dollars at Taiwan Taoyuan International Airport just before their departure.			

IV. THE PROPOSED ACTIONABLE INTELLIGENCE APPROACH FOR THE DPI OF INSIDER THREAT INVESTIGATION

While organizations often spend lots of resources on the awareness training of external criminals, insider risks are likely to result in costly security incidents. The risk of unintentional incidents continues to increase as insiders are often able to capitalize on their familiarity with internal systems to launch lucrative attacks without attracting notice [14]. The personal issue of insider threats is one of the significant factors in cyberattacks. The results of inadequate organization protections can be financial loss of operational capabilities as well as the material loss of business records. Monitoring employee activities may identify the potential warning signs of insider activities and prevent some attacks from causing significant harm to an organization. Organizations should establish a network activity baseline for anomalous behavior on intentional and unintentional insider threats through administrative, technical, and investigative safeguards. The appropriate method may mitigate the risk or any possible effects before an attack occurs.

This section discusses digital evidence processes, actionable intelligence practices, and their follow-up cybercrime investigation countermeasures that help combat insider threats.

Putting the risk management and investigation countermeasure together with technical controls into a single practice is one of the critical challenges of building an effective strategy. The readiness of cybercrime countermeasure is critical to reducing an insider threat. Cybercrime investigators will try their best to find evidence in computers or networks [7]. Investigators will benefit from a specially trained unit for insider threat monitoring and investigations. Such staff should ideally have experience or training in conducting a forensic analysis of an incident [14]. This proposed countermeasure ultimately combines host data and network traffic to raise early red flags for further analysis.

A. Actionable Intelligence as an Investigative Approach

Digital devices help people communicate locally and globally with ease, and can be used criminally. Investigators have much work to do and face the risk of missing evidence. It requires proper tradecraft to find evidence and develop actionable intelligence practices. The exploitation of digital evidence can provide a wealth of useful information. Actionable intelligence can be defined as "having the necessary information immediately available in order to deal with the situation at hand [9]." The international cooperation of mutual assistance in fighting cybercrime has developed to overcome the challenges as mentioned above through relevant laws, information exchange, data analysis, criminal investigations, or digital forensics. Investigators need to implement a prioritized approach to the identification, collection, examination, analysis, and presentation where different pieces of evidence are assessed for different suspects.

1) Cybercrime Investigation Ecosystem

Many international organizations or associations are collaborating and making efforts to combat cybercrime. LEAs are well-advised to consider Private-Public-Partnership (PPP) to bring research into reality for cybercrime investigation. The roles of LEAs include protecting citizens, maintaining law and order, and preventing, detecting and investigating a crime. A strategic cybercrime measure toward PPP needs to be developed in improving cybercrime investigation. The national-level strategy of leading actionable intelligence practices on cybercrime issues is proposed in Table II. It also presents a viewpoint of combating cybercrime ecosystem. This strategy focuses on the following key terms [11]: near-term, mid-term, and long term. Each term is further analyzed from people, process, and technology. Near-term draws a strategic roadmap to combat cybercrime. Mid-term develops Standard Operation Procedures (SOPs) to avoid fear, uncertainty, and doubt. Investigators can collect live data on the running system from endpoints, analyze it, identify the usual status of the system, and determine a deviation. Long-term facilitates cross-border cooperation on private and public organizations.

TABLE II
ACTIONABLE INTELLIGENCE APPROACH ON CYBERCRIME ISSUES

	Near-Term	Mid-Term	Long-Term
Cybercrime Governance	Draw a strategic roadmap to combat cybercrime	Develop SOPs to avoid fear, uncertainty, and doubt	Facilitate cross-border cooperation
People	Cybersecurity capacity building: Train personnel	Cybersecurity reporting mechanism: Collaborate with an international alliance	Private-Public-Partnership: Meet both needs
Process	National agency for cybersecurity: Form a working group	Legal Measures: Amend the existing IT law	International Cooperation: Discuss real-time issues
Technology	Cybersecurity strategy: Define visions, objectives, and action plan	R&D on advanced tools and technology: Develop a new methodology to fight against coming issues	Active Participation: Actively participate in international associations
Tasks	● Create new procedures or policies to deter, respond to, and prosecute cybercrime. ● Enhance the actionable intelligence capability to gather data, process information, and combat cybercrime.		

2) Comprehensive Actionable Intelligence of Cybercrime Investigation

Making sound judgments at low cost is a core role and an essential attribute for investigators, who must maximize the potential and exploit the possibilities to ensure things are what they see. Various kind of intelligence provides critical information on time to an appropriate audience for better-informed decision making. Actionable intelligence is related to the investigation or incident at hand into the broader intelligence mix [1]. Investigators have produced actionable intelligence from criminal investigation to gain knowledge in support of preventing cybercrime or pursuing criminals. The threats from criminals are becoming increasingly complicated. All practitioners, policy-makers, or investigators need to understand how they can find actionable intelligence at the scene. Investigators need to find out the evidence and convict suspects of their crimes with actionable intelligence within a limited period [9]. The effectiveness and efficiency of investigators can be judged in part by the capability to utilize their reasonable collection opportunity to access the digital device, support the evidence-gathering at the scene, collect

volatile/non-volatile evidence in the lab, pursue criminal immediately, and achieve successful prosecutions.

B. Cybercrime Insider Investigation Countermeasure: DPI

Detecting cyberattacks can be difficult to identify what can be done to combat the increased risk of insider threats [14]. Cybercrime investigations have faced difficulties with analyzing evidence in large datasets to verify the impact of an incident. Improving the relevancy, reliability, and sufficiency of incident response is a critical issue in tackling the large volume of computer logs and network packets. This study includes cybercrime insider investigation, which allows a more detailed and comprehensive incident analysis in DPI. While it may be challenging to protect against insider attacks, a practical investigation countermeasure can significantly reduce their impact. The goal is to create a process that allows the investigators to evaluate the digital evidence accurately. The critical part of any investigation is relevant, reliable, and sufficient evidence. Investigators need to prepare a checklist to discover the relevant data, gather evidence, and cross-reference the findings. The following practices in Fig. 1 are proposed to ensure that an investigation is forensically sound in law. Fig. 1 comes with subphases and activities for any digital investigation: civil, criminal, or corporate [2]. Implementation of these countermeasures for preventing insider attacks will provide organization investigative measures that can prevent or facilitate the early detection of many cyberattacks. That includes the following five consecutive/iterative phases: identity, collect, examine, analyze, and present.

