Conference Title

The Third International Conference on Computer Science, Computer Engineering, and Social Media (CSCESM2016)

Conference Dates

May 13-15, 2016

Conference Venue

Metropolitan College, Thessaloniki, Greece

ISBN

978-1-941968-34-5 ©2016 SDIWC

Published by

The Society of Digital Information and Wireless Communications (SDIWC)

Wilmington, New Castle, DE 19801, USA

www.sdiwc.net

Table of Contents

Application Layer DDoS Attack Defense Framework for Smart City using SDN

Narmeen Zakaria Bawany and Jawwad A. Shamsi
nshawoo@gmail.com and jawwad.shamsi@nu.edu.pk
Systems Research Laboratory
FAST-National University of Computer and Emerging Sciences, Karachi, Pakistan

ABSTRACT

Smart city brings enormous opportunities and exciting challenges. In a smart city, operations and services such as traffic, transport, electric power, and water distribution are monitored, operated, and controlled through ICT based infrastructure, smartly. This allows efficient management of resources and facilitates smooth access to services. However, it also induces stringent requirements and challenges for uninterrupted operation and execution of ICT-based monitoring and controlled infrastructure. Cybersecurity is one of the foremost challenges in a smart city network. That is, protecting the smart city application services from cyber-attacks and ensuring continuity of services is utmost desirable. As smart city services typically comprised of web based applications, application level distributed denial of service (AL-DDoS) attack is a major cybersecurity threat that can have catastrophic impact on an extremely critical smart city network. This paper presents an efficient framework for AL-DDoS attack detection and mitigation for a smart city network. The proposed framework utilizes Software Defined Networking (SDN) paradigm to implement resilient design that ensures continuity of smart city application services. The framework integrates a sound mechanism that distinguishes AL-DDoS attack from legitimate flash crowd. This is a novel framework that addresses the flash crowd attack detection and mitigation in a smart city environment using SDN.

KEYWORDS

Smart city, Application level DDoS Attacks, Cyber Security, Flash crowd, Software Defined Networking

1 INTRODUCTION

A metropolitan city that can monitor and control its critical infrastructure including roads, railways, subways, airports, seaports, power plants, communication systems, etc., using Information and communication technology (ICT) is considered to be a smart city[1]. Smart city can plan and optimize its resources and provide efficient services to its citizens. All such services require the execution of several services under an orchestrated coordination. Smart city ICT infrastructure is unique in many respects. First, smart city is a highly complex system due to its enormous structure and heterogeneity. Second, smart city comprises extremely critical city systems. These systems are so vital that their destruction or service disruption can effect security, safety and economy of cities. Third, in smart city network traffic is highly dynamic and unpredictable. For instance, any emergency situation like accidents or earthquakes can cause impulsive load to networks. Fourth, smart city can become a prime target for terrorism and cyber-attacks because of the critical nature of services that it provides. Enemy nations can target smart city networks and application servers to paralyze the city almost instantly.

Cyber-attacks are nearly as old as the Internet itself and the problem has only grown more multifaceted over the period of time. Organizations continue to seek better means of attack prevention, detection and mitigation techniques[2]. Some experts believe that it was cyber-attack that caused the northeast blackout

ISBN: 978-1-941968-34-5 ©2016 SDIWC

of 2003 affecting more than 50 million people in a 9,300-square-mile area, and the massive 2008 Florida blackout that shut down large portions of the power grid[3]. Distributed denial-of-service (DDoS) attacks has become one of the major cyber security threats over the last decade[4][5]. DDoS attacks can consume vast amounts of computing, memory and network resources of the service provider. This, in turn, either causes performance degradation or disruption of services to legitimate users. Public web servers, in particular, has been the main target of DDoS attacks. Utilizing the services of cloud infrastructure providers, attackers are able to launch massive attacks. Most recent attack against a Cloudflare[6] customer was estimated to be around 400Gbps[7]. DDoS attack is major cybersecurity threat that can have catastrophic impact on extremely critical smart city network. Besides, the traditional volumetric DDoS attack that leverage huge amount of traffic to bring down the network services, organizations are now faced with the challenge of low and slow application layer DDoS (AL-DDoS) attacks. AL-DDoS attacks exploits legitimate HTTP requests to overwhelm target resources. AL-DDoS attacks are more challenging because it often mimics or occurs in the flash crowd events of popular websites[8][9].

The strategy to protect a city's cybersecurity is critical for managing risks and improving resilience. AL-DDoS attacks are primarily launched on web servers to disrupt their services [9][10]. Generally, smart city data centers will be hosting numerous web application servers to provide web based services to the citizens thereby making smart city applications highly prone to AL-DDoS attacks. Smart city application services need protection from AL- DDoS attacks that could cause severe stoppages to critical services. Their continued operation will be vital for the well-being of the populace. Defending such a system from AL- DDoS attack is critical as the consequence of downtime may be disastrous.

AL- DDoS attack detection and mitigation is an enormous challenge due the distinct nature of smart city network traffic. Overwhelming volume, velocity and variety of traffic that is generated from across the city makes it a daunting task. Heterogeneity of networks, applications specific and dynamic security policies, emerging threats, high availability and scalability are the basic challenges that need to be accounted for when implementing a detection and mitigation mechanism for AL-DDoS attack in a smart city. Further, distinguishing AL-DDoS attack from legitimate flash crowd traffic in a smart city scenario is a significant challenge as AL-DDoS attack is easily misled by flash crowd traffic[10][11].

This research is motivated by the above mentioned challenges and requirements for a smart city. To this end, the purpose of this research is to propose an efficient mechanism for AL-DDoS attack detection and mitigation. The proposed framework for detection and mitigation of AL-DDoS attack is pragmatic for smart city network. As the framework is based on Software defined Networking (SDN) it exploits the key benefits of the technology including handling heterogeneity issues, controlling key network components from a central controller, etc., inherently [12]. Likewise, separation of control plane from the data plane, in SDN, provides opportunity for implementing and updating of network policies at runtime, making it a prime choice for massive and dynamic smart city system.

2 RELATED WORK

Considering that the proposed framework comprises three major areas that has been extensively studied by researchers, the related work has been divided into three categories, that is, Smart City, Application level DDoS attacks and SDN based DDoS defense mechanisms.

2.1 Smart City

Smart city has been actively studied and researchers have come up with different definitions, frameworks, and implementations of smart city [13] [14],[15][16][17]. The key objective of almost all the research is to present a strategy to mitigate the problems generated by the urban population growth by using information and communication technology. Some researchers have addressed the smart city network and infrastructure requirement proposing cloud based solutions [18][19][20]. However, not much work has been found related to application level DDoS attacks on smart city application servers. This is a critical requirement for a smart city to remain functional.

2.2 Application Level DDoS Attacks

Application layer DDoS attacks are gaining momentum in the cyberspace. These emerging and more prevalent set of DDoS attacks are difficult to detect because it resembles the legitimate traffic. These attacks establish complete TCP connections with target server and then start flooding with several HTTP requests to overwhelm the victim or saturate the available bandwidth through illegitimate traffic. As these are slow and low attacks, it is very difficult to distinguish it from legitimate traffic. Therefore, application layer attacks are more successful tools for attackers to harm victims in current times. Moreover, the key challenge, to date, in this perspective is to differentiate between an attack and a flash crowd[21]. Flash crowd refers to sudden increase in legitimate connections on a server or website occurring at the same time or within a short period [22].The work of discriminating DDoS attacks from flash crowds has been explored for around a decade. Previous work [22], [23],[24] focused on extracting DDoS attack features followed by detecting and filtering DDoS attack packets by the known features. However, these methods cannot actively detect DDoS attacks [21]. Other popular defense mechanism against flash crowd attacks is the use of graphical puzzles or CAPTCHA [25]. Detecting anomalies by modeling legitimate behavior using different statistical models is another common method for differentiating between flash crowd and DDoS attack. For example, XieandYu [26] used the hidden semi-markovmodel, and Awad and Khalil [27] employed the all-Kth Markov model to describe web browsing dynamics. Oikonomou and Mirkovic tried to discriminate mimicking attacks from real flash crowds by modeling human behavior [28].

2.3 SDN based DDoS Detection Techniques

Many researchers have proposed variety of solutions to overcome DDoS attacks in traditional computing environment. However, DDoS attacks are becoming more widespread. Software defined networking has emerged as a new paradigm in networking and has attracted the research community more recently[12] [29]. The capabilities of SDN that includes software based traffic analysis, logical centralized control, global view of the network, and dynamic updating of forwarding rules complements DDoS attack detection and mitigation mechanisms. Braga[30] proposes a light weight detection mechanism based on traffic flow features implemented over a NOX based network. It uses Self Organizing Maps (SOM) [7], an unsupervised artificial neural network, to classify network traffic as either normal or abnormal, i.e. a potential attack, taking statistics about flows as parameters for the SOM computation. However the experiments were conducted on a small scale.
Radware[31] – a commercial cybersecurity solution provider has recently developed DefenseFlow[32] which is the first commercial SDN application that addresses DDoS attacks. Radware has furthermore contributed a simplified open source version of DefenseFlow, Defense4All[33], to the OpenDaylight[34] project. DefenseFlow directs the network

controller to collect specific flow statistics from forwarding devices in the network at a per second resolution. The application measures baseline traffic flows and then monitors for patterns suggestive of a DoS attack. In the event that a threat is detected, a traffic diversion mechanism programmatically redirects suspicious traffic to a dedicated behavioral analysis system for detailed traffic inspection, signature analysis, and threat neutralization. However, Radware does not provide any details of implementation. Also, Martin et al [35] does not considers DefenseFlow as pure SDN solution.

The literature presented above provides a good starting point for understanding the limitations of existing solutions. Most of existing AL-DDoS solutions are tuned up for a specific application environment and are based on traditional networks. However, the research presented in this study focuses on smart city applications and addresses the diverse applications requirement. The proposed framework advocates a more structured attack detection and mitigation approach that leverages an architectural layering in SDNs. Likewise, almost no work has been found for distinguishing flash crowd from DDoS attack for smart city applications. The combination of following three domains exclusively makes this work unique and inspiring:

- Smart city applications context
- Application level DDoS attack detection and mitigation for smart city application servers
- Distinguishing smart city applications legitimate Flash crowd from flash crowd attack

The novelty of this work lies in utilizing SDNs for detecting and mitigating AL-DDoS attacks, explicity identifying flash crowd attacks in smart city context. Moreover, this work presents a comprehensive framework for handling application specific security requirements dynamically.

3 PROPOSED FRAMEWORK

In order to address the aforementioned requirements, a proficient framework is required to detect and mitigate DDoS attacks in a smart city. Such a framework should not only ensure efficient detection and mitigation of DDoS attacks but also distinguish DDoS attack traffic from flash crowd. This work presents a novel framework where the capabilities of SDN are utilized for detection and mitigation of DDoS attack in a smart city environment. The framework, also includes, a dedicated module to distinguish a flash crowd attack traffic from a genuine flash crowd. The objective is to ensure the smooth functioning of smart city application servers by ensuring an efficient defense against DDoS attacks.

SDN has been proposed as a candidate of the next generation Internet architecture and organizations such as Google, Cisco, HP and Intel have already adopted SDN in their internal data centers and WANs [36][37][38]. This makes SDN an ideal choice for smart city network. The proposed framework exploits the inherent benefits of SDNs that are derived by the separation of control plane and data plane. Traditional networking paradigms fail to provide a logical centralized view of the network. The concept of SDN is actually a useful security technique as it supports the customization of devices to the highest level at runtime. The configuration policies at a central controller can be implemented on all network devices instantly resulting in whole new layer of security.

The framework will efficiently analyze and filter the attack traffic flows from legitimate traffic flows. This will prevent the malicious traffic from impacting the performance of services. Legitimate traffic will be forwarded to complete the transactions without being

effected. Eventually, the business continuity will be maintained. The idea is to detect network attack patterns by exploiting machine learning techniques in real-time and to distinguish it from a flash crowd. The attack pattern once detected is shared with application service providers in the smart city. Application specific traffic patterns are accounted for when analyzing network traffic for attack. The proposed solution benefits from existing approaches implemented in traditional networks for DDoS attacks detection and mitigation and combines these with the advantages of SDN. The resultant framework provides comprehensive solution that addresses DDoS attack security requirements in a massive smart city network.

3.1 SDN based Controller Architecture for Smart City Application Servers

Understandably, a smart city network, comprising hundreds of application servers, is a huge network. Therefore, a single point controller cannot be practically efficient. The framework, illustrated in figure 1, lays down three-tier high level depiction of the application servers and controllers. Hierarchical approach is used to counter for application specific application requirements, sharing of threat information, to meet reliability and efficiency requirements, to maintain autonomy of each application service provider and to follow resilience design approach.

3.1.1 Service Controller Layer

The Service Controller Layer (SCL) comprises of all the controllers. Each controller implements its own application specific security requirements. The AL-DDoS attack detection and mitigation module is tuned specific to the requirements of the hosted service. For instance, the live city traffic controller application server will have its own traffic patterns and thresholds based on the

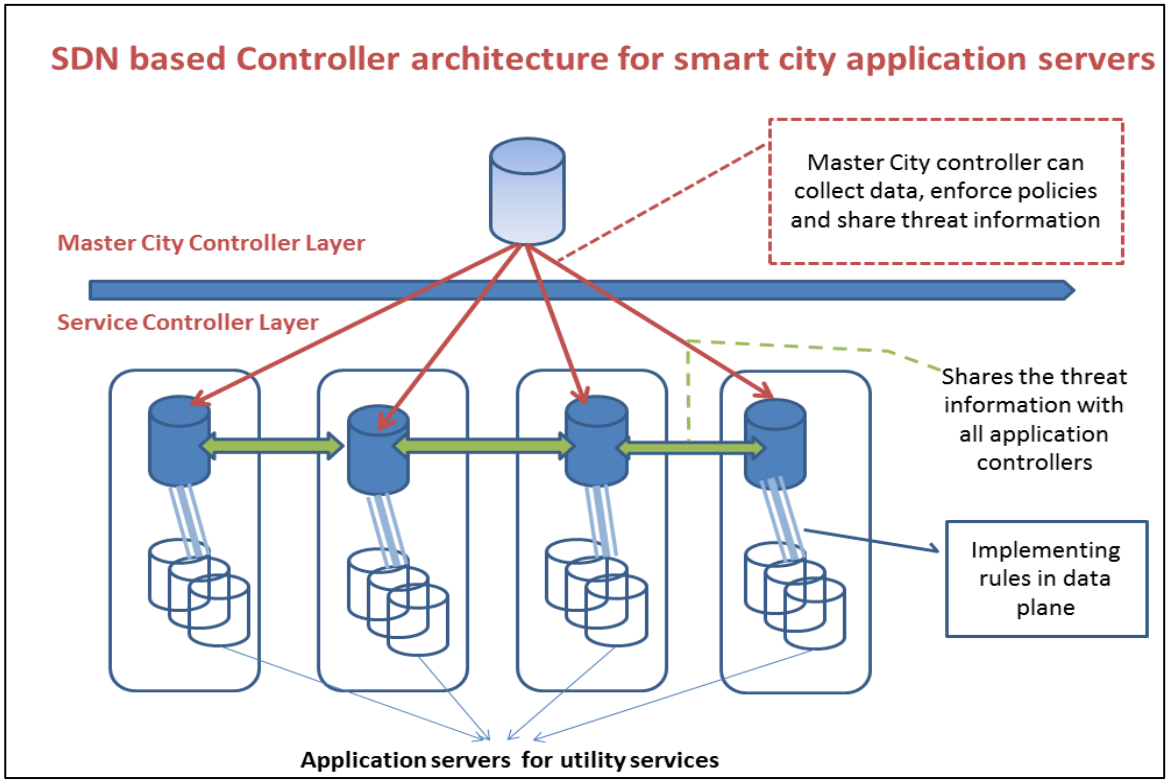


Figure 1: SDN based Controller architecture for smart city application servers

number of users. Similarly, smart grid users will have their unique characteristics with varying number of mobile and non-mobile users. Likewise, mitigation policy will also differ in each case. Therefore, each controller can independently implement and update their security policies across their application servers. Within a service controller layer, each controller can share the threat information with other controllers. This information sharing leads to efficient prevention of the possible attacks.

3.1.2 Master City Controller

Master City Controller (MCC) is basically used for record keeping, monitoring and overall threat analysis across whole city application services. The information collected at this server is critical for city administrators as it gives useful insights about cyber threats and development of city level cyber threat model. MCC can also share the threat information or any other information with SCL. Furthermore, threat model of MCC can be shared with other cities giving rise to country level threat model..

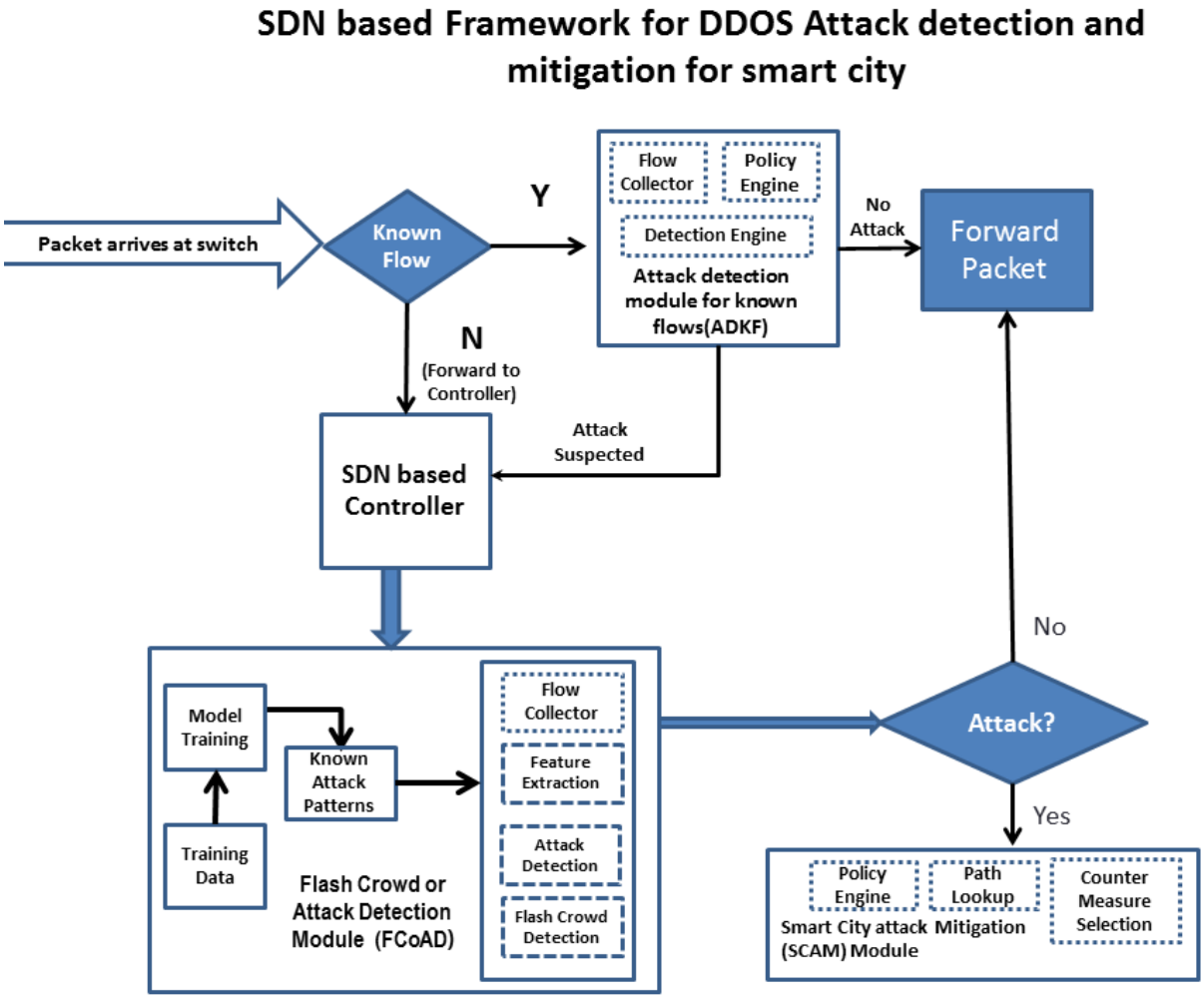


Figure 2: SDN based Framework for DDOS Attack detection and mitigation for Smart City

3.2 Framework for DDOS Attack Detection and Mitigation for Smart City

The work flow of attack detection and mitigation module is depicted in figure 2. When a new packet arrives at the switch checks whether it belongs to existing flow. If so, it updates the flow statistics otherwise it is sent to the controller. Existing flow traffic is also monitored by Attack detection for known flows (ADKF) module. The packets marked as suspicious by ADKF module and the packets that does not have entries in switch flow tables are sent to controller. Controller queries the Flash Crowd or Attack Detection (FCoAD) Module for the packet flow. If the query result indicates an attack, FCoAD issues an alert to Smart City attack Mitigation (SCAM) Module. If the query result is normal, the packet is forwarded to its intended destination.

3.2.1 Attack Detection Module for Known Flows (ADKF)

ADKF consists of Flow Collector, Policy Engine, and Detection engine. Flow collector collects the flow statistics from switch for each flow. OpenFlow switches maintain counters for each flow table and flow entry. The module checks if amount of flow is within the permitted limits and does not violate Quality of service (QoS) parameters set up by policy engine. For e.g., if the flow ' A' exceeds the maximum transmission threshold defined by the policy engine the flow is sent to detection engine for further processing.

3.2.2 Flash Crowd Attack Detection (FCAD) Module

This module consists of many sub modules. Initially, training dataset is provided to tune up the system for normal and attack traffic patterns. Dataset will be updated regularly to improve the attack patterns. Feature Extractor module extracts the traffic flow features from the statistics collected by flow collector. On the basis of features, the traffic is either classified as attack traffic or legitimate traffic by Attack detection module. Flash Crowd detection module specifically deals distinguishing flash crowd attacks and genuine flash crowds.

3.2.3 Smart City Attack Mitigation (SCAM) module

This module receives the traffic that is classified as attack by FCAD module. Administrators can configure mitigation policies for each flow or group flows using Policy Engine. Based on these policies, counter measure is selected by the SCAM module. The path lookup is used to maintain a table of paths. Paths are assigned to flows based on the policies defined by policy engine. For e.g. Malicious flash crowd attack traffic is diverted to a path that lead to sinkhole.

4 Conclusion

Smart city network is a rapidly expanding network. User, applications and services will be increasing at fast pace. Hence, the AL-DDoS detection and mitigation mechanism must be effectively scalable. Secondly, the smart city network being enormous by nature will lead to dynamic network topologies. Nodes will be added or removed very frequently for maintenance, adding or upgrading of services, or any other reasons that cannot be foresighted. Furthermore, the smart city network comprises many critical systems with high availability requirements, like smart grid, smart traffic management, smart transportation, etc., each working autonomously. The infrastructure for all these systems cannot be in place at a time but will be added gradually. This will lead to heterogeneous network infrastructure which cannot afford any downtime. Likewise, diversity of applications is obvious in smart city systems, each application providing specific set of services to users. These applications will

have varying level of network traffic and will need security policies according to their own set of requirements. Moreover, these security policies will be highly dynamic. Changing city situations like natural disasters, accidents or breaking news may require updating of security policies across the smart city network almost instantly. Efficiency of detection and mitigation mechanism along with low overhead is an inherent requirement of such a critical and large scale system. Therefore, it is desirable that DDoS detection and mitigation is lightweight, scalable and easy to manage. Additionally, intimation of threats information across all smart city systems will help in early detection and prevention of service disruption. This paper presents a novel SDN based framework for detection and mitigation of DDOS attack for the smart city application servers. The framework is designed to protect smart city services against known and emerging AL DDoS attacks that threaten the availability of real time services. Moreover, as smart city applications may experience flash crowds more frequently, distinguishing flash crowd attack from legitimate flash crowd traffic leads to more reliable attack detections.

References

[1] H. Chourabi, T. Nam, S. Walker, J. R. Gil-Garcia, S. Mellouli, K. Nahon, T. a. Pardo, and H. J. Scholl, "Understanding Smart Cities: An Integrative Framework," 2012 45th Hawaii International Conference on System Sciences, pp. 2289–2297, Jan. 2012.

[2] A. Bodhani, "Feeling lucky? [Special Report Cyber Security]," Engineering & Technology, vol. 10, no. 1, pp. 44–47, 2015.

[3] S. Harris, "China's Cyber Militia," National Journal, 2008. [Online]. Available: http://www.nationaljournal.com/magazine/china-s-cyber-militia-20080531.

[4] Z. Tan, a Jamdagni, X. He, P. Nanda, and R. P. Liu, "A system for denial-of-service attack detection based on multivariate correlation analysis," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 2, pp. 447–456, 2014.

[5] J. Yuan and K. Mills, "Monitoring the macroscopic effect of DDoS flooding attacks," IEEE Transactions on Dependable and Secure Computing, vol. 2, no. 4, pp. 324–335, 2005.

[6] Cloudflare, "Cloudflare Organization." [Online]. Available: https://www.cloudflare.com. [Accessed: 08-Aug-2015].

[7] S. Musil, "Record-breaking DDoS attack in Europe hits 400Gbps," CNET, 2014. [Online]. Available: http://www.cnet.com/news/record-breaking-ddos-attack-in-europe-hits-400gbps/.

[8] J. Choi, C. Choi, B. Ko, and P. Kim, "A method of DDoS attack detection using HTTP packet pattern and rule engine in cloud computing environment," Soft Computing, vol. 18, no. 9, pp. 1697–1703, 2014.

[9] and C. L. Liao, Qin, Hong Li, Songlin Kang, "Application layer DDoS attack detection using cluster with label based on sparse vector decomposition and rhythm matching," Security and Communication Networks, 2015.

[10] W. Zhou, W. Jia, S. Wen, Y. Xiang, and W. Zhou, "Detection and defense of application-layer DDoS attacks in backbone web traffic," Future Generation Computer Systems, vol. 38, pp. 36–46, Sep. 2014.

[11] S. Yu, W. Zhou, W. Jia, S. Guo, Y. Xiang, and F. Tang, "Discriminating DDoS attacks from flash crowds using flow correlation coefficient," IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 6, pp. 1073–1080, 2012.

[12] W. Xia, Y. Wen, S. Member, C. Heng Foh, D. Niyato, and H. Xie, "A Survey on Software-Defined Networking," Ieee Communication Surveys & Tutorials, vol. 17, no. 1, pp. 27–51, 2015.

[13] R. Giffinger and N. Pichler-Milanović, "Smart cities: Ranking of European medium-sized cities," 2007.

[14] S. Paroutis, M. Bennett, and L. Heracleous, "A strategic view on smart city technology: The case of IBM Smarter Cities during a recession," Technological Forecasting and Social Change, 2013.

[15] R. M. Kanter and S. S. Litow, "Informed and Interconnected: A Manifesto for Smarter Cities," Working Paper, vol. 09–141, pp. 1–28, 2009.

[16] S. Alawadhi and A. Aldama-Nalda, "Building understanding of smart city initiatives," Electronic Government. Springer Berlin Heidelberg, 2012.

[17] S. Idowu, "MASTER ' S THESIS A Development Framework for Smart City Services A Development Framework for Smart City Services."

[18] G. A. Zhang, J. Y. Gu, Z. H. Bao, C. Xu, and S. B. Zhang, "Towards a Smart City based on Cloud of Things, a survey on the smart city vision and paradigms," European Transactions on Telecommunications, vol. 25, no. 3, pp. 294–307, 2014.

[19] R. Petrolo, V. Loscrí, and N. Mitton, "Towards a smart city based on cloud of things," in Proceedings of the 2014 ACM international workshop on Wireless and mobile technologies for smart cities - WiMobCity '14, 2014, pp. 61–66.

