Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
2326-9865

Cyber-Attack Detection Using Optimized Ensemble Classification Model

[1]Dr. Kalaivani Kathirvelu, [2]Yasir A,
[1]Assistant Professor, [2]Research Scholar, School of Engineering,
Department of Computer Science and Engineering,
Vels Institute of Science, Technology and Advanced Studies, Chennai
Email: kalai.se@velsuniv.ac.in, yasircse007@gmail.com

Article Info
Page Number: 4537 - 4546
Publication Issue:
Vol 71 No. 4 (2022)

Article History
Article Received*: 25 March 2022*
Revised*: 30 April 2022*
Accepted*: 15 June 2022*
Publication*: 19 August 2022*

Abstract
Cyberattacks may have far-reaching effects despite their low cost, simplicity of execution, and general inability to be traced back to a specific source. One of the main factors making it hard to pinpoint blame for cyberattacks is the existing state of network infrastructure. Cyber-attacks are difficult to punish because of a lack of enforcement measures in international law, even when the perpetrators have been identified. Since it is challenging to pursue cyberattacks, attribution is not an effective deterrence. For this reason, it may be possible to use social media data to shed light on the causes of cyber-attacks, given that the internet is a freely accessible resource. In this paper a model is developed to detect the DDoS attack. An ensemble classification model is developed to identify the total number of entries and approves the functional access of various devices inside the network. The simulation is conducted to test the efficacy of the model in detecting the attack and the simulation shows that the proposed method achieves higher degree of accuracy than other methods.

Keywords: Cyber-Attack, Virus, Computer, Wannacry, DDoS, Multiple Devices

1. Introduction

We are living in a digital world where there is nothing without internet. We are using various technical equipments to operate that internet [1]. It includes everything from the mobile phones we use to the USB cable used to charge those [2]. A report has been released that cyber threats caused by removable devices such as USB and pen drives have increased [3]. In the '2022 Honeywell Industrial Cyber security USB Threat Report', it has been mentioned that cyber risks have increased by 52 percent due to such removable media devices in 2022 [4]. Experts say the same risk was 32% in 2021, and now it's looming large [5]. The risks of spreading malware and stealing control systems, data, etc [6]. through these devices have increased. In particular, it has been reported that they are more likely to attack industrial systems, because that is where such devices are used the most [7]. It has also been found that Trojans are particularly dangerous in this attack [8]. The research revealed that these hackers mostly use USB-borne malware to attack companies [9]. Therefore, companies should avoid using such methods and adopt safe methods, the report said [10].

Ransomware has taken advantage of the free link to fix vulnerabilities in the operating system provided by Microsoft. Many security researchers predicted that once details of the flaw were leaked, it could lead to the creation of malicious ransomware software that launches automatically [11-12]. It could take as little as two months for malicious hackers to sneak into the network and take advantage of this prediction [13]. It was initially thought that many of the victims were using a very old version of Windows XP, which Microsoft no longer supports [14]. Large enterprises should test the security features of their platform systems service providers. It does not interfere with the network's operating system before allowing those security features to be installed. This may delay the rapid deployment of these security features [15]. Ransomware is a very attractive enterprise for cyber-thieves because it can spread the virus quickly and profitably [16]. They make easy money with the untraceable bit coin virtual currency app. However, it is unusual for the best criminal gangs to use some Bit coin web wallets to collect their ransoms [17]. Due to the fact that there are many online wallets in this regard, it is very difficult to track down the gang [18].

Google Safe Browsing is a free service that protects users from malicious web pages and can provide protection against many types of attacks, including Phishing and drive-by downloads [19]. At the website owner's end, it's a quick way to see if Google thinks your website might be dangerous [20]. The Safe Browsing service is available for Chrome, Firefox and Safari (on Mac) browsers. To use the tool, visit a website and the browser sends some information about the site to Google [21-25]. Redirects are not bad, and some websites use them to send visitors to other pages. There are legitimate reasons for redirects, such as when a website owner wants to direct users from an old web address to its new address. However, redirects are often used maliciously by hackers who want to trick website visitors into visiting a page containing malware or advertisements they are trying to spread [26-30]. To check your site for any suspicious redirects: Check your redirect URLs and make sure they match the target content. You should also pay attention to whether the pages you are redirected to are legitimate and not unusual external pages [31-35]. Alternatively, you can use an online service to scan websites or web pages for redirects. The problem is that tools that offer such comprehensive features can be expensive. A more basic redirect checker such as Analyze only one page at a time