1) Identify: Track the Pathway of an Insider Threat

It is crucial to collect the right data and preserve the crime scene as part of the preliminary investigation. Most auditing tools only alert users at the moment when cybercrime was detected. By contrast, DPI solutions allow investigators to track the insider's pathway by collecting all network packets and identifying any suspicious files. Collected packets are analyzed to generate statistics of used usernames, IP addresses, protocols, port services, type, and duration of the attack [12].

a) Payload-based inspection

Payload-based inspection is based on the analysis of payload in the application layer of network packets. Investigators can use predefined patterns like sensitive digital sources as signatures for each cyberattack and help them to distinguish attacks form each other.

b) Port-based identification

Port-based identification is known to be among the easiest and fastest method for analyzing network packets. Port numbers will not be affected by encryption schemes. Packet identification via port number uses the data in the TCP/UDP headers of the packets to extract the port number which is assumed to be associated with a particular application program.

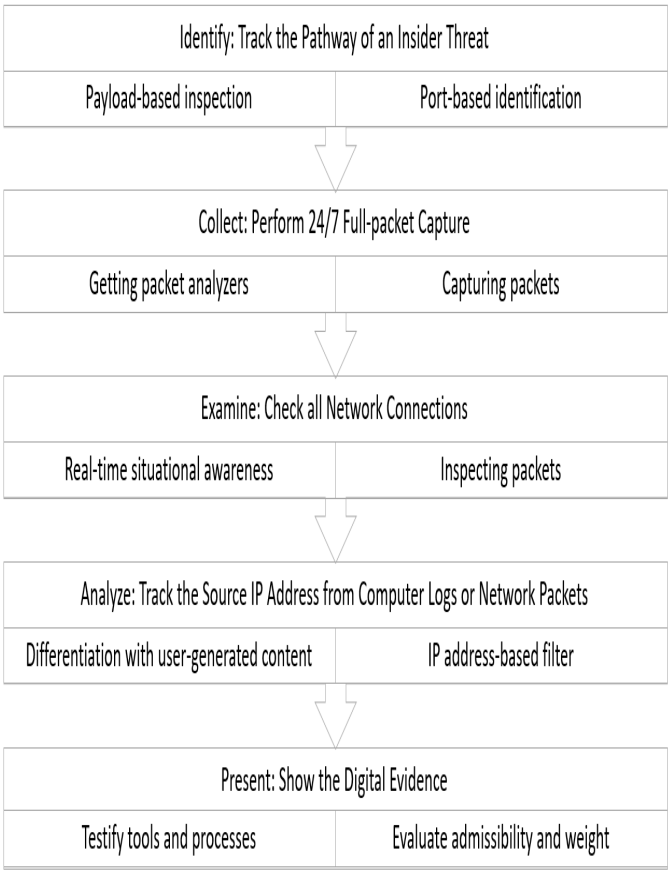

Fig. 1. Proposed cybercrime countermeasure of insider threat investigation

2) Collect: Perform 24/7 Full-packet Capture

As insider threats may occur anytime, DPI is an effective way to identify suspicious content in the headers or the payloads, excepting situations where the payload is encrypted [12]. Identification, tracking, and monitoring of computer systems can help avert or limit the exposure of sensitive data to insider attacks. When investigators monitor vital assets, they can react faster and with more precision to mitigate incidents [13]. Packet analyzers are used to monitor network traffic, detect a cybercrime, or get access to user names and passwords. They allow investigators to see each byte of data that passes from a computer or server across the network.

a) Getting packet analyzers

Network packets often contain a wealth of information that is relevant to the investigation. Investigators can download and install tcpdump, Wireshark or other packet analyzers for Windows, macOS, or UNIX-like systems from its official website.

b) Capturing packets

Much digital evidence can be gathered from the network than the host. Most Internet activities can be discovered and analyzed with the use of network sniffer methods. This countermeasure will introduce and reinforce a network packet mindset that investigators can use any DPI method and produce

worthwhile outcomes in finding out the fact. Investigators can start capturing packets and create a filter based on it.

3) Examine: Check all Network Connections

After a cybercrime occurs on the network, victims often suffer from data leakages for months or years. Investigators can recognize data patterns from the collected network packets to discover any digital trace evidence or identify behavior patterns [5]. By examining the connections among computers and to the Internet, DPI makes it possible to prove that the network is secure.

a) Real-time situational awareness

With DPI, investigators have real-time situational awareness about whether attackers are still present on the network, or whether any computers are still compromised.

b) Inspecting packets

Investigators can debug network protocol implementations, examine security problems, and inspect network protocol internals to view its details. Pattern recognition may help identify the suspicious IP address of the source attack and understanding the meaning or motivation behind anomalous behavior.

4) Analyze: Track the Source IP Address from Computer Logs or Network Packets

Some tools capture only sample traffic, perform statistical sampling of data, and generate reports based on host-based logs. The source IP address of the suspect is a crucial component of this countermeasure because not all possible data can be collected or analyzed simultaneously. Some data (e.g., network packets) may not be available instantaneously.

a) Differentiation with user-generated content

Investigators can differentiate users' activities within a single application from network packets.

b) IP address-based filter

IP address-based filter is a critical task in cybercrime investigations. In order to properly explore network packets, it is vital to recognize different sources of IP addresses.

5) Present: Show the Digital Evidence

Digital evidence may be used to identify the attacker by username, computer name, and private or public IP address.

a) Testify tools and processes

A digital video or camera can help investigators document the location and condition of everything. Hash values of digital sources and files should be created as early as possible. Investigators should be able to testify that they have validated their tools and processes.

b) Evaluate admissibility and weight

Investigators should examine the digital devices, produce an unbiased and accurate document, describe the forensic outcome, and assist the court in evaluating the admissibility and weight of any digital evidence.

