Review Study on Different Attack Strategies of Worm in a Network

Avijit Mondal*
Research Scholar MAKAUT and Assistant Professor, Department of CSE, Techno International Batanagar, India. E-mail: avijit.mondal@tib.edu.in

Arnab Kumar Das
Assistant Professor, Computer Science and Engineering, JIS University, India.
E-mail: arnab.das@jisuniversity.ac.in

Sayan Nath
Assistant Professor, Techno International Batanagar, India. E-mail: sayan.nath@tib.edu.in

Radha Tamal Goswami
Director, Techno International New Town, Kolkata, West Bengal, India.
E-mail: rtgoswami@tict.edu.in

Received June 29, 2020; Accepted August 30, 2020
ISSN: 1735-188X
DOI: 10.14704/WEB/V17I2/WEB17038

Abstract

In today's era Internet worm is a giant threat to the network infrastructure. Although there are different strategies to sense those hazard at early stages. They detect using some signature based approach. But when novel attacks come into the structure, it is very hard to detect them as they do not have any previous signature. For those some signature based methodology is used. In our work we have reviewed different strategies of internet worm detection and prevention and this article also explores the existing techniques to automate signatures for network worms.

Keywords

Network, Worm, Signature, Replicate, Worm Propagation Methodology, Automating Method for Worm.

Introduction

A computer worm is a self-replicating, self-duplicating malevolent symbol that extend without human intercession in networks and attacks susceptible hosts. Internet worms are characteristically classified based on two attributes: methods used to extend and the

methodology used to exploit vulnerabilities. For that purposes now a day's researchers are interested to suggest techniques to automate signature for internet worms.

Internet worms often attack the computer through the development of vulnerabilities arising from low-level memory faults such as stack overflow, format string vulnerability, integer overflow, double free, heap overflow and return-to-libc [14]. Thus, to protect the computer system from the Internet attacks, the scanning process is done for all available network resources using local OS services and the Internet for vulnerable hosts in the network [15]. Many real-world worms have caused notable damage to the network and computers. These worms include "Code-Red" worm in 2001,"Slammer" worm in 2003 [16],"Witty"/ "Sasser" worms in 2004, Storm worm in 2007 [17] and StuxNet worms in 2010-2012.

Currently many software packages are used to detect and remove the internet worms. Usually antivirus software checks each file in the system looking for known cipher (signatures) which uniquely identify an instance of known malcode [18]. Various approaches exist to detect or eliminate the malware code using Intrusion detection systems. These types of intrusion detection used in host level are called host-based intrusion detection systems (HIDS) [19] [20].

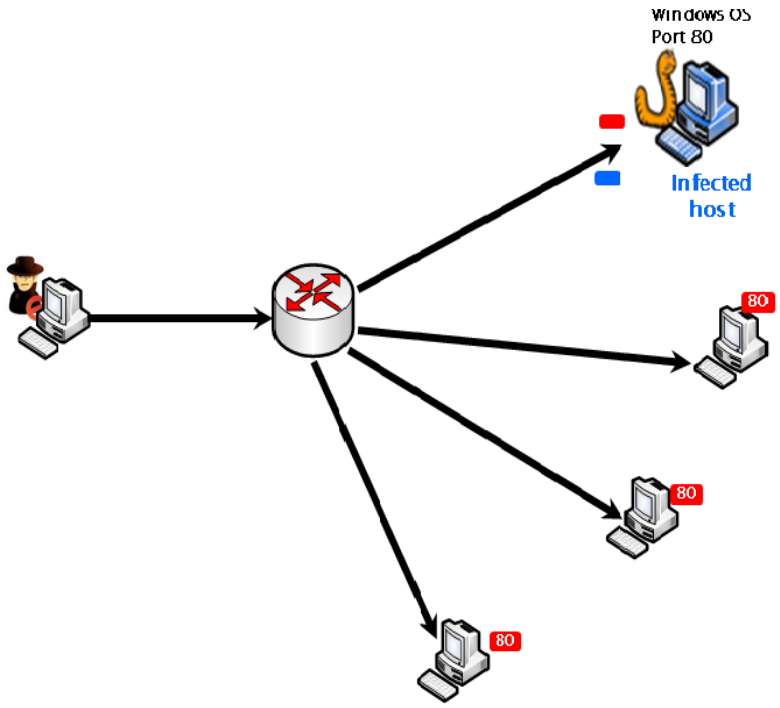

Fig. 1 Depicts worm propagation methodology in a network

Once a worm attacks comes into a system, it will mechanically start to spread that will create obliteration to the network because of overcrowding. It increases the network traffic also.

