THE FLOW BASED TRAFFIC DETECTION AND MONITORING MODEL IN COMPLEX NETWORKS USING PREDICTIVE MANAGEMENT APPROACH

L. Vinitha Sree and A. Amjath

Department of Computer Science and Engineering, Mahendra College of Engineering, India

Abstract

The Network Flow Analyzers are the best way to identify network traffic and its source. In general, Net Flow is a feature that was first introduced in network devices. It can collect IP-based network traffic by monitoring the inflow and outflow of data. This allows the administrator to verify the source and destination of the traffic, the type of service and the cause of the congestion. This makes it easier to understand network traffic and manage it properly. Not only is the process expensive, but it can be effective in the very short term. When you provide more information technology infrastructure Traffics to the network, but do not try to reduce the pressure, the infrastructure will face similar problems encountered before the upgrade again. In this paper, a smart predictive based network flow and traffic monitoring model was proposed. This method describes networking activities with specific and complex user modules. Further predictions can be made to ensure simple and fast data flow by improving the traffic management and avoidance of conjunctions that occur in a particular location in a network.

Keywords:

Network Flow, Traffic Management, IP-based Network Traffic, User Modules

1. INTRODUCTION

There are many legitimate reasons to monitor overall traffic on the network. Information generated by network traffic monitoring tools can be used in many IT functional and security application cases. For example - detecting security vulnerabilities and troubleshooting network-related issues and analyzing the impact of new applications on the overall network. However, an important note in this regard - not all tools for monitoring network traffic are the same. In general, they can be divided into two broad categories - deep pocket inspection tools and flow-based tools. Within these two categories you have the choice of software agents, tools and non-essential tools [1]. In addition, they store tools with infiltration detection systems that monitor historical data, network traffic within the network, and the edge of the network.

Network traffic monitoring is the process of reviewing, analyzing, and managing network traffic for any abnormalities or processes that may affect network performance, availability, and/or security [2]. It is a network management process that uses various tools and techniques to study computer network-based communication/data/pocket traffic. The main purpose of network traffic monitoring is to ensure the availability and smooth operation of the computer network [3]. Network tracking integrates network sniffing and pocket capture techniques in tracking a network. Network traffic monitoring should generally review each incoming and outgoing pocket [4].

Network monitoring is the monitoring of computer activity over a network. This is usually done by companies, governments or individuals to track illegal activities. The network engineer/operator, network equipment manufacturer or service provider must have instructions for performing monitoring tasks related to networking. Network surveillance allows governments and organizations to understand their user base and gather intelligence [5]. However, it is sometimes seen as a threat to the privacy of network users. Almost all network surveillance is done automatically, intrusively and remotely. In networks, pocket sniffing is a common technique used to monitor data traffic [6]. Many technologies are available to assist in network monitoring. Network monitoring can be used to restrict access to information available to the public or to specific user groups. This can become the site of asymmetrical power relationships between the surveyor and the individuals being monitored [7].

Network monitoring also helps to monitor various perimeter techniques such as filtering, blocking, bypassing and intercepting network traffic. Network monitoring protocol provides a comprehensive analysis of the overall level of monitoring and network health. Network tracking also provides inputs for real-time data tracking, traffic upgrades, quality of service measurements, remote protocol analysis and adjustment [8]. One of the most important benefits of network monitoring is the ability to detect and locate fraud. From a government perspective, network surveillance can help monitor threat levels, maintain social control, and prevent illegal and criminal activities [9].

Infiltration detection is another task performed by the staff responsible for the company's information, while ensuring protection against attacks. Intrusion detection active process It detects a hacker trying to infiltrate a computer [10]. At best, such a system will only give a warning when attempting to infiltrate. Infiltration detection helps when the attacker identifies active threats by alerts and warnings that attack the information needed for the attack. In fact, this is not always the case. Invincible detection systems (IDs) appeared a long time ago. The first of them can be considered a night watch and guard dogs. Personal and security dogs performed two tasks: they defined suspicious activities initiated by someone and stopped attack intrusion [11]. As a rule, robbers avoid meetings with dogs and, in most cases, try to cross the side of the building guarded by dogs. The same can be said about the clock at night. Do not want to see weapons or guards or guards causing the police [12].