[20] N. Mitton, S. Papavassiliou, A. Puliafito, and K. S. Trivedi, "Combining Cloud and sensors in a smart city environment," EURASIP Journal on Wireless Communications and Networking, vol. 2012, no. 1. p. 247, 2012.

[21] S. Yu, S. Member, S. Guo, and I. Stojmenovic, "Fool Me If You Can : Mimicking Attacks and Anti-Attacks in Cyberspace," vol. 64, no. 1, pp. 139–151, 2015.

[22] J. Jung, B. Krishnamurthy, and M. Rabinovich, "Flash crowds and denial of service attacks: Characterization and implications for CDNs and web sites," in Proceedings of the 11th international conference on World Wide Web (WWW '02), 2002, pp. 293–304.

[23] G. Carl, G. Kesidis, R. Brooks, and S. Rai, "Denial-of-service attack-detection techniques," Internet Computing, IEEE, 2006.

[24] Y. Chen and K. Hwang, "Collaborative detection and filtering of shrew DDoS attacks using spectral analysis," Journal of Parallel and Distributed Computing, 2006.

[25] S. Kandula, D. Katabi, M. Jacob, and A. Berger, "Botz-4-sale: Surviving organized DDoS attacks that mimic flash crowds," Proceedings of the 2nd conference on Symposium on Networked Systems Design & Implementation. USENIX Association, vol. 2, pp. 287–300, 2005.

[26] Y. Xie and S. Yu, "A large-scale hidden semi-Markov model for anomaly detection on user browsing behaviors," Networking, IEEE/ACM Transactions on, 2009.

[27] M. A. Awad and I. Khalil, "Prediction of user's web-browsing behavior: Application of markov model," IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics, vol. 42, no. 4, pp. 1131–1142, 2012.

[28] G. Oikonomou and J. Mirkovic, "Modeling human behavior for defense against flash-crowd attacks," in IEEE International Conference on Communications, 2009.

[29] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, "A survey of intrusion detection techniques in Cloud," Journal of Network and Computer Applications, vol. 36, no. 1, pp. 42–57, Jan. 2013.

[30] R. Braga, E. Mota, and A. Passito, "Lightweight DDoS Flooding Attack Detection Using NOX / OpenFlow," pp. 408–415, 2010.

[31] Radware, "http://www.radware.com." .

[32] R. Meyran, "DefenseFlow: The First Ever SDN Application that Programs Networks for DoS/DDoS Security," 2013. [Online]. Available: http://blog.radware.com/security/2013/04/defenseflowdosddos-security/.

[33] Radware, "DefenseFlow NetFlow and SDN based DDoS Attack Defense," 2013. [Online]. Available: http://www.radware.com/Products/DefenseFlow/.

[34] Linux Foundation, "http://www.opendaylight.org." .

[35] M. Vizváry and J. Vykopal, "Future of DDoS Attacks Mitigation in Software Defined Networks," Monitoring and Securing Virtualized Networks and Services. Springer Berlin Heidelberg, 2014.

[36] S. Jain, A. Kumar, and S. Mandal, "B4: Experience with a globally-deployed software defined WAN," ACM SIGCOMM Computer Communication Review, vol. 43, no. 4, 2013.

[37] "Business Case for Cisco SDN for the WAN," ACG Research, 2014.

[38] S. H. Sterling Perrin, "Practical Implementation of SDN and NFV in the WAN," 2013.

Mitigating Malware for Effective Utilization of Network Resources at ISPs

Narmeen Zakaria Bawany [1] , Sheeraz Ahmed [2], Jawwad A. Shamsi [3]
Systems Research Laboratory
FAST-National University of Computer and Emerging Sciences, Karachi, Pakistan
k133501@nu.edu.pk [1] , sheeraz@gmail.com [2] and jawwad.shamsi@nu.edu.pk [3]

ABSTRACT

The effect of network-based malware can be massive on Internet Service Providers (ISPs). Malicious users, that are among the ISP customers, can consume large amount of network bandwidth. This behavior could be overwhelmingly damaging as legitimate ISP users may experience performance degradation or complete denial of service. Subsequently, as network-based malware spreads out, number of malicious users increase, causing distributed denial of service (DDoS) attack. This paper proposes a novel idea of mitigating network-based malwares at ISP level. The proposed solution - ISPMonitor, monitors various traffic patterns to detect the timely onset of malware attack. It detects the attack and applies a mitigation mechanism to protect the ISP network. The ISPMonitor, is a DNS based solution that monitors the rate of DNS lookup requests. An anomaly based approach is used to detect malware. The proposed mechanism was investigated on a live wireless ISP with 80,000 customers spanned across three major cities of Pakistan. Results reveal that this approach was not only highly effective in detecting and mitigating the malicious traffic but also has improved network bandwidth utilization considerably.

KEYWORDS

Network Security, network-based malware, malware detection and mitigation, ISP level mitigation, DDoS attack

1 INTRODUCTION

Malware-based network attacks are capable of causing severe damage. Such attacks have the ability to inadvertently consume a major portion of network bandwidth, by sending large number of network packets to malicious hosts. Consequently, the attack would deny network access to legitimate network traffic. The effect of such an attack could be disastrous for an Internet Service Provider (ISP), as this could consume ISP's bandwidth and deny service to a large number of legitimate users of an ISP.

There could be many types of network-based malicious attacks such as bots, worms etc. However, all of them would have a similar pattern, that is, large number of network packets originating from infected hosts and destined to one or more malicious hosts.

Understandably, effect of such an attack could be more destructive on ISPs. The network traffic generated by infected users could be overwhelming and may disturb the capacity and planning of an ISP. For instance, ISPs allocate network bandwidth in order to meet expected quality of service (QoS) requirements of users. They also utilize idle resources of inactive users in order to efficiently manage their resources. However, in case of malware attacks originating from malicious users, network bandwidth may be consumed excessively. Specifically, assuming that the infected user is inactive, the malware still continue to use ISP resources by generating false traffic. Subsequently, denial of service may be experienced by legitimate users. This implies that it will become difficult for ISPs to provide assurance of QoS to their users which may lead to revenue loss[1] . Therefore, various malicious attacks on the Internet service providers (ISP) has been a major concern[2][3][4].

Though, various solutions have been explored to overcome this problem, network based malware such as botnets, still remains one of the most significant threats to the Internet [5] . DDoS Threat Landscape reported over twelve million botnet-let DDoS attack per week [6]. Malware mitigation is profoundly dependent on the end user security behavior. Risky security behavior is not obvious to end users and as a consequence devices become vulnerable. Using outdated and un-patched operating system and other vulnerable software utilities, such as freeware and shareware, makes the device an easy target for attackers. Controlling user's behavior is however not possible in an environment where users own their devices.

During our study and analysis of a major ISP in Pakistan, we observed that there are a large number of malicious and infected users with in the ISP. These users consume enormous network bandwidth originating from malicious hosts leading to inefficient utilization of network resources and performance degradation.

In this paper, we are motivated by the above mentioned problem. To this end, we focus on detection and mitigation of network-based malware at ISP-level and propose an effective framework. Our proposed solution, - ISPMonitor, utilizes DNS based, efficient and cost effective technique that can be deployed by any ISP to suppress the malicious traffic generated from network-based malware. ISPMonitor detects the malicious traffic by monitoring the rate of DNS traffic generated by a user. ISPMonitor is able to detect zero day vulnerabilities and DNS Fast flux attack.

ISPMonitor was deployed and tested in a wireless ISP having around eighty thousand customers across three major cities of Pakistan. Results reveal that network-based malware traffic is not only successfully detected but also mitigated - leading to improved utilization of network bandwidth. By denying access to malicious traffic, legitimate users were able to utilize the available bandwidth fully, decreasing denial of service attacks. Briefly, ISPMonitor focuses on:

- Detection and mitigation from network-based malware attack at a control point, that is, ISP
- Effective utilization of network resources
- Detection of zero day vulnerabilities
- Prevention against fast flux DNS attack

The rest of the paper is structured as follows. Section II presents brief overview of background and related work, followed by section III that discusses the proposed solution. Detailed results and observation after the deployment of solution are covered in section IV. Section V concludes the paper, highlighting the significance of this work and suggesting future directions.

2 BACKGROUND AND RELATED WORK

The purpose of this section is to present background information relevant to our work. The section also highlights the signification research related to DDoS attack detection and mitigation.

2.1 Background

Spectrum provided to Wireless Internet Service Providers (ISP) by state governed authorities is a most valuable asset of an organization. ISPs makes an all-out effort to enhance the spectral efficiency using various methods. ISPs usually allocate more channel bandwidth for downlink as compared to uplink due to inherent downloading requirements. However, in case of malware-affected users, this provisioning may not work effectively. Home users and small businesses users typically maintain inadequate level of security which makes them a soft target for attackers. Infected devices, may continue to send malicious traffic thereby consuming both the uplink and downlink channels of an ISP.

The effect of this behavior could be drastic as legitimate traffic may be denied and ISP users may experience denial of service[7]. The ISP-level mitigation of network-based malware is critical due to the overwhelming control ISPs possess over their customers.[2][8]

In wireless ISP setup - idle mode of a device, could be effective in conserving the spectral efficiency for the wireless medium [9]. Wireless broadband network uses IEEE 802.16e WiMAX standard. One of the features provided by the WiMAX standard developers to save radio resources is idle mode [10]. A subscriber can go idle, i.e. a time when no Internet activity is performed by the end user. Idle mode leads to efficient power management. Power amplifier of the subscriber terminal is switched off in idle mode, saving battery life of terminal. Using idle mode can also avoid excessive and unnecessary uplink transmission. This helps in reducing interference due to co-channel reuse of frequency. At ISP level, idle mode configuration helps in saving per subscriber resources such as dedicated traffic uplink and downlink channel. However, when a device enters the idle mode, it periodically check for broadcast messages sent by the base station to see any downlink frames that have been sent to it [11].

Today, in many cases, the attackers compromise the devices owned by home internet users and small businesses who are unaware of the fact that their devices have been compromised. These compromised devices generate malicious traffic creating a critical problem for ISPs. For instance, wireless ISPs with malicious users will not be able to take advantage of WiMAX idle mode as the compromised devices will continue to send malicious traffic wasting the ISP resources and leading to service degradation.

2.2 Related work

Studies suggests that infected end user machines of home users and small and medium size enterprise (SME) users are major source of security vulnerabilities[7],[12]. Providing an ISP-level solution is significant for the security of such users. The role of ISPs in detecting and mitigating the botnet attack is presented by Micheal et al. [13]. Considering ISPs as an important control point in mitigation of botnet attack, the study is based on the empirical analysis of spam generated by ISP. Stalmans and Irwin [14] proposed a framework for DNS based detection and mitigation of malware infections on a network in which they classify domains as either potentially malicious or legitimate. They treated domain classification problem as a binary classification problem. Leyla Bilge et al. [15] introduced a system which is referred to as EXPOSURE to detect domains with malicious activities using passive DNS traffic analysis. This is purely based on the characteristics of DNS traffic, it characterizes different DNS names and their querying pattern . The detection of malicious activities after the analysis is not only limited to malware, but domains involved in spamming and phishing are also identified. Manasrah et al. [16] proposed a framework called the BDM (Botnet Detection Mechanism) for botnet detection in a network environment which consists of three phases that capture the DNS traffic, extract MAC address, query name from this DNS packet and store it in the database for further analysis. DNS traffic is classified by BDM according to the behavior. Proposed framework is capable of classifying the domain names into normal and abnormal domain names, consequently, detecting the botnet activity within the network.

The work presented in this paper is inspired by the above mentioned studies, nevertheless, this solution is novel in terms of both efficiency and simplicity. Unlike current work on malware mitigation at ISP level, ISPMonitor is effective for efficient network planning for an ISP. Suppression of malicious network traffic from infected users allows efficient utilization of bandwidth and enhanced utilization of idle mode. ISPMonitor is also capable of

successfully preventing DDoS attacks, as more bandwidth is available for legitimate users, that is, ISP customers. In addition, ISPMonitor is useful for users who do not have adequate level of security mechanisms installed on their devices. Unlike many existing DNS-based techniques of malware mitigation, ISPMonitor is effective against zero-day vulnerabilities as well. It relies on DNS traffic rate to detect malicious behavior. Therefore, new malicious web domains, which are not included in the blacklist, can also be detected. Further, as malicious behavior is identified through hyper activity of users, ISPMonitor can also provide protection against DNS flux attack, that is malicious sites which bypass blacklist based filtering by rapidly changing DNS domains. Table I summarizes the novel contribution of this research.

Table 1. Comparison between ISPMonitor and other solutions

	ISP level mitigation	Finger Printing	Idle mode configuration for efficient bandwidth utilization	Zero day vulnerability detection
[14]	No	No	No	Yes
[15]	Yes	No	No	Yes
[16]	No	No	No	Yes
[19]	Yes	No	No	Yes
[20]	Yes	No	No	Yes
ISPMonitor	Yes	Yes	Yes	Yes

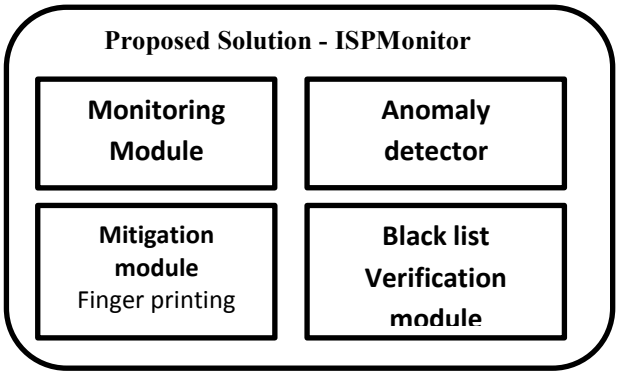


Figure 1: ISPMonitor Modules

3 PROPOSED SOLUTION – ISPMONITOR

Realizing the significance of providing a security mechanism at some control point which is independent of user behavior we propose ISPMonitor– an ISP-level solution for monitoring, detecting, and mitigating network-based malware. It uses anomaly based detection mechanism.

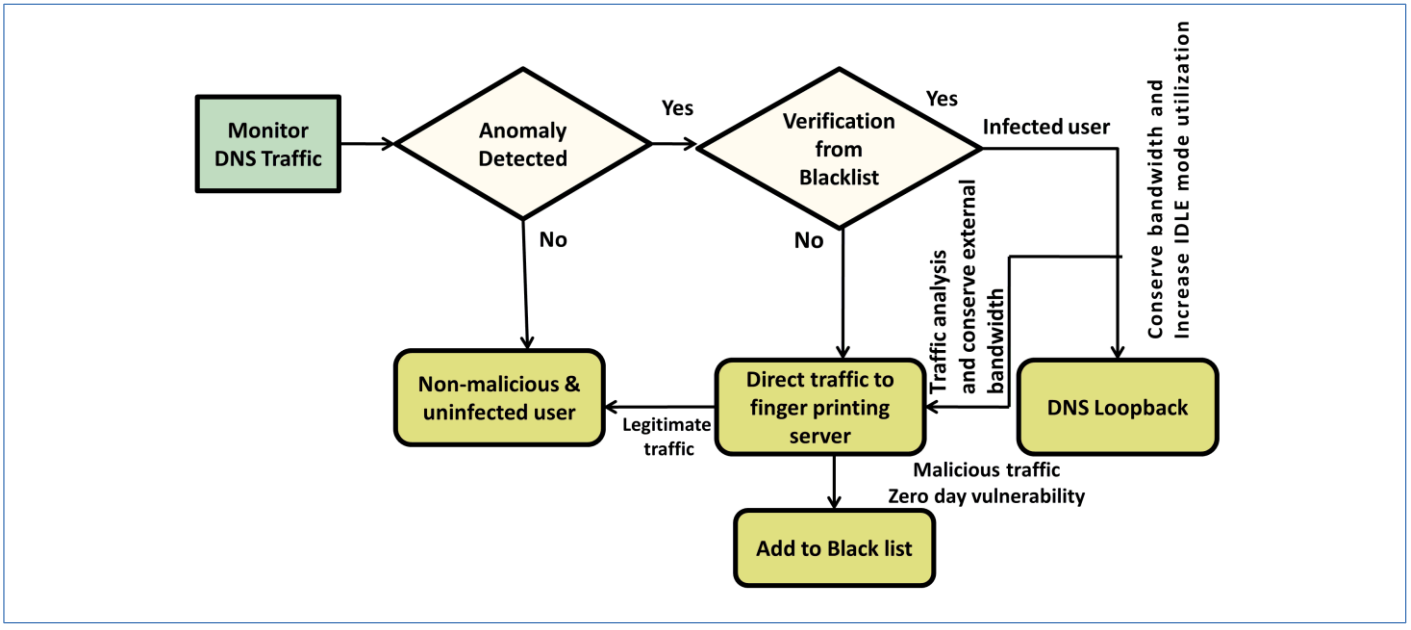


Figure 2: ISPMonitor Process

Figure 1 illustrates the key functionalities of ISPMonitor and figure 2 shows the flow diagram of the system. The 'monitoring module' continuously monitors the DNS traffic and collect statistics. The 'anomaly detector module' notifies any unusual activity from users, such as massive number of DNS requests in short time span. This activity is marked as suspicious and is verified by black list verification module which maintains the list of reported malicious domains [16]. Once verified, the malicious requests are filtered and forwarded to mitigation module. Mitigation module comprises a finger printing (FP) server and DNS loopback mechanism. The malicious traffic is mitigated by redirection ,thereby blocking the illegitimate traffic from exiting the ISP network. This, in turn, saves the uplink bandwidth of an ISP. Also, FP technique is useful for vulnerability analysis of ISP users.

4 RESULTS AND OBSERVATIONS

ISPMonitor was deployed on an existing wireless ISP in Pakistan having around 80,000 live customers. The wireless ISP was providing services in three major cities at the time of deployment. DNS servers were distributed in a way that each city had its own DNS server.

After the deployment of the solution, the malicious activities were detected and mitigated efficiently. The real time data of DNS logs that was collected over the period of time gives some interesting insights. Most of the compromised hosts were the one that either had out of date or unpatched operating systems. Users, generally were not aware that their devices has been compromised and was generating malicious traffic. Hosts, running updated operating systems and antivirus tools were less prone to malware attacks. It was also observed that, comparatively, compromised devices generated high DNS traffic. The data collected for the period of one year shows significant reduction in malicious traffic leading to efficient bandwidth utilization. Effectiveness of ISPmonitor was tested by comparing various network characteristics before and after the deployment. Below are the key results substantiating the significance of this solution.

4.1 Effective Utilization of network resources

Idle mode configuration is beneficial for efficient utilization of spectral efficiency. Resources from idle users are withdrawn and are assigned to active users. Figure 3 illustrates the idle mode requests data for the period of one year. Before the deployment of our solution, average idle mode request by devices was around 46%. However, when ISPMonitor was deployed and malicious traffic from network-based malware was filtered, the average idle mode request by devices increased to 80%. As malicious traffic is prevented from leaving the network, uplink bandwidth of the ISP is utilized more effectively.

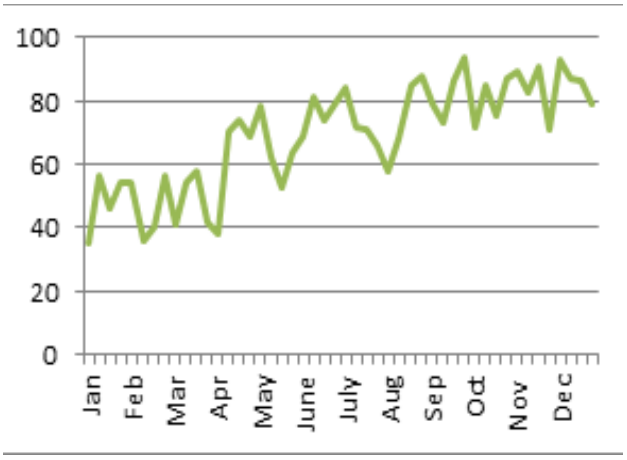


Figure 3: Percent increase in idle mode requests after the deployment of ISPMonitor in April

4.2 Efficient solution- low overhead

The operational cost of ISPMonitor ,in terms of time, was also evaluated. ISPMonitor verifies the DNS query against the black list when an anomaly is reported. The time for serving the DNS requests for cached and un-cached queries was observed. Figure 4 shows the time comparison of minimum, average, and maximum time for lookup requests using DNS

benchmark in milliseconds. The difference is negligible indicating that the cost in terms of time is minimal.

Before deploying ISPMonitor					
180.178.120.100	Min	Avg	Max	Std.Dev	Reliable
- Cached Name	0.000	0.000	0.000	0.000	100.0
- Uncached Name	0.117	0.208	0.452	0.097	100.0
- DotCom Lookup	0.126	0.200	0.278	0.069	100.0
After deploying ISPMonitor					
180.178.120.100	Min	Avg	Max	Std.Dev	Reliable
- Cached Name	0.000	0.004	0.019	0.004	100.0
- Uncached Name	0.127	0.298	1.050	0.176	100.0
- DotCom Lookup	0.129	0.265	0.966	0.177	100.0

Figure 4: Comparison of minimum, average, and maximum time for lookup requests using DNS Benchmark in milliseconds

4.3 Effective prevention from DoS attacks

After the deployment of ISPMonitor, DoS attack on the ISP servers reduced considerably. As malicious traffic is blocked, network bandwidth and other resources are fully available to legitimate users. Consequently, DoS attacks on ISP server were reduced substantially. Figure 5 shows the reduction rate of 60%.

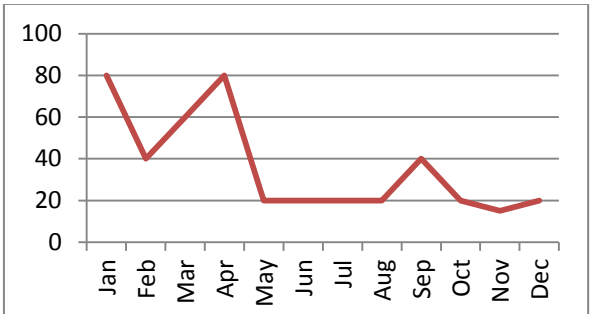


Figure 5: Reduction in DoS attack after deployment of ISPMonitor in April

4.4 Reduction in failed DNS queries

Prior to the deployment of ISPMonitor, it was observed that the ISP's DNS servers were receiving a large number of illegitimate DNS queries, thereby creating a false load on DNS servers causing denial of service to legitimate users. After the deployment of ISPMonior, illegitimate DNS queries were successfully blocked as shown in figure 6. Consequently, average number of failed DNS queries were reduced by 50% leading to efficient performance of DNS server. This improved the response time for the users leading to enhanced performance.

4.5 Prevention against fast flux DNS attack and zero day vulnerability

Fast flux attacks provides anonymity to attackers as they usually use multiple domain names for their activities. ISPMonitor mines the live traffic to discover the high rate of DNS requests from a host, therefore it is able to detect network-based malware using flux networks. Further, any unusual activity detected by anomaly detector module of ISPMonitor, is verified by black list module to confirm the malicious domain. However, if malicious domain is not in the black list, it is sent to FP server for further analysis. This helps in detecting the zero day vulnerability.

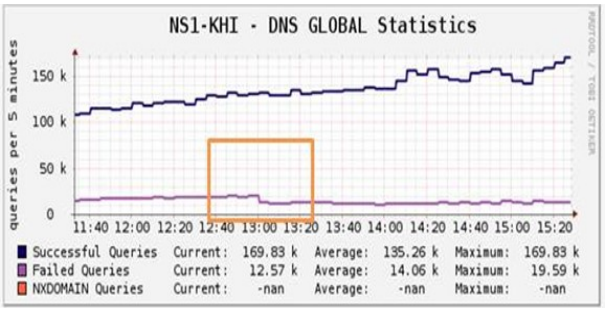


Figure 6: Decrease in failed DNS queries

ISBN: 978-1-941968-34-5 ©2016 SDIWC

4.6 Analysis of malicious users

The finger printing server was used to analyze the characteristics of the infected users. It was observed that majority of the compromised devices had outdated or unpatched operating systems. Specifically, around 45% devices had Windows XP and 20% had Windows 7 installed as shown in figure 7. Many malicious requests were reported from mobile devices running Android operating system . Figure 7 illustrates the complete report logged by finger printing server. The results highlights the fact that device owners negligence makes the devices more vulnerable to attacks.

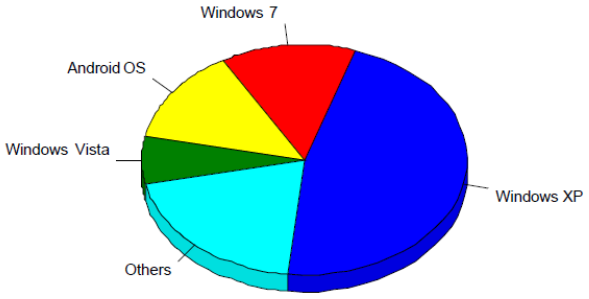


Figure 7: Analysis of infected users

5 CONCLUSION AND FUTURE WORK

ISP-level mitigation of malware is important in effectively utilizing network bandwidth [18]. ISPMonitor is a low-cost solution, which is based on commodity hardware. It is capable of mitigating the inbound DDoS attacks and the outbound malware traffic. The solution was deployed on a wireless ISP having around 80,000 live users across three cities of Pakistan. Results indicate sharp decrease in malicious traffic leading to high utilization of network resources. The significant increase in idle mode entry requests by devices lead to improved utilization of spectral efficiency. The solution is able to protect users from many harmful activities of network-based malware such as data theft, spam [19], user privacy, and access to confidential information. The ISPMonitor is a feasible solution and can be deployed by any ISPs.

Precisely, this does not imply that ISPMonitor is a fool proof system with no false negatives. Network-based malware with low DNS query rates will not be detected by ISPMonitor. However, a novel contribution of this research is to highlight the significance of ISP-level mitigation of network-based malware and illustrate the benefits through live deployment and analysis. An important direction for research is to study patterns of malware traffic in order to better understand the threats. Current solution is implemented with an assumption of single customer premises equipment (CPE) for each user. However, with increase in device technology and with growth in the number of users, the framework can extended as per requirements.

REFERENCES

[1] Y. Y. Heung, “Korea’s Experience of Massive DDoS attacks from botnets.” 2011.

[2] M. O. J. Livingood, N. Mody, “Recommendations for the Remediation of Bots in ISP Networks draft-oreirdan-mody-bot-remediation-16,” Internet Engineering Task Force, no. c, pp. 1–33, 2011.

[3] H. Asghari, “Botnet Mitigation and the Role of ISPs,” 2010.

[4] S. Hofmeyr, T. Moore, S. Forrest, B. Edwards, and G. Stelle, “Modeling Internet-Scale Policies for Cleaning up Malware,” in Workshop on the Economics of Information Security, 2011, p. 13.

[5] Wang, Ping, et al. "Analysis of Peer-to-Peer Botnet Attacks and Defenses." Propagation Phenomena in Real World Networks. Springer International Publishing, 2015. 183-214.

[6] “Lerner, Zach. "Microsoft the Botnet Hunter: The Role of Public-Private Partnerships in Mitigating Botnets." Harv. J. Law & Tec 28 (2014): 237-325..

[7] B. Rowe, D. Wood, D. Reeves, and F. Brain, “The Role of Internet Service Providers in Cyber Security,” no. June, pp. 1–12, 2011.

[8] D. Barroso, "Botnets-the silent threat," European Network and Information Security Agency (ENISA) 15 (2007): 171. 2007.

[9] H. J. Thontadharya, D. Shwetha, M. Subramanya Bhat, and J. T. Devaraju, "Effect of idle mode on power saving in mobile WiMAX network," Advances in Intelligent Systems and Computing, vol. 174 AISC, pp. 491–499, 2013.

[10] S. Ahmadi, "An overview of next-generation mobile WiMAX technology - [WiMAX update]," IEEE Communications Magazine, vol. 47, no. 6. pp. 84–98, 2009.

