LEMBAR
HASIL PENILAIAN SEJAWAT SEBIDANG ATAU *PEER REVIEW*
KARYA ILMIAH : JURNAL ILMIAH

Judul Jurnal Ilmiah (Artikel)	:	Smart Agent and Modified Master-Backup Algorithm for Auto Switching Dynamic Host Configuration Protocol Relay through Wireless Router		
Jumlah Penulis	:	3 orang (Wahyul Amien Syafei, Yosua Alvin Adi Soetrisno, **Agung Budi Prasetijo**)		
Status Pengusul	:	penulis ke-3		
Identitas Jurnal Ilmiah	:	a. Nama Jurnal	:	International Journal of Communication Networks and Information Security (IJCNIS)
		b. Nomor ISSN	:	2073-607X (Online)
		c. Vol, No., Bln Thn	:	Vol 12, No 2 (2020)
		d. Penerbit	:	Institute of Information Technology, Kohat University of Science and Technology
		e. DOI artikel (jika ada)	:	-
		f. Alamat web jurnal	:	https://www.ijcnis.org/index.php/ijcnis/article/view/4478
		Alamat Artikel	:	https://www.ijcnis.org/index.php/ijcnis/article/download/4478/402
		g. Terindex	:	Scopus, Q3

Kategori Publikasi Jurnal Ilmiah (beri ✓ pada kategori yang tepat) :

√	Jurnal Ilmiah Internasional
	Jurnal Ilmiah Nasional Terakreditasi
	Jurnal Ilmiah Nasional Tidak Terakreditasi

Hasil Penilaian *Peer Review* :

Komponen Yang Dinilai	Nilai Reviewer		Nilai Rata-rata
	Reviewer I	Reviewer II	
a. Kelengkapan unsur isi jurnal (10%)	3,50	3,80	3,65
b. Ruang lingkup dan kedalaman pembahasan (30%)	11,00	11,50	11,25
c. Kecukupan dan kemutahiran data/informasi dan metodologi (30%)	11,50	10,50	11,00
d. Kelengkapan unsur dan kualitas terbitan/jurnal (30%)	11,70	11,60	11,65
Total = (100%)	**37,70**	**37,40**	**37,55**
Nilai Pengusul = (40% x 37,55) / 2 = 7,51			

Semarang, 15 Juli 2021

Reviewer 2

Dr. Adian Fatchur Rochim, S.T., M.T.
NIP. 197302261998021001
Unit : Dept. Teknik Komputer FT UNDIP

Reviewer 1

Dr. Ir. R. Rizal Isnanto, S.T., M.M., M.T., IPM
NIP. 197007272000121001
Unit : Dept. Teknik Komputer FT UNDIP

LEMBAR
HASIL PENILAIAN SEJAWAT SEBIDANG ATAU *PEER REVIEW*
KARYA ILMIAH : JURNAL ILMIAH

Judul Jurnal Ilmiah (Artikel)	:	Smart Agent and Modified Master-Backup Algorithm for Auto Switching Dynamic Host Configuration Protocol Relay through Wireless Router		
Jumlah Penulis	:	3 orang (Wahyul Amien Syafei, Yosua Alvin Adi Soetrisno, **Agung Budi Prasetijo**)		
Status Pengusul	:	penulis ke-3		
Identitas Jurnal Ilmiah	:	a. Nama Jurnal	:	International Journal of Communication Networks and Information Security (IJCNIS)
		b. Nomor ISSN	:	2073-607X (Online)
		c. Vol, No., Bln Thn	:	Vol 12, No 2 (2020)
		d. Penerbit	:	Institute of Information Technology, Kohat University of Science and Technology
		e. DOI artikel (jika ada)	:	-
		f. Alamat web jurnal	:	https://www.ijcnis.org/index.php/ijcnis/article/view/4478
		Alamat Artikel	:	https://www.ijcnis.org/index.php/ijcnis/article/download/4478/402
		g. Terindex	:	Scopus, Q3