2. RELATED WORKS

Lagkas et al. [2] introduced a Spectral Traffic Optimization technique for classified the primary and secondary user management in 5G communication network environment. In that the primary users of a network getting higher priority compare then the secondary users. Because the primary users have license to use the spectrum band and the secondary users are utilize the spectrum band in the random time manor. So, the primary users are getting more priority level.

Yuan Ai et al. [3] provided a smart mechanism of Joint Traffic allocation. Here the radio Traffic of the network can allocate both the primary and secondary users without any connection lost. So, the user groups (both primary and secondary users) are unable to suffer the Traffic utilization problem. Then the authors include here an admission control technique to the user groups. This controls the secondary user occupancy of the spectrum.

Khumalo et al. [4] proposed a Reinforcement Learning-based Computation Traffic Allocation technique to separate the specific Traffics to the user group of a network. There the primary user attributes are registered and the secondary user group's attributes are not registered. So, the entry of primary users can register in a sequential manner and the entries of secondary users are in random manner.

Wang et al. [7] analysed the traffic issues between the user groups of the network. The conjugation occurs when the primary users and secondary users are tried to come the network at the same time. At that time, more emphasis will be placed on the primary users and they will be allowed to enter. Meanwhile, the secondary user will then have to wait. As the waiting time were increases, then the chances of exiting the network increase.

Huang et al. [9] provided an energy efficient approach between the primary and secondary users. If the bandwidth allocation was increased, then the spectrum utilization automatically increased. In a cut-off range, the number of secondary users utilized more energy of the network shows the inefficiency of the network. Because the primary users are utilizing very low energy.

3. PROPOSED NETWORK MODEL

The proposed flow-based prediction algorithm (FBPA) design consists of the following important blocks;