[11] S. a Ahson and M. Ilyas, Wimax: Standards and Security. 2007.

[12] J. Bauer, M. Van Eeten, and T. Chattopadhyay, "ITU Study on the Financial Aspects of Network Security: Malware and Spam," ICT Applications and Cybersecurity Division, no. July, 2008.

[13] M. Van Eeten, J. M. Bauer, H. Asghari, S. Tabatabaie, and D. Rand, "The Role of Internet Service Providers in Botnet Mitigation An Empirical Analysis Based on Spam Data 1," in Workshop on Economics of Information Security, 2010, vol. 2010/05, pp. 1–31.

[14] E. Stalmans and B. Irwin, "A framework for DNS based detection and mitigation of malware infections on a network," 2011 Information Security for South Africa - Proceedings of the ISSA 2011 Conference, 2011.

[15] L. Bilge, E. Kirda, C. Kruegel, M. Balduzzi, and S. Antipolis, "EXPOSURE : Finding Malicious Domains Using Passive DNS Analysis," Ndss, pp. 1–17, 2011.

[16] A. M. Manasrah, A. Hasan, O. A. Abouabdalla, and S. Ramadass, "Detecting Botnet Activities Based on Abnormal DNS traffic," p. 8, 2009.

[17] J. Lee, J. Kwon, H. J. Shin, and H. Lee, "Tracking multiple C&C botnets by analyzing DNS traffic," 2010 6th IEEE Workshop on Secure Network Protocols, NPSec 2010, pp. 67–72, 2010.

[18] J. A. Morales, A. Al-Bataineh, S. Xu, and R. Sandhu, "Analyzing DNS activities of bot processes," 2009 4th International Conference on Malicious and Unwanted Software, MALWARE 2009, pp. 98–103, 2009.

[19] François, Jérôme, Issam Aib, and Raouf Boutaba. "FireCol: a collaborative protection network for the detection of flooding DDoS attacks." IEEE/ACM Transactions on Networking (TON) 20.6 (2012): 1828-1841.

[20] Sahay, R., Blanc, G., Zhang, Z., & Debar, H. (2015, February). Towards autonomic ddos mitigation using software defined networking. In SENT 2015: NDSS Workshop on Security of Emerging Networking Technologies. Internet society.

[21] Alexiou N, Basagiannis S, Katsaros P, et al (2010) Formal analysis of the Kaminsky DNS cache-poisoning attack using probabilistic model checking. Proceedings of IEEE International Symposium on High Assurance Systems Engineering 94–103. doi: 10.1109/HASE.2010.25

[22] Shamsi, J. A., Hameed, S., Rahman, W., Zuberi, F., Altaf, K., & Amjad, A. (2014, January). Clicksafe: Providing security against clickjacking attacks. In High-Assurance Systems Engineering (HASE), 2014 IEEE 15th International Symposium on (pp. 206-210). IEEE.

[23] Savolainen, S., Ridell, M., Lehtonen, M., & Rathod, P. (2015, September). eGuard. In Computer Science, Computer Engineering, and Social Media (CSCESM), 2015 Second International Conference on (pp. 37-42). IEEE.

[24] Shepherd, Lynsay A., Jacqueline Archibald, and Robert Ian Ferguson. "Perception of risky security behaviour by users: Survey of current approaches." Human Aspects of Information Security, Privacy, and Trust. Springer Berlin Heidelberg, 2013. 176-185.

Command-driven Decentralized Event Processing Approach for Monitoring Networked Android & Windows Devices

Sirojan Tharmakulasingam, Nirushan Rathakrishnan,Nirosh Jayaratnam, Jeyatharsini Jeyaganeshan, Gihan Dias
Department of Computer Science and Engineering, University of Moratuwa.
Kadubedda 10400, Sri Lanka.
{sirojan.11, nirushan.11, nirosh.11, jeyatharsini.11, gihan}@cse.mrt.ac.lk

ABSTRACT

We live in an era where we rely on devices for most of our activities. Organizations use huge amount of devices for their business operations and activities. Those devices are used by different types of personnel where there are no control over their proper usage. In order to ensure their proper usage, the devices should be monitored. Most of these devices used in organizations are connected via network. Monitoring of networked devices require certain amount of resources from devices and network bandwidth based on the transmission of data. Our research mainly focuses on monitoring the networked devices efficiently in terms of required resources and bandwidth. We use decentralized event processing approach in which partial event processing (command-driven, lightweight processing) happens at the devices and remaining processing (complex event processing) happens at the central node where events from all devices are collected. Major objective of command-driven lightweight processing on the devices is to truncate unwanted events for current context of monitoring in order to save the required bandwidth and resource utilization of devices. This paper presents our implemented system for monitoring Windows & Android devices based on this approach and achieved gain in resource utilization and bandwidth.

KEYWORDS

Event Monitoring, Complex Event Processing, Agents, Siddhi, Apache Thrift, Android Devices, Windows Devices

1 INTRODUCTION

Nowadays number of devices in use at organizations and business institutions are exponentially increasing. Each of those devices generates huge collection of events based on the intervention with operator of that device. If an organization wants to ensure the proper usage of their devices, they need to monitor devices by analysing events that are generated by those devices. Since it is not feasible to monitor all the devices separately, organizations need a centralized controller to monitor and control the devices.

The research experiences with monitoring systems over the years show that there is a danger of turning monitoring systems into databases. It seems that collecting and sending events to a central server in the system is often done without analysing whether the data is relevant to the current context of analysing or not. There are some previous researches based on some static pre-processing techniques which are not aware of current context of monitoring. As a consequence, the event processing system requires a huge amount of processing power and network bandwidth for transmission. It also loses its function of providing meaningful information to the current monitoring task. This means that the system needs to be designed in a way that the event data is systematically filtered, collected, checked, aggregated, and used according to the current demand. Experiences have shown that it is very important to develop

such a system in a participatory way, meaning that the outlines, the procedures of the system should be agreed upon by international standards.

The major challenge in implementing such a system is heterogeneity in devices. Devices can be varied based on their hardware, architecture and operating systems. The proposed solution in this paper uses separate agents to run on heterogeneous devices. In general, most of the devices generate huge amount of events with high transaction rates. Therefore huge amount of resources such as memory, processor cycles, and high network bandwidth are needed for storing, processing, and exchanging information between devices and central node. To overcome this issue, agents are used in the proposed solution which are responsible for collecting event data from devices on which they are running and performing command-driven lightweight event processing. These agents should not impose load on the devices. In addition to that, agents should be bandwidth-efficient. Since we are using decentralized event processing approach, agents perform partial, command-driven, lightweight event processing on the devices in order to reduce the load on the devices as well as required bandwidth to send the processed event to central node for further complex processing. As the result of complex event processing at central node, unintentional activities, policy violations and potential threats can be detected.

Our event monitoring system Hydra has been implemented based on the aforementioned approach. Agent and Central Node are the two major components of our system. Agent runs on the device, collects data and event logs, and performs some lightweight processing based on the commands given by Central Node. Since the scope of this research is limited to Windows PCs and Android devices, we have developed two types of agents: Windows agent and Android agent. Central Node acts as a controller of agents and it is also capable of doing complex event processing in order to trigger real time alerts.

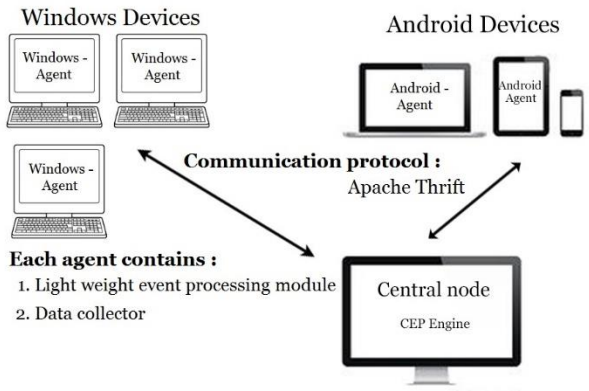


Figure 1. Our Solution

The rest of the paper is organized as follows. Section 2 discusses about some important data & events that can be collected for monitoring of Android Devices. While section 3 discusses about data collection & log collection from Windows devices and outlines some useful events that can be used for monitoring those devices, section 4 describes our command driven light weight processing approach that we used in our Android agent and Windows agent. Section 5 provides the outline of our central node implementation details. Section 6 contains the discussion about communication protocol that we used to establish communication between agents and central node. Section 7 summarizes the experimental results of the implemented system and presents some sample scenarios where our system can be used. The final section 8 provides an outlook to future directions of this research.

2 ANDROID DATA COLLECTION

Mobile devices usage is rising exponentially in today's business context. Google, Apple, Research in Motion (RIM), and Microsoft are the major players in the mobile device market. A survey says that, Google Android ranked as the top smartphone platform with 82.8% market share in 2015 [1]. Research In Motion (RIM) is

an exception as corporate customers can deploy a BlackBerry Enterprise Server and setup their devices to send mobile data to the central server so that central server will collect and do an analysis. Most of the organizations consider transitioning from RIM to new smartphone systems which in turns strengthen the requirement of a monitoring system for mobile devices.

As per the emerging requirement in monitoring the mobile devices, first requirement is to collect the important events and data from mobile devices which could be useful in monitoring. In our research, we limited our scope to Android devices since they cover a major portion in mobile device usage.

Application installation/removal, browser navigation, browser search, calendar event, call log, contact list, device accounts, device ID, GPS location, MMS, picture gallery, screen lock status, SMS and third-party application logs are the events collected for Android forensics [2].

In the latest Android versions (Jelly Bean or higher), third party applications are not allowed to access Android log files without root access. In addition to the above-mentioned data, we collected running processes list and their resource utilization such as CPU usage, RAM usage, and network usage. Along with that, we also focused on collecting the available sensor data. All these collected data will be sent through a lightweight processing module which is controlled by the commands given by the central node. After the partial processing, if the network connection is available then partially processed data will be sent to the central node. Else, it will be locally stored in a SQLite database. Locally stored data will eventually reach the central node when the connection becomes available. This approach prevents event losses if there is a network interruption between agent and central node.

3 WINDOWS DATA COLLECTION

In Windows, performance counters can be used to collect information about the performance of operating system, applications, services, and drivers. There are roughly one thousand performance counters that together reflect the current state of the system. Those performance counters can be accessed using Windows registry API. Since working directly with the registry is too complex, Microsoft provides a more abstract API called Performance Data Helper (PDH) which can be used to access performance counters. PDH is responsible to access the performance counters in the registry and the conversion of their raw values into appropriate numbers.

The registry collects values from performance counters using kernel and makes them accessible directly or using Performance Data Helper (PDH) library. A research team has built a system named WatchTower using PDH. WatchTower is a system that simplifies the collection of Windows performance data for monitoring and usage profiling of Windows machines. Their approach towards this large amount of data is to treat it as a dimensionality reduction problem, where each counter corresponds to a dimension [3]. The major problem of this approach is that only performance data is considered to build a monitoring tool and their dimensionality reduction technique is static. The dimensions are already predefined without the awareness of real-time monitoring task. Our system Hydra collects Windows event logs in addition to performance data such as running processes, and their CPU, memory, and network usage, total CPU, memory, and network usages using PDH library for precise monitoring. Collecting performance data using PDH library is reliable and less overhead. In contrast to their approach, our solution is dynamic (context-aware) which uses command-driven processing. Because of this dynamic nature, agents only send the relevant data to the central node. This increases

the accuracy of monitoring tasks as well as improves the efficiency of the system in terms of resource utilization.

3.1 Windows Log Collection

Event logging is significant to detect errors, to find out the cause behind the error, and to prevent the error from recurring. The event logging service receives events from various sources and stores them in a single collection called an event log [4]. Monitoring and analysing of event logs should be automated to make system administrators' life easy since the number of Windows event logs has grown over the years [5].

Windows provides facility in Event Viewer to setup own Event Log Notification System for automation to export and to filter log entries and then to email or save it in a text file. It is inadequate for monitoring large size network because it only supports limited static functionalities. Since it is configured using static scripts, there is no awareness about current monitoring task in the process of log collection. This leads to a chance that irrelevant logs for the current analysis also get collected and it will be sent through the network. Because of this, bandwidth usage of system is high and human intervention is heavily required for detailed analysis. In contrast, our solution tries to minimize the required bandwidth and human intervention by having command-driven context-aware log collection and complex event processing techniques such as pattern matching respectively.

There are two identified alternatives to collect logs from Windows. Logs can be collected in binary format from unallocated space or using Event Logging API from allocated space. Polling log data at regular intervals from allocated space using programming interface immediately after logging of events is preferred over getting logs from unallocated space. Because getting logs earlier helps to predict some bad outcomes before they occur or at least immediately after their occurrence. So our agent uses Event Logging API to automate the process of collecting of events.

Centralized collection of log data from Windows PCs is important because processing event logs on local machine is not safe due to intensive or non-intensive failures of local machines. P. K.Sahoo, R. K. Chottray and S. Pattnaiak [6] have proposed a solution to centralize event logs. Their system retrieves Windows event logs, translates them to Syslog format, and sends to a central server. It stores in a database after processing them based on a set of rules that specified in the Winsyslog configuration. Syslog messages can be displayed by Windows GUI and reports are generated automatically based on data from database by "monitor ware console". Above solution requires more bandwidth as it sends all the logs without doing any processing in order to reduce its size. In their research, centrally collected logs are only used to generate some reports regarding the statistical information of the collected logs. However, those collected logs can be utilized to detect unintended activities and any kind of policy violations by doing further processing. In our solution, we process those collected logs partially on agents based on central node commands and then partially processed logs are transferred to central node for complex event processing in order to detect anomalies.

Stephan Grell and Olivier Nano [7] have implemented a system to monitor large scale internet services using central node with Complex Event Processing Engine(CEP) as it is able to do fast and real time in-memory processing of events (filtering, grouping and aggregating) as long as resource consumption are kept within limits. In our solution also, a CEP engine is used at central node for complex event processing and lightweight processing engines are used in distributed agents. We limit the resource consumption of distributed devices by switching central node commands based on

resource availability of networked devices. For instance, once the remote device is running out of resources we skip processing on that device and do entire processing in the central node. In our solution, load is dynamically balanced by central node commands.

Even though events are processed on the distributed nodes in the solution of Stephan Grell and Olivier Nano [7], processing is done without knowing the current demand or context. But in our solution, central node sends command which consists the events to be considered and summarization level to process events in dynamic manner based on the current demand as well as restrictions. Our agents are capable of handling those commands and they can provide data as per those commands. This is the main value addition in our product.

3.2 Useful Events for Analysis in Windows Logs

Each event can be categorized under one of the five event types: error, warning, information, success audit, and failure audit. Events marked as errors and warning are more important than other categories for analysis purpose.

Spotting the Adversary with Windows Event Log Monitoring [8] recommends some important events to be collected that can be helpful in monitoring devices. It identifies some suspicious event IDs related with events of application whitelisting, application crashes, system or service failures, Windows update errors, Windows firewall, clearing event logs, software and service installation, account usage, kernel driver signing, group policy errors, Windows defender activities, mobile device activities, external media detection, printing services, pass the hash detection, and remote desktop logon detection. In our research, we make use of those events while collecting and detecting unusual events.

Russ Anthony [9] talks about some of important observations related with process creation events which can be useful for monitoring devices. Even though process creation seems to be not important due to the high frequency of its occurrence, it is important to identify the process names for long string of empty spaces, misspelled words, and non-standard path in order to detect suspicious processes. Other than that he talks about events related to privilege escalation which is also very useful since this might be an entry step for an attack or violation.

As stated in this section, these are some of the useful events considered in our solution, which are useful in detecting policy violations, intellectual property theft, misuse, and any attack simulations.

4 COMMAND-DRIVEN LIGHTWEIGHT PROCESSING

Processing events in a resource constrained environment is the major challenge which should be addressed here. Since the devices have limited resources and capabilities, a special care is needed in designing of event processing module. Because of this we have designed lightweight, bandwidth-aware and resource utilization-aware event processing modules for agents which can be controlled by commands given by central node. Because of the awareness about bandwidth and resource utilization, event processing plan is switched time to time in the devices based on the resource availability and demand. In order to have this awareness, central node continuously monitors resource utilization of connected devices and sends commands to agents based on that. For instance, event processing on some devices can be completely skipped especially when resource utilization is high in those devices and high-bandwidth is available to transmit data. This kind of dynamic adjustment is possible in our system since we use command-driven approach and distributed event processing between remote devices and central node based on load.

In our agent-based system, agents run on devices that need to be monitored. Agents consist of a data collector designed for a particular platform and a lightweight event processing engine. Other than the agents, we are having central node which is dedicated for complex event processing and event analysis. Since commands are dynamically sent to agents from central node, our lightweight processing modules in the agents need to act based on those commands and get back the results to central node. So our lightweight processing modules are designed in such a way that we can deploy dynamic commands. Based on the deployed commands, our agents collect specified events, perform processing at a specified level, and send those partially processed events to central node for further analysis. Since all the connected agents are fully controlled by central node commands, the output of the agents are very relevant to current monitoring task, and as a result of that, irrelevant resource consumptions can be avoided.

4.1 Command-driven Lightweight Processing on Android Agent

Command-driven pre-processing module of Android agent is written in Java. Since we collect a bunch of data from Android devices as mentioned in section 2 of this paper, there is a demand to reduce the size of data that needs to be transferred to the central node in order to reduce the required bandwidth. A lightweight command-driven module is included in the agent to achieve this demand.

The lightweight processing engine of Android agent is capable of filtering and aggregating data based on the given filtering parameters and aggregation time limit respectively. These parameters are given by central node commands based on the current demand of monitoring tasks. Based on these parameters the partial processing happens on android devices in order to reduce the size of data that need to be transferred, and then partially processed data is transferred to central node for further analysis.

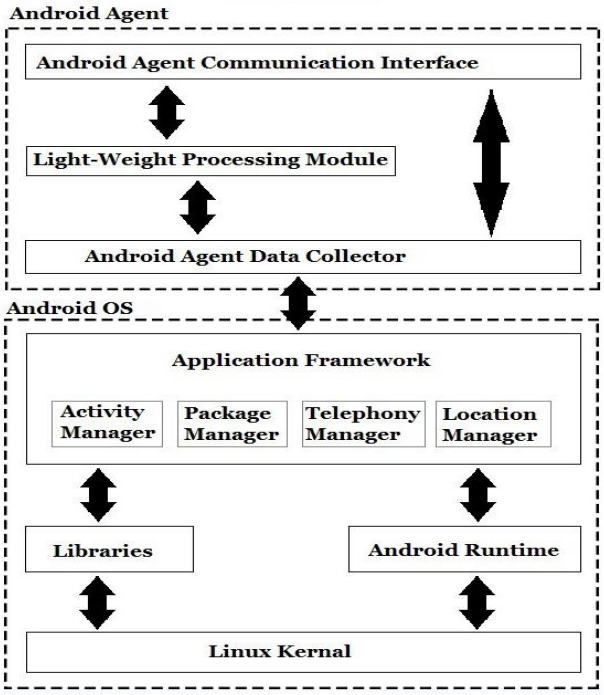


Figure 2. High level architecture of Android Agent

4.2 Command-driven Lightweight Processing on Windows Agent

Command-driven pre-processing module of Windows agent is written in C++. Since C++ is the native language for Windows platform, it is very easy to access the native APIs for event collection. It increases the performance of the agent and reduces load on the device.

The lightweight processing engine in Windows agent also has same features as Android agent in order to process the performance data collected from Windows. In addition to performance data, we also collect log data from Windows devices. In Android devices, we can't collect logs of third party application due to the restriction in the latest Android versions. Pre-processing of log data is also a prominent task that needs to be done since the size of the log file is large. It will take huge bandwidth to transfer as raw data to the central node. Therefore, only the relevant events which specified in the previous section

should be extracted out efficiently from the log files and transferred to the central node.

As per the discussion above, our lightweight processing module of Windows agent can do different levels of summarization. Summarization of event logs uses the information and attribute hierarchy of event logs. Event logs may contain information related to provider, object, subject, network, layer, filter, change, callout, application, access request, rules, errors, processes, logon type, impersonation level, account for which logon failed, failures, new logon and detailed authentication. All of these information have their own attributes. Based on the importance level, some of the information are dropped during high level summarization and some of the attributes are dropped during medium level summarization. Attributes or information to be dropped have been determined from previous researches. Attributes or information to be dropped is determined with the help of previous researches. Attributes or information which are highlighted in the analysis can't be dropped even in high level summarization. Low informative details can be dropped during the processing on devices since they are less important for analysis. It saves required bandwidth by only sending the content-rich information to the central node.

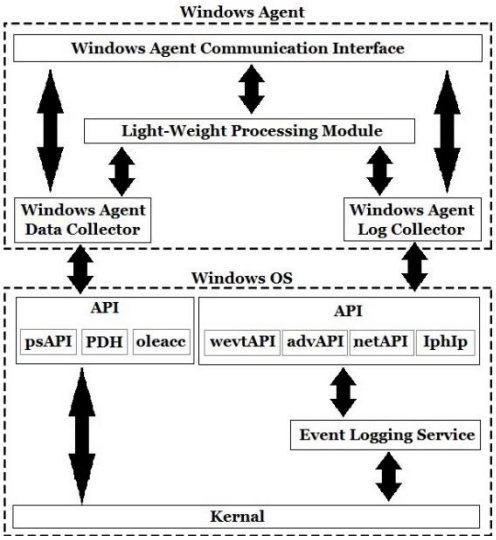


Figure 3. High level architecture of Windows Agent

5 CENTRAL NODE

This is a central instance which includes a complex event processing engine, registration module for remote devices, and bandwidth plus resource aware command application module. It contains an embedded database where the rules for the complex event processing engine can be persisted. Each module is allocated for their own set of responsibilities. Device registration module keeps track of registered devices as well as the connections regardless of the mobility of those devices. Command application module continuously keeps track of the available bandwidth for each connection and resource utilization of remote devices. Based on those contexts, it switches the commands that are sent to remote agents. Based on received commands, agents crawl data from remote devices and partially process it and send it as an event stream to the central node.

The data stream which is pushed by agents from remote devices is directly fed into CEP Engine in the central node. We found Siddhi [10] and Esper [11] are the two CEP engines which provide required functionalities for Complex event processing. While Esper has restricted some features in commercial license Siddhi is fully open source application. In addition to that, Siddhi performs much better than Esper in terms of throughput [12]. Siddhi also provides CEP query support. We can send events using Apache Thrift [13], web services, Java message service, and emails. Because of these competitive advantages of Siddhi over Esper, we use Siddhi engine for complex event processing in our central node.

Central node is facilitated with user interface to write the CEP rules for the engine as well as to configure the event processing parameters for the agents in order to do the analysis with the objective of detecting policy violations, intellectual property theft, misuse, embezzlement, sabotage, and espionage. By writing custom rules and patterns, device

monitoring can be conducted with reduced utilization of resources, which is the major objective of this research.

There are four major alternatives in the event processing commands that are chosen by central node based on the available bandwidth and resources.

		Available Resources in Remote Devices	
		Low	**High**
Available Bandwidth	**Low**	Skip processing at devices, Send predefined critical events only	Allow significant amount of processing at devices
	High	Skip processing at devices and send all events	Allow user defined commands

Table 1. Alternative Event Processing Plans & Conditions

6 COMMUNICATION PROTOCOL

Since this product is most concerned with performance and efficiency, native programing languages are used to develop the agents. Windows Agent is developed in C++ and Android Java is used to develop Android agent. The central node is developed using Java. Therefore, a standard cross platform communication protocol is required in order to establish the communication between the agents and central node for command and data transmissions.

Remote Procedure Calls (RPC) can be used to establish the communications between the agents and the central node. Apache Thrift [13] software framework is used to build RPC servers and clients that will help to communicate seamlessly across programming languages. This enables the server side to be written in Java, when one client is written in C++ to run on windows platform and other client is written in Android Java to run on Android platform. There are several alternatives for Apache thrift such as Protocol buffers [14], JSON-RPC [15] and Avro [16]. In contrast to the Apache Thrift, Protocol buffers doesn't generate ready to use servers. JSON-RPC has a significant amount of communication overhead than Apache thrift. Error handling and extensibility support are also good in Apache thrift than Avro. These comprehensive advantages of Apache thrift make it fit for our monitoring system.

7 EXPERIMENTAL RESULTS

We deployed our agents in a lab and continuously profiling its resource utilization. The below graphs show the average utilization of resources at the remote nodes by agents.

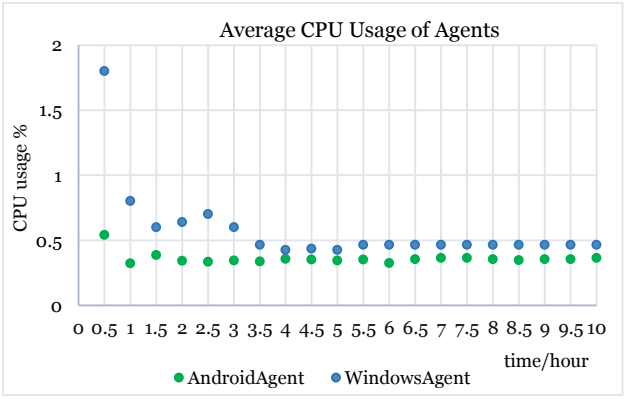


Figure 4. Average CPU usage of agents

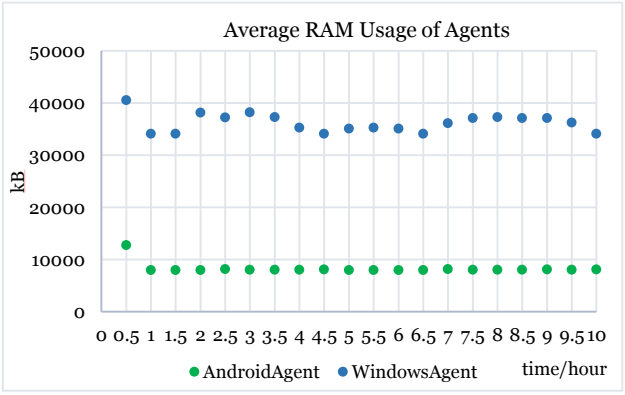


Figure 5. Average RAM usage of agents

CPU & RAM utilization by agents seems to be fair because those are very small fragments of available resources. RAM usage is a bit high for Windows agent since we process both log data and performance data where in Android agent we only consider performance and sensor data.

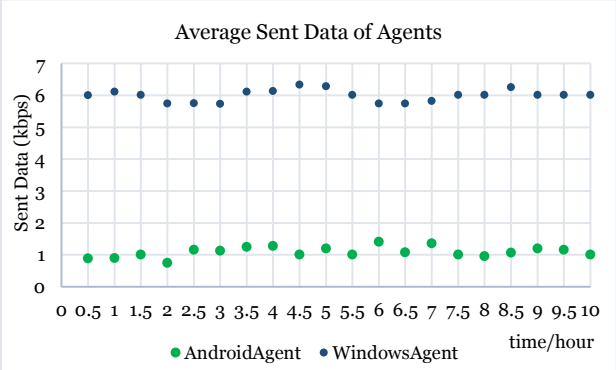


Figure 6. Average sent data from agents

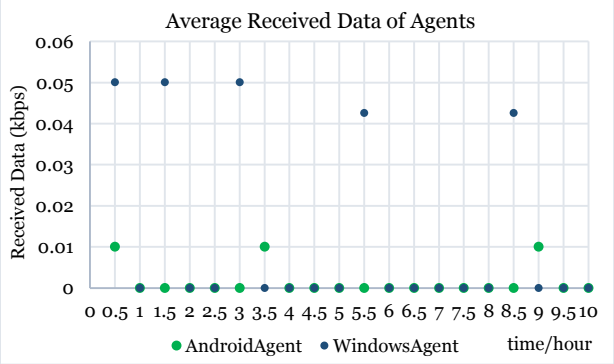


Figure 7. Average received data to agents

Send & received data also seems to be fair because it only requires very little amount of bandwidth compared to other existing systems. Send & received data is a bit high for Windows agent since we send the processed log data as mentioned above. The above graph shows the data reduction due to the partial processing on remote devices. If partial processing is not performed in remote devices, the required bandwidth becomes significantly high due to high data transfer. So, using command-driven decentralized event processing approach gives significant gain in resource utilization and bandwidth consumptions.