Kategori Publikasi Jurnal Ilmiah (beri ✓ pada kategori yang tepat) :
- [√] Jurnal Ilmiah Internasional
- [ ] Jurnal Ilmiah Nasional Terakreditasi
- [ ] Jurnal Ilmiah Nasional Tidak Terakreditasi

Hasil Penilaian *Peer Review* :

Komponen Yang Dinilai	Nilai Maksimal Jurnal Ilmiah			Nilai Akhir yang Diperoleh
	Internasional [40]	Nasional Terakreditasi [ ]	Nasional Tidak Terakreditasi [ ]	
a. Kelengkapan unsur isi jurnal (10%)	4,00			3,50
b. Ruang lingkup dan kedalaman pembahasan (30%)	12,00			11,00
c. Kecukupan dan kemutahiran data/informasi dan metodologi (30%)	12,00			11,50
d. Kelengkapan unsur dan kualitas terbitan/jurnal (30%)	12,00			11,70
Total = (100%)	**40,00**			**37,70**
Nilai Pengusul = (40% x 37,70) / 2 = 7,54				

Catatan Penilaian artikel oleh Reviewer :

1. **<u>Kesesuaian dan kelengkapan unsur isi jurnal:</u>**
   Isi jurnal International Journal of Communication Networks and Information Security (IJCNIS) sudah cukup lengkap, paper-paper yang diterbitkan juga sesuai dengan cakupan topik dari jurnal IJCNIS ini. Editorial Team dan Table of Contents telah sesuai, dan layak disebut sebagai jurnal internasional yang terindeks Scopus. Kategori jurnal adalah Q3 dengan SJR 0.216.
2. **<u>Ruang lingkup dan kedalaman pembahasan:</u>**
   Ruang lingkup adalah membahas Smart Agent dan algoritma Modified Master-Backup untuk Auto-Switching Dynamic Host Configuration Protocol Relay melalui Wireless Router. Pembahasan pada *Evaluation Process* dan *Conclusion* telah dilakukan cukup mendalam dan terperinci. Tingkat kemiripan menggunakan Turnitin dari paper cukup bagus yaitu 23%
3. **<u>Kecukupan dan kemutakhiran data/informasi dan metodologi:</u>**
   Data/informasi yang disajikan cukup mutakhir, ada 15 referensi yang digunakan yang berasal dari Jurnal Internasional, Prosiding Internasional yang cukup mutakhir dari tahun-tahun terbaru. Metodologi telah disajikan secara lengkap dan terstruktur.
4. **<u>Kelengkapan unsur dan kualitas terbitan:</u>**
   Kualitas terbitan cukup bagus untuk kategori jurnal *online*. Unsur terbitan dari jurnal sudah sesuai dengan kaidah yang disepakati dalam jurnal internasional.

Semarang, 15 Juli 2021
Reviewer 1

Dr. Ir. R. Rizal Isnanto, S.T., M.M., M.T., IPM
NIP. 197007272000121001
Unit : Dept. Teknik Komputer FT UNDIP

LEMBAR
HASIL PENILAIAN SEJAWAT SEBIDANG ATAU *PEER REVIEW*
KARYA ILMIAH : JURNAL ILMIAH

Judul Jurnal Ilmiah (Artikel)	:	Smart Agent and Modified Master-Backup Algorithm for Auto Switching Dynamic Host Configuration Protocol Relay through Wireless Router		
Jumlah Penulis	:	3 orang (Wahyul Amien Syafei, Yosua Alvin Adi Soetrisno, **Agung Budi Prasetijo**)		
Status Pengusul	:	penulis ke-3		
Identitas Jurnal Ilmiah	:	a. Nama Jurnal	:	International Journal of Communication Networks and Information Security (IJCNIS)
		b. Nomor ISSN	:	2073-607X (Online)
		c. Vol, No., Bln Thn	:	Vol 12, No 2 (2020)
		d. Penerbit	:	Institute of Information Technology, Kohat University of Science and Technology
		e. DOI artikel (jika ada)	:	-
		f. Alamat web jurnal	:	https://www.ijcnis.org/index.php/ijcnis/article/view/4478
		Alamat Artikel	:	https://www.ijcnis.org/index.php/ijcnis/article/download/4478/402
		g. Terindex	:	Scopus, Q3 SJR 0,22