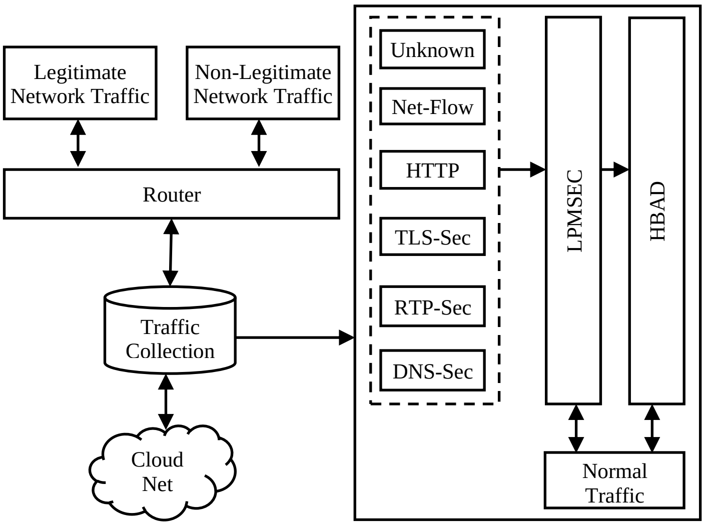

Fig.1. Proposed system design

- ***Legitimate and Non-Legitimate Network:*** Network flow monitoring software that supports protocols such as NetFlow, IPfix, GeFlow, SFlow provides complete visibility of network traffic. With Motadata, the IT sector can generate intelligence reports on the following types and types of traffic [13]. The legitimate and non-legitimate networks shows in the above fig.(1)
- ***Identification of slow applications:*** Speed plays an important role in user experience. One of the most elevated help desk tickets is about slowing down or crashing the application (web application, meeting, Skype, etc.). There may be 100s for reasons where only one or two are relevant at any given time [14]. Identifying the cause is not only time consuming, it is expensive. The next generation flow detector software can filter and report the exact cause. By combining internal data reports with external sources, the system administrator can learn a lot about the computer and the faulty network [15].
- ***The Detection of spyware and other hacks:*** When these worms invade your network, they create a very unusual data flow inside and out. With the help of flow detector, it is easy to detect these unusual patterns. If you do not use some data analyzer, these forms are often not validated because they are designed to fool the human administrator. Most of these worms often cause non-financial problems by creating a bad image for the company [16]. However, in some cases, the impact of these worms may include higher financial loss rates.
- ***Detecting of Customers' Personal Information:*** This point is especially applicable to companies dealing with payment gateways or payment card industry. A good payment gateway will never allow customer personal information to be leaked from its computer [17]. In a particular hack, such information can be reported instantly by flow detector software.
- ***Sectored bandwidth usage:*** If you are concerned about the overall usability of the network and cannot figure out which sector is making the most use of the data flow, flow detector may come in handy [18]. It can monitor and point out IPs and devices that use network Traffics. Management can take appropriate action to reduce the pressure on the network.

4. RESULTS AND DISCUSSION

The proposed flow-based prediction algorithm (FBPA) is evaluated among the active algorithms with various performance metrics like Traffics blocking, Traffic dropping, and utilization of bandwidth, of the network. Every performance measurement of the proposed system is confirmed for its value with the active techniques such as FUE-sub-channel matching algorithm (FSMA), and Joint sub-channel and power allocations algorithm (JSPA). The Network Simulator (NS-2) used for the simulation with the following parameters. In graphical representation, the blue and red indicates existing FSMA and JSPA whereas, green indicates the proposed FBPA respectively

Table.1. Simulation Parameters

Parameter	Value
Simulation period	8000 frames
Preamble length	122ms
Discovery Connectivity	0.5

Frame Length	120 ms
Primary user Active State	4
Primary User on Idle State	2
Maximum Interference Ratio	0.3
Permission Connectivity	0.8

4.1 TRAFFIC MANAGEMENT (%)

Normally the usage of bandwidth was calculated by the number of primary users used the Traffics of the network. If the primary users of the network are in active state, then the secondary users are unable to enter the network. After the primary users are away from the network, it shows the spectrum is in idle state. When the spectrum is in idle state the secondary user will be allowed to use it [19]. The process of blocking secondary user, while the primary user in active state, is called the Traffic Blocking of a network.

Then, the Traffic blocking of a network is given by

$$Traffic\,Management = \sum_{s=1}^{h} K_j \tag{1}$$

where, K_j is dented here the total number of users in the spectrum

The Table.2 presents the analysis of Traffic Management between existing FSMA, JSPA and proposed FBPA.

Table.2. Analysis of Traffic Management

Flow Rate	FSMA	JSPA	FBPA
1000	77.21%	84.57%	92.68%
2000	78.25%	85.21%	93.65%
3000	79.58%	86.97%	93.87%
4000	80.21%	87.87%	94.47%
5000	81.57%	88.65%	95.21%

The Table.3 shows the Traffic blocking comparison. When compared with the existing algorithms, the proposed FBPA algorithm achieves high Traffic blocking because the primary user spectrum utilization was increased and the number of secondary user spectrum allocation was reduced. From Table.2, if the spectrum was in active state, then the primary user utilizes the spectrum and the secondary users of a spectrum are in waiting state.

4.2 TRAFFIC DROPPING (%)

If a spectrum is in high usage, then the usage time of its users should be more. That is, the time used by the primary users should be calculated first and that spectrum should be passed on to the secondary users in their absence [20]. If the secondary user logs in again at the time allotted to the secondary user, the secondary user should be immediately relocated. Thus, the effectively handling of both the primary user and the secondary user is called the Traffic management. Anyone who is unable to connect on the time of spectrum usage, and then they will leave the network without any intimation. This is called the traffic dropping of a network.

$$D_x(t)\text{=(dropped users under the active state of spectrum}(x,t))/ \text{(non-block user arrivals under time }(x,t)) \tag{2}$$

The Table.3 presents the analysis of Traffic dropping between existing FSMA, JSPA and proposed FBPA.