We deployed our Windows agent onto 10 Windows PCs at the university lab and monitored important events for 5 days. The graph below shows the statistics.

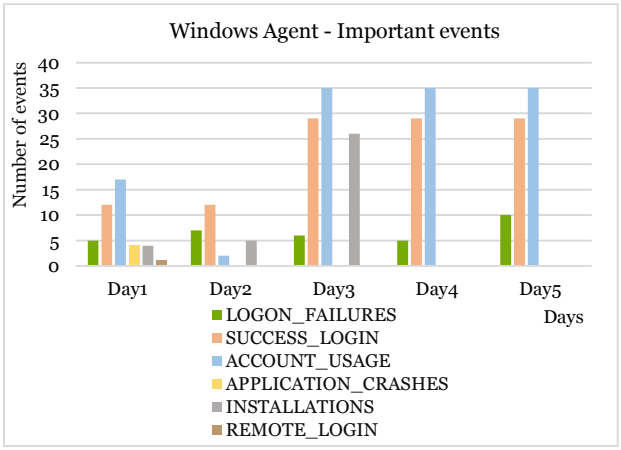


Figure 8. Important events detected

These are some important events which are detected by Windows agent during 5 days. Agents are capable of detecting these kind of important events based on central node commands and transfer them to central node for further analysis. When our system is asked to detect any policy violations or unintentional activities, it uses these important event collection to detect the anomalies.

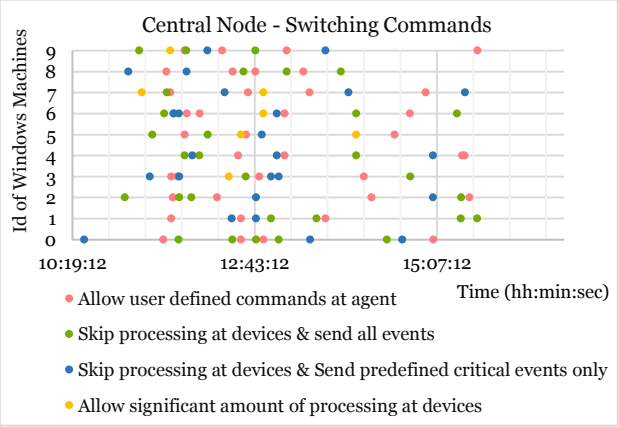


Figure 9. Statistics of Central Node commands switching

The graph above shows the statistics of different commands sent by the central node over time based on the available network bandwidth and

resource availability in the remote devices. Since our system itself can dynamically adjust, it could be able to use the available resources efficiently in order to achieve its monitoring tasks.

7.1 Example Application Scenarios

Our system can be used in detection of any attack simulation. We simulated a Denial of Service (DoS Attack) which is an attempt to make a computer resource unavailable to its intended users. In our case, we have detected UDP flood attack using our system. UDP flood is based on sending the overwhelming number of UDP packets to random ports on a remote host. We have used LOIC Tool [17] to perform the UDP flood attack. The tool takes the IP of the target machine and performs the attack. We have mounted the attack on port 80 since firewalls cannot prevent that attack because they can't distinguish good traffic from DoS attack traffic. Our system can detect these kind of attacks by monitoring the network traffic pattern continuously via agents and alert if there is an anomaly detected.

Let's consider another scenario where an online exam is conducted in a university. Students are not permitted to access any lecture notes (via power point slides or pdf documents). In order to monitor any violations, we can simply write a rule in our central node such that if an agent notifies any foreground processes other than one web browser or more than one tab is used in that web browser then our system detects that as a violation of the specified rule and fires a real time alert.

Since complex event processing engine is provided with Event Processing Language (EPL) which is a declarative language for dealing with high frequency time-based event data, we could be able to write customized rules (Organization policies, suspicious event patterns) based on our requirements. Then our system will alert any violations on deployed rules.

8 FUTURE WORK

Future research on this event processing system includes development of agents for other platforms such as Linux, Mac, iOS and IoT (Internet of Things) devices as same as already developed for Windows and Android agents. Those agents should be compatible with the existing protocol. Since our communication protocol is Apache thrift and it supports cross platform communication, the extension of this solution to other platforms will not be a rough task to do.

Machine learning assisted rule generation module can be added in the central node. Since we are having light weight processing engine in the agents and complex event processing engine in the central node, it will be better to have such an automated rule generation module. This will be an additional step up in the journey of automated monitoring of devices in a distributed environment.

9 CONCLUSION

The system developed through this research serves as a prototype for monitoring system in a distributed environment. The major objective of this research is to develop agents which can survive in resource constraint environment and provide the relevant data based on the current context instructed by the central node. From the collected data we could be able to detect some policy violations, attack simulations, and misuse of resources. Since we collect data from native APIs of Windows and Android as much as possible, this research also serves as a guide for accessing the data through native APIs. Presence of complex event processing technology enhances the real time monitoring since it is a convenient technology to process events and discover complex patterns among multiple streams of event data through filtering, grouping, aggregating the event streams. In this Post-PC era, it is very much useful to have such

automated monitoring systems to detect the unintended activities.

REFERENCES

[1] IDC Research, Smartphone OS Market Share, 2015 Q2 [Online]. Available: http://www.idc.com/prodserv/ smartphone-os-market-share.jsp.

[2] J. Grover, "Android forensics: Automated data collection and reporting from a mobile device," Digital Investigation, vol. 10, pp. S12–S20, 2013.

[3] M. Knop, J. Schopf, and P. Dinda, "Windows Performance Monitoring and Data Reduction using WatchTower," Proceeding 11th IEEE Symp. High-Performance Distrib. Comput., pp. 1–14, 2002.

[4] Microsoft Corporation, Windows API Index [Online]. Available: https://msdn.microsoft.com/en-us/ library/ windows/desktop/ ff818516(v=vs.85).aspx.

[5] M. D. Mullinix, "An Analysis of Microsoft Event Logs", December 2013.

[6] P. K.Sahoo, R. K. Chottray, and S. Pattnaiak, "Research Issues on Windows Event Log," Int. J. Comput. Appl., vol. 41, no. 19, pp. 40–48, 2012.

[7] S. Grell and O. Nano, "Experimenting with complex event processing for large scale Internet services monitoring," Complex Event Processing for the future, 2008.

[8] Network Components and Applications Division, National Security Agency, United States of America, 'Spotting the Adversary with Windows Event Log Monitoring'. [Online]. Available: https://cryptome.org/ 2014/01/nsa-windows-event.pdf.

[9] Russ Anthony, "Detecting Security Incidents Using Windows Workstation Event Logs," SANS Institute, June. 2013.

[10] Sriskandarajah Suhothayan, Isuru Loku Narangoda, Subash Chaturanga. "Siddhi-CEP - high performance complex event processing engine," 2011.

[11] A. Mathew, "Benchmarking of Complex Event Processing Engine – Esper," 2014.

[12] Sriskandarajah Suhothayan, Isuru Loku Narangoda, Subash Chaturanga. "Siddhi: A Second Look at Complex Event Processing Architectures," November 2011 ACM 978-1-4503-1123-6/11/1.

[13] Randy Abernethy. The Programmer's Guide to Apache Thrift. MEAP12.Manning Publications, 2015.

[14] Google Inc, Protocol Buffers: What Are Protocol Buffers? GOOGLE. Google Developers [Online]. April 2, 2012. Available: https://developers.google.com/protocol-buffers/.

[15] JSON-RPC Working Group. (2013) JSON – RPC: Specifications. JSON-RPC Google Group [Online] Available: http://www.jsonrpc.org/specification.

[16] Jim Scott, "Avro – More Than Just A Serialization Framework", Chicago Hadoop Users Group, April 2012. [Online]. Available: https://vimeo.com/ 40776630.

[17] Verma, Deepanker. "LOIC (Low Orbit Ion Cannon) - DOS Attacking Tool - Infosec Resources". InfoSec Resources. N.p., 2011. Web. 23 Jan. 2016. Available: http://resources.infosecinstitute.com/loic-dos-attacking-tool/

Modern Windows Server Operating Systems Vulnerabilities

Theodoros Arambatzis, Ioannis Lazaridis, Sotirios Pouros
AMC Metropolitan College
14th El. Venizelou Str., 54624, Thessaloniki, Greece
t.arambatzis@outlook.com

ABSTRACT

The scientific paper identifies the vulnerabilities in modern Windows Server Operating Systems. Contemporary tools, which can be found on the Internet, have been used in order to provide statistical and quantitative evidence regarding vulnerabilities in most Windows server OS ranging from Windows Server 2003 to Windows Server 2016. Two scanning methods are implemented, each with three vulnerability scanners. These scanners reveal the plethora of vulnerabilities and the efficiency of the released service packs. The conclusions from the comparison between various vulnerability scanners are presented.

KEYWORDS

Vulnerability Assessment, Vulnerability Scanning, Nessus, Nexpose, OpenVAS, Windows Server, Vulnerability Scanner

1 INTRODUCTION

Certain criteria, regarding security flaws in a computer system, compose the vulnerability assessment definition. The criteria are: identification, definition, quantification, classification and prioritization. A vulnerability assessment reveals the severity of a risk in a computer system. Furthermore, an assessment may predict the effectiveness of countermeasures and evaluate their significance after being examined [1-8].
Vulnerability scanning is an automated process targeted to computer systems associated with a network environment. The scanner opens TCP/UDP ports, interprets malware sensitivity level and tries to identify misconfigured security settings. Moreover, the system's response is being audited. A report is extracted in order to provide the procedure details including the results of the assessment for the security manager to assess [9-13].
This research is the continuation of a previous work [14] that presented quantitative evidence regarding Windows client operating systems.

2 METHODOLOGY

The paper provides results on detected vulnerabilities of the most commonly used Windows server operating systems. The methodology incorporates a real life scenario [15]. The assessment took place with three well known vulnerability scanners, which are freely available online. Licenses were obtained in order for Nessus and Nexpose to be installed respectively, while OpenVAS was already preinstalled in a Kali Linux environment.

2.1 Operating Systems

The server operating systems examined in the vulnerability assessment scenarios include a Technical Preview of Windows Server 2016 and a wide range of Service Packs. Windows Server 2003 has also been included and it can still be found across many computer systems [16], even though it is extremely not advised. The examined operating systems are listed in the table below.

Table 1. Windows Server Operating Systems

Windows Server OS	Service Packs	Architecture
2003 Enterprise	0, 1, 2, R2	x64
2008 Enterprise	0 (SP1), 2, R2	x64
2012 Datacenter	0, R2	x64
2016 Technical Preview	2	x64

2.2 Vulnerability Scanners

The vulnerability scanners used are available without any cost. The three vulnerability scanners [17-20] are listed in the table below.

Table 2. Vulnerability Scanners

Distributor	Name	Version	Edition
Tenable	Nessus	6.3.7 x64	Home
Rapid7	Nexpose	5.15.1 x64	Community
Open Source	OpenVAS	8 x64	-

2.3 Workbench

One of the personal computers, used in the research, was a notebook with the following specifications:

- Fujitsu AH530/HD6 Machine
- Intel Core i5 460M @2.53GHz Processor
- 8GB DDR3 1066MHz System Memory
- Kali Linux 1.1.0a x64 Operating System

Within Kali Linux 1.1.0a, three vulnerability scanners were installed (Nessus, Nexpose and OpenVAS).

The second computer used was a desktop with the following specifications:

- Intel Core i7 4790K @4GHz Processor
- 16GB DDR3 1600MHz System Memory
- Windows 8.1 Pro x64 Operating System

Additionally, the VMware Workstation 11 was installed. The program provides the capability of loading an image file containing an operating system. The two computers were operating in a LAN.

2.4 Implementation

While adjusting the applicable settings for each vulnerability scanner, a bootable image containing an operating system was loaded with the following settings: one processor, variable amount of RAM ranging from 1GB to 4GB, variable amount of storage ranging from 40GB to 80GB and a bridged network connection. Once the operating system was fully virtually installed with adequate virtual hardware available the firewall was disabled on each operating system.
This kind of action, to temporary disable the firewall is very common in a vulnerability assessment, as long as it is being performed under full control and awareness.
The vulnerability scanners conducted a basic scan and an advanced scan. The basic scan settings were slightly different in each tool due to the different settings approach of the creators. Therefore, all three applications had to have their settings tuned, in order to scan a target in a similar way. The advanced scan has every possible setting included for the conduction of the scan. At the end of every scan, a report was generated and stored. The result was: six reports for every operating system - three for a basic scan and three for an advanced scan.

3 RESULTS

The number of vulnerabilities detected in each operating system is listed in the tables below.
Table 3 depicts many critical vulnerabilities, basically in Windows Server 2003. Few critical vulnerabilities were discovered in Windows Server 2008 Enterprise and Windows Server 2012 Datacenter. Nessus's basic scan did not

manage to detect vulnerabilities in Windows Server 2012 Datacenter R2 and in Windows Server 2016 Technical Preview 2.

Table 3. Number of Vulnerabilities Found with Nessus, Basic Scan

Windows	Nessus Home - Basic Scan				
	Total	Low	Medium	High	Critical
2003 Enterprise	10	0	2	1	7
2003 Enterprise SP1	6	2	3	0	1
2003 Enterprise R2	2	0	2	0	0
2008 Enterprise (SP1)	3	0	1	0	2
2008 Enterprise SP2	1	0	1	0	0
2008 Enterprise R2	2	0	1	0	1
2012 Datacenter	1	0	1	0	1
2012 Datacenter R2	1	0	1	0	0
2016 Technical Preview 2	1	0	1	0	0

Table 4. Number of Vulnerabilities Found with Nessus, Advanced Scan

Windows	Nessus Home - Advanced Scan				
	Total	Low	Medium	High	Critical
2003 Enterprise	10	0	2	1	7
2003 Enterprise SP1	11	3	5	2	1
2003 Enterprise R2	2	0	2	0	0
2008 Enterprise (SP1)	3	0	1	0	2
2008 Enterprise SP2	1	0	1	0	0
2008 Enterprise R2	2	0	1	0	1
2012 Datacenter	1	0	1	0	1
2012 Datacenter R2	1	0	1	0	0
2016 Technical Preview 2	1	0	1	0	0

Table 4 illustrates, the differences between Nessus basic and advanced scan.

Table 5. Number of Vulnerabilities Found with OpenVAS, Basic Scan

Windows	OpenVAS - Basic Scan			
	Total	Low	Medium	High
2003 Enterprise	2	0	2	0
2003 Enterprise SP1	0	0	0	0
2003 Enterprise R2	2	0	2	0
2008 Enterprise (SP1)	2	0	2	0
2008 Enterprise SP2	2	0	2	0
2008 Enterprise R2	2	0	2	0
2012 Datacenter	2	0	2	0
2012 Datacenter R2	2	0	2	0
2016 Technical Preview 2	2	0	2	0

Table 5 presents the OpenVAS's basic scan results. It performed in the exact same way in every Windows server operating systems.

Table 6. Number of Vulnerabilities Found with OpenVAS, Advanced Scan

Windows	OpenVAS - Advanced Scan			
	Total	Low	Medium	High
2003 Enterprise	3	0	2	1
2003 Enterprise SP1	5	2	1	2
2003 Enterprise R2	3	1	2	0
2008 Enterprise (SP1)	4	2	2	0
2008 Enterprise SP2	3	1	2	0
2008 Enterprise R2	3	1	2	0
2012 Datacenter	3	1	2	0
2012 Datacenter R2	3	1	2	0
2016 Technical Preview 2	3	1	2	0

On the other hand, OpenVAS advanced scan was able to discover more vulnerabilities, as table 6 illustrates. Thus, the increase of the amount of the detected vulnerabilities. Only three critical vulnerabilities were detected overall. Finally, OpenVAS did not manage to supersede Nessus functionality regarding the discovered vulnerabilities.

Table 7. Number of Vulnerabilities Found with Nexpose, Basic Scan

Windows	Nexpose - Basic Scan			
	Total	Moderate	Severe	Critical
2003 Enterprise	15	2	3	10
2003 Enterprise SP1	12	2	2	8
2003 Enterprise R2	5	2	2	1
2008 Enterprise (SP1)	8	3	2	3
2008 Enterprise SP2	5	3	2	0
2008 Enterprise R2	5	3	2	0
2012 Datacenter	5	3	2	0
2012 Datacenter R2	5	3	2	0
2016 Technical Preview 2	5	3	2	0

As shown in table 7, Nexpose's basic scan results are similar to Nessus's basic scan. It managed to exceed the amount of vulnerabilities Nessus found and it greatly surpassed OpenVAS.

Finally, in table 8, it is shown that Nexpose's advanced scan was not able to detect more vulnerabilities than the basic scan. In fact, it failed to identify vulnerabilities in Windows Server 2012 Datacenter in both versions.

Table 8. Number of Vulnerabilities Found with Nexpose, Advanced Scan

Windows	Nexpose - Basic Scan			
	Total	Moderate	Severe	Critical
2003 Enterprise	15	2	3	10
2003 Enterprise SP1	12	2	2	8
2003 Enterprise R2	5	2	2	1
2008 Enterprise (SP1)	8	3	2	3
2008 Enterprise SP2	5	3	2	0
2008 Enterprise R2	5	3	2	0
2012 Datacenter	3	3	0	0
2012 Datacenter R2	3	3	0	0
2016 Technical Preview 2	5	3	2	0

4 FUTURE WORK

Linux Desktop and Server distributions, along with Android operating systems will be evaluated in the future. A similar vulnerability assessment could be performed and as a result, the number and significance of vulnerabilities will possibly increase the targeted audience.

5 CONCLUSIONS

Security wise, these results may help customers in choosing which Windows server operating system they might purchase according to their needs.

The vulnerability assessment amongst Windows server operating systems is presented. As of July 14th (extended support), Windows Server 2003 Enterprise are no longer supported; labeling the operating system as insecure (for example: SMB vulnerability that allows remote code execution and RPC Request that allows remote code execution). Users should enable SMB Signing, as Nessus and Nexpose indicate and instruct upgrading to R2 Service Pack 2 [21] [22].

Microsoft suggests migrating to Windows Server 2012 Datacenter [23]. Regarding the security of Windows Server 2008 R2 Enterprise, Microsoft will be distributing security updates until January 14th, 2020.

By providing the results of the vulnerability assessment, users have the ability to be fully aware regarding the amount of the security issues each server operating system encounters. As a user upgrades to a newer version of Windows Server, he is less likely to expose himself in an insecure environment.

To conclude, Windows Server operating systems maintain vulnerabilities, from low to critical. Apply service packs or updates as soon as possible and invest reasonably in security.

REFERENCES

[1] J. Vacca, Managing Information Security, Second Edition, London, Elsevier, October 2013.

[2] N. Mansourov, D. Campara, System Assurance, First Edition, London, Elsevier, 2010.

[3] K. Julisch, C. Kruegel, Detection of Intrusion and Malware, and Vulnerability Assessment: Second International Conference, DIMVA 2005, Vienna, Austria, July 2005, Proceedings, Wien, Springer, 2005, pp. 2-20.

[4] T. R. Peltier, J. Peltier, J. A. Blackley, Managing A Network Vulnerability Assessment, First Edition, Boca Raton, Auerbach Publications, May 2003.

[5] J. Vacca, Computer and Information Security Handbook, First Edition, London, Elsevier, July 2009.

[6] T. Holz, H. Bos, Detection of Intrusion and Malware, and Vulnerability Assessment: Eighth International Conference, DIMVA 2011, Amsterdam, The Netherlands, July 2005, Proceedings, New York, Springer, 2005, pp. 2-20.

[7] A. Jones, D. Ashenden, Risk Management for Computer Security, First Edition, London, Elsevier, April 2005.

[8] Á.M. Eduardo and C.V. Alfredo, Vulnerability Assessment of Spatial Networks: Models and Solutions, Combinational Optimazation, Third International Symposium 2014, Houten, Springer, 2014, pp. 433-444.

[9] EC-Counsil, Network Defense: Security and Vulnerability Assessment, First Edition, Boston, Cengage Learning, April 2010.

[10] M. Dowd, J. McDonald, J. Schuh, The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities, First Edition, Boston, Addison - Wesley Proffesional, November 2006.

[11] P. S. Anton, R. H. Anderson, R. Mesic, M. Scheiem, Finding and Fixing Vulnerabilities in Information Systems: The Vulnerability Assessment and Mitigation Methodology, Santa Monica, RAND Corporation, January 2004.

[12] S. Manzuik, A. Gold, C. Gatford, Network Security Assessment: From Vulnerability to Patch, First Edition, Rockland, Syngress, November 2006.

[13] D. Maynor, T. Wilhelm, Metasploit Toolkit for Penetration Testing, Exploit Development, and Vulnerability Research, First Edition, Rockland, Syngress, October 2007.

[14] http://sdiwc.net/digital-library/modern-windows-operating-systems-vulnerabilities.html (last accessed 4th of April 2016).

[15] T. Jaeger, Operating System Security, California, Morgan & Claypool Publishers, October 2008.

[16] http://sdiwc.net/digital-library/modern-windows-operating-systems-vulnerabilities.html.(last accessed 4th of April 2016).

[17] J. Beale, C. van der Walt, R. Deraison, Nessus Network Auditing, First Edition, Rockland, Syngress, October 2004.

[18] N. Archibald, G. Ramirez, N. Rathaus, J. Burke, B. Caswell, R. Deraison, Nessus, Snort, & Ethereal Power Tools: Customizing Open Source Security Applications, First Edition, Rockland, Syngress, August 2015.

[19] J. Broad, Mastering Nexpose and Metasploit: A Lab-Based Approach to Mastery, First Edition, Rockland, Syngress, November 2015.

[20] H. Reibold, OpenVAS kompakt, Saarbrücken, Brain-Media.de, June 2013.

[21] http://www.tenable.com/plugins/index.php?view=single&id=35362 (last accessed 4th of April 2016).

[22] http://www.tenable.com/plugins/index.php?view=single&id=34477 (last accessed 4th of April 2016).

[23] https://www.microsoft.com/en-us/server-cloud/products/windows-server-2003/default.aspx. (last accessed 4th of April 2016).

Recommendation System for Engineering Students' Specialization Selection Using Predictive Modeling

Rosemarie M. Bautista, rosemarie.m.baustista@gmail.com
Menchita Dumlao, menchdumlao@yahoo.com
Melvin A. Ballera, maballera@yahoo.com.ph
Villa Arca Subdivision Baesa – Quezon City
AMA University

ABSTRACT

Educational data mining (EDM) can be used in extracting useful patterns in students' academic records which may aid in management decision making on determination of engineering students' specialization track once the general engineering academic requirements were completed. The objective of the research is to provide a specialization selection recommendation for engineering students through application of data mining algorithm and adoption of the rule sets generated by a predictive model. The attributes that may be significant in creating prediction were determined using correlation-based feature selection. Comparative analysis among known algorithms shows that the highest accuracy was considered. A decision tree classification model using WEKA and J48 produced an accuracy value of 80.06. The study revealed that Gender, Algebra, Calculus and physics courses found to have significant effect in predicting the engineering specialization, thus strengthening the general notion that for engineering students to be more successful, the academic performance with the above courses should be highly considered.

KEYWORDS
Data Mining, Educational Data Mining, Predictive Modeling, Recommendation System, Selection, Tree Classification

1 INTRODUCTION

There are invaluable information and hidden patterns that can be mined in databases which makes proper management of knowledge derived from databases becomes essentially important [1].The increasing interest to explore large databases to generate business intelligence paves the way for data mining. Data mining is a process of finding interesting, useful and novel patterns, as well as descriptive and predictive models from large databases [2][3]. Thus, it becomes an effective tool for analysis and prediction [4]. Moreover, as entities whether government, commercial, or academic strive for excellence, the need to properly manage available information in every organization's data banks became crucial. This opens door to an interesting field of data mining termed as educational data mining or "EDM". EDM deals with the extraction of useful patterns in education arena [5]. It, in most cases, is used to analyse current and historical attributes to gain understanding of some academic situations, student behaviour, scholastic and enrolment data that may improve decision making and management of scholastic-related issues and student pedagogical performance [6] [7][8].

A study conducted by [9] determines how data mining algorithms used in business can effectively be applied in education field. Several studies to mine useful knowledge from educational databases were conducted and became important concern.

Decision tree algorithm Iterative Dichotomiser 3 (ID3) was used by [10] to develop model used in analysing demographic data, entry grades in secondary school and entrance examination scores to predict the graduation grades of university students.

Another study was conducted by [11] which focused on measuring the efficiency of decision tree algorithms in creating predictions regarding performance of students in the final examinations. The results revealed that C4.5 is efficient and accurate in predicting the outcome. It has at the same time showed faster response time in deriving the tree.

ID3 algorithm was also applied by [13] in evaluating student's performance to create predictions as to whether a student is suitable for enrolment in a specific course.

Decision tree C4.5was utilized by [14] to predict and recommend course itinerary alternatives based on discovered patterns in the academic performance of students with approximately the same profiles and academic performance as the student being guided. Similarly, J48 classification tree algorithm, WEKA implementation of C4.5 was used by [15] in the prediction and recommendation of academic track in basic Jordanian schools.

The main objective of this study is to provide specialization selection recommendation for engineering students using predictive model. This study specifically aimed to: first, determine the most distinctive attributes that exert significant contribution in predicting and recommending appropriate engineering specialization; second, identify the data mining algorithm best suited in the defined task and; and lastly, evaluate the acceptability of the developed predictive model.

The rest of this paper is organized as follows: Section 2 discusses the methodology used in the study. Section 3 describes the results and discussions. Finally, this paper is concluded in Section 4.

2 METHODOLOGY

Upholding quality graduates in higher education requires thorough analysis of existing measures and conservancy of contributors to good standing. In this study, patterns on students' academic performances were determined to provide recommendation in specialization selection for incoming third year engineering students. In order to achieve the general objective of the study, the Knowledge Discovery (KDD) process was used. KDD process involves discovering hidden patterns and knowledge from databases through application of data mining techniques and algorithms [16].

2.1 Data Selection

Demographic and academic records of engineering students from 2009 to 2015 were requested from registrar's office. Records of students who successfully completed engineering courses within the five prescribed year and instances without nulls were extracted from the files using Structured Query Language. The records obtained were treated as the data set divided into train and test sets. The columns included are attributes gender, grades for first year and second year for math and science subjects. Data format is presented in Table 1.

Table 1. Possible Attributes for the Recommendation System

Variable	Description	Possible Values
Gender	Gender of Student	{Male=1; Female=0}
Algbr	Grade in Algebra	Numerical value from 1.0 to 5.0
Trigo	Grade in Trigonometry	Numerical value from 1.0 to 5.0
AnltcGeo	Grade in Analytic Geometry	Numerical value from 1.0 to 5.0
SldMens	Grade in Solid Mensuration	Numerical value from 1.0 to 5.0
IntgrlCalc	Grade in Integral Calculus	Numerical value from 1.0 to 5.0
DiffCalc	Grade in Differential Calculus	Numerical value from 1.0 to 5.0
Phys1	Grade in Physics 1	Numerical value from 1.0 to 5.0
Phys2	Grade in Physics 2	Numerical value from 1.0 to 5.0
Chem1	Grade in Chemistry	Numerical value from 1.0 to 5.0
Specialization	Target Specialization	{CE, EE, ECE, ME, COE, IE, MEE, MEEM}

ISBN: 978-1-941968-34-5 ©2016 SDIWC

Table 1 shows possible values that may be assigned to the variables used in the study. Gender attribute holds only values 1 and 0 for male and female respectively. The ordinal variable grade was based on the numerical parameter used in the local education institution with 1.0 considered as the highest having an equivalent grade percentage of 97-100 and 5.0 considered as the lowest. The target specialization may fall under any of the following: Civil Engineering (CE); Electrical Engineering (EE); Electronics and Communications Engineering (ECE); Mechanical Engineering (ME); Computer Engineering (COE); Industrial Engineering (IE); Mechatronics Engineering (MEE); and Manufacturing Engineering (MEM).