Literature Review

Zhou, J., Heckman et.al, (2007), In this particular paper, we suggest an organized method that primarily abstracts the fundamental building blocks in terms of skills shipped between strikes then utilizes them to determine the skills. Most features in various levels of a technique abstraction are identified by an individual method. The meaning is much more communicative as well as accurate compare to the predicates utilized by various other aware correlation techniques.

We subsequently abstract IDS signals in the terminology of ability sets as well as derive rational associations between various abilities in regards to inference guidelines. This method can deal with lacking strikes and also get equivalent consequences of various strikes. Many algorithms are produced to relate alerts grounded on cautious abstractions as well as inference guidelines. The expertise of ours in modeling a huge selection of signatures of three favorite NIDSs reveals it helps with the process of improving the ability sets depending on the model of ours [1]. The experimental outcomes of several real-world and well-known intrusion finding datasets indicate the strategy is guaranteeing at aware fusion as well as correlation.

A lot of given alerts are sensibly engaged in an individual multi-stage intrusion event along with a protection officer typically would like to evaluate the entire event rather than every person basic attention. This particular paper recommends a well-defined style which summaries the rational relation in amid the alerts causing an effort to help automated association of all defined alerts active in the exact identical intrusion. The fundamental foundation of the unit is a consistent formulation referred to as an ability. Capability is used by us to abstract precisely and consistently almost all expanses of accesses gotten through the assailant in every phase of any multistage intrusion.

Therefore, gain implication guidelines to explain rational associations amid of several abilities. According to the product as well as the inference guidelines, many novel alert correlation algorithms have been developed by us as well as applied a prototype awake correlator. The investigational success of given correlator by using many intrusion data values show the strategy works well equally aware fusions as well as awake correlation as well as possesses the capability to associate alerts of complicated multistage intrusions.

Now by some situations, the aware correlator effectively linked over 2 1000 Snort alerts associated with substantial checking incidents [2]. Additionally, it aided us to locate double multistage intrusions that have been skipped in reviewing with the help of the protection officers.

Li, P., Salour, M., &Su, X. (2008), have been recommended numerous algorithms before to try and capture as well as quit the spread of Internet worms. Although an extensive category of the current detection, as well as containment methods, are given by not one of the documents, many research documents talk about initiatives that are generally associated with the proposed work of theirs.

A survey along with evaluation of Internet worm detection as well as containment methods consists of this article. The methods depending on the variables applied to every plan are categorized by the research of ours [3]. These groups are when matched in contradiction of worm attributes, thus the inadequacy of existing methods is keen out. Right after noticing the presence of worms, the subsequent thing is containing them. The present techniques utilized to retard and quit the spread of worms are explored by this particular report. The places to implement containment and detection, in addition to every one of the method scopes, are usually checked out in level at every level.

Mishra, B. K., & Jha, N. (2010), Vulnerable- subjected- quarantined -infectious – improved type in terms of the communication of malicious items in computer system is industrialized the balance of theirs are additionally discovered with cyber mass actions likelihood. The infected portion continues as well as the achievable area is a collinear balance area for the prevalent equilibrium declare. Mathematical techniques are used to resolve as well as mimic the device of formulas created [4][5]. The result of quarantine on recovered nodes is examined. We've additionally examined the actions of the vulnerable, quarantine, infected, exposed, and also recovered nodes in the computer system.

The activity of malicious items across a system could be analyzed by utilizing epidemiological versions for illness propagation. Depending on the classical pandemic design, dynamical versions for malicious items propagation had been suggested, supplying estimations for sequential improvements of septic nodes based on community variables discussing topological facets of the system. The approach type was put on to email propagation systems as well as changes of SIR airers produced manuals for disease prevention by utilizing the idea of the epidemiological threshold [6]. Below, we proposed a longer SEI (susceptible-exposed-infected) design to mimic virus propagation.

Nevertheless, they don't display the duration of latency and get into account the effect of antivirus application.

The unit SEIR suggested by the experts assumes that healing hosting companies enjoy a lasting immunization phase with a particular likelihood, and that isn't in line with a circumstance that is actual. To be able to conquer limitation, provide an SEIRS design with latent as well as short-term immune times that may expose typical worm propagation. Lately, extra analysis interest continues to be given on the blend of virus propagation models as well as antivirus countermeasures to learn the occurrence of quarantine, virus immunization, for example, and virus. To extend the SEIRS type of Saini and Mishra, brand new compartment quarantine continues to be created as well as the consequence of its continues to be examined in this paper.