Kategori Publikasi Jurnal Ilmiah (beri ✓pada kategori yang tepat) :

√	Jurnal Ilmiah Internasional
	Jurnal Ilmiah Nasional Terakreditasi
	Jurnal Ilmiah Nasional Tidak Terakreditasi

Hasil Penilaian *Peer Review* :

Komponen Yang Dinilai	Nilai Maksimal Jurnal Ilmiah			Nilai Akhir Yang Diperoleh
	Internasional [40]	Nasional Terakreditasi [ ]	Nasional Tidak Terakreditasi [ ]	
a. Kelengkapan unsur isi jurnal (10%)	4,00			3,80
b. Ruang lingkup dan kedalaman pembahasan (30%)	12,00			11,50
c. Kecukupan dan kemutahiran data/informasi dan metodologi (30%)	12,00			10,50
d. Kelengkapan unsur dan kualitas terbitan/jurnal (30%)	12,00			11,60
Total = (100%)	**40,00**			**37,40**
Nilai Pengusul = (40% x 37,40)/2 = 7,48				

Catatan Penilaian artikel oleh Reviewer :

1. **Kesesuaian dan kelengkapan unsur isi jurnal:**
   Kelengkapan jurnal cukup, dengan petunjuk untuk penulis, aplikasi submission online, namun demikian belum memiliki/berlanggan DOI. Paper ini memiliki kelengkapan dan kesesuaian unsur yang lengkap, baik abstrak, pendahuluan yang memunculkan masalah penelitian dari fenomena gap di sub-bab 1 (*introduction*), kajian pustaka, metode penelitian dan pengukuran release time menggunakan empat sistem yg berbeda). Artikel ditutup dengan kesimpulan dan saran (*future work*).
2. **Ruang lingkup dan kedalaman pembahasan:**
   Ruang lingkup tepat dan sesuai dengan scope jurnal, kedalaman pembahasan cukup dalam dengan memberikan gambaran ttg DHCP relay mampu menurunkan rejection rate koneksi client ke wireless router.
3. **Kecukupan dan kemutakhiran data/informasi dan metodologi:**
   Riset merupakan hasil penelitian eksperimental dengan memodifikasi DHCP melakukan backup, cukup berkontribusi dengan referensi *uptodate*. Literatur mengambil dari konferensi dan jurnal IJCNIS.
4. **Kelengkapan unsur dan kualitas terbitan:**
   Kualitas terbitan cukup baik, dengan indeks SJR 0,216

Semarang, 15 Juli 2021
Reviewer 2

Dr. Adian Fatchur Rochim, S.T., M.T.
NIP. 197302261998021001
Unit : Dept. Teknik Komputer FT UNDIP

Document type
Article

Source type
Journal

ISSN
20760930

View more

International Journal of Communication Networks and Information Security • Volume 12, Issue 2, Pages 248 - 255 • 2020

Smart agent and modified master-backup algorithm for auto switching dynamic host configuration protocol relay through wireless router

Syafei W.A.[a], Soetrisno Y.A.A.[a], Prasetijo A.B.[b]

Save all to author list

[a] Department of Electrical Engineering, Faculty of Engineering, Diponegoro University, Indonesia

[b] Department of Computer Engineering, Faculty of Engineering, Diponegoro University, Indonesia

Abstract

Potential problems in a wireless router are the number of connected clients to DHCP (Dynamic Host Configuration Protocol) services and the durability of connectivity. Practically, some of the wireless router limits the number of the client to 15 clients due to bandwidth consumption management. DHCP is one of the services needed by wireless router , but it might be interrupted when the memory or CPU is full. This article proposes a modification of the backup algorithm in DHCP relay to overcome this situation when the memory or CPU in the wireless router is limited. The proposed backup algorithm will automatically switch the main router to the backup router