Table.2. Analysis of Traffic dropping

Flow Rate	FSMA	JSPA	FBPA
1000	22.79%	15.43%	7.32%
2000	21.75%	14.79%	6.35%
3000	20.42%	13.03%	6.13%
4000	19.79%	12.13%	5.53%
5000	18.43%	11.35%	4.79%

The Table.3 depicts the Traffic dropping comparison. When compared with the existing algorithms, the proposed FBPA algorithm achieves low Traffic dropping because the user switching process effectively performed by the FBPA algorithm. The proposed algorithm was performing the dynamic spectrum allocation work very comfort. So, the utilization of spectrum was high and the number of dropping user was low.

4.3 UTILIZATION OF BANDWIDTH

At a particular time, the highest amount of data packets over the spectrum transferred is called the bandwidth utilization of a network.

$$\text{BU (\%) = (Total messages transmitted and received)/ (speed of transmission)} \times 100 \tag{3}$$

The Table.4 shows the bandwidth utilization of a spectrum and compared between existing FSMA, JSPA and proposed FBPA.

Table.4. Analysis of Bandwidth Utilization

Devices	FSMA	JSPA	FBPA
10	70.47%	75.49%	96.62%
20	69.58%	74.48%	93.86%
30	67.42%	73.29%	91.1%
40	65.41%	72.37%	88.34%
50	64.82%	71.39%	86.58%

The Table.4 shows the bandwidth comparison between existing and proposed systems. From Table.4, the primary users utilize the spectrum with highly efficient manner and they do not require any authentication to join the network. When the spectrum is in idle state, then the secondary users are allowed to use the spectrum. So, the maximum bandwidth was utilized by the primary and secondary users.

5. CONCLUSION

In general, these types of traffic violations that occur on the network can create a variety of problems. And these kinds of irregularities will only exacerbate the problems of various complex configuration modules. So, any of the information that is there will be very high in their pressure without getting complete. This will significantly reduce the network speed. Sometimes the intensity goes so far as to completely reset the network. Since problems such as the right amount of speed and conjunction are eliminated from the top tier in the way currently proposed, its bandwidth is calibrated after the right amount of information is first stored in each system there. Based on these measurements the various data that are there will start to travel. His different locations will handle that data when more data comes in the scale. The information bags containing the said information will soon go to the user module. This methodology enables maximum traffic management as data protection and its management work effectively.

REFERENCES

[1] E. Hossain, D. Niyato and Z. Han, "*Dynamic Spectrum Access in Cognitive Radio Networks*", Cambridge University Press, 2009.

[2] T.D. Lagkas, D. Klonidis and I. Tomokos, "Joint Spatial and Spectral Resource Optimization over Both Wireless and Optical Fronthaul Domains of 5G Architectures", *Proceedings of 22nd International Conference on Transparent Optical Networks*, pp. 1-6, 2020.

[3] Yuan Ai, Gang Qiu and Sun Chenxi, "Joint Resource Allocation and Admission Control in Sliced Fog Radio Access Networks", *China Communications*, Vol. 17, No. 8, pp. 14-30, 2020.

[4] N. Khumalo, O. Oyerinde and L. Mfupe, "Reinforcement Learning-based Computation Resource Allocation Scheme for 5G Fog-Radio Access Network", *Proceedings of International Conference on Fog and Mobile Edge Computing*, pp. 353-355, 2020.

[5] A. Kaloxylos, "A Survey and an Analysis of Network Slicing in 5G Networks", *IEEE Communications Standards Magazine*, Vol. 2, No. 1, pp. 60-65, 2018.

[6] S.A. Syed, K. Sheela Sobana Rani, G.B. Mohammad and V.P. Sundramurthy, "Design of Resources Allocation in 6G Cybertwin Technology using the Fuzzy Neuro Model in Healthcare Systems", *Journal of Healthcare Engineering*, Vol. 2022, pp. 1-7, 2022.