2.2 Preprocessing and Transformation

In this step, the features or attributes of the data set were analyzed using WEKA data mining tool. The attributes were filtered using Correlation based Feature selection (CFS) Best First searching technique in cross validation modeto rank the attributes based on their relevance to the study. Irrelevant attributes with no predictive information were removed from the list of attributes considered in the study, leaving only those attributes that indicate significant contribution in the generation of appropriate prediction for choosing engineering specialization.

2.3 Data Mining

After determining significant attributes, the train data set was evaluated in various data mining algorithms. Literature shows that many of the researches that focused on prediction and recommendation used decision tree learning algorithms mostly using ID3, C45 and CHAID. In this purpose, aside from the mentioned decision trees, other algorithms implemented in WEKA and SPSS such as regression for multiple-variable target, neural network and nearest neighbor were utilized. The data mining algorithm that yields the highest accuracy was considered in searching for patterns in the data set. The rules sets generated were then used as foundation in building the model for predicting and recommending specialization to engineering students.

2.4 Evaluation

Necessary testing and evaluation of the system performance was performed. The acceptability of the model was evaluated using the accuracy percentage.

The model generated by running the train data set using the best algorithm was checked by running the test data set through the same model. This was done to validate whether the model developed can be used properly when put to use or will not break down when new data is applied on it. The percentage of the correctly classified instances or accuracy percentage in both the train and test set verified the model's performance.

Analysis of other evaluation parameters such as precision, recall, and ROC area results was also completed.

3 Results and Discussions

3.1 Distinctive Attributes

The first goal of the study is to determine the most distinctive attributes that exert significant contribution in predicting appropriate engineering specialization. This is relatively important in constructing model with less redundant and misleading data at the same time building simpler model but with higher predictive value [17].

In order to come up with a model that will generate reliable predictions, feature selection process was done to automatically search for the best subset of the attributes in the dataset.

Attributes significant to the model were determined through *Correlation-based Feature Selection* (CFS) *SubsetEval* using *BestFirst* technique. All irrelevant attributes with no predictive information were removed from the original data sets in order to decrease model training time and to avoid over fitting of the decision tree which ensure optimal splits in attribute values [18]. The subset selection process improves the learning algorithm processing time and produces a more comprehensible representation of the target concept [19]. Using CFS *SubsetEval BestFirst* technique, only six out of the ten listed attributes were selected to be significant as shown in Table 2.

Table 2. Attribute Selection Output Using CFS SubsetEval

Attribute Selection: 10-Fold cross validation		
Number of Folds	%	Attribute
10	100 %	Gender
10	100 %	Algbr
1	10 %	Trigo
0	0 %	AnltcGeo
0	0%	SldMens
10	100 %	IntgrlCalc
10	100 %	DiffCalc
10	100 %	Phys1
8	80%	Phys2
0	0%	Chem1

In this study, 10-fold cross-validation was used to compare attributes. It is a statistical method that divides the dataset into ten mutually exclusive set to compare learning algorithms and to choose proper model parameters [20][21].

Attributes *Gender, Algbr, IntglCalc, DiffCalc, Phys1* appeared 10 times (100%) in 10-fold validation whereas *Phys2* appeared 8 times (80%), thus were considered significant predictors. The rest of the attributes appeared only 1 or 0 times, thus were considered not contributing predictors in the study conducted.

3.2 Best Suited Algorithm

Some experiments were carried out to evaluate the performance and usefulness of different classification algorithms for predicting engineering specialization in order to provide appropriate recommendation. The training data set was run in several data mining classifiers available in SPSS and in WEKA. This time only the six attributes found to be significant were used. The dataset was tested in WEKA Naïve Bayes, Function Logistic classifier and J48 tree classifier. It was also tested in SPSS Nominal Regression, Decision Tree CHAID, Neural Network, and Nearest Neighbor classifiers. Table 3 shows the summary of the accuracy test done in different classifiers.

Table 3. Comparison of Accuracy in Different Classifiers

Tool	Classifier	Percentage Accuracy
WEKA	J48 Tree Classifier	80.05
	Logistic Function Classifier	64.30
	Naïve Bayes Classifier	60.11
SPSS	Nominal Regression	64.00
	CHAID Tree Classifier	68.20
	Neural Network Multilayer Perception	71.30
	Neural Network Radial Basis Function	61.00
	Nearest Neighbor	71.20

Among the classifiers tested, J48 tree classifier yields the highest number of correctly classified instances. J48 is the C4.5 decision tree implementation in WEKA software tool. C4.5 is well-known for its predicting performance as statistical classifier [22]. Experiment performed reveals an 80.05% accuracy for the J48 Tree Classifier. This was relatively higher compared to other WEKA classifiers Function Logistic and Naïve Bayes expressing only 64.30% and 60.11% accuracy respectively. It was also far better than the

other SPPS classifiers evaluated. The SPSS classifier, neural network multilayer perception that displayed the highest accuracy percentage of 71.30% was still behind J48 by almost 10%.

Although some studies suggests better algorithms than decision tree, the No Free Lunch Theorem attests that methods have significant variability across various problems. Thus, it suggests that there is no universally best learning algorithm. Even the best algorithm may sometimes show poor performance, and algorithms with poor average performance may exceptionally perform well on few problems or metrics [23].

In the experiment conducted, J48 shows the highest percentage of correctly classified instances, thus, the model it generated was used in this study.

3.3 Acceptability of the Model

The test data set was run through the model to check if the percentage of the total correct prediction in the train set and test set was close enough. This was done to validate whether the model will not break down when new data is applied on it.

The confusion matrix generated by the classifier is shown in Table 4.

Table 4.Confusion Matrix
for the Supplied Test Set

CONFUSION MATRIX								
a	b	c	d	e	f	g	h	Classified as
81	0	3	0	0	31	0	0	a = CE
4	108	1	2	0	0	6	0	b = COE
12	15	158	1	0	1	1	7	c = ECE
1	1	4	57	0	0	0	9	d = EE
0	0	0	1	39	0	1	0	e = IE
30	1	2	0	0	51	0	0	f = ME
0	0	0	11	0	0	29	0	g = MEE
0	1	5	0	3	0	0	33	c = MEM

The resultant confusion matrix, also known as contingency table, shows information of the actual and predicted data generated by the classifier. It should be given attention in weighing the accuracy of a model since it gives obvious indication where the classifier goes wrong. The columns of the table represent the predictions and the rows are the actual class.
An overall accuracy percentage of 78.3099% was obtained after running the supplied test set through the generated model which indicates that the rules can be used and applied to new data.

Other performance measures: precision, recall, and ROC area resultswere also checked. These measures allow analysis of individual performance on class labels.

The portion of the retrieved instances that is correctly predicted [24]is referred to as the ***Precision*** which is calculated using the formula in (1).

$$Precision = \frac{True\ Positives}{True\ Positives + False\ Positives} \quad (1)$$

True positives are the number of correct predictions whereas false positives are the summation of all the values predicted to be instances of a particular attribute but in fact are not. In specialization COE for example, the true positive is equal to 108 and false positive equals 18 (computed from 15+1+1+1). Therefore, the precision is equivalent to 0.857. This means that out of the times COE was predicted, 85.7 % of the time the system was correct.

The portion of the correctly predicted instances that are retrieved [24] is referred to as the ***Recall*** which is calculated using the formula in (2).

$$Recall = \frac{True\ Positives}{True\ Positives + False\ Negatives} \quad (2)$$

False negatives are the summation of all the values that are predicted to be not instances of an attribute but in fact are. False negative in COE equals 13 (computed from 4+1+2+6). Therefore, the recall is equivalent to 0.893. This means that out of the times COE should have been predicted, 89.3 % COE was correctly predicted.

F-measure is the mean of precision and recall [24]. The formula is shown in (3).F-measure in COE equals 0.874 or 87.4%.

$$F - Measure = \frac{(2 * Recall * Precision)}{(Recall + Precision)} \qquad (3)$$

The relationship between false positives and true positives are described using relative operating characteristic curve or ROC curve. Accuracy is measured by the area under the ROC curve shown in Figure1. ROC area of 1 represents a perfect test; 0.90-1 is excellent; 0.70-0.80 is fair; 0.60-0.70 is poor; 0.50-0.60 is fail; and an area of .5 represents a worthless test [25].

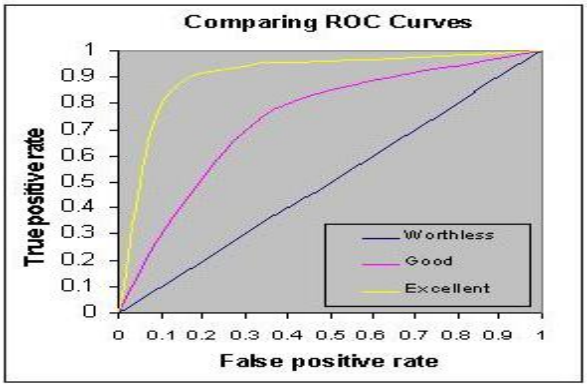


Figure. 1.ROC Curves Interpretation

The ROC area results in individual specialization indicate that test results are excellent. The weighted average of 0.948 indicates that the resultant curve will also indicate excellence.

4 CONCLUSION

Attributes *Gender*, *Algbr*, *IntglCalc*, *DiffCalc*, *Phys1*, and *Phys2* were found to have significant effect in predicting engineering specialization based on the result generated the CFS SubsetEval BestFirst attribute selection technique conducted in this study. The performance measure results of the evaluated classifier shows high acceptability of the predictive model considered. The study may provide valuable information for the management in giving decision about what engineering specialization may be most appropriate to advise to students.

REFERENCES

[1] Suman, A.,& Pooja, M. (2014). A Comparative Study on Role of Data Mining Techniques in Education: A Review. *International Journal of Emerging Trends & Technology in Computer Science*. 3(3). Pp65-69.

[2] Zaki, M. J., & Meira Jr, W. (2014). *Data mining and analysis: fundamental concepts and algorithms*. Cambridge University Press.

[3]Baradwaj, B. K., & Pal, S. (2012). Mining educational data to analyze students' performance. *arXiv preprint arXiv:1201.3417*.

[4] Baker, R. S., & Yacef, K. (2009). The state of educational data mining in 2009: A review and future visions. *JEDM-Journal of Educational Data Mining*, *1*(1), 3-17.

[5] Ali, D. M. M. (2013). Role of data mining in education sector. *International Journal of Computer Science and Mobile Computing, IJCSMC*, *2*(4), 374-383.

[6] Al-Azmi, A. A. R. (2013). Data, text and web mining for business intelligence: a survey. *arXiv preprint arXiv:1304.3563*.

[7] Yadav, S. K., & Pal, S. (2012). Data mining application in enrollment management: A case study. *International Journal of Computer Applications*,*41*(5).

[8]Bienkowski,M.,Feng, M.,& Means, B. "Enhancing Teaching and Learning Through Educational Data Mining and Learning Analytics: An Issue". U.S. Department of Education. October 2012.

[9]Kumar, S. A., & Vijayalakshmi, D. M. (2011, February). A Novel Approach in Data Mining Techniques for Educational Data. In *Proc 2011 3rd International Conference on Machine Learning and Computing"(ICMLC 2011), Singapore, 26th-27th Feb* (pp. V4-152).

[10]Ogunde, A. O., & Ajibade, D. A. (2014). A Data Mining System for Predicting University Students' Graduation Grades Using ID3 Decision Tree Algorithm.*Journal of Computer Science and Information Technology*, *2*(1), 21-46.

[11] Kumar, S. A., & Vijayalakshmi, D. M. (2011, February). A Novel Approach in Data Mining Techniques for Educational Data. In *Proc 2011 3rd International Conference on Machine Learning and Computing"(ICMLC 2011), Singapore, 26th-27th Feb* (pp. V4-152).

[12] Yadav, S. K., & Pal, S. (2012). Data mining application in enrollment management: A case study. *International Journal of Computer Applications,41*(5).

[13]Vialardi, C., Bravo Agapito, J., Shafti, L. S., & Ortigosa, A. (2009).*Recommendation in higher education using data mining techniques*. Barnes, T., Desmarais, M., Romero, C., & Ventura, S.

[14] Yadav, S. K., & Pal, S. (2012). Data mining application in enrollment management: A case study. *International Journal of Computer Applications,41*(5).

[15] Al-Radaideh, Q., Ananbeh, A. A., & Al-Shawakfa, E. M. (2011). A classification model for predicting the suitable study track for school students. *Int. J. Res. Rev. Appl. Sci*, *8*(2), 247-252.

[16] Fayyad, U., Piatetsky-Shapiro, G., & Smyth, P. (1996). From data mining to knowledge discovery in databases. *AI magazine*, *17*(3), 37.

[17] Brownlee, J. (2014, March 12). Feature Selection to Improve Accuracy and Decrease Training Time

[18] Hall, M. A. (1999). *Correlation-based feature selection for machine learning*(Doctoral dissertation, The University of Waikato).

[19]. Pal, A. K., & Pal, S. (2013). Classification model of prediction for placement of students. *International Journal of Modern Education and Computer Science,5*(11), 49.

[20] Arlot, S., & Celisse, A. (2010). A survey of cross-validation procedures for model selection. *Statistics surveys*, *4*, 40-79.

[21] Refaeilzadeh, P., Tang, L., & Liu, H. (2009). Cross-validation. In *Encyclopedia of database systems* (pp. 532-538). Springer US.

[22]. Bhatt, H., Mehta, S.,&D'mello,L. R. (2015). Use of ID3 Decision Tree Algorithm for Placement Prediction. *International Journal of Computer Science and Information Technologies*[Online]. 6 (5), 4785-4789.

[23] Caruana, R., & Niculescu-Mizil, A. (2006, June). An empirical comparison of supervised learning algorithms. In *Proceedings of the 23rd international conference on Machine learning* (pp. 161-168). ACM.

[24]Brownlee, J. (2014, March 12). Classification Accuracy is Not Enough: More Performance

[25] Tape, T. G. (2006). Interpreting diagnostic tests. *University of Nebraska Medical Center, http://gim. unmc. edu/dxtests*.

Vision Based Bin Picking Method Using Hierarchical Image Analysis

Kyekyung Kim[1], Sangseung Kang[1], Jaeyeon Lee[1] and Jinho Kim[2]
[1]Intelligent Cognitive Technology Research Department, ETRI, Daejeon, Korea
[2]Department of Electronics, Kyungil University, Daegu, Korea
[1]{kyekyung, kss, leejy}@etri.re.kr http://www.etri.re.kr
[2] ho@kiu.ac.kr http://www.kiu.ac.kr

ABSTRACT

In this paper, we describe vision based bin-picking system for robot application using multiple local features, which are extracted from single camera. Multiple features are extracted from texture on object surface that has used to estimate surface rotation angle and distance to object to be picked. Challenging problem is to estimate accurate picking point and distance to object. It is difficult to solve aforementioned problem because the distorted image affected by illumination has caused reflection on the image surface or feature data loss of texture. In this paper, we proposed hierarchical analysis using multiple cues by multi-resolution images to estimate picking points of piled objects in the bin. The estimation of object location by coarse image and picking point by fine image have processed. We have tested to evaluate performance on ETRI database, which have captured under various lighting condition in the pilot system, which is constructed like industrial environment.

KEYWORDS

Bin-picking, Object detection, Pose estimation, Hierarchical analysis, Multi-resolution images

1 INTRODUCTION

The industrial robot appeared in factory automating systems has been used as an effective means for solving challenges in industrial sites such as automation task, production cost saving, etc. As vision sensor technology has developed in a manufacturing line, object recognition method has applied to factory automation.

In recent years, due to introduction of cell production methods for producing various types of products in one line, need to estimate a type and a posture angle of a component and accurately mount the component is being gradually increased. Bin picking method of pick out piled object has studied intensively to perform works using industrial robot at cell manufacturing system because of cost saving by removing component feeding equipment, enhancing competitiveness of flexible manufacturing cell production systems.

Even in a machine component process had a low rate of automation, industrial robots are introduced to perform works at a manufacturing line instead skilled workers using various IT technologies of a control or machine and elements technologies such as a vision sensor, a force sensor, etc. As a sensing technology among element technologies applied to an industrial robot is enhanced and thus performance in a 3D visual sensor is also significantly improved, a need to develop an intelligent robot capable of performing a bin picking work in which a needed component is recognized and picked from a stacked pile is being increased. However, a vision based bin-picking method or technology has not developed sufficiently to apply to manufacturing line and has low recognition performance.

Bin-picking can be mainly applied to pick or assembly process of components using the detection of object location and pose estimation of x, y, z axis with 2D or 3D vision sensors [1-5]. 2D vision based bin-picking methods using stereo camera or single camera has extracted features from shape of object and estimated object pose

by calculating distance from extracted features [1-2]. Meanwhile, 3D vision based bin-picking method [3-4] has captured depth information of object using laser sensors or structure lighting pattern. An existing bin-picking method has extracted simple cue such as a circle or a rectangle from object and estimated object location and pose. A method using a camera image and a CAD model, and a method for modeling a 2D curved surface with both laser measurement and images to recognize a position and direction of a 3D object.

However, it is actually difficult to estimate accurate angle of component disposed at a variety of angles in piles and illuminations changed according to an actual production environment. Therefore, bin-picking task has considered non-trivial task because those problem have low reliability in performing task such as location detection or pose estimation. Many researchers have studied steadily to solve aforementioned problem and to get more accurate performance result because of fits to many application fields, which were be needed high demand of production automation

In this paper, bin picking method using 2D vision sensor has proposed that uses multiple local features extracted from multi-resolution image and hierarchical analysis to estimate picking point of piled components. Candidate picking components have detected with low resolution image, which selected by extracting simple cue such as a rectangle. And then, multiple local features are extracted to estimate pose or distance of a picking component with high resolution image. An accurate pose or distance has estimated using multiple local features calculated from transformed geometric data according to x, y, z axis. To evaluate performance of position detection and pose estimation of picking component, we have tested bin picking algorithm using image data, which has captured on various lighting condition by time passing. We have constructed a pilot system like a real working environment and tested picking task using robot by providing calibration coordinate to drive robot.

2 VISION BASED BIN PICKING SYSTEM

The vision based bin picking system has composed of several processes such as image processing, feature extraction, candidate component selection, object location detection and pose estimation [6-11]. Bin picking target object are various kinds of material components, which includes reflection object like a metal, plastic wrapped object. A polarizing filter has used and image filtering technique has strengthen because of a reflection object. Bin picking pilot system and target object has shown in Figure 1.

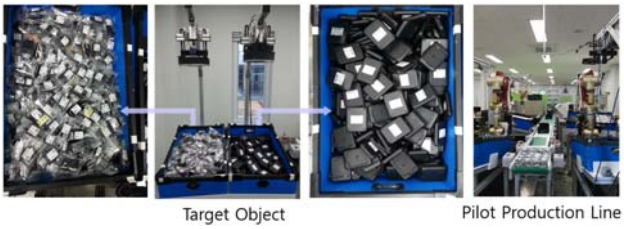


Figure 1. Bin picking pilot system and target object

2.1 Image Processing

An image processing includes image smoothing, edge detection, binarization, noise remove steps. An image preprocessing configured to extract a plurality of edges of a picking component from an input image. The edge detection includes a second derivative calculation by applying Gaussian filter to the component image. Blobs in the input image are detected by applying the local adaptive binarization technique [6] to the component image. The image preprocessing unit combines the detected second component edge and detected component by analyzing intensity of local region in input image. The combination result builds up component, which keeps more features and are saved to detect bin picking component. It is robust to illumination variation that is very important factor to apply into real environment condition.

A polarizing filter has installed to reduce illumination effect for atypical bin picking object such as reflection material surface component, plastic wrapped component. Figure 2 shows the

example of edge detection and local adaptive binarization image.

Figure 2. Image processing results

2.2 Candidate Object Detection

Object detection has made progress using hierarchical image analysis with multiple resolution images. Candidate positions of components to be picked have detected with low resolution image, and then more detailed features are extracted to estimate accurate component position, pose and distance from vision sensor to camera with high resolution image.

Candidate picking objects are selected by extracting simple cue feature like a rectangle, which offers to a reference position to pick a component and is used to calculate center point of a picking component. The simple cue for picking position by extracting features in interior component is detected with low resolution image. A rectangle feature in label has extracted even the feature has transformed or distorted due to illumination.

The rectangle has also used to estimate distance from camera to a picking component. Camera position and distance to component can be estimated using area or length for four sides of rectangle. Real distance for rectangle in the real world is calculated by matching geometric information of rectangle and related real distance in the world [7].

Final decision of picking component has fixed through calculation of area, geometric transform factor according to x, y, z axis, respectively. The optimal component to be picked has chosen by verifying whether the component is in advantageous picking location by examining the component located on the top or less rotation to each axis. The center point of rectangle is selected as picking point of component.

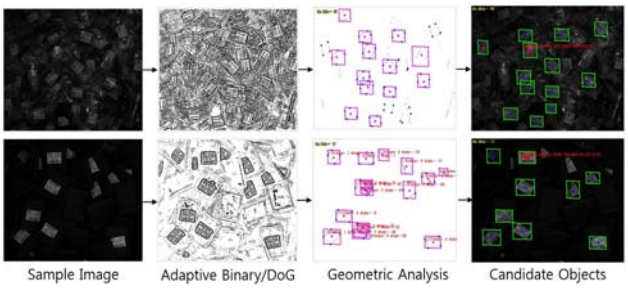


Figure 3. Candidate object detection using simple cue in low resolution image

2.3 Pose estimation

More features are extracted to estimate accurate component location, pose and distance to pick component. Some characters and symbols are appeared in rectangle on label those are extracted in high resolution image. However, some characters and symbols are missed or distorted because of illumination effect. Therefore, interior features are trained to extract more features even missing or distorted features are included in rectangle area. Hierarchical image analysis using multiple image resolution has processed to estimate accurate picking point decision as shown in Figure 4.

It is very difficult to get a surface orientation of a rotated component according to x, y, z axis. Therefore, several processes are applied to estimate pose of picking component. A pose estimation has processed by detecting maximal axis of component that has investigated by recognizing multiple features of component in a label. The multiple features include the direction information of component, which is used to assemble with right position.

Another pose estimation has processed to detect surface orientation of x, y, z axis. An extracted rectangle has used to analyze several factors, which are defined to examine geometric transformed parameter of rectangle and used to estimate surface orientation.

ISBN: 978-1-941968-34-5 ©2016 SDIWC

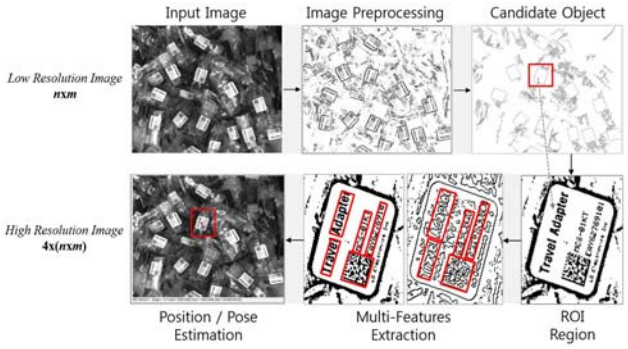


Figure 4. Hierarchical image analysis with multi-resolution images

Scale, length and angle of four sides of rectangle, b={b1, b2, b3, b4, b5}, are calculated. An accurate pose of component is estimated as shown in Figure 5.

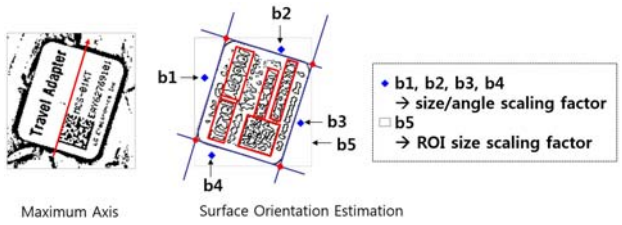


Figure 5. Pose estimation using multiple feature extraction and surface orientation factors

Multiple features are trained using neural network to estimate accurate pose of component and component position, as shown in figure 6.

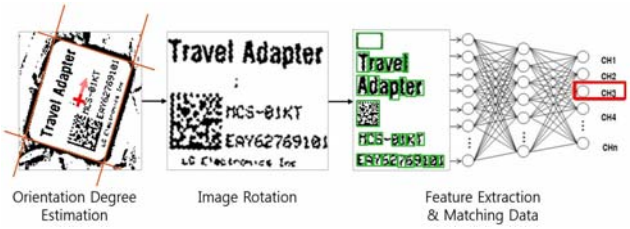


Figure 6. The training process for pose estimation using neural network

3 EXPERIMENTS

Experiment environment has set to evaluate proposed bin picking method which includes pilot system like real factory for bin picking and working table for capturing taring or testing data.

Working table has consisted of supplying bin of 600x400x200(mm), LED ring light of 200x200x25(mm) / 21W, vision sensor of Matrix Vision mvBlueCOUGAR-X225G. Vision sensor has mounted within 1m distance to supplying bin. Bin picking robot has located at the center of supplying bins. Figure 7 shows bin picking working environment and target components to be picked. Bin picking components have randomly piled in a bin and input images of 2248x2050 grey 8bit BMP have captured. Bin picking components include a plastic wrapped component and formal shape component. Training and testing database have built under various lighting condition and pilot system during 3 years.

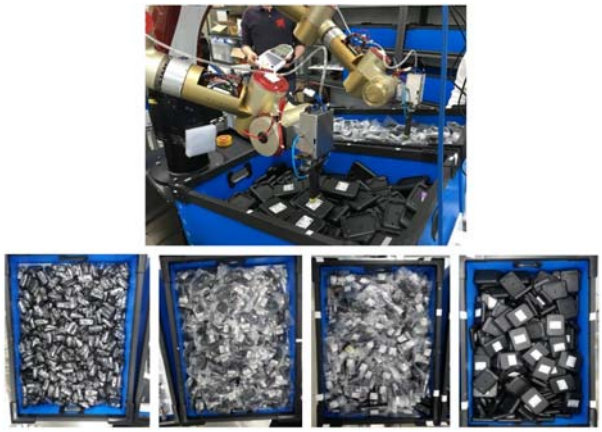


Figure 7. Bin picking using dual arm robot

Surface orientation estimation data have captured and calculated the length of four sides of rectangle and matched real distance in the real world with database captured according to different distance as shown in Figure 8. Codebook has created with database captured by different distance level that has picking distance from camera to component, x, y, z orientation degree.

Figure 8. Database captured under different distances for codebook generation

ISBN: 978-1-941968-34-5 ©2016 SDIWC

Performance evaluation of object detection and pose estimation has processed with 400 image data acquired from images in ETRI and pilot line in KIMM. 7 kinds of components have used to test object recognition performance such as position detection and pose estimation of object and bin picking robot has linked to experiment. Table 1 shows the detection rates and pose estimation of picking component in a bin. 1 to 4 components are randomly piled in a bin.

Table 1. The detection rate and pose estimation of 4 kinds of picking components

Kind of comp.	Testing no. of sample image	No. of detection image	Comp. detection rate(%)	Pose estimation (°)
Set1	100	97	97	0.9
Set2	100	98	98	0.7
Set3	100	96	96	0.9
Set4	100	95	95	1.2
Total	400	386	96.5	0.92

It is difficult to estimate accurate pose, distance to component and surface rotation to x, y, z axis, respectively. To solve the challenges problem, multiple features are extracted and trained to estimate pose of picking component. A heterogeneous features such as SIFT can be combined to enhance pose and distance by generating feature vector.