Online ISSN: 2073-607X

IJCNIS

International Journal of Communication Networks and Information Security

International Journal of Communication Networks and Information Security (IJCNIS)

ISSN: 2073-607X (Online)

International Journal of Communication Networks and Information Security (IJCNIS) is a scholarly peer reviewed international scientific journal published three times (April, August, December) in a year, focusing on theories, methods, and applications in networks and information security. It provides a challenging forum for researchers, industrial professionals, engineers, managers, and policy makers working in the field to contribute and disseminate innovative new work on networks and information security. The topics covered by this journal include, but not limited to, the following topics:

- Broadband access networks
- Wireless Internet
- Software defined & ultra-wide band radio
- Bluetooth technology
- Wireless Ad Hoc and Sensor Networks
- Wireless Mesh Networks
- IEEE 802.11/802.20/802.22
- Emerging wireless network security issues
- Fault tolerance, dependability, reliability, and localization of fault
- Network coding
- Wireless telemedicine and e-health
- Emerging issues in 3G and 4G networks
- Network architecture
- Multimedia networks
- Cognitive Radio Systems
- Cooperative wireless communications
- Management, monitoring, and diagnosis of networks
- Biologically inspired communication
- Cross-layer optimization and cross-functionality designs
- Data gathering, fusion, and dissemination
- Networks and wireless networks security issues

IJCNIS publishes:

- Critical reviews/ Surveys
- Scientific research papers/ contributions
- Letters (short contributions)

To keep the price affordable to libraries and subscribers, we do not send complimentary reprints or complimentary copies to authors.

Peer Review

All manuscripts will be subject to a well established, fair, unbiased peer review and refereeing procedure, and are considered on the basis of their significance, novelty and usefulness to the Journals readership. The review output will be either accept or reject. A paper once rejected will not be considered again for review. The review process may take approximately two months to be completed. For accepted paper, should authors be requested by the editor to revise the text and minor changes, the revised version should be submitted within 1 month.

When paper is submitted, it is assigned to one of the Area Editor. If the submitted paper has scholarly contribution, the Area Editor assign the paper to two or three reviewers. For acceptance of paper, at least two postive reviews are required.

Indexing/ Abstracting

· SCOPUS
· INSPEC
· EBSCO
· Cabell's Directory
· International Abstracts in Operations Research (IAOR)
· Ulrich's
· TOC Premier
· Computer and Information Systems Abstracts
· Computers and Applied Sciences Complete
· SciTech Journals
· Technology Journals
· Computer Science Journals
· Telecommunication Journals
· Science Journals
· Google Scholar
· International Security & Counter-Terrorism Reference Center
· Scirus
· ScientificCommons
· Genamics JournalSeek
· Advanced Technology and Aerospace Journals
· NewJour - Electronic Journals and Newsletters
· Intute - Science Engineering and Technology
· Open J-Gate
· Computing - ProQuest

IJCNIS
Online ISSN: 2073-607X
International Journal of Communication Networks and Information Security

Editorial Team

Institute of Computing, International Journal of Communication Networks and Information Security (IJCNIS) ISSN: 2073-607X (Online)

IJCNIS
Online ISSN: 2073-607X
International Journal of Communication Networks and Information Security

Vol 12, No 2 (2020)

Table of Contents

Research Articles

Efficient Load Balancing for Cloud Computing by Using Content Analysis PDF
Preecha Somwang, (Rajamangala University of Technology Isan Thailand)

Abstract views : 17 | PDF views : 5

Smart Agent and Modified Master-Backup Algorithm for Auto Switching Dynamic Host Configuration Protocol Relay through Wireless Router PDF
Wahyul Amien Syafei, (Diponegoro University Indonesia)
Yosua Alvin Adi Soetrisno, (Diponegoro University Indonesia)
Agung Budi Prasetijo, (Diponegoro University)