S. Singh, C. Estan, G. Varghese, and S. Savage [7]"The first bird process for producing signatures to identify worms were described by savage. This particular process measures packet content occurrence within a one-time monitoring factor like a networking DMZ. By counting the selection of unique resources as well as destinations connected "with strings which repeat usually in the payload, Early bird differentiates benign recurrences from pandemic articles. Original bird, also love Honeycomb as well as Autograph, creates signatures comprising of an individual, adjoining substring of a worm's payload to complement each worm situations. These signatures, nonetheless, neglect to complement everything polymorphic worm occurrences with low false positives along with low false negatives.

Every infection are generated by just about all the devices, much like the system of ours,. Just about all the methods record the package payloads from a wireless router, hence in the toughest situation, the methods might find a couple of polymorphic worms nonetheless every one of them exploits an alternative vulnerability from one another. Since various vulnerabilities are exploited by them. The assailant sends a single example of a polymorphic worm towards networking, so this particular worm in each and every disease instantly tries to alter the payload of its to produce various other situations. Thus, in case we have to catch everything polymorphic worm situations.

Tang, Y., & Chen, S. (2005, March) [10][11], we briefly present the common community intrusion detection methods associated with the worm detection right here because they may provide us some awareness to structure the systems of ours on anti-worm safeguard, specifically for stealthy worms. But there are available many methods for intrusion detection. The statistical functions of regular site traffic are derived by anomaly-based

systems. Any deviation from the profile is going to be viewed as distrustful. Although such methods are able to detect before unfamiliar strikes, additionally, they result in substantial bogus pluses as the actions of genuine pursuits is primarily unforeseeable.

On the flip side, misuse guidance methods appear to be for specific, explicit indications of episodes like the design of malicious site traffic payload. They are able to identify the presence of recognized worms but crash on those which are a newbie. Many deployed worm detection methods are signature-based. That should be on the misappropriation detection class. They search €or certain byte sequences (named hit signatures) which are recognized to show up in the visitors produced by some attacks. Usually, hit signatures are physically displaying man pros through thorough evaluation of the byte sequence by shot assault visitors. An effective signature must be the camera that regularly turns up to the strike visitors but seldom is found in regular site traffic. The signature-based procedures hold the benefit with the anomaly-based methods in they're able and simple to work on the internet in time that is actual.

The issue is which they are able to just identify recognized strikes with determined signatures which are taken by professionals. Automatic signature development for completely new strikes is incredibly hard as a result of 3 causes. To begin with, to produce an assault signature, we should find as well as separate the strike visitors from therespectable site traffic. Automated documentation of completely new worms is of utmost crucial, and that is the basis of some other safeguard methods. Second, the signature development has to be common adequate to record each strike traffic of some forms while simultaneously certain adequate to stay away from the overlap with the items in genuine visitors in directive to lessen false positives.

Generally, there is missing an organized option for this particular issue that has thus distant management of an ad hoc option primarily founded on man judgment. Lastly, the device should be versatile adequate to cope with the polymorphism in the assault visitors. Or else, worms might be planned to somewhat change the cases of themselves intentionally every time they duplicate, therefore very easily trick the security system. Given particular paper tries to handle the already-mentioned issues. Novel double honeypot modeled process that is certainly organized in a neighborhood community for worm strikes automated discovery coming through the Internet [8].

The product has the ability to identify the strike visitors from the likely large quantity of regular visitors on the record. It not merely permits us to cause alerts but additionally capture the strike situations of an ongoing worm pandemic. We recapitulate the

polymorphism methods which a worm might work with to avoid the detection through present defense methods. A brand-new kind of position-aware division signature (PADS) which is effective at detection of polymorphic worms some kind will be talked about [9].

The signature refers as set of place mindful byte frequency circulations, that is much more adaptable compared to the standard signatures of repaired strings and much more exact compared to position unaware statistical signatures. Here explains the way to complement a byte sequence from the "non-conventional". The outcomes indicate the signature-based security structure of ours could effectively sort brand new alternatives of the worm after the standard history by utilizing the PADS signature produced from history samples.