2. Literature Survey

Ransomware is malicious computer software that locks files on a computer until a demanded payment is made. However, if they failed to update their computer security systems over the weekend, the number of people affected by this cyber attack could increase when they turn on their computers when they come to work on Monday [1]. Cyber security experts say that many of the malicious features of this ransomware computer virus are at risk of working in a new way. The WannaCry virus only infects computers running on the Windows operating system. If you do not use the software enhancements provided by the Windows operating system, or are not careful when opening and reading e-mails, you are also at risk of being infected [4]. However, home computer users are believed to be at minimal risk as far as this cyber attack is concerned. Download and run software development software, firewalls, and

antivirus software on the computer. Be careful when reading email messages [8]. Keep another version of your files. So, if your files are infected with virus, you can unlock your files without paying ransom. It is better to have another version as there is no guarantee that you will be able to open your files even after paying the ransom [10].

This is due to malicious computer software known as WannaCry. It is spread by a virus known as self-replicating computer software. More than other malicious computer software, this virus has the power to crawl into a network on its own [12]. Other viruses depended on human activity, such as clicking on it, triggering a link that stored attack data. Once a WannaCry infiltrates an organization, it searches for vulnerable machines and infects them with viruses. This causes maximum impact [13]. Many of the machines in each of the affected companies were of less than required standards. In earlier days, this would have been a vital resource, but luckily individuals are helping to protect their sites [15]. If you are using a web application, remember to check your database with Word Press. These changes are difficult to detect as they often don't appear on your website [17].

3. Proposed Model

After a certain point during a distributed denial of service (DDoS) attack, a server will cease accepting connections from legitimate users because it has run out of resources. A victim server resources can be drained in one of two ways: either its bandwidth or its buffer size is overwhelmed. The victim total probability of resource exhaustion as a result of the occurrence is given by the equation (1).

$$Attack = 1-\left(1-p^{\beta}\right)\left(1-p^{M}\right)$$

The victim is more likely to exhaust all available resources if the buffer size is small, the number of open channels is low, and the time between attacks is short.

$$Attack = 1-\left(1-p^{\beta}\right)\left(1-p^{M}\right) = Attack \rightarrow \text{large}$$

The results led us to settle on the median time between arrivals as the statistical measure we'll use to spot attacks. The interval between simultaneous use of two different IP addresses is called the inter-arrival time. This term describes the interval between when individual data packets reach their final destination. Here, we analyze the arrival time using a sliding window of ten seconds. The average time (T_{mean}) between arrivals is calculated.