A different kinds of features in a label have extracted by SIFT algorithm using stereo images. The features extracted from stereo images are used to get a close distance and surface orientation angle. Distances are calculated by matching features of candidate components from stereo image. Stereo based 3D restoration has processed and surface normal vector has generated to each component.

4 CONCLUSIONS

In this paper, we have proposed vision based bin picking using multiple local features with multi-resolution images for automation factory using industrial robot. The working environment setting for bin picking, the detection of object position, pose estimation, distance measurement and surface orientation angle detection steps have included in bin picking system. Hierarchical image analysis has processed to estimate picking point of piled components in a bin. Candidate picking components have detected with low resolution image and multiple local features are extracted to estimate accurate pose or distance of a picking component with high resolution image. Multiple local features have trained to detect component position and estimate pose and distance to picking component. An accurate pose or distance has estimated from transformed geometric data according to x, y, z axis.

For evaluating the proposed bin picking method, we have tested on database, which have captured in various lighting condition and pilot system. In addition to, the vision based bin picking method has had linked testing with dual arm robot.

In the future, heterogeneous local features will be combined to get more precise object position, distance to object, surface orientation to each axis. And also, the research to enhance bin picking performance will be processed by combining sensors, optimizing lighting condition, increasing reliability and analyzing error factors.

ACKNOWLEDGMENTS

This work was supported by the R & D program of MOTIE & KEIT [10038660, Development of dual-arm robot system based on multi-robot cooperation for cell manufacturing process of IT products]

REFERENCES

[1] J. K. Oh, S. H. Lee and C. H. Lee, “Stereo Vision Based Automation for a Bin-Picking Solution,” International Journal of Control, Automation, and Systems, vol. 10, no. 2, pp. 362-373, 2012.

[2] K. Rahardja, and A. Kosaka, “Vision-based bin-picking : Recognition and localization of multiple complex objects using simple visual cues,” IEEE Proc. of International Conference on Intelligent Robots and System, vol. 3. pp. 1448-1457, 1996.

[3] O. Kazuya, H. Toshihiro, F. Masakazu, S. Nobuhiro, S. Mitsuharu, "Development for Industrial Robotics Applications, IHI Engineering review," vol . 42, no. 2, pp. 103-107, 2009.

[4] S. Lee, J. Kim, M. Lee, K. Yoo, L. G. Barajas and R. Menassa, "3D Visual Perception System for Bin Picking in Automotive Sub-Assembly Automation," 8th IEEE International Conference on Automation Science and Engineering, pp. 706-713, 2012.

[5] K. Ikeuchi, B. K. P. Horn and S. Nagata, "Picking up an Object From a Pile of Object," Artificial Intelligence Lab. of the Massachusetts Institute of Technology, A.I. Memo, no. 726, pp. 1-26, 1983.

[6] F. Shafait, D. Keysers and T. M. Breuel, "Efficient Implementation of Local Adaptive Thresholding Technique Using Integral Images," Document Recognition and Retrieval XV, Proceedings of the SPIE, vol. 6815, pp. 681510-681510-6, 2008.

[7] J. Lee, "A New Solution for Projective Reconstruction Based on Coupled Line Camera," ETRI Journal, vol. 35, no. 5, pp. 939-942, 2013.

[8] D. Lee and M. S. Nixon, "Vision-based finger action recognition by angle detection and contour analysis," ETRI Journal, vol. 33, no. 3, pp. 415-422, 2011.

[9] P. F. Felzenszwalb and J. Schwartz, "Hierarchical matching of deformable shapes," Computer Vision and Pattern Recognition, pp.1-8, 2007.

[10] C. Lu, N. Adluru, H. Ling, G. Zhu, L. J. Latecki, "Contour based object detection using part bundle," Journal of Computer Vision and Image Understanding, vol. 114, issue 7, pp. 827-834, 2010.

[11] V. Ferrari, L. Fevrier, F.Jurie, and C. Schmid, "Groups of adjacent contour segments for object detection," IEEE Trans. on Pattern Anal. Mach. Intel., vol 30, no. 1, pp.36-51, 2008.

Design of an IEC 61850 Based Safety Management System for Virtual Power Plants

Shinyuk Kang, Ilwoo Lee
Electronics and Telecommunications Research Institute
ameba@etri.re.kr, ilwoo@etri.re.kr

ABSTRACT

In this paper, we design an IEC 61850 based safety management system for VPP (Virtual Power Plant) management. The designed system gathers a various type of information such as vibration data, noise level data, temperature value data, current fuel level data, and an oil pressure date from sensors which placed on managed VPP. The main purpose of the safety management system is to detect the risk of a VPP through the gathered information for the stability of the system. This safety management system is designed to receive data based on IEC 61850 MMS protocols in order to manage the various VPP.

KEYWORDS

Virtual Power Plant, Smart Grid, IEC 61850, Safety Management System, Emergency Generator.

1 INTRODUCTION

The energy consumption growth in the world increased for several years. VPP is the one of answers to solve this problem. However, to utilize VPP to overcome of the power supply, the need for VPP management have also been raised. Distributed Energy Resources (DER) communication interface of VPP for safety management accordingly also has emerged as a very important issue. In this paper, VPP target resource was selected emergency generator. It is obliged that emergency generators have been held in buildings over a certain size by law. So there are already installed considerable capacity in the country. And new capacity also continues to increase [1]. This paper proposes a safety management system based on IEC 61850 data communication for VPP.

2 RELATED STANDARDS

This chapter discusses an overview of IEC 61850-7-420 that specifies the information model for VPP. The title of IEC 61850-7-420 is a basic communication structure – distributed energy resources logical nodes. IEC 61850-7-420 defines IEC 61850 information models to be used in the exchange of information with DER, which comprise dispersed generation devices and dispersed storage devices, including reciprocation engines, fuel cells, microturbines, photovoltacics, combined heat and power, and energy storage [3].

The IEC 61850 series define the communication between Intelligent Electronic Devices (IED) in substation and the related system requirements [2]. The IEC 61850 virtualizes actual devices and functions into hierarchical data structures by information modeling, and performs certain functions by data exchange with the Abstract Communication Service Interface (ACSI) between different communication entities. Mapping between different communication protocols is implemented through Specific Communication Service Mapping (SCSM), achieving maximum compatibility and avoiding impacts imposed by the development of communication protocol stacks [2].

IEC 61850-7-4 specifies the information model of devices and functions generally related to common use regarding applications in systems for power utility automation. In particular, it

specifies the compatible logical node names and data object names for communication between IED. This includes the relationship between logical nodes and data objects [4].

3 Design of a Safety Management System for VPP

The information model for VPP safety management system can be customized by defining additional information such as values measured by environment sensors or unique DER characteristics on the basis of IEC 61850-7-420 information model. Figure 1. Shows core components of an IEC 61850 based safety management system. The designed system consists of the following core components: Emergency generator (VPP) with various sensors, CTTS controller, IEC 61850 Server and Safety management system with a 61850 client.

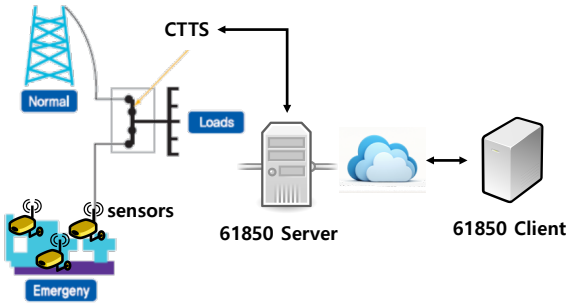


Figure 1. Core Components of an IEC 61850 based safety management system

The CTTS controller gathers vibration, noise, and temperature values measured by environment sensors placed around VPP. The 61850 Server provides a function to get VPP related raw data from a CTTS controller through a serial communication and coverts the delivered Modbus data into IEC 61850 data objects. To improve processing performance of the information data of VPP, designed system use shared memory access. Table. 1 Shows data processing improvement comparison between designed system and conventional Modbus based system.

The data objects are transferred to a 61850 client by Manufacturing Message Specification (MMS) read and write services. [5] The safety management system can show you the various safety management data provided by this MMS services. Table. 1 Shows data processing improvement comparison between proposed system and conventional Modbus based system.

Table 1. Data processing improvement

	Conventional Modbus Overall Transfer Time (ms)	Proposed System Overall Transfer Time(ms)	Improvement Ratio (%)
Average	71.02	25.94	63.5
Maximum	132	31	76.5
Minimum	39	24	38.5

The main function of VPP safety management are as follows:

- VPP safety data management function
- VPP safety alarm management function
- VPP safety real-time monitoring function
- VPP safety data presenting function

VPP safety data management function provides safety data set function, safety data get function, and local database management function. When configuring the data sets, it is important to understand that certain data attribute types are defined by IEC 61850 to have a data change trigger, quality change trigger, or data update trigger [2]. Figure 2. shows monitoring safety data lists and 61850 logical node address. Figure 3. shows monitoring GUI.

Figure 2. Safety data management GUI

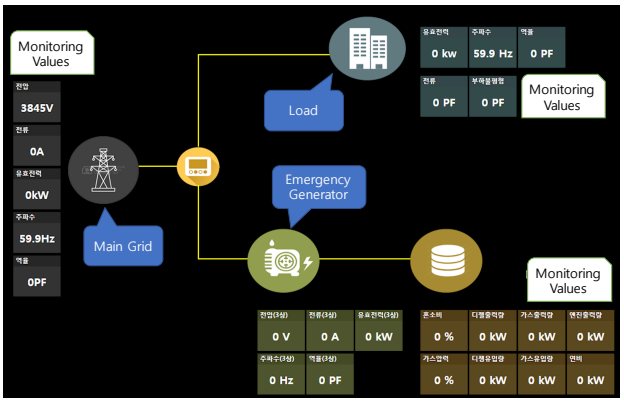


Figure 3. Real-time Monitoring GUI

VPP safety alarm management function means that checking the values from sensors attached on VPP and shows the status of VPP in a main user interface. As shown in Figure 4, red represents a problem in the VPP and green indicates that VPP is normal status. Figure 5. shows main GUI of safety management system.

Figure 4. Alarm management GUI

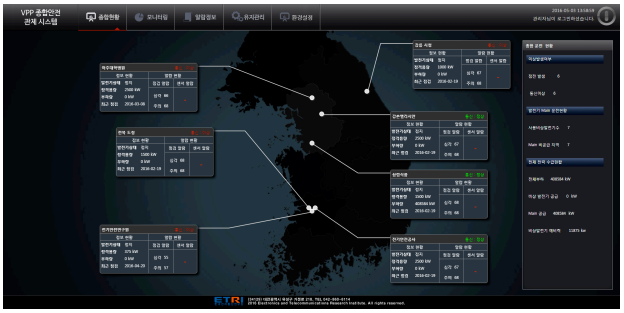


Figure 5. Main GUI of safety management system

VPP safety real-time monitoring function shows continuous data flow about selected data set. It can be one or more. Figure 6. shows continuous monitoring data.

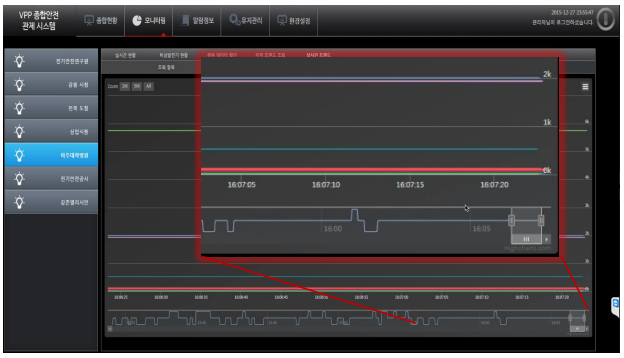


Figure 6. Monitoring GUI of continuous data flow

With displaying the status of each VPP on the main map, we are able to identify its safety status on the map.

4 Conclusion

This paper presents function design and implementation of safety management of emergency generator for VPP. A safety management system provides safety status monitoring function based on IEC 61850 data communication. This also provides the ability to manage the VPP resource efficiently.

5 ACKNOWLEDGEMENT

This work was supported by the R&D program of MOTIE and KETEP, Republic of Korea, under Grant of no. 20131010501760, “Development of an Integrated Energy Management System based on VPP”

REFERENCES

[1] YS Yoo, IW Lee, and JK Choi, “An Emergency Generator Asset Management for Virtual Power Plant Infrastructure” International Smart Grid Conference, pp.303-305, Oct. 2015.

[2] IEC, “Communication Networks and Systems for Power Utility Automation – Part 7-1: Basic Communication Structure - Principle and Models,” IEC 61850-7-1, 2011.

[3] IEC, “Communication Networks and Systems for Power Utility Automation – Part 7-420: Basic Comuunication Structure – Distributed Energy Resources Logical Nodes,” IEC 61850-7-420, 2009.

[4] IEC, "Communication Networks and Systems for Power Utility Automation – Part 7-4: Basic Comuunication Structure – Compatible Logical Node Classes and Data Object Classes," IEC 61850-7-4, 2010.

[5] TI Hwang, YS Yoo, SY Kang and IW Lee, "Design of an IEC 61850 Based Communication System for DER Management" International Conference on Electrical, Electronics, Computer Engineering and their Applications, pp.1-5, Nov. 2014.

Analysis and Modeling of Symmetric Slab Dielectric Structures to Solve Electrical and Magnetic Transverse Modes

Abdulati Abdullah[1] and Moussa Hamdan[2]
[1,2]Electrical and Communications Department, Azzaytuna University, Libya
[1]abdulatiabdullah@gmail.com and [2]moussahamdan2@gmail.com

ABSTRACT

Optics devices have recently witnessed considerable improvement by fabricating them in terms of the change in integrated optical circuits' properties. Previously, the optical devices were adequate to propagate electromagnetic fields, whereas they are not appropriate for present integrated optics devices because the optical devices (e.g. glass lenses) were very large compared to the wavelength. This paper concerns with solving the guided modes. It is useful to start with a simple case of slab structure. The symmetric dielectric planar waveguides are the simple case to demonstrate the mechanisms of solving the TE-Mode and TM-Mode of optical structures. The optical wavelength is selected to be $1\mu m$ which provides the appropriate propagation constant modes (β) . This gives an effective refractive index which meets the condition of the field confinement in the core region. By including the active semiconductor lasers, the optical structures have experienced a significant improvement since they operate at sub-wavelength compared to the conventional structures. Simulations are carried out using MATLAB with Simulink tools to study the fields' behavior.

Keywords: propagation constant mode, effective refractive index, thickness, semiconductor lasers, modal gain.

1 INTRODUCTION

The fundamental element in the technology of integrated photonic is the optical waveguide. Waveguides can be introduced as an optical structure that enables the confinement of light within its boundaries depending on the theory of total internal reflection [1]. They are also known as a physical devices which guide the electromagnetic waves in the form of an optical signal. It is therefore possible to bound the optics signal by a system contaning various media, which can form the optical waveguides and surrounded by another media with refreactive indexe lower than that of core layer. The performace of this stracture is basically based on the phenemian of the total internal reflection as shown in figure(1) [2].

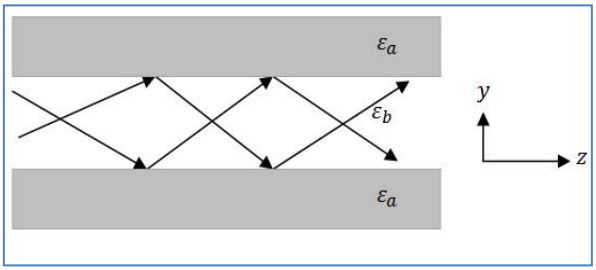
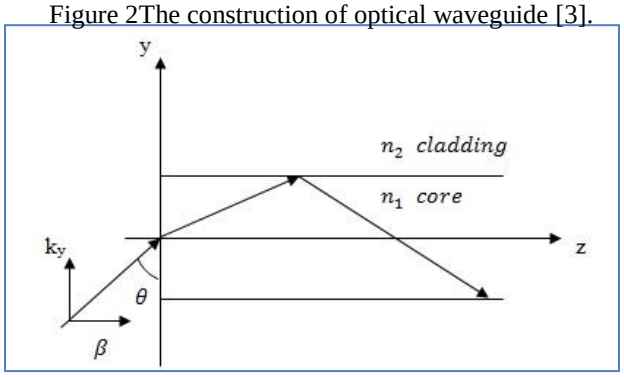


Figure 1 Total internal reflection [1].

Moreover, The optical waveguides can be classified in terms of mode structure , for instance, a single mode and multi-mode [1]. The principle means of solving waveguides theory can be derived by using Maxwell's equations since the simple configuration of the optical waveguides consists of three layers (substrate, core and cladding). Therefore, several mechanisms have been improved for the optical waveguides modeling to treat the field comprising both guided and radiated modes. The main mechanism of utilizing optical waveguide is based on the confinement of the optical waves within the core region as shown in figure (2) [3].

This phenomenon can be obtained when the total internal reflection (TIR) occurs. According to Snell's law, the beam has a curvature towards the normal pattern during its movement from lower to higher refractive index of the material [1] &[2]. At critical angle, the beam has a reflection by angle 90°; afterward the beam is totally reflected back to the core.

Figure 2The construction of optical waveguide [3].



Total internal reflection is also another concept which should be considered. It demonstrates how to confine the field within the desirable region, especially in the case of confining the field in the outmost layers [4].The formulation of Snell's law is:

$$n_1 \sin\theta_1 = n_2 \sin\theta_2 \quad (1)$$

Then, to obtain the (TIR), $\theta_2 = 90°$, and $\theta_1 = \theta_{critical}$.

$$\theta_{critical} = \sin^{-1}\frac{n_2}{n_1} \quad (2)$$

When the incident angle exceed $\theta_{critical}$ an *evanescent wave* occurs along the interface, which is decayed exponentially in the second media. This wave can be bounded tightly towards the interface and named as surface wave which satisfies the boundary conditions at the interface [2].

2 DIELECTRIC SLAB WAVEGUIDE

To solve the propagation modes in the dielectric slab waveguide structures, it is more advantageous to begin with the simple case of having a symmetric slab waveguide. This is therefore considered to be more helpful to understand the guided modes of the waveguide structures shown in the following figures. Figure (3) introduces the whole model of the structure, while figure (4) shows a simple structure of slab waveguide which is the basic stage of demonstrating the field distribution in terms of both TE-Mode and TM-Mode cases. The assumption is made to have TE- Mode; meant electric field does not exist in the trend of the wave travel. The propagating of the electromagnetic wave is assumed to be in Z-direction. In this case, all fields must be tangential at the interface $(y = w/2)$ to satisfy the boundary conditions [2].

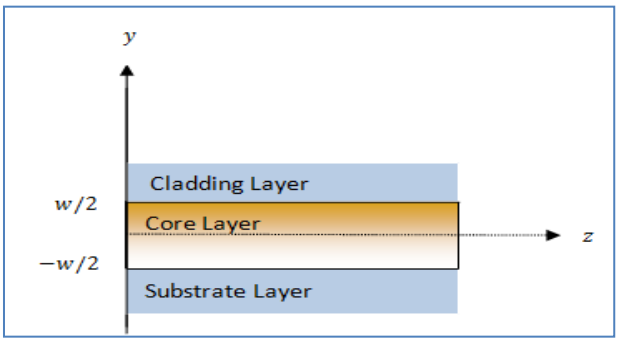


Figure 3 Dielectric slab structures [2].

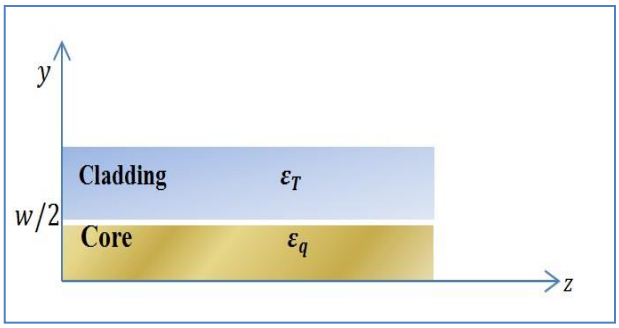


Figure 4 A schematic of a symmetric step-index slab waveguide [2].

2.1 Electric & Magnetic Modes Modeling Equations

The analysis of dielectric slab waveguide will consider the symmetric property, therefore; one interface is tested instead of whole structure. As it is shown in figure (4), the thickness at $(y = \frac{w}{2})$ represents the interface between the core and cladding layers where all fields must be continuous. This condition is achieved when

the propagation constant mode (β) is similar for both layers at the interface [2]. The mathematical method of solving this structure can be derived as follows.

Assume a plane wave that travels through the lossless dielectric medium. Its travelling plane is in y-z. Therefore, there is no field variation in x-direction. All Fields *F*(*y*, *z*) must satisfy electromagnetic wave equation: [2]

For core region where $y < \left|\frac{w}{2}\right|$ the electromagnetic wave equation is

$$\frac{\partial^2 F_q(y,z)}{\partial y^2} + \frac{\partial^2 F_q(y,z)}{\partial z^2} + k_q^2 F_q(y,z) = 0 \quad (3)$$

For cladding region where $y > \left|\frac{w}{2}\right|$

$$\frac{\partial^2 F_T(y,z)}{\partial y^2} + \frac{\partial^2 F_T(y,z)}{\partial z^2} + k_T^2 F_T(y,z) = 0 \quad (4)$$

According to that, both TE modes and TM modes are possible to be solved.

In TE-Mode,

$E_z = 0$, and $\frac{\partial}{\partial_x} = 0$. Then, $\frac{\partial}{\partial_y} E_y = 0$.

The field at the interface must match all z values at $(y = w/2)$ to achieve the tangential field components and $[\beta = \beta_q = \beta_T]$ must be the same in all regions.

$$E_{qx}(y,z) = E_{qx}(y) e^{-j\beta z} \quad (5)$$

$$\frac{d^2}{dy^2} E_{qx}(y) - \beta^2 E_{qx}(y) + k_0^2 \varepsilon_q E_{qx}(y) = 0 \quad (6)$$

Where, ε_q : is the permittivity of the core layer

$$\frac{d^2}{dy^2} E_{qx}(y) + (k_0^2 \varepsilon_q - \beta^2) E_{qx}(y) = 0 \quad (7)$$

Suppose $k_q^2 = (k_0^2 \varepsilon_q - \beta^2)$

$$\frac{d^2}{dy^2} E_{qx}(y) + k_q^2 E_{qx}(y) = 0 \quad (8)$$

The solution of this equation is

$$E_x(\mathrm{y}) = A_q e^{-j(k_q y)} + B_q e^{j(k_q y)} \quad (9)$$

In the core region the wave equation will be simplified to the following expression in a symmetric configuration as shown in figure

$$E_{xq}(y) = A_q \cos(k_q y) + B_q \sin(k_q y) \quad (10)$$

Since the attention is given to one interface, it is possible to select one part of the above equation. The first part is chosen because of symmetry [2]

$$E_{xq}(y) = A_q \cos(k_q y) \quad (11)$$

The magnetic field can be derived from Maxwell equation

$$-jw\,\mu_0 H_q(y) = \begin{pmatrix} u_x & u_y & u_z \\ 0 & \frac{\partial}{\partial_y} & \frac{\partial}{\partial_z} \\ E_{Xq} & 0 & 0 \end{pmatrix}$$

$$-jw\,\mu_0 H_{qx} = 0$$

$$-jw\,\mu_0 H_{qy} = -\,(0 - \frac{\partial}{\partial_z} E_{Xq})$$

$$H_{qy}(y) = \frac{\beta}{\omega\mu_0} E_{Xq} = \frac{\beta}{\omega\mu_0} A_q \cos(k_q y)$$

$$-jw\,\mu_0 H_{qz} = (0 - \frac{\partial}{\partial_y} E_{Xq})$$

$$H_{qz}(y) = \mathrm{j}\frac{\mathrm{kq}}{\omega\mu_0} A_q \sin(k_q y)$$

For top layer

$$E_x(\mathrm{y}) = A_T e^{-j(k_T y)} + B_T e^{j(k_T y)} \quad (12)$$

In the top layer the field should decay in order to achieve the light confinement and obtain the maximum field distribution in the core region. Therefore, it is essential to assume $k_T = j|k_T|$,

$$E_{Tx}(\mathrm{y}) = A_T e^{|k_T| y} + B_T e^{-|k_T| y} \quad (13)$$

The incident amplitude (A_T) is considered to be zero, and then the second part will provide field decaying. The reason of having $A_T e^{|k_T| y} = 0$ to achieve the light confinement; otherwise, the field will spread to propagate away from the desirable area and become impossible to have field confinement.

$$E_{Tx}(\mathrm{y}) = B_T e^{-|k_T| y} \quad (14)$$

$$-jw\,\mu_0 H_T(y) = \begin{pmatrix} u_x & u_y & u_z \\ 0 & \frac{\partial}{\partial_y} & \frac{\partial}{\partial_z} \\ E_{Xq} & 0 & 0 \end{pmatrix}$$

$$-jw\,\mu_0 H_{Tx} = 0$$

$$H_{Ty}(y) = \frac{\beta}{\omega\mu_0} B_T e^{-|k_T| y}$$

$$H_{Tz}(y) = \frac{j|k_T|}{\omega\mu_0} B_T e^{-|k_T| y}$$

By deriving the electric field and magnetic field in both layers, it is possible to apply the boundary conditions at the interface (y=+w/2).

$$E_{qz}\left(y = +\frac{w}{2}\right) = E_{Tz}\left(y = +\frac{w}{2}\right)$$

$H_{qz}\left(y=+\frac{w}{2}\right)=H_{Tz}\left(y=+\frac{w}{2}\right)$

Then;

$A_q\cos(k_q\frac{w}{2})= B_T e^{-|k_T|\frac{w}{2}}$ (15)

$j\frac{kq}{\omega\mu_0}A_q\sin(k_q\frac{w}{2}) = \frac{j|k_T|}{\omega\mu_0}B_T e^{-|k_T|\frac{w}{2}}$ (16)

Dividing eq. (16) by eq. (15), the result will be,

$k_q\frac{w}{2}\tan(k_q\frac{w}{2}) = \frac{w}{2}\mid k_T\mid$

Let $u = k_q\frac{w}{2}$ and $v = \frac{w}{2}\mid k_T\mid$ then,

$utan(u) = v$ (17)

Since $k_q^2 = k_0^2\,\varepsilon_q - \beta^2$ and $k_T^2 = k_0^2\,\varepsilon_T - \beta^2$

$k_T = j|k_T|$, then $-|k_T|^2 = k_0^2\,\varepsilon_T - \beta^2$

After substitution, the equation will be reformed as follow:

$\beta^2 = k_0^2\,\varepsilon_q - k_q^2 = k_0^2\,\varepsilon_T + |k_T|^2$ (18)

$|k_T|^2 + k_q^2 = k_0^2\,\varepsilon_q - k_0^2\,\varepsilon_T$

Where k_0 , ε_q and ε_T are given, which are used to find k_q , k_T .

$u = \frac{w}{2}\ k_q$, $v = \frac{w}{2}\mid k_T\mid$

$Q = \frac{w}{2}(|k_T|^2 + k_q^2) = k_0^2\,\varepsilon_q - k_0^2\,\varepsilon_T$

$Q = \frac{w}{2}k_0^2\sqrt{\varepsilon_q - \varepsilon_T}$ (19)

Now, it is possible to find the propagation constant mode in terms of u and v,

$\beta^2 = \left(\frac{2}{W}\right)^2(v^2+u^2)$ (20)

$\begin{cases} u\,tan(u) = v \\ Q^2 = u^2 + v^2 \end{cases}$ For symmetric TE-Mode (21)

In case of TM mode, the formula of the propagation wave for both fields will be as follows:

$H(y,z) = u_x H_x(y,z)$

$E(y,z) = u_y E_y(y,z) + u_z E_z(y,z)$

The same principle is applied to obtain the TM symmetric modes which results in,

$\begin{cases} utan(u) = \frac{n_2^2}{n_3^2}v \\ Q^2 = u^2 + v^2 \end{cases}$ For symmetric TM –Mod (22)

These are the main equations of obtaining the propagation constant mode (β) and the effective refractive index which play an important role in the design of optical devices.