Abstract views : 21 | PDF views : 13

MRGM: An Adaptive Mechanism for Congestion Control in Smart Vehicular Network PDF
Gurpreet singh Shahi, (Lovely Professional University India)
Ranbir Singh Batth, (Lovely Professional University India)
Simon Egerton, (La Trobe University)

Abstract views : 25 | PDF views : 12

Vehicular Networking Road Weather Information System Tailored for Arctic Winter Conditions PDF
Timo Sukuvaara, (Finnish Meteorological Insitute, Arctic Space Centre Finland)
Kari Mäenpää, (Finnish Meteorological Insitute, Arctic Space Centre Finland)
Daria Stepanova, (Finnish Meteorological Insitute, Arctic Space Centre Finland)
Virve Karsisto, (Finnish Meteorological Insitute, Meteorological Research Finland)

Abstract views : 16 | PDF views : 6

Surveys/ Reviews

Cyber Security Concerns in Social Networking Service PDF
Abdul Hamid, ( )
Monsur Alam, ( )
Hafsina Sheherin, ( )
Al-Sakib Khan Pathan, (Independent University, Bangladesh Bangladesh)

Abstract views : 47 | PDF views : 23

Symmetric Encryption Algorithms: Review and Evaluation Study PDF
Mohammad Nasser Alenezi, (Public Authority for Applied Education and Training Kuwait)
Haneen Khalid Alabdulrazzaq, (Public Authority for Applied Education and Training Kuwait)
Nada Qasem Mohammad, (Public Authority for Applied Education and Training Kuwait)

Abstract views : 50 | PDF views : 32

Institute of Computing, International Journal of Communication Networks and Information Security (IJCNIS) ISSN: 2073-607X (Online)

Smart Agent and Modified Master-Backup Algorithm for Auto Switching Dynamic Host Configuration Protocol Relay through Wireless Router

Wahyul Amien Syafei[1*], Yosua Alvin Adi Soetrisno[1] and Agung Budi Prasetijo[2]

[1]Department of Electrical Engineering, [2]Department of Computer Engineering
Faculty of Engineering, Diponegoro University, Indonesia

***Abstract*:** Potential problems in a wireless router are the number of connected clients to DHCP (Dynamic Host Configuration Protocol) services and the durability of connectivity. Practically, some of the wireless router limits the number of the client to 15 clients due to bandwidth consumption management. DHCP is one of the services needed by wireless router, but it might be interrupted when the memory or CPU is full. This article proposes a modification of the backup algorithm in DHCP relay to overcome this situation when the memory or CPU in the wireless router is limited. The proposed backup algorithm will automatically switch the main router to the backup router every time the main router's memory is busy. Two main scenarios are conducted in this research to examine the proposed backup algorithm. First, Cisco DHCP relay services combined with OpenWRT wireless router. Second, Mikrotik original "Capsman" protocol DHCP relay combined alternatively with wireless-enabled and OpenWRT wireless router. Run test results show that the proposed backup algorithm with DHCP relay which are configured in OpenWRT wireless router can extend the number of connected clients and the durability of the wireless router when run its services as DHCP forwarder to DHCP relay and DHCP server. These combinations slightly affect the IP release time compared to regular DHCP which employs a direct connection.

***Keywords*:** auto-switching, DHCP, release time, backup algorithm, wireless router, smart

1. Introduction

A wireless router is a common interface used in the network today because of portability and compatibility. The main function of wireless router is to provide connectivity to the internet and provide automatic IP address allocation to the client. The arrangement of IP allocation made with DHCP service. DHCP service is IP allocation service that managed by the wireless router. However, a wireless router is not able to provide an IP address to the client when DHCP service is running out. DHCP service does not take a lot of memory, but if a wireless router is running out of memory because of other services, the DHCP service may also become unavailable. When DHCP service is not available, the user must set the IP manually on the device [1]. Potential problems that always exist in the wireless router are the number of clients that request the DHCP service and the durability of that router serves DHCP service.