[7] Y. Wang, K. Wang, H. Huang, T. Miyazaki and S. Guo, "Traffic and Computation Co-Offloading with Reinforcement Learning in Fog Computing for Industrial Applications", *IEEE Transactions on Industrial Informatics*, Vol. 15, No. 2, pp. 976-986, 2019.

[8] T. Karthikeyan and K. Praghash, "Improved Authentication in Secured Multicast Wireless Sensor Network (MWSN) using Opposition Frog Leaping Algorithm to Resist Man-in-Middle Attack", *Wireless Personal Communications*, Vol. 78, pp. 1-17, 2021.

[9] L. Huang, X. Feng, C. Zhang, L. Qian and Y. Wu, 'Deep Reinforcement Learning-Based Joint Task Offloading and Bandwidth Allocation for Multiuser Mobile Edge Computing", *Digital Communications and Networks*, Vol. 5, No. 1, pp. 10-17, 2019.

[10] Y. Mao, J. Zhang, S.H. Song and K.B. Letaief, "Stochastic Joint Radio and Computational Resource Management for Multi-User Mobile-Edge Computing Systems", *IEEE Transactions on Wireless Communications*, Vol. 16, No. 9, pp. 5994-6009, 2017.

[11] T.O. Olwal, K. Djouani and A.M. Kurien, "A Survey of Resource Management Toward 5G Radio Access Networks", *IEEE Communications Surveys and Tutorials*, Vol. 18, No. 3, pp. 1656-1686, 2016.

[12] J. Logeshwaran and R.N. Shanmugasundaram, "Enhancements of Resource Management for Device to Device (D2D) Communication: A Review", *Proceedings of International Conference on IoT in Social, Mobile, Analytics and Cloud*, pp. 51-55, 2019.

[13] Z. Chen, Z. Zhou and C. Chen, "Code Caching-Assisted Computation Offloading and Resource Allocation for Multi-User Mobile Edge Computing", *IEEE Transactions on Network and Service Management*, Vol. 18, No. 4, pp. 4517-4530, 2021.

[14] Y. Wei, F. R. Yu, M. Song and Z. Han, "Joint Optimization of Caching, Computing, and Radio Resources for Fog-Enabled IoT Using Natural Actor-Critic Deep Reinforcement Learning", *IEEE Internet of Things Journal*, Vol. 6, No. 2, pp. 2061-2073, 2019.

[15] H. Mazouzi, N. Achir and K. Boussetta, "Dm2-Ecop: An Efficient Computation Offloading Policy for Multi-User Multi-Cloudlet Mobile Edge Computing Environment", *ACM Transactions on Internet Technology*, Vol. 19, No. 2, pp. 1-24, 2019.

[16] S. Cical and V. Tralli, "QoS-Aware Admission Control and Resource Allocation for D2D Communications Underlaying Cellular Networks", *IEEE Transactions on Wireless Communications*, Vol. 17, No. 8, pp. 5256-5269, 2018.

[17] Q.D. La, M.V. Ngo, T.Q. Dinh, T.Q.S. Quek and H. Shin, "Enabling Intelligence in Fog Computing to Achieve Energy and Latency Reduction", *Digital Communications and Networks*, Vol. 5, No. 1, pp. 3-9, 2019.

[18] Y. Sun, D.W.K. Ng, Z. Ding and R. Schober, "Optimal Joint Power and Subcarrier Allocation for Full-Duplex Multicarrier Non-Orthogonal Multiple Access Systems", *IEEE Transactions on Communications*, Vol. 65, No. 3, pp. 1077-1091, 2017.

[19] B. Di, L. Song and Y. Li, "Sub-Channel Assignment, Power Allocation, and User Scheduling for Non-Orthogonal Multiple Access Networks", *IEEE Transactions on Wireless Communications*, Vol. 15, No. 11, pp. 7686-7698, 2016.