$$T_{mean} = \frac{1}{N}\sum_{i=1}^{N} IP_i^{Time}$$

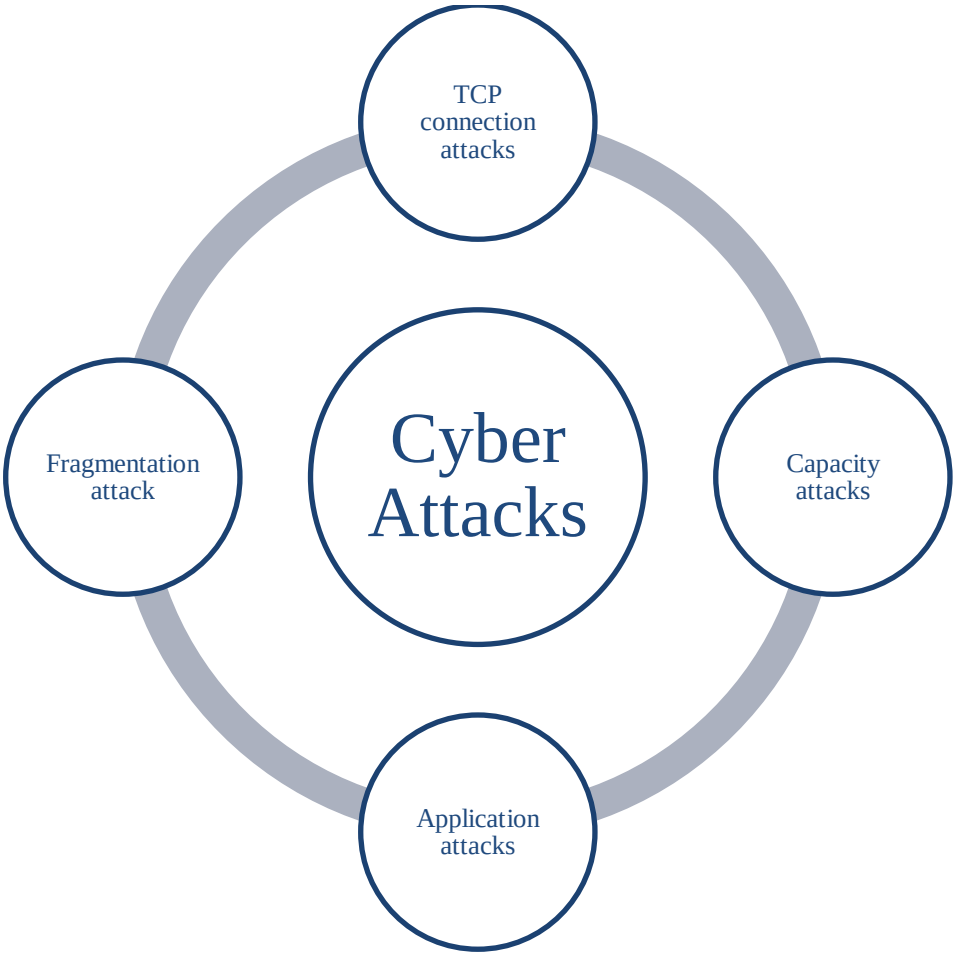

Fig 1: Different types of cyber attacks

Malicious viruses are known to target entire web servers in attempts to create bot nets. Among these efforts, common targets include web server architectures and typically include publicly available exploits. These advanced and intensive efforts can often overcome less flexible web hosting providers. Fortunately, once discovered, vulnerabilities are usually patched fairly quickly by most web hosts. The algorithm used in the proposed method is shown below,

Step 1: Use Proxy Protection
Step 2: Keep the system bandwidth
Step 3: Protect the IP address
Step 4: Retrieve the status of IP address
Step 5: Apply Detection algorithm
Step 6: Check the genuineness of the packets
Step 7: Check if the attack is identified

Checking log files is the best way to determine if your website has been hacked. Log files are a record of all activity on your website. They contain information about visitors and what they did while on the site, such as when they visited or which pages they viewed. Log files

may also contain information about hackers who have attempted to access your site. Some log files you may want to examine are shown in fig 2:

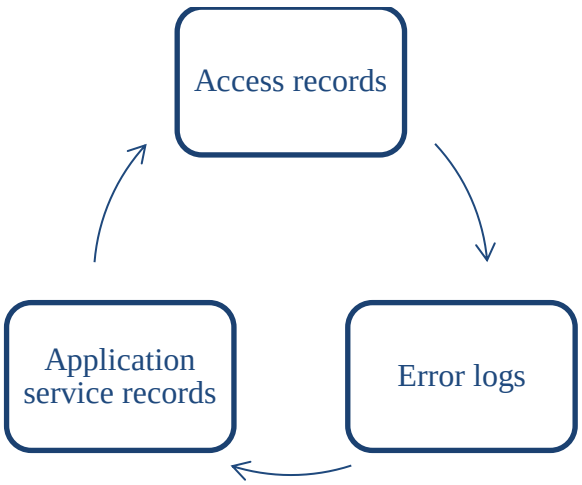

Fig 2: Proposed log-files handling

- Access records
- Error logs
- Application service records

Hackers usually leave traces about themselves when they try to access a website. Checking such activity can help you determine if someone has accessed your account to spy on user activity or steal valuable data from public forums or databases.

Web hosting companies always have internal security measures that scan websites on their servers. If your website is hacked, it won't take long to receive notifications from your web host. Alerts are the most common types of notifications that say an attempt has been made to access certain areas of the site or that someone has tried to upload something malicious. These notifications will help you determine whether or not the hacker gained access to your site, what type of activity they attempted, and what corrective actions you need to take. However, keep in mind that not all suspicious activity is necessarily due to hacking; some may be due to faulty code or other issues unrelated to hackers.

4. Results and discussion

The proposed optimized Ensemble Classification model (OECM) was compared with the existing Optimized cyber-attack detection method (OCADM), robust cyber-attack detection and identification algorithm (RCDIA), Data-driven Cyber-attack Detection (DDCAD) and an artificial intelligence cyber security algorithm (AICSA).

Shared hosting accounts are like big data. Although each account has its own share of the available resources, they all share the same environment. Everything you need to work with your files, materials, and data is stored in one central location. Sites hosted under the same account automatically get connected to one another. All sites are vulnerable if the root directory is compromised as in Table 1.