V. CONCLUSIONS

The connections among terrorists, cybercriminals, and organized crime groups appear to be on the rise. An increasing trend of malicious/unintentional insider threats becomes one of the challenging cybersecurity issues. The involved employees can abuse their access privileges to steal funds from customer accounts or the organization. The ubiquity of the Internet has increased the accessibility of data sources, knowledge, or skills. The cost is high when terror or online attacks succeed. Most organizations do not have a dedicated team in detecting insider threats. They take a reactive approach and deploy resources when a problem is detected. A proactive approach to looking for insider threats is critical for an organization to look for the problem. If the investment is low, it is impossible to know the true extent of cyberattacks. A promising approach to ensure an efficient and effective strategy is a collaboration between various private and public organizations. Security agencies, intelligence agencies, and LEAs can apply similar techniques to advance counter-cybercrime measures to keep citizens safe or to prevent, pursue, protect, and prepare against cybercrime. They need to enhance their investigative ability to identify, collect, acquire, and preserve evidence. Its importance is growing to keep citizens, communities, and commerce safe. This study introduces the DPI method that can help investigators in developing new techniques and performing the digital investigation process in a forensically sound and timely fashion manner. This study also provides a survey of the packet inspection in cybercrime insider investigation. Case studies illustrate that DPI can be used to extract knowledge or insights from computer logs or network packets for cybercrime reconstruction. Efficient continuation efforts of data analysis fields such as statistics, machine learning, data mining, knowledge discovery, and predictive analytics are necessary for data extracting and analyzing in less period. Future research will analyze packets and identify the traces left by cyber threats.

REFERENCES

[1] Akhgar, B., Bayerl, P. S., Sampson, F. (Eds.), *Open Source Intelligence Investigation: From Strategy to Implementation*, Springer Publishing, pp. 1-68, 2016.

[2] Arnes, A., *Digital Forensics*, John Wiley & Sons Ltd, pp. 46-318, 2018.

[3] Cole, E., "Defending Against the Wrong Enemy: 2017 SANS Insider Threat Survey," SANS Institute, pp. 3-21, Aug. 2017.

[4] Dalfonso, S., "ATM Malware: The Next Generation of ATM Attacks," https://securityintelligence.com/atm-malware-the-next-generation-of-atm-attacks/, 2014.

[5] Davis, J. J., *Machine Learning and FeatureEngineering for Computer Network Security*, Dissertation, Faculty of Science and Engineering, Queensland University of Technology, pp. 1-33, 2017.

[6] Homoliak, I, Toffalini, F., Guarnizo, J., Elovici, Y., Ochoa, M., "Insight into Insiders and IT: A Survey of Insider Threat Taxonomies, Analysis, Modeling, and Countermeasures," *ACM Computing Surveys (CSUR).* Vol. 52, No. 2, 2019.

[7] Kävrestad, J., *Guide to Digital Forensics: A Concise and Practical Introduction*, Springer International Publishing, pp. 3-8, 2107.

[8] Law and Regulations Retrieving System, "Criminal Appeals No.593/106 in Taiwan High Court," Judicial Yuan, May 18, 2017.

[9] Pearson, S. and Watson, R., *Digital Triage Forensics: Processing the Digital Crime Scene*, Elsevier Inc., Burlington, pp. 13-144, 2010.

[10] Rayman, N., "The World's Top 5 Cyber Crime Hotspots," http://time.com/3087768/the-worlds-5-cybercrime-hotspots/.

[11] Rishi, R., Kumar, P., and RAWAT, D. S., *Strategic National Measures to Combat Cybercrime: Perspective and Learnings for India*, Ernst & Young LLP, pp. 6-21, 2015.

[12] Rodrigues, G. A. P., Albuquerque, R. O., Deus, F. E. G., Sousa. R. T., Oliveira Júnior, G. A. O., Villalba, L. J. G., Tai-Hoon Kim, T. H., "Cybersecurity and Network Forensics: Analysis of Malicious Traffic towards a Honeynet with Deep Packet Inspection," *Applied Sciences*, Vol. 1082, pp. 1-29, Jul. 2017.

[13] Schulze, H., "Insider Threat 2018 Report," CA Technologies, pp. 3-31, 2018.

[14] SIFMA, *Cybersecurity: Insider Threat Best Practices Guide (2nd Edition)*, Securities Industry and Financial Markets Association, pp. 5-53, Feb. 2018.

[15] Stephenson, P., *Official (ISC)*$^{2®}$ *Guide to the CCFP CBK*, Boca Raton, FL: Auerbach Publications, pp. 293-404, 2014.

[16] Thuraisingham, B., Masud, M. M., Parveen, P., Khan, L., *Big Data Analytics with Applications in Insider Threat Detection*, CRC Press, pp. 181-432, 2017.

Da-Yu Kao received the B.S. and M.S. degree in Information Management from Central Police University, Taiwan, in 1993 and 2001, the Ph.D. degrees in Crime Prevention and Correction from Central Police University, Taiwan, in 2009, respectively. From 1993 to 1996, he was with Taipei City Police Department, Taiwan, where he was an information technology police officer involved in the development of policing information systems. From 1996 to 2007, he was with Criminal Investigation Bureau, National Police Administration, Taiwan, where he was a detective and forensic police officer in cybercrime investigation and digital forensics. From 2007 to 2013, he was with Maritime Patrol Directorate General, Coast Guard Administration, Taiwan, where he was an information technology section chief in the department of information and communication. Since 2013, he has been with Central Police University, Taiwan, where he is currently an associate professor in the Department of Information Management. His research interests include cybercrime investigation, digital forensics, digital evidence, information management, criminal profiling, and cyber criminology.