Generally, a wireless router can serve 253 clients if the network is in the C class type network for IPv4 [2]. A wireless router does not limit the number of the client in practice, but for SOHO (small office home office) device, the number of the client sometimes is limited to 15 clients in several brands. In other brands, there is a problem that wireless connectivity becomes corrupted when the device serves many clients in more than one day. Client or other activity could overload the wireless router with low memory and low CPU, so the router becomes stuck. Stuck could mean that the DHCP service is not running very well and needed to be restarted. Switching of DHCP service served by the wireless router to DHCP relay could become an alternative solution for this problem because the DHCP relay takes the handling of the load.

This solution also overcomes the proprietary limitation on some brands. In the market today, some wireless controllers which act as the DHCP server for DHCP relay only can be connected to the same brand. They do not match with other brands available in the market. To bridge this problem, OpenWRT can be used. After it is installed, the wireless router can be connected to some generic brand routers. [3]. This research used the generic router with OpenWRT modified operating system (OS) scenario rather than used the factory default firmware wireless controller.

Some DHCP researches had been conducted. Hooda, et al. manipulated the information of each network by using the relay agent. It provided extra IP information with some layer overlay. It was done by encapsulating the current layer of the network parameter request with information data extracted from the process that was passed in the network. The method used a relay agent to add information data into an information field and might comprise a DHCP option "82" field. In this research, information that was triggered by the agent was routing configuration in a generic router. [4].

Miao et al, worked in the behavior aware adaptive configuration in a wireless LAN. There was a combination of adaptive IP lease time and dynamic IP pool range. The adaptive lease time function was used to reduce IP peak usage based on usage pattern and user roles. Beside the adaptive lease time, there was a VLAN consideration based on spatial-temporal mobility correlation with a client. Resource allocation in this research was purely based on network segment allocation and consideration. Lease time was not set to be adaptive because every user must join to the selected area which was connected by the wireless network. [5].

The idea to save the configuration or MAC address table somewhere in the network was done in [6]. It limited the DHCP broadcast by storing information of MAC address in a

Image Malware Detection using Deep Learning

Jamal El Abdelkhalki, Mohamed Ben Ahmed, Boudhir Anouar Abdelhakim

Computer Science, Systems and Telecommunication Laboratory, (LSIT), University AbdelmalekEssaadi, Tangier, Morocco

Abstract: We are currently living in an area where artificial intelligence is making out every day to day life much easier to manage. Some researchers are continuously developing the codes of artificial intelligence to utilize the benefits of the human being. And there is the process called data mining, which is used in many domains, including finance, engineering, biomedicine, and cyber security. The utilization of data mining, artificial intelligence algorithms like deep learning is so vast that we can't even name them all. This technology has almost touched every industry and cyber security is the most beneficial. The process of enhancing cyber security with the help of deep learning methods has come out of the theory books and many organizations are utilizing them rather than using a traditional piece of software to defend against online threats. Especially in the field of recognizing and classifying codes or malware. And this is essential, because, with the advent of cloud computing and the Internet of Things, expand potential malware infection sites from PCs to any electronic device. This makes our day to day life very unsafe. In this post, first, we will describe in brief how deep learning can be the most useful and promising techniques to detect malware. Besides this we will go through a deep neural network, ResNet for malware dynamic behavior classification jobs.

Keywords:Malware,detection,Malware,CNN,ResNet, Cyber security.

1. Introduction

Nowadays, data analysis is a crucial step for any project in several areas such as IT, marketing, finance. In this context, the analysis of the log files motivated a large number of researchers. The latter conducted their research studies on the different data are in the volumetric log files[1].This particular method of data analyzing is showing a promising feature in the context of malware detection. Therefore, Malware detection is a process of analyzing any suspicious applications that exist in the PC[2]. It is a key part of software safety research.