Table 1: Handling of Shared hosting issues

Entries	DDCAD	OCADM	RCDIA	AICSA	OECM
500	0.980392	0.980392	0.98039	0.97059	0.96078
1000	0.970588	0.960784	0.96078	0.96078	0.96078
1500	0.980392	0.980392	0.98039	0.97059	0.97059
2000	0.921569	0.901961	0.91176	0.91176	0.96196
2500	0.833333	0.715686	0.77451	0.82353	0.98627
3000	0.931373	0.970588	0.95098	0.93137	0.97059

Despite the fact that all hosting accounts are susceptible to software vulnerabilities, shared servers present an especially high risk. Due to the high volume of accounts on a single server, there may be a wide variety of software installed, all of which needs to be kept up-to-date. Resource dispersal is a fundamental advantage of cloud hosting, but it may also be a point of weakness. In the cloud, you are only as reliable as your weakest component (Table 2).

Table 2: Handling of Software Vulnerabilities

Entries	DDCAD	OCADM	RCDIA	AICSA	OECM
500	0.97059	0.95098	0.95098	0.95098	0.97059
1000	0.96078	0.96078	0.95098	0.96078	0.96078
1500	0.97059	0.95098	0.95098	0.95098	0.97059
2000	0.90196	0.80392	0.89216	0.84314	0.90196
2500	0.7451	0.81373	0.68627	0.7451	0.96471
3000	0.95098	0.92157	0.83333	0.88235	0.93137

Malware, like software vulnerabilities, can have a significant effect on a shared hosting server if not dealt with properly. There are a number of entry points that these malicious applications might use to infiltrate shared hosting accounts and cause damage. The sheer variety of malware means that everything could be compromised as in Table 3.

Table 3: Handling of Malware

Entries	DDCAD	OCADM	RCDIA	AICSA	OECM
500	0.882353	0.901961	0.88235	0.89216	0.95216
1000	0.882353	0.892157	0.89216	0.85294	0.95196
1500	0.980392	0.980392	0.98039	0.98039	0.98039
2000	0.980392	0.980392	0.98039	0.98039	0.98039
2500	0.833333	0.931373	0.88235	0.83333	0.94118
3000	0.823529	0.803922	0.81373	0.82353	0.95392

When using a shared hosting service, your account's IP address will be shared with other users. In a shared hosting environment, several different domains use the same IP address. This creates a can of worm issues. If one of these websites is misbehaving, then all of the others that use the same IP address will also be blacklisted. It's not easy to get an IP address

taken off a blacklist. The information contained on a website is the foundation upon which the site itself rests. Predictions, analyses, and other applications rely on it as in Table 4.

Table 4: Handling of Shared IP

Entries	DDCAD	OCADM	RCDIA	AICSA	OECM
500	0.86275	0.89216	0.86275	0.87255	0.95275
1000	0.87255	0.85294	0.91176	0.88235	0.95275
1500	0.98039	0.98039	0.98039	0.98039	0.98039
2000	0.98039	0.98039	0.98039	0.98039	0.98039
2500	0.88235	0.83333	0.94118	0.88235	0.95392
3000	0.81373	0.81373	0.80392	0.81373	0.95471

Virtual private servers (VPSs) and cloud hosting are more secure than shared hosting plans simply because of their design. The incentive for hackers is higher, though, because they may be able to gain access to more sophisticated networked servers. As a result, more advanced ways of infiltration can be expected. Most hackers have a deep understanding of computer programming and can easily craft malicious front-end scripts as in Table 5.

Table 5: Handling of Virtual Private Server

Entries	DDCAD	OCADM	RCDIA	AICSA	OECM
500	0.901961	0.980392	0.94118	0.76471	0.95176
1000	0.83333	0.73529	0.87255	0.80392	0.91275
1500	0.97059	0.97059	0.65686	0.70588	0.98039
2000	0.95098	0.96078	0.97059	0.95098	0.98039
2500	0.97059	0.97059	0.87255	0.87255	0.95176
3000	0.89216	0.89216	0.86275	0.86275	0.95529

5. Conclusion

To identify the types of violence that can be traced to DDoS attack, we have developed a model. We provided cyberattacks focusing on those that were most likely sparked by deeply antagonistic impulses. Avoid using hosts with inadequate security measures if at all possible. Some may even go to the extent of collaborating with well-known cyber businesses, while others may actively develop their own internal security tools and solutions. It is important to be vigilant and check your website for signs of hacking. A hacked website can be a disaster as hackers can hijack your website and steal customer data or use it to distribute malware.