Conservation Genetic Algorithm to Solve the E-commerce Environment Logistics Distribution Path Optimization Problem

Rui FU*, Mohammed Abdulhakim Al-Absi*, Ahmed Abdulhakim Al-Absi**, Hoon Jae Lee*

* *Dongseo University, Busan, Republic of Korea*

** *Kyungdong University Gangwon-do, Republic of Korea*

furui.qilianteng@gmail.com, Mohammed.a.absi@gmail.com, absiahmed@kduniv.ac.kr, hjlee@dongseo.ac.kr

***Abstract*—E-commerce is a business activity that uses modern information technology to process cash flow and logistics to achieve transactions. With the increase of evolutionary algebra, saving genetic algorithm and genetic algorithm all tend to be more optimal. The evolutionary starting point of saving genetic algorithm is much lower than the evolutionary starting point of genetic algorithm. The evolutionary algebra and the population size in the conservation genetic algorithm also have certain influence on the performance of the algorithm. The maximum running distance of the vehicle is different when the trucks have distance limitation and have no-distance limitation. This paper can improve the efficiency of logistics distribution and shorten the distribution distance, which is of great significance for saving logistics costs and improving customer service level.**

***Keywords*— logistics and distribution, vehicle routing problem, saving algorithm, logistics costs**

I. INTRODUCTION

In the traditional logistics distribution, there are unreasonable factors such as low automation, untimely information reception, and low network level, which hinder the efficiency of logistics distribution. The logistics distribution under e-commerce is a new logistics distribution mode that can shorten the distribution cycle, optimize the service quality and improve the competitiveness of enterprises by combining information network technology and logistics distribution in an open network environment.

This kind of distribution mode is conducive to the improvement of logistics distribution efficiency. Logistics distribution under the e-commerce environment has many characteristics such as a large number of customers, relatively small customer demand, obvious customer respectability, and time requirements.

E-commerce logistics and distribution is to meet the customer's satisfaction, and it is the basic goal of the enterprise to find ways to minimize the transportation cost during the operation [1], [2].

Characteristics of E-commerce logistics distribution are a large number of customers, size of each customer's demand is relatively small, dispersion of customers is obvious, customer has high requirements for the timeliness of arrival of the goods, high customer service needs, and suppliers strive to save costs as showing in the Fig. 1.

The Vehicle Routing Problem (VRP) [3] is a typical NP-hard problem. It has a wide range of applications in computer science, operations research and engineering optimization. The algorithms of solving VRP problems mainly include precise algorithms, traditional heuristic algorithms, simulation algorithms and artificial intelligence algorithms. The exact algorithm [4] uses the mathematical programming method to obtain the optimal path solution. The exact algorithm is suitable for solving small-scale VRP problems. The traditional heuristic algorithm [5] refers to a feasible solution to the combinatorial optimization problem to be solved under the premise of acceptable computation time and space. The simulation method [6] obtains the optimized solution of the vehicle route through computer simulation experiments. The artificial intelligence optimization algorithm [7] finds the optimal solution of the problem by revealing and simulating

Manuscript received on Jan. 1, 2019. This work supported by the Institute for Information and Communications Technology Promotion (Grant Number: 2018-0-00245) and it also supported by the Basic Science Research Program through the National Research Foundation of Korea funded by the Ministry of Education, Science, and Technology (Grant Number: NRF2016R1D1A1B01011908), and a follow-up of the invited journal to the accepted & presented paper entitled "Conservation Genetic Algorithm to Solve the E-commerce Environment Logistics Distribution Path Optimization Problem" of the 21th International Conference on Advanced Communication Technology (ICACT2019).

Rui FU. Currently, she is a Ph.D. student in the Department of Computer Engineering at Dongseo University, South Korea. (E-mail: furui.qilianteng@gmail.com)

Mohammed Abdulhakim Al-Absi. Currently, he is a Ph.D. student in the at Dongseo University, South Korea. (E-mail: Mohammed.a.absi@gmail.com)

Ahmed Abdulhakim Al-Absi. Currently is an assistant professor and head of smart computing department at Kyungdong University - Global Campus in South Korea. (E-mail: absiahmed@kduniv.ac.kr)

Hoon Jae Lee. Currently, he is a professor in the Department of Information Communication Engineering at Dongseo University, South Korea. (corresponding author, phone: +82-10-2801-3735, email: hjlee@dongseo.ac.kr)

natural phenomena. It is global optimization performance, strong robustness, and strong versatility and is suitable for parallel processing. It is widely used to solve large-scale VRP problems. [8] E-commerce is a business activity that uses modern information technology to process cash flow and logistics to achieve transactions. Under the e-commerce environment, whether an item can reach to the customer accurately is a key factor to enhance the company's image. Therefore, how to efficiently select the algorithm to solve the vehicle routing problem is an urgent problem to be solved. In this paper, the genetic algorithm and the conservation algorithm [9], [10]-[11] are combined to construct the conservation genetic algorithm to study the logistics distribution path optimization problem under the e-commerce environment and the experimental results are verified in the simulation environment.

This paper consists of six sessions. Session 1 is introduction. It introduce the problems of logistics distribution under the background of e-commerce and the current algorithm to solve the vehicle routing problem(VRP).Session 2 is e-commerce environment logistics distribution. In this session mainly introduce four basic streams and the characteristics of e-commerce environment logistics distribution. Session 3 is problem description. In the session it establishes a mathematical model to solve the NP hard problem. Session 4 is Saving Genetic Algorithm. Describing about saving algorithm and genetic algorithm respectively and combing the two methods to saving genetic algorithm. Session 5 is simulation. Get the result of using saving genetic algorithm and compare with genetic algorithm. Session 6 is conclusion as well as acknowledgement and references.

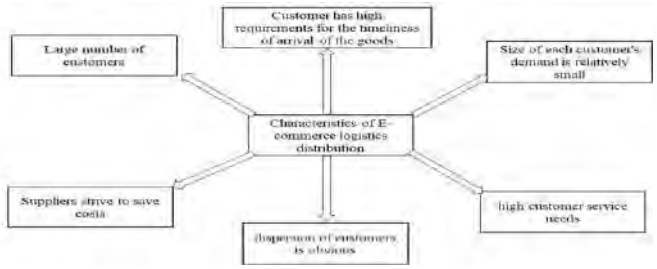

Fig. 1. Characteristics of E-commerce logistics distribution

II. E-COMMERCE ENVIRONMENT LOGISTICS DISTRIBUTION

E-commerce environment logistics distribution process includes procurement operation process, warehousing operation process, delivery operation process, return and follow-op operation process.

Any transaction in e-commerce contains four basic streams. That is logistics, business flow, capital flow and information flow.