2.2 Numerical Solution for (TE-Mode) Symmetric Slab Waveguide

The numerical method of solving slab waveguide in this paper is based on the mathematical calculation that is presented in detail in the previous section and then simulated by using Matlab. The test is made to examine the propagation modes for slab symmetric structure in terms of searching for a desired value of the propagation constant mode (β) . Afterward, it is possible to find the other parameters to obtain the bound mode in the structure shown in figure (5) [2].

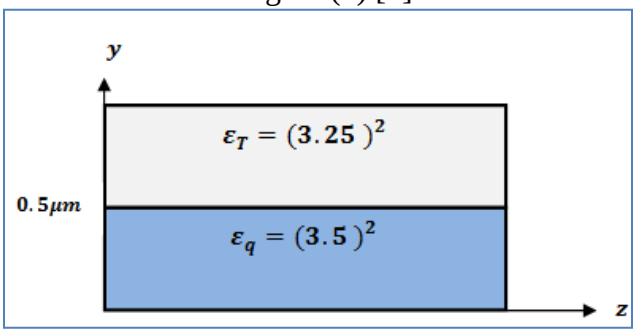


Figure 5 Symmetric slab waveguide ($\varepsilon_q > \varepsilon_T$)

As it is demonstrated in figure (5), a simple slab waveguide (symmetric) is introduced with parameters as follows:

- The permittivity of the core region $is\ \varepsilon_q = (3.5)^2$, this therefore gives refractive index is $n_q = 3.5$, where $n_q = \sqrt{\varepsilon_q}$.
- The permittivity of the cladding (top) region is $\varepsilon_T = (3.25)^2$,$n_T = 3.5$
- The free space wavelength is $\lambda = 1\mu m$.
- The thickness is $d = \frac{w}{2} = 0.5\mu m$.

The numerical analysis begins with equation (17). Mathematically, this equation has no solution; therefore it is only solved by the following way:

$u\,tan(u) = v$. Substituting v in$Q^2 = u^2 + v^2$

$Q^2 = u^2 + (u\,tan(u))^2$, Q = $\frac{w}{2}k_0\sqrt{\varepsilon_q - \varepsilon_T}$.

The final formula of this equation is

$$f(u) = u + \mathrm{Q}\cos(\mathrm{u}) \quad (23)$$

Since the equation (23) has no a mathematical solution, consequently; the only solution is to search for the value of (u) at $f(u) \approx 0$. This can be achieved by giving a range to u and search for the value of $f(u)$. When the $f(u)$ value equals to or close to zero, in this case the corresponding value of (u) is selected to be used in this simulation to find the other parameters. The following figure (6) shows the curve changes from negative to positive sign when $f(u) \approx 0.0119$ at value of $u = 1.26$

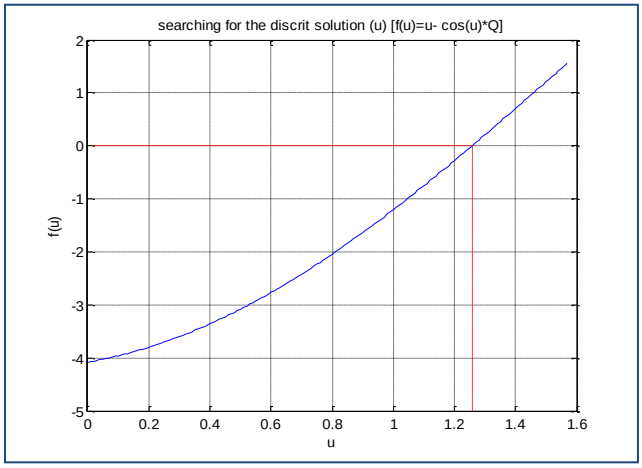


Figure 6 The value of the discrete solution($f(u) = u - cos(u)Q$).

According to the value of (u) , all other parameters in this structure can be obtained. The main condition to solve a dielectric waveguide structure is to find the propagation constant mode (β) as introduced in equation (18).

This is the propagation constant mode for the core layer, and also the cladding layer. It must be equal for both layers to ensure the field is matched at the interface. To obtain the propagation constant mode, the normalized propagation constant parameters such as $k_{0,}\ k_q and\ k_T$ must firstly be calculated.

Since,

$$k_0 = \frac{2\pi}{\lambda}\ ,\ v = \sqrt{Q^2 - u^2}\ \ ,\ k_q = \frac{u}{d}\ ,\ k_T = \frac{v}{d}\ \ and\ \ n_{eff} = \frac{\beta}{k_0}.$$

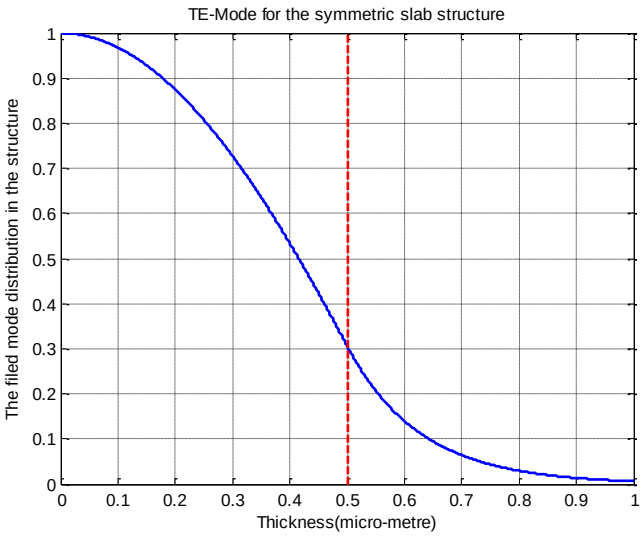


Figure 7 Field distributions in TE-Mode with core thickness (0.5µm).

The second condition is to calculate the effective refractive index. The validation of this test is to have the value of n_{eff} within the interval between the two of core and cladding indexes. In this test, the value of n_{eff} must satisfy the following relation.

$$n_T < n_{eff} < n_q$$

Figure (7) shows the field distribution for symmetric structures. The y-axis shows the field mode distribution, while x-axis represents the thickness of the layer. For this simulation the thickness d is given 0.5 μm at where the red dashed line demonstrated. The dashed red line represents the interface between the core and top layer.

The above figure assures the condition of optical structures, since there is an exponential decay toward the interface and most field amount bounded in the core layer.

In case of the thickness $d = 0.5\mu m$, the propagation constant mode equals$(21.8463\mu m^{-1})$. This gives effective refractive index of(3.4769). It is a sufficient result to achieve the bound mode in the core layer, since n_{eff} lays between the refractive indexes of core and outmost layer and it is closer to refractive index of the core than that of the cladding one.

To test the strength of the bound mode, the structure is modified to have various thicknesses of the core region. As it is represented in the table (1),

Table 1 Results of TE-Mode for a symmetric dielectric slab waveguide ($\varepsilon_q = (3.5)^2, \varepsilon_T = (3.25)^2$)

TE-Mode						
$d(\mu m)$	u	Q	k_q	k_T	$\beta(\mu m^{-1})$	n_{eff}
0.5	1.26	4.0810	2.5200	7.7633	21.84	3.47
0.4	1.2	3.2648	3	7.5908	21.78	3.46
0.2	0.95	1.6324	4.7500	6.6376	21.47	3.41

The modification is made on figure (8) to have thicknesses $0.4\mu m$, $0.2\mu m$ respectively. These result in having propagation constant modes $(21.7856\ \mu m^{-1})$ and $(21.4720 \mu m^{-1})$ with effective refractive indexes $(3.4673)\ and\ (3.4174)$ respectively. From these results, it is pointed out that the increase in the thickness enhances the mode to be stronger and more bounded. Therefore, when the thickness is $0.5\mu m$, the effective refractive index (n_{eff}) has a value which is the closest to the refractive index of the core region (n_q).

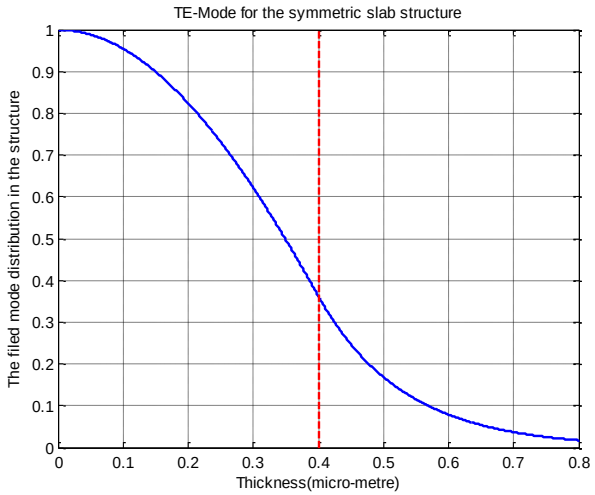


Figure 8 Field distributions in TE-Mode with core thickness $(0.4\mu m)$.

Figure (7) and figure (8) show a decaying in the field from the cladding layer towards the interfaces that are represented in red dashes.
In Figure (7) the field has more confinement than that in figure (8) because of the thickness. Not only the thickness can enhance the field, but also the refractive index and the material of the layers can play a significant role for modifying the optical structure. All of the results above are presented in terms of having symmetric TE-Mode.
It is therefore possible to simulate the whole structure shown in figure (3) to prove that the transverse electric field profile is symmetric as shown in Figure (9). It shows the field mode distribution of the whole structure evaluates the validity of the symmetry case that is assumed and derived in figures above. The both dashed red lines show the thickness width of core layer between (-0.5) and (0.5). This figure ensures the valid condition of optical structures, where the field experiences decay for both the substrate and cladding (top) layers, while more field bounded in the core (desired) region. This can be obtained if and only if the following assumptions applied:

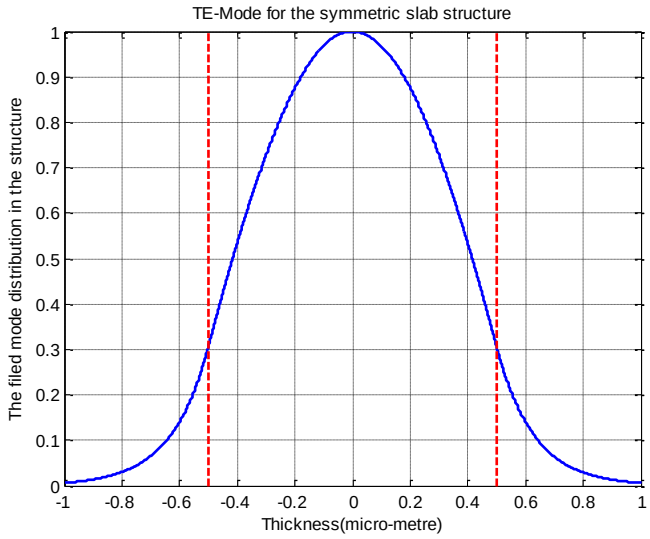


Figure 9 Field distribution of whole lab structure

1. Necessity of surrounding the high index (core) layer, where majority of the

radiation energy is confined, by low refractive index (cladding) media.

2. Propagation mode β must be resulted from integrating total internal reflection and constructive interference. This can be performed by invoking the tangential components continuity of the electric and magnetic fields at the interfaces.

2.3 Numerical solution for (TM-Mode) symmetric slab waveguide

It is essential to clarify that there is no magnetic field propagates along the direction of the wave travel (z- direction) in case of TM-Mode. The same slab waveguide structure in figure (5) is used to solve TM-Mode [2]. In this case the simulation steps are the same; however, equation (21) is used instead.

$$f(u) = u\sqrt{1 + \frac{\varepsilon_T}{\varepsilon_q}\tan(u)} - Q$$

The results are also obtained according to the variation the thickness of the core such as at $0.5\,\mu m$ and $0.4\,\mu m$ as shown in both figures (10) & (11).

The equation above cannot mathematically be solved, and then the possible method is to change the value of(u). This value is selected when$f(u) \approx 0$

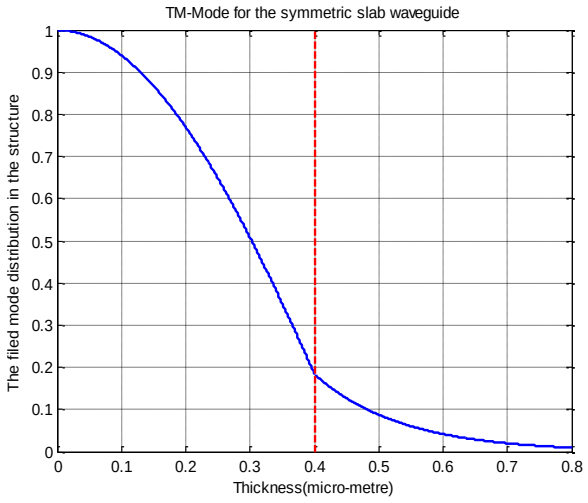


Figure 10 Field distributions in TM-Mode with core thickness (0.4μm).

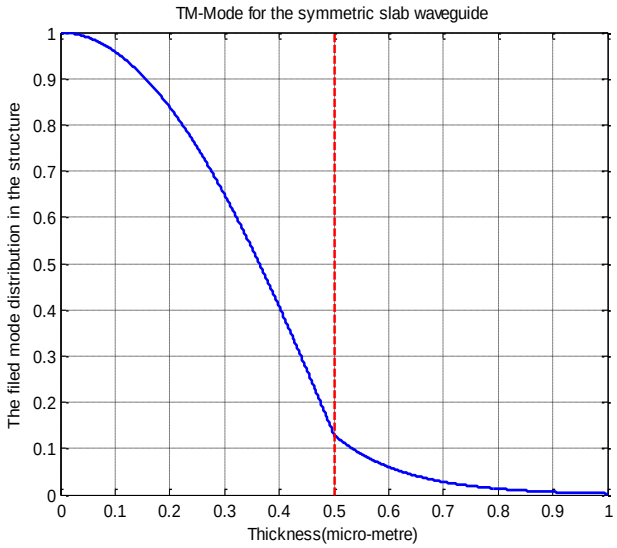


Figure 11 Field distributions in TM-Mode with core thickness (0.4μm).

Table 2 Results of TM-Mode for a symmetric dielectric slab waveguide ($\varepsilon_q = (3.5)^2, \varepsilon_T = (3.25)^2$)

TM-Mode						
$d(\mu m)$	u	Q	k_q	k_T	$\beta\ (\mu m^{-1})$	n_{eff}
0.5	1.44	4.08	2.89	7.631	21.79	3.46
0.4	1.38	3.26	3.46	7.391	21.71	3.45

In case of TM- Mode, table (2) shows the results based on two thicknesses $0.5\,\mu m$ and $0.4\,\mu m$. Both of them meet the condition of having field confinement and an effective refractive indexes lay between the core and cladding indexes. The results achieved from TE-Mode and TM-Mode demonstrates that the thickness has a vital impact on the strength of the field, since there is a forward proportional between the thickness and field strength. This is represented in the figures (10) and (11).

3 OPTICAL STRUCTURE WITH ACTIVE CORE

The best candidate material is recently used in the application of the optical circuits is Gallium Arsenide GaAs. This compound consists of a

combination of Gallium and Arsenide [5]. It has played a major role since was being used in the diodes and then in the integrated electronic circuits [5]. The main reason of using this compound is because it works efficiently in the ultra- high frequencies. Furthermore, it produces less noise which makes it beneficial in case of having weak signal amplification. According to its physical properties, it is placed instead of using silicon to manufacture advanced digital integrated circuits [6].

The major goal is to design a single mode index guided of Gallium Arsenide *(GaAs)* to work at room temperature($300kelven$). This is an active core which is encapsulated by cladding called Aluminium Gallium Arsenide *($Al_x\ Ga_{1-x}\ As$)* [7]. The variable (x) is defined as a number that varies between 0 and 1 referring to the mixture between *GaAs* and *Al As*. It can be seen that *$Al_x\ Ga_{1-x}\ As$* is utilized as material depends on the heterostructure devices. This provides more confinement of the electrons towards *GaAs* area [7]. Assuming $x = 0.25$, the target is to calculate the propagation modes to hit the lasing threshold. Figure (12) shows the symmetric slab with an active core of semiconductor. This kind of structure has a tiny active core thickness.

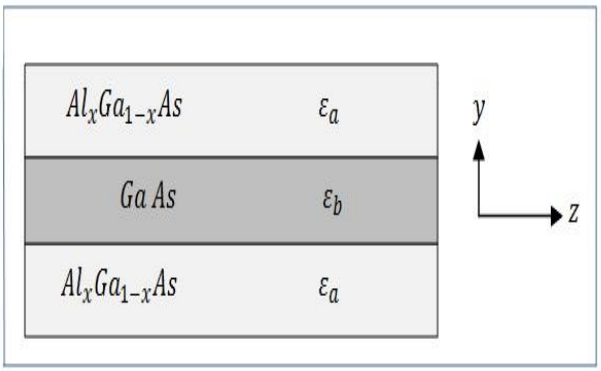


Figure 12 Active (Ga As) semiconductor structure [7].

The simulation is conducted in case of having both an active mode with a real permittivity as well as an active mode with complex permittivity

3.1 Simulating Semiconductor Laser Core with A Real Permittivity

To test this structure, there is a need to define the initial values which are as follows:

- The permittivity of the cladding $\varepsilon_a = (3.5)^2,\ n_a = 3.5$.
- In case of $\varepsilon_b = (n_a + \Delta n)^2$, as Δn^2 is very small variation ,then $\varepsilon_b = {n_a}^2 + 2\, n_a \Delta n.$ $\varepsilon_a = (3.5)^2 + 2(3.5)(0.62x)$, where x=0.25.
- The wavelength is $\lambda = 0.8\mu m$ and the thickness is $0.1\ \mu m$.

The procedure of solving this device is the same as those in the ordinary waveguide. In this case, TE-Mode is tested using the equation (18) to find the propagation constant mode. The results are achieved as in the following table since the thickness is considered be$(0.1\ \mu m)$.

Table 3 Results of TE-Mode for a symmetric active core slab waveguide ($\varepsilon_a = (3.5)^2, \varepsilon_b = 13.3350$)

TE-Mode						
$d(\mu m)$	u	Q	k_b	k_a	β	n_{eff}
0.1	0.65	0.818	6.5	4.69	27.934	3.556

The implementation is extended to include the optical structures with an active core region instead. This makes the fabrication more efficient for introducing a device with more lasing and better field confinement. The useful selection is to use semiconductor laser with heterostructure devices. From figure (12), the $(GaAs)$ compound is used as active medium encapsulated by$(Al_x\ Ga_{1-x}\ As)$. The permittivity of the cladding is given. However, to derive the permittivity of the core, the value of the parameter x must be taken into account because it represents the percentage of mixing $GaAs$ and $Al\ As$, in this simulation $x = 0.25$. From table (3) the propagation constant β=27.9343 which is greater than those in the dielectric waveguide. That gives $n_{eff} =$

3.5567 which is a suitable result to provide stronger mode within the active region as shown in figure (13).

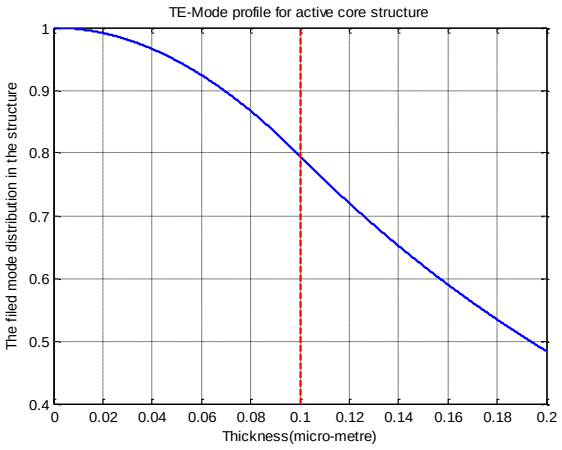


Figure 13 Field distributions in TE-Mode with active core thickness ($0.1\mu m$).

For more realistic paradigm, the modeling is improved to consider the material gain and modal gain to determine the confinement factor of the lasing action. To achieve that, it is more efficient to modify the structure with complex permittivity. The material gain is always given to determine the imaginary refractive index of the core. Once it is obtained, the complex permittivity can be calculated.

3.2 An Active Core Semiconductor Lasers with A Complex Permittivity

In this stage of the modification, it becomes obvious that there is a considerable possibility to achieve the optical gain. That is because the present structure is introduced with a very small perturbation in the core permittivity. Therefore, it is important to introduce the definition of the material gain and the modal gain since the relation between them results in the confinement factor.

Modal gain is defined as a fundamental aspect of modeling or shaping the optical amplifiers and semiconductor lasers. The ratio of modal to material gain can simply be achieved. This relation is known as a gain factor [8]. The following equation introduces the confinement factor that is defined as the ratio of the optical power in the active zone to the power of the whole structure.

$$\Gamma \text{ (confinement factor)} = \frac{\int_{-d}^{d} |s(z)| dz}{\int_{-\infty}^{\infty} |s(z)| dz} \quad (24)$$

Where, the numerator part of the equation represents the expected poynting vector in the particular region (active core region) while, the denominator defines the poynting vector of whole structure. Based on the derivation of the electromagnetic plane waves, the optical gain can be obtained from the poynting vector (s_z) since the refractive index is complex [9].

$$n = n_r + jn_i \text{ , and } k_o = \frac{2\pi}{\lambda}$$

$$s_z = \frac{1}{2}|A|^2 e^{-2(k_o n_i)z} \frac{k_o n_r}{w \mu_0} \quad (25)$$

Using this equation to establish the modification for the material permittivity in terms of the optical gain or loss, since

$$s_0 = \frac{1}{2}|A|^2 \frac{k_o n_r}{w \mu_0} \text{ and } g = \pm 2(k_o n_i) \quad (26)$$

After calculating the case of having an active core semiconductor laser with purely real permittivity, now the attention is being shifted to the active region with complex permittivity. This is more crucial step due to including the material gain to calculate the imaginary part of the permittivity. The following calculation demonstrates the procedure of obtaining the complex permittivity for the active core region [9].

$$\varepsilon_c = \varepsilon_b + j\,\varepsilon_i \quad (27)$$

Since ε_i is the small variation used for device modification, where $\varepsilon_i = n_i{}^2$.

The material gain is always given which is generated from the stimulated emission of moving the electrons from the lower to upper layer. In this case, $g = 200cm^{-1}$

$n_i = \frac{g}{2k_o}$, where,$\lambda = 0.8\mu m$, then $k_o = \frac{2\pi}{\lambda}$

After calculating the imaginary part of the refractive index, the complex permittivity becomes ($\varepsilon_c = 13.3350 + j0.0093$). It can be seen that the very small variation which

provides the modification for all other parameters.

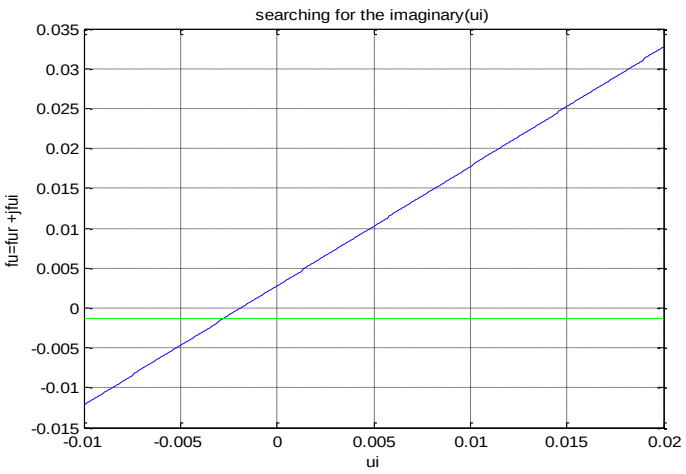


Figure 14 Searching for the discrete solution of u_i ($u_i = -0.0025$).

Since, $g = 200cm^{-1}$,$\lambda = 0.8\mu m$, then $k_o = \frac{2\pi}{\lambda} = 7.8540x10^{-4}cm^{-1}$

$n_i = \frac{g}{2k_o} = 0.0013$.

Then, $\varepsilon_c = (n_a + j\, n_i)^2 = 13.3350 + j0.0093$

This fabrication uses the same principles as in the dielectric and active structures starting with searching for discrete solution (u_i). In this simulation the imaginary part is provided in figure (13) since $u_i \approx -0.0025$. Then, the complex discrete solution is $u_c = u_r + ju_i = 0.65 - j0.0025$. The propagation constant mode is 27.9342-j0.0056. To calculate the confinement factor, the first step is to find the modal gain,

$\alpha = 2\beta_i$, where

$\beta_i = 0.0056$, $G = \alpha\, z = 151cm^{-1}$

Γ (confinement factor) = $\frac{151}{200} = 0.5750$

This is the confinement factor for achieving lasing action and the result is an appropriate percentage seems to be acceptable although for better reflection the confinement factor should be 0.3.

However, the metals that are used in optical structure are lossy because of their physical properties. Due to their properties, their permittivity becomes negative at the optical frequencies. This phenomenon leads to discovering a more suitable surface used at the interface to minimize the amount of loss and provide more lasing named surface plasmons. In this case the electromagnetic waves travels close to the interface.

4 DISCUSSIONS OF RESULTS

It is generally seen that solving waveguide structure is based on the field profile confinement in the core region in conjunction with a decaying for the field form outermost layers towards the surface. According to the results, there is a noticeable improvement in the bound mode based on the improvement of the optical waveguide modification. Starting with a simple case of dielectric slab waveguide, by applying the boundary conditions, all fields must be continuous at the interface. The solution of these structures is based on the transcendental equations (21) to obtain the dispersion relations $u = Q\cos(u)$ where Q contains the free space wavelength and the permittivity of the core and cladding.

As a result, calculating propagation constant mode (β) is a fundamental step to modify the device. If (β) is obtained, the effective refractive index can be simply achieved based on the relation between them. The results show that the n_{eff} lays between both indexes of the core and the cladding. According to table (1) the values of n_{eff} as a function of the thickness variation are 3.4769, 3.4673 and 3.4174, which emphasis that the n_{eff} exists at any value between 3.25 and 3.5 for the core and cladding. That means it becomes possible to obtain the bound mode as represented in the figures (7) and (8) which are related to TE-Mode of the symmetric dielectric slab waveguide.

The same procedures and conditions are applied for TM-Mode symmetric dielectric slab waveguide. The variation of the core's thickness impacts on the strength of the bound mode. As a result, due to the increase in the

thickness, the mode becomes stronger. In this paper the test is made by assuming the thicknesses$0.5\mu m$, $0.4\mu m$ *and* $0.2\mu m$. When the thickness is $0.5\mu m$ the effective refractive index n_{eff} has a result that closer to the refractive index of the core compared to the other thicknesses as shown in table (1).

The results that are interpreted above have led to the desire for knowing the quantity of the gain in the structure. For this reason, the semiconductor laser is introduced to the structure. In this case, the structure consists of a thin active core region which is a compound of gallium arsenide coating by$(Al_x\, Ga_{1-x}\, As)$. The value of propagation constant increases to result in approximately $27\mu m^{-1}$ compared to above $21\mu m^{-1}$in dielectric slab waveguide. This in turn enhances the confinement of the bound mode. However, to achieve the modal gain, it was useful to fabricate the structure to a complex permittivity instead. Therefore, the modal gain is obtained from the imaginary part of the propagation constant mode. The material gain is given and modal gain can be achieved based on the amount of the power in the core, therefore, the confinement factor can be obtained. In this test the result of the confinement factor is0.5750.However, based on the other studies, the confinement factor should be around 0.3 to achieve better lasing.