Generally, to detect and classify malware, there are clear sets of detection methods. Since there are many methods to detect malware, the result is not the same all the time. Most of the time, we see users are making use of generic anti-virus software to shield against malicious applications or software. However, this is not a trustworthy system, to begin with[3].This software most of the time are unable to classify and unable to detect malware mutation, variants, and rapid code changes. As a result, the user left the PC vulnerable to numerous threats.What is making his worse is the continuous changes in the way malicious software or codes are being made. And, besides this, every now and then there's new malware popping up in the market. According to "China Internet Security Report for the First Half of 2018": with the help of 360 Internet Security center, researchers found out that in the

first half of 2018 alone, there were more than 140 million occurrences of new malicious programs, which were detected by the Internet Security software and 795,000 new malicious software were being intercepted regularly. Amongst them, the number of malicious software built for the PC was 149,098,000 hence 779,000 new harmful applications were being intercepted per day. The same program detected about 2.831 million malicious programs build to affect the Android platform, and they were intercepting about 16,000 new malicious programs every day. After going through the stats, we can obviously see why it is becoming more and more difficult to find a suitable solution to detect malware. However, it is a concern for everyone who needs a proper and efficient answer[4]. The method that can actively used in order to answer to the problem of detecting or classifying malware, is the method of deep learning.

In this paper, we study, at the beginning, the research work in relation to malware especially those based in detection malware using different methods. We presented a deep learning model for malware detection using malware image. Deep learning is widely used in image recognition.

2. Related works

Family since different anti-virus software has different tags for one group. Marcos Sebastiain[5] advocated AV Class which makes use of the semantic analysis of malicious program name tags produced by various engines to recognize the same familiarly Bartos[6] stated that undiscovered malicious code variants could be identified by drawing out statistical characteristics from the network stream without proper code fingerprints features. YuFeng et al. [7] advised to make use of a method called ASTROID. This exceptional method can automatically extract common malicious features from a known malware family database to detect new malicious codes. This technique changes the homogeneous harmful code detection into highest satisfiability problem solving by exploring the most suspicious common subgraph (MSCS) from a small number of identified malware family examples. The outcomes show that the suggested method is better to the manual technique in detection efficiency and accuracy rate, also can defeat behavioral obfuscation and other counter measures. Advancement of malware technologies. And today, if we research a bit about different types of malware detection technologies, we will be able to find a few exceptional detection methods of malware codes, and here they follow: Rules-based method[8], Heuristic Analysis[9], DNA Analysis[10],and Deep Learning Method[11], [12].

They aim to prove how gene sequence classifier can be applied to classify malware and how rapidly it acts as opposed to other hybrid techniques. BIG15 dataset consists of another important which is family classification, the reason is, to understand how malware affects the affected device, recognizing the family classification is crucial to know threat level they pose, and how to defend against them [13]. Various machine learning methods have been employed so far for malware family classification. Some use opcodes or instructions of assembly code to predict representative

Enhanced Dynamic Bandwidth Allocation Algorithm for Intelligent Home Networks

[1]Themba L. Nkosi, [2]Maredi Mphahlele, [3]Sunday O. Ojo, and [4]Topside E. Mathonsi

[1,2,3,4]Department of Information Technology, Tshwane University of Technology, South Africa

***Abstract*:** Internet of Things (IoT) has been seen playing a tremendous change in the Information Technology (IT) environments, and thus its importance has also been realized and played a vital role within Intelligent Home Networks (IHNs). This is because IoT establishes a connection between things and the Internet by utilizing different sensing devices to implement the intelligence to deal with the identification and management of the connected things. IHNs use intelligent systems to perform their daily operations. Meanwhile, these networks ensure comfort, safety, healthcare, automation, energy conservation, and remote management to devices and users. Apart from that, these networks provide assistance in self-healing for faults, power outages, reconfigurations, and more. However, we have realized that more and advanced devices and services continue to be introduced and used in these networks. This has led to competitions of the limited available network resources, services, and bandwidth. In this paper, therefore, we present the design and implementation of a Novel Dynamic Bandwidth Allocation (NoDBA) algorithm to solve the performance bottleneck incurred with IHNs. The proposed algorithm deals with the management of bandwidth and its allocation. In the proposed algorithm, this study integrates two algorithms, namely; Offline Cooperative Algorithm (OCA) and Particle Swarm Optimization (PSO) to improve the Quality of Service (QoS). PSO defines the priority limits for subnets and nodes in the network. Meanwhile, OCA facilitates dynamic bandwidth allocation in the network. The Network Simulator-2 (NS-2) was used to simulate and evaluate the NoDBA and it showed improved results compared to the traditional bandwidth allocation algorithms. The obtained results show an average throughput of 92%, an average delay of 0.8 seconds, and saves energy consumption of 95% compared to Dynamic QoS-aware Bandwidth Allocation (DQBA) and Data-Driven Allocation (DDA).