- Information flow refers to the dissemination and flow of information.
- Business flow refers to the process of transferring the ownership of the transaction object, the ownership of the goods in the trade and the change of ownership between the purchase and sale. Including the payment process, the transfer process.
- Capital flow refers to the transfer of funds in the course of trade with the transfer of ownership of goods. The capital expenditure and income process including per-sales, prepayments, and advance receipts.
- Logistics is the final link in the completion of commodity goods transactions, and is also an important link in the realization of e-commerce. Companies need to choose the right logistics method based on the different nature of the traded goods.

E-commerce logistics and distribution is to meet the customer's satisfaction. During the operation, the basic goal is to find a minimize cost transportation way during the whole process-commerce environment logistics distribution have the following characteristics:

- A large number of customers;
- The size of each customer's demand is relatively small;
- The dispersion of customers is obvious;
- The customer has high requirements for the timeliness of arrival of the goods;
- High customer service needs;
- Suppliers strive to save costs.

How to quickly and efficiently deliver goods to customers in B2C mode and how to minimize transportation costs is essential to improve the overall competitiveness of enterprises. By studying the vehicle routing problem, it is possible to rationally use the transportation tools, optimize the transportation route and reduce the transportation cost of the enterprise.

III. PROBLEM DESCRIPTION

In the e-commerce environment, the logistics distribution path optimization problem can be described as follows: According to the customer's order status of the e-commerce enterprise, obtain the demand quantity of each customer's goods, determine the actual distribution network of the time period, and optimize the design of a vehicle. The delivery route completes the delivery tasks required by the customer under various constraints, so that the total cost of delivery is minimized.

In this paper, the maximum distance traveled by the vehicle is used as a limiting condition, and the saving algorithm and the genetic algorithm are combined to solve the optimal path. The delivery personnel take the list from the distribution center and deliver the goods to the customer points of known coordinates. When the total distance exceeds the maximum distance traveled by the truck, return to the distribution center to refuel, and then continue from the distribution center to the next waiting. The customer service department delivers the

goods until all the customers are served, and finally the vehicle travels back to the distribution center and can quickly effectively meet customer needs.

A) Model hypothesis

- There is only one central site that provides delivery services and provides fueling services;
- The location coordinates of the central site and each customer are known;
- The demand for each customer point is known;
- Only one truck is available in the entire area;
- The sum of the distance traveled by the vehicle during the delivery process shall not exceed its maximum travelable distance;
- Each customer has one and only one visit;
- Each customer's distribution needs must be met.

B) Model establishment

Each customer's representation is

$$p_i = p(x_i, y_i), i = 1, 2, ..., N$$

In the formula, x_i is the abscissa of the point where the customer is located; y_i is the ordinate of the point where the customer is located; N is the number of customers in the area who need the service. The coordinate point of each customer is known, so the distance between any two customers is known.

Define the decision variable as

$$X_{ij} = \begin{cases} 1, & Passing\ the\ vehicle\ on\ the\ line(i,j) \\ 0, & Otherwise \end{cases}$$

In the formula, (i, j) shows the car travelling from i to j.

1. The objective function for calculating the shortest path to travel is

$$D = \min \sum_{i=1}^{N} \sum_{j=1}^{N} d_{ij} \times x_{ij} + d_{1o} + s_o + d_{no} \quad (1)$$

In the formula, d_{ij} is the straight line distance between adjacent customers i and j; d_{1o} is the distance from the distribution center to the first customer point; s_o indicating that when the vehicle travel route is limited by the maximum travel distance, the extra travel time is added back and forth; d_{no} is the distance from a customer to the distribution center.

2. Each customer is visited once.

$$s.t. \sum_{i=1}^{N} x_{ij} = 1, \quad (i \neq j; j = 1, 2, ...N) \quad (2)$$

$$\sum_{j=1}^{N} x_{ij} = 1, \quad (i \neq j; i = 1, 2, ..N) \quad (3)$$

In the formula, $\sum_{j=1}^{N} x_{ij}$ represents the total number of times from the customer i to the customer j (the value ranges from 1 to N); $\sum_{i=1}^{N} x_{ij}$ shows the total number of times from the customer i to the customer j (the value ranges from 1 to N). The combination of formula (2) and formula (3) means that each customer can only be served once, and the service cannot be repeated.

3. The maximum distance that a truck can travel at one time during the delivery process and cannot exceed the maximum distance that can be traveled that L is

$$\sum_{i=1}^{k} x_{ik} + x_{k0} \leq L \quad (4)$$

In the formula, x_{ik} means that the vehicle travels from the customer i to the customer k; $\sum_{i=1}^{k} x_{ik}$ indicates the total distance that the vehicle has traveled to the point of k; x_{k0} indicates the distance from the point k to the origin.

IV. SAVING GENETIC ALGORITHM

A) Conservation algorithm

Conservation algorithm, also known as the C-W, which was proposed by Clarke and Wright [12] in 1964. Its basic idea is to first connect each point to the origin separately, c_{ij} the distance between the point i and the point j, from 1 to the total distance is

$$z = \sum_{i=1}^{l} c_{oi} + \sum_{i=1}^{l} c_{io} \quad (5)$$

Then define the savings of the distance between the points of i and j

$$s(i, j) = c_{oi} + c_{io} + c_{oj} + c_{jo} - (c_{oi} + c_{ij} + c_{jo}) = c_{io} + c_{oj} - c_{ij} \quad (6)$$

$$s(j,i) = c_{jo} + c_{oi} - c_{ji} \quad (7)$$

In the formula, the distance between the point and the point; for the path saving value, the steps of the saving algorithm are as follows:

1. Calculate the savings value of the route, arranged in a tabular form according to the value of the savings. And choose the maximum savings.

2. Check whether the two points corresponding to the saved value satisfy the following points:

- If the corresponding two points in the saved value are not on the already constructed line, get the line segment and turn to step 3.
- If the corresponding two points in the saved value are on the formed line and not the inner point of the line (i.e., not directly connected to the origin), the connection is obtained or the line is turned to step 3.
- If the corresponding two points in the saved value are on the different lines that have been constructed, and they are not internal points, the line is obtained and turned to step 3.
- If the corresponding two points in the saved value are on the formed line, then the connection cannot be made again, and turn to step 3.