5 CONCLUSIONS

To sum up, according to the appropriate results that have been obtained, there is a gradual improvement for fabricating the optical integrated circuits. The modification is conducted to begin with the implementation of the dielectric slab waveguide and then considering the active medium. These structures are the platform for designing and developing the optical circuits. The result confirmed the validation of optics field profiles. All figures shows that the most field is obligated to travel through the core layer rather than the outmost layers. This can only be applicable if the refractive index for the core layer greater than the surrounded one. However, it was strongly recommended to consider the demand for miniaturizing the optical devices which is based on the power consumption and the type of the metal used. The purpose behind that is some materials are not suitable at optical frequencies due their physical properties. The direction towards smaller optical devices with less power consuming indicates that the tangential and ray (geometrical) optics are not applicable. That is because the metal at the optical frequencies behaves as plasma based on the free electron and holes of the materials. This is similar to the ionosphere layer at the radio frequencies. For this reason, the heterostructure compound is the most appropriate structure to be used to validate the achievement of laser and confining the field within the desirable area.

6 REFERENCES

[1] M. L. Calvo and V. Lakshminarayanan, *Optical waveguides: from theory to applied technologies*: CRC Press, 2010.

[2] L. Gin´es, *Integrated Photonics: Fundamentals* , John Wiley & Sons Ltd, England,2003.

[3] V. Krishnamurthy, *Theoretical investigation of photonic crystal and metal cladding for waveguides and lasers*: ProQuest, 2009.

[4] K. Vahala, *Optical microcavities*: World Scientific, 2004.

[5] A. Podhorodecki, J. Andrzejewski, M. Motyka, R. Kudrawiec, J. Misiewicz, J. Wojcik,"Optical properties of InGaAsP quantum well for infrared emission investigated by modulation spectroscopy," *Optica Applicata*, vol. 35, p. 509, 2005.

[6] S. M. Sze and K. K. Ng, *Physics of*

semiconductor devices: John Wiley & Sons, 2006.

[7] J. S. Smalley, Q. Gu, M. Puckett, and Y. Fainman, "Temperature dependences of metal-clad subwavelength semiconductor lasers (MCSELs): geometric invariance and the spontaneous emission factor," in *SPIE OPTO*, 2014, pp. 89800X-89800X-10.

[8] C. Ning, "Semiconductor nanolasers," *physica status solidi (b)*, vol. 247, pp. 774-788, 2010.

[9] H. Kressel, *Semiconductor Lasers and Herterojunction LEDs*: Elsevier, 2012.

Application and Implementation of Wearable Sensor for Real-Time Activity Tracking

Nesrine Amin Elessawy *Mohamed Saad Zaghloul* *Roshdy Abdel-Rasoul*
Electronics and Communication Department
Arab Academy for Science and Technology
Alexandria, Egypt
nesrine.elessawy@yahoo.com dr_mszaghloul@yahoo.com roshdy.aa@gmail.com

ABSTRACT

The aim of this paper is to summarize the latest applications in the field of bioelectronics with wearable sensor techniques and activity tracking systems. The main work focused on health and wellness, safety, home rehabilitation, assessment of treatment and early detection of disorders. This is especially important for diabetes patients who require regular monitoring of their blood sugar levels and constant analysis of physiological movements and signals in real-time under certain conditions to allow them to live independently longer and help them in case of emergency.

KEYWORDS

(Wearable Sensors; Biomedical Tracking Systems; Disease Control; Telemedicine)

1 INTRODUCTION

Our bodies radiate signals in a continuous way, but most of us don't know how to deal with those signals. However, with the latest technology of wearable sensors and trackers we can have some control on our daily activities [1].

Diabetes is becoming largely one of the major causes of premature illness that lead to immediate death. According to the World Health Organization's (WHO) [2] estimates, 347 million people in the world have diabetes. 90% of them suffer from type 2 diabetes which is largely caused by excess body weight and physical inactivity.

With the help of combining wearable technology with bio sensors [3], it is now more possible to gather and monitor the data that comes from our body in real-time, Simply by wearing sensors that can process all data simultaneously in real time, we can then monitor and control them using our handy smart phones and send them to doctors to be analyzed. Unfortunately, diabetes greatly increases the risk of stroke [4] so in this research we have designed a wearable belt that contains a non-invasive glucometer sensor and a high precocious 3-axis accelerometer to help in case of emergency to monitor patient's movements.

The common old technique of measuring blood sugar level can be painful especially to children, messy as

it consists of different parts. It is not reliable at all for measurements because most of type 1 diabetes patients measure their sugar blood level once a day instead of measuring 4 times as recommended [5] and by that they can put their life in danger. The proposed system will take all of the measurements according to its pre-set time and it can easily be reprogrammed as required. The more considerable part in the project enables the patient to monitor their results throughout the day instantly and in case there is a slight change in measurements, it alerts the patient through the application. Furthermore, in case there is a significant change in the measurements, the patient's doctor or relative can be notified automatically on their mobile phone or even through their email in order to provide immediate assistance to the patient.

2 PRACTICAL WORK

The wearable biometric system is divided into three autonomous modules that consist of hardware components, software protocol and a monitoring device shown in the form of a block diagram in Fig.1. The main components to be used are a 3-axis Accelerometer Compass sensor [6] as shown in Fig.2. for precious measurements with gravity. It gives the exact direction of the human body towards Earth's alignments, a non-invasive Glucometer that consists of a light source e.g. (LEDs) and a detector. The amount of near infrared light that passes through the skin depends on the glucose in the blood and the amount of Near Infrared (NIR) light source applied on the skin, while a receiver is attached on the other side to receive the attenuated light signal. Photodiodes of wavelength range (1150nm-2200nm) are preferably used [7]. The amount of blood can be estimated by red and infrared (IR) light to differentiate between skin levels to get saturated oxygen. A green light emitting diode is used to measure skin thickness for precious results, then light signals are amplified and sampled to be processed by a flora type Arduino compatible controller [8] as shown in Fig.3. We have chosen it as it has external pins that can be easily sewed to a belt with other sensors for easy use and then the data is collected from both the Accelerometer sensor and glucometer to be sent via a Bluetooth module through the user's smart phone platform application. It enables monitoring and sharing with the desired person to get it analysed and recorded.

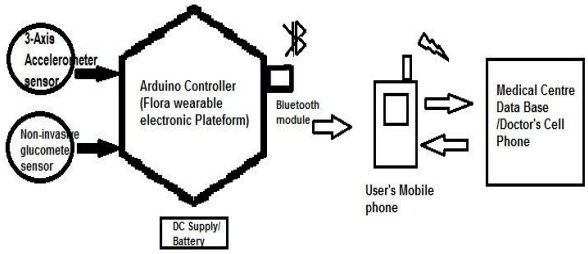


Figure 1. Process Configuration of the whole system

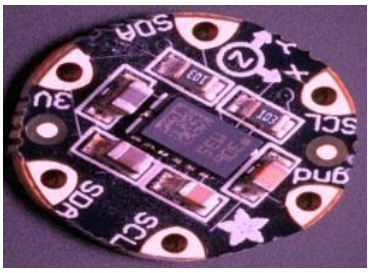


Figure 2. 3-Axis Accelerometer Sensor manufactured by Adafruit

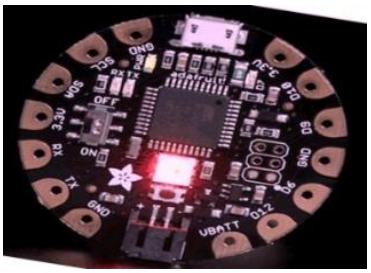


Figure 3. Controller Arduino compatible electronic device with external pins sensors to be sewed to the belt

Generation of training data by a Matlab program to be processed by the accelerometer for motion detection in a 3 dimensional figure by defining the 3 axis points (X-Y-Z) is shown below in Fig.4. The accelerometer sensor is connected to a Matlab program on a computer and tested several times for both behaviors; normal human being motion and in

the case of shock movements as shown on the graphs Figures 5 and 6.

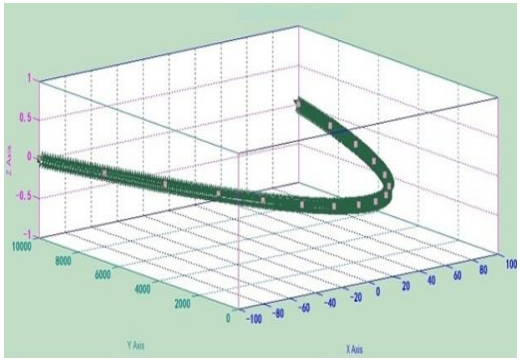


Figure 4. Training data 3D plot for motion detection by Matlab program

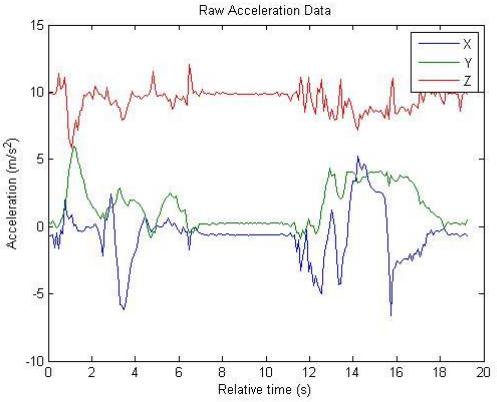


Figure 5. Normal accelerometer data behavior

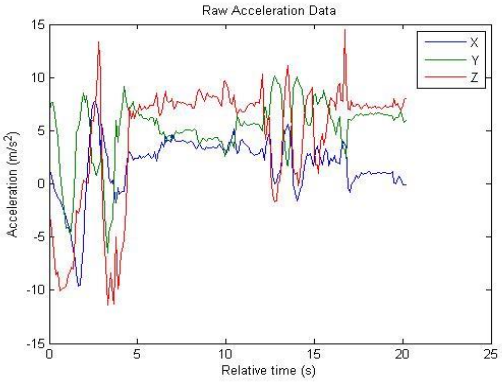


Figure 6. Shock Case data behavior

The Non-Invasive Glucometer sensor used in this study is one of the applications of Raman Scattering theory of light [9]. When the light is emitted from a light source most photons are scattered elastically. The scattered photons have the same frequency as the photons from the source. In Fig. 7 we can see near infrared behavior on different types of surfaces. As it is known when we apply a near infrared light to the skin, it will pass through a certain thickness of tissue [10] as shown below in Fig.8. Light emitted from the LED that can penetrate the skin's surface is absorbed by its tissue due to low scattering due to its high wavelength.

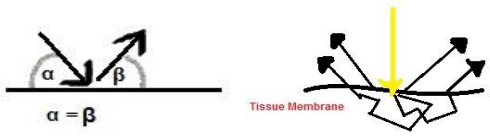


Figure 7. Light reflectance behavior in case of a flat glossy white surface where complete reflectance occur and on tissue surface where reflection and scatter occurs

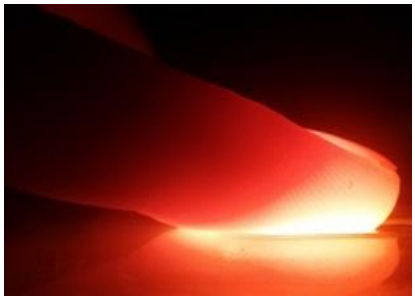


Figure 8. Flash light exposed through finger tissue in a dark room

As the light from the diode penetrates the tissue surface it will reflect back from the tissue membrane at a specific angle then it is detected by the sensor. Difference of angles refers to the amount of the glucose in the dermis as shown in the relation below for Θ which represents the angle of near infrared reflected back of dermis and **S** is the Glucose concentration in the blood. The angle value of reflected light is directly proportional to the glucose concentration in the blood.

$$\Theta \propto S \qquad (1)$$

3 RESULTS

We are wearing the sensors that can process all the data in real time by health monitoring systems so we

can have a better life style and minimize the occurrence of stroke. According to the international diabetes federation in 2013 [11] China is one of the top countries that recorded the highest diabetic cases of population of 98.4 million and India comes in the second place of diabetic cases of 65.1 million. It is also found that diabetes disease is expected to increase worldwide by 55% in 2035. Hence, starting recently many biomedical companies have raised their investments on new techniques and inventions that are related to glucose monitoring projects. Thanks to non-invasive glucometer projects, the reimbursement for test strips of old glucose measuring techniques decreased from the end of 2013 until the year of 2015 [12]. The most considerable component that the precious non-invasive glucometer system doesn't require is calibration. This is because the data to be measured is related directly to the concentration of glucose beneath dermis so each reading is considered to be the exact result.

4 CONCLUSION

In this study, we have presented a tele-medical monitoring system with non-invasive glucometer by near infrared diodes and 3 axis accelerometer sensors which allows us to monitor the measured data in real-time through our smart phones through a certain graphical user interface application via a Bluetooth connection. When a reading changes slightly, the patient is notified on the spot so that they are aware and can easily control and maintain their glucose level without constantly being worried about it. The accelerometer sensor can do the job and get the readings continuously to be monitored and shared with doctors in case of emergency instead of patients having their fingers pricked from time to time. This allows diabetes patients to improve their health status over time, allows them to easily maintain a healthy life style and live independently longer.

REFERENCES

[1] S. Patel, H. Park, P. Bonato, L. Chan and M. Rodgers. "A Review of Wearable Sensors and Systems with Application in Rehabilitation", Journal of Neuro Engineering and Rehabilitation, pp.9,21, 2012.

[2] World Health Organization "Global status report on non-communicable diseases", 2014 in Press.

[3] M. Tamsin, "Wearable Biosensor Technologies", vol. 13, no. 2, pp. 697–703, February 2015.

[4] T. Cade, "Diabetes-Related microvascular and macrovascular diseases in the physical therapy setting." Phys. Ther. 88, 1322-1335, November 2008.

[5] D.K. McCulloch, MD, " Patient information: Self-blood glucose monitoring in diabetes mellitus (Beyond the Basics)", 2015.

[6] D.A.D. Gómez, S.A. González, "Implementation of an Algorithm to Calculate Position using a 3-axis Accelerometer", 2015.

[7] M. Ahmad, A. Kamboh, A. Khan, "Non-invasive Blood Glucose Monitoring using Near-infrared Spectroscopy", 2013, in Press.

[8] B. Stern, " FLORA - Wearable electronic platform: Arduino-compatible - v2", Adafruit, 2015, in Press.

[9] J.J. Cael, K.H. Gardner, J.L. Koenig and J. Blackwell, "Infrared and Raman spectroscopy of carbohydrates. Paper V. Normal coordinate analysis of cellulose I", 1975.

[10] J.L. Smith, "The Pursuit of Noninvasive Glucose" Vol. 3, 2015.

[11] Anon., The International Diabetes Federation, "World Diabetes Cases Graph", Vol. 6, 2013.

[12] S.K. Vashist, P.B. Luppa, L.Y. Yeo, A. Ozcan, J.H.T. Luong, " Emerging Technologies for Next-Generation Point-of-Care Testing",vol. 33, pp. 692-705, 2015.

Evaluation of Digital Forensics Tools on Data Recovery and Analysis

Ioannis Lazaridis, Theodoros Arampatzis, Sotirios Pouros
AMC Metropolitan College
14th El. Venizelou Str., 54624, Thessaloniki, Greece
jnlazaridis@gmail.com

ABSTRACT

This paper presents a comparison and evaluation of several digital forensics tools on data recovery scenarios. Modern tools have been tested and evaluated in order to provide evidence regarding their capabilities in qualitative analysis and recovery of deleted data from various file systems. Results derived from the comparisons, present the capability of each digital forensics tool. Based on variables and specifications, the tool with the best performance is considered the most suitable application for analysing and retrieving files. A comparison between digital forensics tools takes place as well, alongside conclusions.

KEYWORDS

Forensic analysis, Data Recovery, Encase, Autopsy, FTK imager, DFF, OSForensics, Recuva

1 INTRODUCTION

Digital forensics is the science which deals with the discovery, validation and interpretation of digital evidence found in electronic devices, often in accordance to a computer crime. The main goal is to recover and preserve digital evidences to its original form, since it might be used to support a legal case. [1-8]. There is a significant variety of digital evidence sources, including personal computers, servers, laptops, hard drives, flash drives, smartphones and networks. In most cases the digital evidence is a common file or it is stored in a file such as:

- Image/Video/Audio Files
- System/Server/Network Log Files
- Emails
- Browser History/Cache
- Document Files such as .doc/.txt/.xml/.pdf

Hard drives are likely to include an Operating System (or more than one), application programs and user data stored in files. Hard drives also provide additional storage for system information used by the processor if necessary (backing store) [9-15].

The hierarchy of files is divided in six levels:

- Level 0 (Regular Files): The information contained in the file system. It includes the file names, file attributes and file content. Can be accessed directly.
- Level 1 (Temporary Files): Temporary files, including printed files (print spooler), the cache of the browser and files in the Recycle Bin. Many users believe that the system will automatically delete this data or even worst, they don't even know they exist.
- Level 2 (Deleted Files): When a file is deleted from the file system, most operating systems do not replace the blocks on the hard drive that the file is written - they simply remove the record reference from the containing directory. The blocks of the "erased" file are tagged as free for registration.

- Level 3 (Retained data blocks): Level 3 data include information of the virtual memory, slack space, backing store and level 2 data which are partially replaced and cannot be fully recovered.
- Level 4 (Vendor Hidden blocks): This layer consists of blocks of data that can be accessed only by using specific instructions provided by the manufacturer (Vendor). This level includes the control unit programs and data used for the block management.
- Level 5 (Overwritten data): It is believed by many experts that there is a possibility, data can be retrieved from a hard drive, even after the replacement (overwriting) of the blocks in which they were registered. Level 5 is reserved for such data [16].

Tools, techniques and methodologies for forensic investigation, collection and analysis of evidence are used worldwide. Besides recovering the evidences, it is important to maintain their integrity, throughout the investigation [17]. The modern digital forensic analysis tools are used to retrieve information and evidences from a hard disk. Thus, analysts can process hard drives regardless the operating system and file system, but also they can be sure that the integrity is maintained since tools analyse a virtual copy of the hard disk (disk image).

2 METHODOLOGY

The purpose of this paper is to provide practical results from data recovery scenarios, experimenting on different file systems and hard drive technologies, using several modern digital forensics tools. The tools are compared based on the number of deleted files detected and the percentage of their usability. Files such as photographs and videos that have been partially recovered, (e.g. miss some pixels), are considered a successful attempt, since those files can still be used as acceptable digital evidences. Continuing, the same tactic is used in specific experimental files (.zip .doc .jpeg .txt .avi) which have been written and deleted from from the digital devices.

2.1 Tools and evidences

The digital forensics tools that used were free, except Encase forensic software which was provided from AMC Metropolitan College as a part of the research. Specifically, the selected tools were Encase 7, Autopsy 3.1.2, OSForensics 2.2, FTK Imager 3.1.1.8 and Digital Forensics Framework (DFF). Finally, on that list of tools another one was added, (Recuva) which is not considered a digital forensic tool, but it can be used to recover deleted files.

• Windows 8.1 (NTFS) 640GB SATA III
• Windows 8.1 (NTFS) 128 GB SSD SATA III
• Kali Linux (ext4) 80GB SATA II Partition of 320GB
• Flash Drive (FAT32) 8GB

The list above includes all the discs that have been tested. Initially, it was necessary to ensure the integrity of the evidences. FTK Imager was used to create the E01 image files for each disc [20]. Recuva was used, from a third party laptop, since it doesn't support image analysis.

It should be noted that FTK Imager and DFF are not included in the first three scenarios for each image. That is because they don't include an image analysis feature which makes it impossible to calculate the total number of deleted/recovered files.

3 RESULTS

It should be mentioned that the research doesn't give a general assessment of each tool and all its features, but it compares the tools based on their capabilities in analysing and recovering of deleted files.

3.1 Windows 8.1 (NTFS) 640 GB

Table 1. Number of deleted files detected and recovered by each tool.

Encase	Autopsy	OSForensics	Recuva
281.924	27.953	9.354	19.046

The results in Table 1 indicate Encase's superiority compared to the other tools. Autopsy coming in the second place with almost 90% less detected files from Encase. Recuva comes in the third place with 19.046 files, with OSForensics coming last. The number of deleted files found by Recuva exceeds the number of OSForensics, which is offered as a digital forensics tool rather than as a simple file recovery tool.

Table 2. Percentage of file usability after restoration.

Encase	Autopsy	OSForensics	Recuva
60%	70%	60%	20%

While observing the results of Table 2 we understand that a large percentage of files identified by the Recuva is useless.

Table 3. Time required for disk analysis.

Encase	Autopsy	OSForensics	Recuva
7:38:00	3:12:00	0:00:50	0:00:07

Table 3 presents process time, which obviously differs between tools. Encase required more than 7 hours and Autopsy approximaterly 3 hours.

All of the tools were able to find an retrieve the experimental files, except Recuva which found four out of five. One of the retrieved files was useless in OSForensics, DFF and Recuva.

3.2 Windows 8.1 (NTFS) SSD 128 GB

Table 4. Number of deleted files detected and recovered by each tool.

Encase	Autopsy	OSForensics	Recuva
502.373	100.303	51.507	62.295

Table 4 illustrates that Encase managed to detect five times more files compared to Autopsy. The results are more or less same as the previous measurements (HDD), but the number of detected files for all the tools has been multiplied.

Table 5. Percentage of file usability after restoration.

Encase	Autopsy	OSForensics	Recuva
60%	70%	60%	20%

The percentage of the restored files usability, from the SSD image, is impresive, as shown in Table 5.

Table 6. Time required for disk analysis.

Encase	Autopsy	OSForensics	Recuva
5:22:34	1:18:00	0:00:45	0:00:17

Table 6 indicates the process time needed for each tool to analyse the evidence. The process time differs, especially with Encase and Autopsy, from the previous results (Table 3).

All tools, but Recuva, were able to locate and succesfully recover the experimental files.

From the results on the SSD image is clear that the number of deleted files found is almost double compared to HDD's results. It should be stated that TRIM was enabled on the SSD, before the E01 image was taken.

3.3 Linux Ubuntu Image E01 (ext4) 80GB

Table 7. Number of deleted files detected and recovered by each tool.

Encase	Autopsy	OSForensics
537.898	62.012	77

Regarding the Linux image, once again it is noticeable that Encase comes first with more than 500.000 files, followed by Autopsy which detected 62.000, while OSForensics managed to detect only 77 files. The results are presented in Table 7.

ISBN: 978-1-941968-34-5 ©2016 SDIWC

Table 8. Percentage of file usability after restoration.

Encase	Autopsy	OSForensics
15%	20%	16%

In Table 8 it can be noticed that most of the files detected were useless, they had been partially replaced, since most of them were system files which have been altered from several distribution updates.

Table 9. Time required for disk analysis.

Encase	Autopsy	OSForensics
3:52:00	3:08:00	0:00:57

Table 9 indicates that Autopsy required the same process time to analyse an 80GB ext image with a 640GB NTFS image.

Encase, Autopsy and FTK Imager were able to detect and recover all five experimental files. DFF detected three and recovered successfully two, while OSForensics recovered only one.

Recuva was excluded from these measurements, since it doesn't support any ext file systems.

3.4 USB Stick (FAT32) 8GB

Table 10. Number of deleted files detected and recovered by each tool.

Encase	Autopsy	OSForensics	Recuva
12.757	7.817	3.156	12

Table 10 illustrates that Encase was able to detect the most files, unlike Recuva which identified only 12.

Table 11. Percentage of file usability after restoration.

Encase	Autopsy	OSForensics	Recuva
55%	66%	60%	10%

From these initial results in Table 11, we may tell that the usability of the restored files was great since all of the tools were able to restore successfully at least 50% of the files, except Recuva which partially restored only one.

Table 12. Time required for disk analysis.

Encase	Autopsy	OSForensics	Recuva
0:36:00	0:22:00	0:00:54	0:00:11

It must be noted that the tools were not able to recover the image (jpeg), except Recuva which even failed to detect it.

Table 13. Number of deleted files detected and recovered by each tool.

Encase	Autopsy	OSForensics	Recuva
436	23	14	14

Results after formatting and installing Kali Linux into the USB are impressive. Table 13 presents that Encase managed to detect only 436 files from 12.700. Autopsy detected only 23 (from 7817), while OSForensics and Recuva recovered only 14.

Table 14. Percentage of file usability after restoration.

Encase	Autopsy	OSForensics	Recuva
15%	20%	16%	8%

Table 14 depicts that the usability of the detected files has been plummeted, since all of the tools could only partially recover files.

Table 15. Time required for disk analysis.

Encase	Autopsy	OSForensics	Recuva
0:24:00	0:09:00	0:00:25	0:00:09

As it is illustrated in Table 15 the time required for the image analysis, was slightly less, compared to the previous results in the USB image (Table 12).

None of the tools was able to detect or recover any of the experimental files.

4 FUTURE WORK

The next step would be to acquire product licenses from companies such as Paraben, AccessData, Belkasoft, TechPathways and X-ways, which would allow the implementation of high-level comparison scenarios based on the high end digital forensics tools. The tools could also be evaluated based on the system resources required such as CPU and RAM consumption.

5 CONCLUSIONS

Analysing the results for each image the conclusion derived is that among tools that

have been compared, Encase, followed by Autopsy, can be considered the most appropriate and reliable tool for data recovering in a professional level [19]. It should be borne in mind that all tools failed to recover the prerequisite number of digital evidences in the USB stick, since they are operating in the second level (Deleted Files) of the hierarchy of evidences, as mentioned in introduction [18]. It can be concluded, from the USB stick results, where all disk blocks have replaced their content, that it is impossible to properly recover files. It should be noted that there are different methods/tools which can be used in order to (partially) recover overwritten data.

6 REFERENCES

[1] A Yasinsac, R. E., 2003. Computer forensics education . From: s.l.:IEEE, pp. 15-23.

[2] ACPO, 2012. Good Practice Guide for Computer-Based Electronic Evidence, s.l.: ACPO.

[3] Akhgar, B., 2014. Cyber Crime and Cyber Terrorism Investigator's Handbook. s.l.: Syngress.

[4] Arpaci-Dusseau, R. H. A. C., 2014. File System Implementation.

[5] Bhanu Prakash Battula, B. K. R. R. S. P. T. S., n.d. Techniques in Computer Forensics: A Recovery Perspective. s.l.:s.n.

[6] Brenner, S. W., 2010. Cybercrime: Criminal Threats from Cyberspace.

[7] Buse, J. W., 2013. linux.org. Available at: http://www.linux.org/threads/ext-file-system.4365/[Accessed on 10 04 2016].

[8] Casey, E., 2009. Handbook of Digital Forensics and Investigation. From: s.l.:s.n., p. 567.

[9] Eoghan, C., 2004. Digital Evidence and Computer Crime. Second Edition επιμ. s.l.:Elsevier.

[10] GL Palmer, I. S. H. V., 2002. Forensic analysis in the digital world. International Journal of Digital Evidence.

[11] Horenbeeck, M. V., 2008. Mobile forensics. From: Technology Crime Investigation. s.l.:s.n.

[12] Jean-Loup, R., 2013. From Young Hackers to Crackers. International Journal of Technology and Human Interaction.

[13] John, J. L., 2012. Digital Forensics and Preservation. s.l.:DPC Technology Watch Report.

[14] Jones, K. J., 2005. Real Digital Forensics: Computer Security and Incident Response. s.l.:s.n.

[15] K.K. Arthur, H. V., 2007. AN INVESTIGATION INTO COMPUTER FORENSIC TOOLS. Pretoria: University of Pretoria.

[16] A Yasinsac, R. E., 2003. Computer forensics education . From: s.l.:IEEE, pp. 15-23.

[17] ACPO, 2012. Good Practice Guide for Computer-Based Electronic Evidence, s.l.: ACPO.

[18] Akhgar, B., 2014. Cyber Crime and Cyber Terrorism Investigator's Handbook. s.l.: Syngress.

[19] Sommer, P., 2004. The future for the policing of cybercrime. *Computer Fraud & Security 2004*, pp. 8 - 12.

[20] Welch, T., 1999. Handbook of information Security Management. s.l.:CRC Press LLC