Keywords: IHNs, Dynamic Bandwidth Allocation, PSO, OCA, QoS, NoDBA.

1. Introduction

In the recent past, the Internet of Things (IoT) has played a tremendous change in the Information Technology (IT) industry. This is because IoT establishes a connection between things and the Internet by utilizing different sensing devices to implement the intelligence to deal with the identification and management of the connected things. The information sensing devices include Radio Frequency Identification Devices (RFID), infrared sensors, Global Positioning System (GPS), laser scanner devices, and more [1]-[28]. These devices are all connected to the Internet to implement remote perception and control. This has led to the advent of computer networks, and thus, there has been a consistent need to have these sensing devices in any environment. This further aids in communication among various devices to share the available network resources and services. Over the past few years, the need for communication among these devices has resulted in the connection of home devices, thus creating networks called Intelligent Home Networks (IHNs). IHNs provide and ensure comfort, safety, healthcare, automation, energy conservation, and remote management to devices and users within it [1]-[28].

IHNs use intelligent systems to perform their daily operations. The benefits of using intelligent systems in IHNs provide assistance in self-healing for faults, power outages, reconfigurations, and more [2]. In addition, these networks can be accessed and managed either locally or remotely, enabling monitoring, scheduling, and controlling of various devices and users. In its most general form, IHNs are comprised of sub-networks (subnets) such as Wireless Fidelity (Wi-Fi), ZigBee, Smart Grid, Bluetooth, Body Area, Ultra Wide Band (UWB), and more [3]. In this study, these subnets have been given different priorities based on their importance and workflow procedures. For remote communications, the devices in each subnet are connected to Sub Network Gateways (SNGs). On the other hand, the SNGs are connected to Home Network Gateways (HNGs). The responsibility of HNGs is to enable the integration of IHNs with other networks such as the Internet and more.

However, it has been realized that more and advanced devices and services continue to be introduced and used in these environments. On the other hand, the current migration from Internet Protocol version 4 (IPv4) to IPv6 standards also plays its vital role in IHNs. Apart from that, the addition of more and advanced devices and network resources into these networks also plays its impact and has resulted in congestion problems. On the other hand, this addition of more devices leads to competitions of the limited available network resources and services as well as available bandwidth. These networks, therefore, continue to experience and suffer from poor Quality of Service (QoS) when performing operations both locally and remotely. Furthermore, the poor QoS results to unavailable, unreliable and inefficient bandwidth to the consumers of these networks. The research in [4] concurred that effective resource allocation algorithms are important for bandwidth management in order to improve QoS and to satisfy the demands of its customers as well.

In this paper, therefore, we propose enhanced bandwidth management and allocation algorithm for IHNs known as Novel Dynamic Bandwidth Allocation (NoDBA) algorithm. The primary reason is that none of the existing research considered developing bandwidth management and allocation algorithms for IHNs. Moreover, we realized that the current existing bandwidth allocation algorithms were developed for wireless networks such as Wireless Mesh Networks (WMNs) and more. The proposed algorithm allocates the available bandwidth according to the workflow procedures of each subnet in the IHN. The algorithm ensures that each subnet is assigned or allocated bandwidth based on