3. If the row or column is removed, the point can no longer be connected to other points, and the point cannot be reached by other points.

4. After all elements are crossed, a qualifying line is obtained and the algorithm terminates. Otherwise, select the largest element from the elements that are not crossed, and turn to step 3.

B) Genetic algorithm

The genetic algorithm draws on the natural selection process of the survival of the fittest in the biological world and shows the excellent selection process in nature. Darwin kept the outstanding individuals in the selection process, and the process of bad individuals being eliminated was called survival of the fittest [13]. The robustness of genetic algorithm is relatively strong, simple and universal, and has strong advantages in parallel processing, and the application of genetic algorithm is wide. Therefore, genetic algorithm is listed as one of the important intelligent computing methods. Similarly, genetic methods are also one of the computational mathematics to solve the optimal search method. Evolutionary algorithms include genetics, natural selection, crossover, and mutation [14].

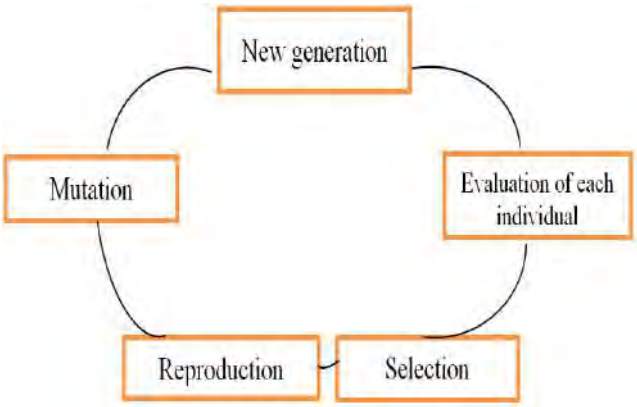

Fig. 2. The process of Genetic Algorithm

The genetic algorithm begins with a feasible solution set that represents a problem, and the population consists of a certain number of individuals genetically encoded [15]. As a chromosome carrying a gene, it also determines the external appearance of the individual's shape and characteristics. For example, genes in a chromosome determine the characteristics of a person's hair color and height. Therefore, the primary task of the algorithm is to perform the mapping from the external phenotype to the intrinsic genotype, which can also be understood as the coding work. Genetic algorithms basically use binary encoding for encoding work. After the initial population is generated, the genetic operators of natural genetics are used for cross-combination and mutation, and the evolutionary inferior principle is used to evolve more and more optimal solutions. The best individuals in the last generation population can be decoded the optimal solution to the problem.

The basic idea of genetic algorithm can be described from the above terms: starting from a population of optimization problems (a set of feasible solutions), according to the principle of survival of the fittest and the principle of survival of the fittest, evolved one by one to produce a better and better one (a set of feasible solution). In each generation, according to the fitness of the individual (feasible solution) (the objective function value), select some excellent individuals to copy (reproduce) to the next generation, and cross and mutate them to produce a new solution set population. This process will result in the population being like natural evolution. The progeny population is more adaptive to the environment than the parent (the new feasible solution is closer to the optimal solution of the problem than the old feasible solution), and the optimal individual in the whole evolution process is the final problem.

Genetic concepts in genetic algorithms and their effects are as follows [16][17]:

- Individual (individual) : Refers to an entity with a characteristic chromosome
- Chromosome: Encoding of the solution represented by a string or vector

- Gene: Elements in the chromosome
- Fitness: Individual fitness for the environment
- Population: The selected number is a set of solutions for the group size
- Reproduction: A set of solutions selected based on fitness function values
- Choose: Eliminate inferior individuals and choose excellent individuals
- Crossover: Gene interaction in chromosome
- Mutation: Genetic changes in chromosome

The genetic algorithm has a good global search ability, which can quickly search out the whole solution in the solution space without falling into the fast falling trap of the local optimal solution; and with its inherent parallelism, it can be easily distributed computing, speed up the solution. However, the local search ability of the genetic algorithm is poor, which makes the simple genetic algorithm more time-consuming, and the search efficiency is lower in the late evolution. In practical applications, genetic algorithms are prone to the problem of premature convergence. The choice of methods to maintain good individuals and maintain group diversity has always plays an important role in genetic algorithms. In the process of using the algorithm, we must develop strengths and avoid weaknesses, combined with other algorithms to avoid the shortcomings of the algorithm.

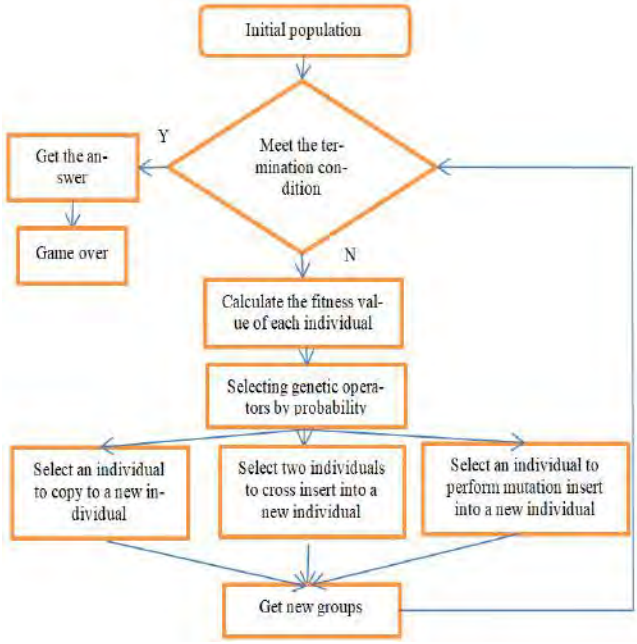

Fig. 3. The operational steps of the genetic algorithm

C) *Conservation genetic algorithm*

The combination of the conservation algorithm and the genetic algorithm [18] can improve the efficiency of the genetic algorithm. The specific steps of the algorithm are as follows:

- Required information.
- Initial population
- Fitness function.
- Select.
- Cross.
- Variation.
- control parameter

V. SIMULATION

It is assumed that within a certain period of time, a distribution demand order issued by 30 customers randomly selected in a region is received, and the maximum number of iterations is 200. Each order is analyzed by a conservation genetic algorithm, and the distribution center performs the vehicle on the vehicle loading to achieve logistics and distribution.