References

[1] Adeli, M., Hajatipour, M., Yazdanpanah, M. J., Hashemi-Dezaki, H., & Shafieirad, M. (2022). Optimized cyber-attack detection method of power systems using sliding mode observer. Electric Power Systems Research, 205, 107745.

[2] Logeshwaran, J. (2021). AICSA - an artificial intelligence cyber security algorithm for cooperative P2P file sharing in social networks. ICTACT Journal on Data Science and Machine Learning, 3(1), 251–253

[3] Ghafoori, M. S., & Soltani, J. (2022). Designing a robust cyber-attack detection and identification algorithm for DC microgrids based on Kalman filter with unknown input observer. IET Generation, Transmission & Distribution.

[4] Wan, Y., & Dragicevic, T. (2022). Data-driven Cyber-attack Detection of Intelligent Attacks in Islanded DC Microgrids. IEEE Transactions on Industrial Electronics.

[5] Aluko, A. O., Carpanen, R. P., Dorrell, D. G., & Ojo, E. E. (2022). Real-Time Cyber Attack Detection Scheme for Stand-Alone Microgrids. IEEE Internet of Things Journal.

[6] Parizad, A., & Hatziadoniu, C. (2022). Cyber-Attack Detection Using Principal Component Analysis and Noisy Clustering Algorithms: A Collaborative Machine Learning-Based Framework. IEEE Transactions on Smart Grid.

[7] Li, Q., Zhang, J., Zhao, J., Ye, J., Song, W., & Li, F. (2022). Adaptive Hierarchical Cyber Attack Detection and Localization in Active Distribution Systems. IEEE Transactions on Smart Grid, 13(3), 2369-2380.

[8] Yuvaraj, N., Chang, V., Gobinathan, B., Pinagapani, A., Kannan, S., Dhiman, G., & Rajan, A. R. (2021). Automatic detection of cyberbullying using multi-feature based artificial intelligence with deep decision tree classification. *Computers & Electrical Engineering*, *92*, 107186.

[9] Chen, J., Gallo, A. J., Yan, S., Parisini, T., & Hui, S. Y. R. (2022). Cyber-Attack Detection and Countermeasure for Distributed Electric Springs for Smart Grid Applications. IEEE Access, 10, 13182-13192.

[10] Cuzzocrea, A., Fadda, E., & Mumolo, E. (2022). Cyber-attack detection via non-linear prediction of IP addresses: an innovative big data analytics approach. Multimedia Tools and Applications, 81(1), 171-189.

[11] Sutharasan, M., & Logeshwaran, J. (2016). Design intelligence data gathering and incident response model for data security using honey pot system. International Journal for Research & Development in Technology, 5(5), 310–314

[12] Hu, J., Qi, L., Zhang, Z., Yang, X. T., Wang, H., & Li, X. (2022). A detection method for cyber-attack on connected signal phase and timing information. Transportmetrica B: transport dynamics, 10(1), 731-751.

[13] Yuvaraj, N., Srihari, K., Dhiman, G., Somasundaram, K., Sharma, A., Rajeskannan, S. M. G. S. M. A., ... & Masud, M. (2021). Nature-inspired-based approach for automated cyberbullying classification on multimedia social networking. Mathematical Problems in Engineering, 2021.

[14] Mousavi, A., Aryankia, K., & Selmic, R. R. (2022). A distributed FDI cyber-attack detection in discrete-time nonlinear multi-agent systems using neural networks. European Journal of Control, 66, 100646.

[15] Amal, M. R., & Venkadesh, P. (2022). Review of Cyber Attack Detection: Honeypot System. Webology, 19(1), 5497-5514.

[16] Liu, Z., Wang, C., & Wang, W. (2022). Online Cyber-Attack Detection in the Industrial Control System: A Deep Reinforcement Learning Approach. Mathematical Problems in Engineering, 2022.

[17] Raja, R. A., Karthikeyan, T., & Praghash, K. (2022). Improved authentication in secured multicast wireless sensor network (MWSN) using opposition frog leaping algorithm to resist man-in-middle attack. Wireless Personal Communications, 123(2), 1715-1731.

[18] Yusof, N. N. M., & Sulaiman, N. S. (2022, August). Cyber Attack Detection Dataset: A Review. In Journal of Physics: Conference Series (Vol. 2319, No. 1, p. 012029). IOP Publishing.

[19] Zhang, J., & Ye, J. (2022, March). Cyber-Attack Detection for Active Neutral Point Clamped (ANPC) Photovoltaic (PV) Converter using Kalman Filter. In 2022 IEEE Applied Power Electronics Conference and Exposition (APEC) (pp. 1939-1944). IEEE.