Each customer is numbered starting with 0 in decimal. And the demand for each customer is known.

Set the $N = 200$ $p_c = 0.9$ $p_m = 0.1$ $p_s = 0.6$ maximum evolution algebra $gen\max$ to increase with the number of customers, assuming that the maximum driving distance of the vehicle is 30km. In order to verify the validity of the algorithm and obtain the optimal path, the results obtained by the two algorithms of genetic algorithm and conservation genetic algorithm are compared respectively. The results are shown in Table I.

TABLE I
SIMULATION CALCULATION RESULTS

Method	Customer	Average Best Value	Best Result	Relative Deviation /%	Average Iterations
GA	30	427.7	412.7	3.6	162
CWGA	30	410.4	401.3	2.2	72

Note: Relative deviation= [(Single measurement-Measurement average)/Measurement average]*100% It can be seen from Table 1 that the average optimal value and the best result of the GA algorithm are larger than the CWGA algorithm when the number of customers is 30, which shows that the CWGA obtains the optimal path better; The relative error of CWGA is smaller than the relative error of GA, which indicates that the fluctuation of the CWGA result is smaller and more stable. The comparison of the average number of iterations shows that the convergence speed of the CWGA algorithm is much faster than that of GA. In summary, under a limited number of iterations, the algorithm CWGA as a new type of optimization algorithm is easier and faster to determine an optimized distribution path and reduce the delivery distance. The optimization process when the number of customers N=30 is as shown in Fig. 4.

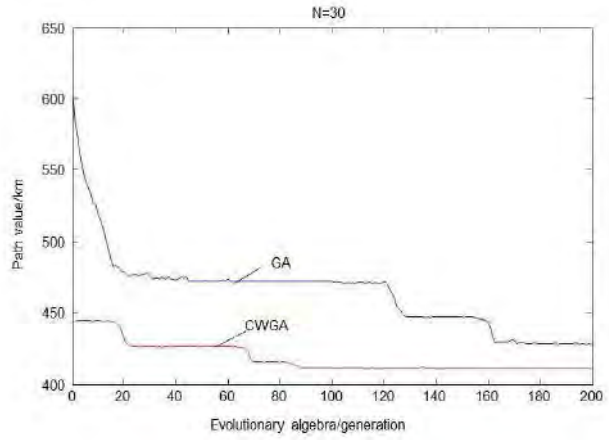

Fig. 4. Optimization process when the number of customers is N=30

Fig. 4 reflects the convergence of the path lengths of the two algorithms in the iterative process. The graph trends are gradually convergent. The CWGA algorithm requires less convergence than the GA algorithm, and runs to 200 generations. The shortest path finally obtained by CWGA is significantly improved compared to the shortest path obtained by the GA algorithm. Therefore, using the conservation algorithm to generate the initial population combined with the genetic algorithm makes the CWGA evolutionary starting point high and easy to find the optimal solution. 30 customer points are randomly selected. When considering the distance limit and not considering the distance limit, the route of the optimal path is obtained. One unit in the table indicates 1 km. The results are shown in Table II.

TABLE II
SIMULATION CALCULATION RESULTS

Customer	$N=30$
Consider the distance limit	Order：2 12 7 0 23 4 18 19 17 24 20 11 25 29 6 3 13 22 9 10 14 27 28 5 1 26 15 8 21 16 Distance：413.7km
No distance limit	Order：2 12 7 0 23 4 17 18 19 5 24 20 6 11 25 16 29 3 13 9 10 14 27 28 22 1 26 15 8 21 Distance：76.7km

In the conservation genetic algorithm, the population size (PS) is fixed, and this process does not conform to the actual biological evolution in the process of biological evolution. The population size cannot be constant in the process of human and biological evolution. Only one fixed population size in an algorithm cannot visually compare the results of the comparison. Poor population size will affect the quality of the solution. When the population size increases, if the set evolutionary algebra increases, the efficiency and accuracy of the conservation genetic algorithm do not necessarily increase.

TABLE III
CHANGES IN POPULATION SIZE AND CONVERGENCE ALGEBRA

PS	EGN	Optimal path
30	150	298.17
60	142	239.09
90	146	227.19
120	132	218.97
150	124	209.61
180	126	228.69
210	107	299.15
240	113	311.80
270	105	293.80
300	104	291.09

The evolutionary algebra of the conservation genetic algorithm is the number of cycles set in the program. A certain number of cycles will converge to a certain interval, which is the convergence algebra (EGN). The more the number of loops, the more values the algorithm traverses, and the results obtained are not necessarily closer to the optimal value.

3) N= 30, P_c= 0.9, P_m =0.1, the program runs 5 times to find the shortest path, convergence algebra (EGN) and population size (PS) are shown in Table 3 and Fig. 5:

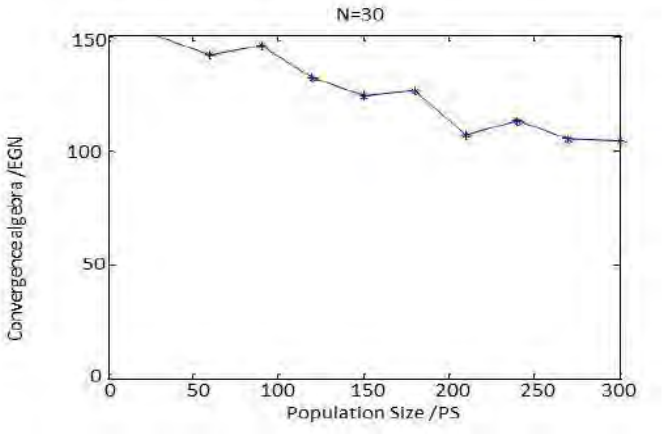

Fig. 5. Changes in population size and convergence algebra

VI. CONCLUSION

The logistics distribution of e-commerce has many characteristics such as there are lots of customers and uneven distribution of customers. Taking the e-commerce B2C model as the research background and do some research which in a certain area those different customers have different needs, finally the mathematical model is established. Combined with the saving genetic algorithm, the influence of the maximum

distance that the truck can travel on the vehicle distribution problem is detailed. Processing and obtaining an optimal path that is more realistic than previous studies. Future work, there are still a lot of deficiencies where the problem algorithm itself still needs a long calculation time, and the calculation degree is more complicated.