[20] Raja, R. A., & Kousik, N. V. (2021). Analyses on Artificial Intelligence Framework to Detect Crime Pattern. Intelligent Data Analytics for Terror Threat Prediction: Architectures, Methodologies, Techniques and Applications, 119-132.

[21] Xiao, J., & Feroskhan, M. (2022). Cyber Attack Detection and Isolation for a Quadrotor UAV with Modified Sliding Innovation Sequences. IEEE Transactions on Vehicular Technology.

[22] Abou Jawdeh, S., Choi, S., & Liu, C. H. (2022, March). Model-Based Deep Learning for Cyber-Attack Detection in Electric Drive Systems. In 2022 IEEE Applied Power Electronics Conference and Exposition (APEC) (pp. 567-573). IEEE.

[23] Kumar, C. V. (2022). A real time health care cyber attack detection using ensemble classifier. Computers and Electrical Engineering, 101, 108043.

[24] Rathish, C. R., and A. Rajaram. "Efficient path reassessment based on node probability in wireless sensor network." International Journal of Control Theory and Applications 34.2016 (2016): 817-832.

[25] S Rahamat Basha, Chhavi Sharma, Farrukh Sayeed, AN Arularasan, PV Pramila, Santaji Krishna Shinde, Bhasker Pant, A Rajaram, Alazar Yeshitla, "Implementation of Reliability Antecedent Forwarding Technique Using Straddling Path Recovery in Manet," Wireless Communications & Mobile Computing (Online), vol. 2022, 2022.

[26] Rathish, C. R., and A. Rajaram. "Hierarchical Load Balanced Routing Protocol for Wireless Sensor Networks." International Journal of Applied Engineering Research 10.7 (2015): 16521-16534.

[27] D. N. V. S. L. S. Indira, Rajendra Kumar Ganiya, P. Ashok Babu, A. Jasmine Xavier, L. Kavisankar, S. Hemalatha, V. Senthilkumar, T. Kavitha, A. Rajaram, Karthik Annam, Alazar Yeshitla, "Improved Artificial Neural Network with State Order Dataset Estimation for Brain Cancer Cell Diagnosis", BioMed Research International, vol. 2022, 10 pages, 2022.

[28] P. Ganesh, G. B. S. R. Naidu, Korla Swaroopa, R. Rahul, Ahmad Almadhor, C. Senthilkumar, Durgaprasad Gangodkar, A. Rajaram, Alazar Yeshitla, "Implementation of Hidden Node Detection Scheme for Self-Organization of Data Packet", Wireless Communications and Mobile Computing, vol. 2022, 9 pages, 2022. https://doi.org/10.1155/2022/1332373.

[29] Rajaram and K. Sathiyaraj, “An improved optimization technique for energy harvesting system with grid connected power for green house management,” Journal of Electrical Engineering & Technology, vol. 2022, pp. 1-13, 2022.

[30] M. Dinesh, C Arvind, S.S Sreeja Mole, C.S. Subash Kumar, P. Chandra Sekar, K. Somasundaram, K. Srihari, S. Chandragandhi, Venkatesa Prabhu Sundramurthy, "An Energy Efficient Architecture for Furnace Monitor and Control in Foundry Based on Industry 4.0 Using IoT", Scientific Programming, vol. 2022, Article ID 1128717, 8 pages, 2022. https://doi.org/10.1155/2022/1128717.

[31] S Kannan, A Rajaram, "Enhanced Stable Path Routing Approach for Improving Packet Delivery in MANET," Journal of Computational and Theoretical Nanoscience, vol. 4, no. 9, pp. 4545-4552, 2017.

[32] RP Prem Anand, A Rajaram. "Effective timer count scheduling with spectator routing using stifle restriction algorithm in manet," IOP Conference Series: Materials Science and Engineering, vol. 994, no. 1, pp. 012031, 2022.

[33] Rathish, C. R., and A. Rajaram. "Efficient path reassessment based on node probability in wireless sensor network." International Journal of Control Theory and Applications 34.2016 (2016): 817-832.

[34] Kumar, K. Vinoth, and A. Rajaram. "Energy efficient and node mobility based data replication algorithm for MANET." (2019).

[35] CR Rathish, A Rajaram, "Sweeping inclusive connectivity based routing in wireless sensor networks," ARPN Journal of Engineering and Applied Sciences, vol. 3, no. 5. pp. 1752-1760, 2018.