ACKNOWLEDGMENT

This work was supported by Institute for Information and Communications Technology Promotion (IITP) grant funded by the Korea government (MSIT) (No.2018-0-00245), And it was also supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science, and Technology (grant number: NRF2016R1D1A1B01011908).

REFERENCES

[1] L. Weijian. “Research on logistics distribution route optimization under B2C e-commerce mode”, *Beijing Jiaotong University*. 2007.

[2] D. Liyan, Z Wei. “Logistics Foundation Beijing” *Tsinghua University Press*, 2000, 78-79.

[3] C. Xueli, Ma Liang, Fan Bingquan. Ant colony algorithm for vehicle routing problem (VRP) [J]. *Systems Engineering*, 2004, 19(4): 418-422.

[4] S. Lijun, H. Xiangpei, W. Zheng, “Research progress on vehicle path planning problems and solving methods”, *Systems Engineering*, 2006 (24): 31-36.

[5] L. Yufeng, Li Jun. Dynamic programming heuristic algorithm for solving time-varying vehicle scheduling problems [J]. *Systems Engineering Theory and Practice*, 2012 (32): 1712-1718.

[6] L. Xiang, L. Yanhui. Cross-regional VRP model for e-commerce distribution and its heuristic algorithm [J]. *Journal of Tsinghua University*, 2006, 46(z1): 1014-1018.

[7] H. D Ratliff, A. S.Rosenthal, “Order picking in a rectangular warehouse: A solvable case of the traveling sa leman problem [J]. Operations research, 2002, 2 (31): 507-521.

[8] W. Dingwei, “Modeling and optimization in e-commerce” [M]. Science Press, 2008.

[9] Y. Jian, L. Jin, L Houqing,”Annealing network solution for VRP in stochastic demand situation”, *Systems Engineering Theory and Practice*, 2002, 22(3): 109-114.

[10] L. Jiali, M. Zujun, “There are vehicle rental and sharing and there are time windows and multiple distribution centers open loop VRP”. *Systems Engineering Theory and Practice*, 2013, 33(3): 666-672.

[11] L. Yuqin, W. Peiru, “Research on the traditional storage picking path of logistics center”, Supplementary city name: Taiwan Mingxin University of Science and Technology, 2005.

[12] G. Clarke, J. W. Wright, “Scheduling vehicle from a central delivery depot to a number of delivery points”, *Operations Research*, 1964, 32(8): 568-581.

[13] W. Lihua, J. Bai, Z. YJ, G.S. Tan, “Application of Structure Optimization Design Based on Matlat Genetic Algorithm”.44-47. DOI:10.3969/j.issn.1009-9492.2017.10.012

[14] R. FU, M. A. Alabsi, M. Sin, H.J. Lee. “General Study of E-commerce Logistics Distribution. *International Conference on Culture Technology(ICCT)* pp. 404-407 (2018)

[15] T. J. min, Z. X. Zhang, W. C.Y. Wang, “Multipoint Location of TDOA based on Improved Genetic Ant Colony Algorithm DOI:10.3969/j.issn.1002-0802.2018.07.015

[16] W. s. Chen, Y. F, “Research on User Behavior Path 0ptimization of Internet+ Logistics Information Security Management” DOI:10.3969/j.issn.1000-7695.2018.16. 027

[17] X. Binglei, S. Yi, L. Rongxi. “Genetic algorithm for solving the problem of collecting travel salesma”, *Journal of Shaanxi Institute of Technology*, 2002, 18(1): 70-75.

[18] L. Maoxiang, H. Siji, “Research on solving the problem of logistics distribution route optimization by hybrid genetic algorithm”, *Chinese Management Science*, 2002, 10(5): 51-56.

Rui FU was born in China 1990, received her (MS) degree in System Theory from Qingdao University - China in 2012-2015. Currently, She is a Ph.D. student in the Department of Information and Communication Engineering at Dongseo University, Korea. Her research interests include Logistics Transportation and Mathematics.

Mohammed Abdulhakim Alabsi was born in Yemen 1987, received his BS in Computer Application from Bangalore University in India. He earned his (MS) degree at Dongseo University, South Korea in 2018. Currently, he is a PhD. student in the Department of Information and Communication Engineering at Dongseo University, South Korea. His research interests include IoT, VANET, UAV, artificial intelligence, cryptology, network security, computer networks and digital communications.

Ahmed Abdulhakim Al-Absi was born in Yemen 1984, he is an Assistant Professor and Head of Smart Computing Department at Kyungdong University – Global Campus in South Korea. He earned his PhD in Ubiquitous Computing at Dongseo University, South Korea in 2016. His research interests include database systems, big data, hadoop, cloud computing, distributed systems, parallel computing, high-performance computing, VANET, and bioinformatics. He received a Master of Science (MS) degree in Information Technology at University Utara Malaysia, Malaysia in 2011 and a Bachelor of Science (BS) degree in Computer Applications at Bangalore University, India in 2008.

HoonJae Lee was born in Korea 1962, received his BS, MS, and Ph.D. degrees in electronic engineering from Kyungpook National University, Daegu, Rep. of Korea, in 1985, 1987, and 1998, respectively. He is currently a professor in the Department of Information Communication Engineering at Dongseo University. His current research interests include Password Theory, Network Security, Side-Channel Attack, and Information Communication/Information Network.

Volume 8 Issue 4, July. 2019, ISSN: 2288-0003

ICACT-TACT JOURNAL

GIRI
Global IT Research Institute

1713 Obelisk, 216 Seohyunno, Bundang-gu, Sungnam Kyunggi-do, Republic of Korea 13591
Business Licence Number : 220-82-07506, Contact: tact@icact.org Tel: +82-70-4146-4991