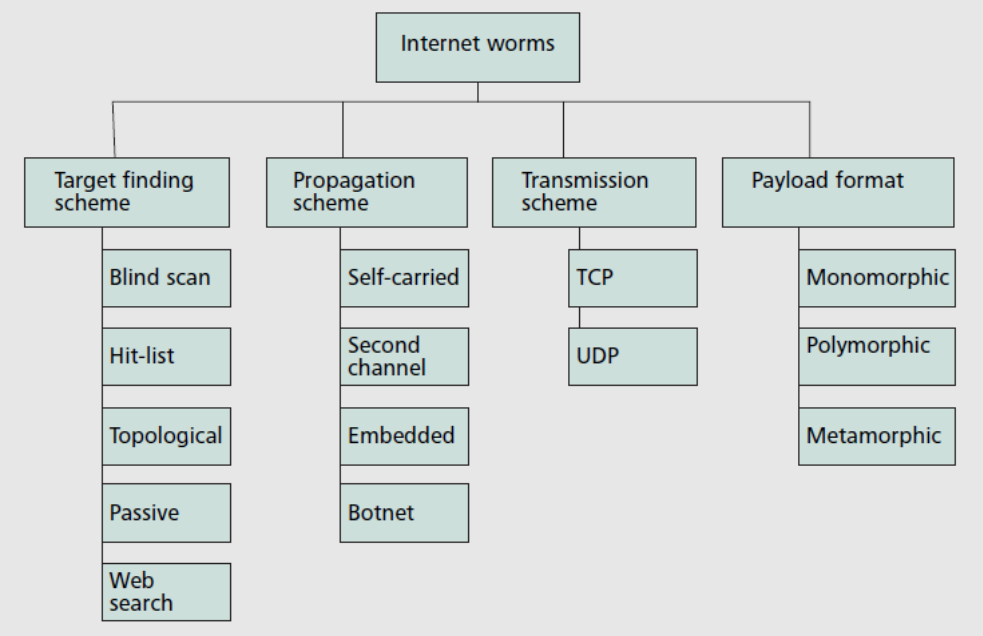

Fig. 2 Categorization of worm characteristics

Diverse techniques have been used to sense network worms and dissimilar parameters are used to get the correctness of recognition. Even satisfactory level of accurateness is achieved, there may be certain boundaries on memory and system affect rates. Network worms are to be detected before distressing the network and the projected approach overcomes the existing limitations.

In Fig 3 we have discussed some Literature review on worm detection techniques used by some authors and the metrics and observation taken for those techniques also.

Robert Mosvitch et al. [2008] used Bayesian Networks which has True Positive Rate, False Positive Rate & Total Accuracy. The major observation was “Mean detection accuracy is achieved with low false positive rate”.

Wei Yu et al.[2010] used Game Theory that has Infection Rate, False Positive Rate. The key inspection was "Worms are classified based on growth rate propagation".

Wei Yu et al.[2011] used Power Spectral Density Distribution which has Infection Ratio, Detection, Time, Detection Ratio and the examination was "Both time and frequency domain are used for analyzing and reducing effective countermeasures".

Nir Nissim et al. [2012] used Support Vector Machine containing True Positive Rate, False Positive Rate, Total Accuracy and finding was "Reduces misleading instances using selective sampling and different kernels with SVM used for classifying unknown worms on hosts".

Year	Author	Technique(s) used	Metrics Used	Observations
2008	Robert Mosvitch et al.	Bayesian Networks	True Positive Rate, False Positive Rate, Total Accuracy	Mean detection accuracy is achieved with low false positive rate
2010	Wei Yu et al.	Game Theory	Infection Rate, False Positive Rate	Worms are classified based on growth rate propagation
2011	Wei Yu et al.	Power Spectral Density Distribution	Infection Ratio, Detection, Time, Detection Ratio	Both time and frequency domain are used for analyzing and reducing effective countermeasures
2011	Qian Wang et al.	Statistical Estimation	Error Rate Detection	Estimation methods perform better for identifying worm infection sequence
2012	Gil Tahan et al.	Boosted Decision Tree	False Positive Rate, Accuracy, AUC (Area Under ROC) Curve	Malwares are detected at the segment level using n-grams
2012	Nir Nissim et al.	Support Vector Machine	True Positive Rate, False Positive Rate, Total Accuracy	Reduces misleading instances using selective sampling and different kernels with SVM used for classifying unknown worms on hosts

Fig 3 Literature Review of Worm Detection

Automating Method for Worm Signatures

The following Fig 4 shows the Double Honeypot System structure. The intention of Double honeypot is inbound is not authoritative to make an outbound association. But when an attack comes it tries to construct outbound connection as worm consist self-replication assets, and malicious codes are forwarded to outbound honeypot. The packets are checked by the protocol classifier which classifies packets in terms of dissimilar protocols (TCP/UDP) and port numbers.

Then the Known-network worms filter component filters out known-network worm samples and pass the left over samples (unknown network worms) to the Signature Generation Algorithms component which extracts all the distinct tokens in the samples. Then it clusters the distinct tokens according to their similarity. The set of tokens in each cluster is used as a signature for that cluster. The total number of the signatures is equals the total number of clusters [22].

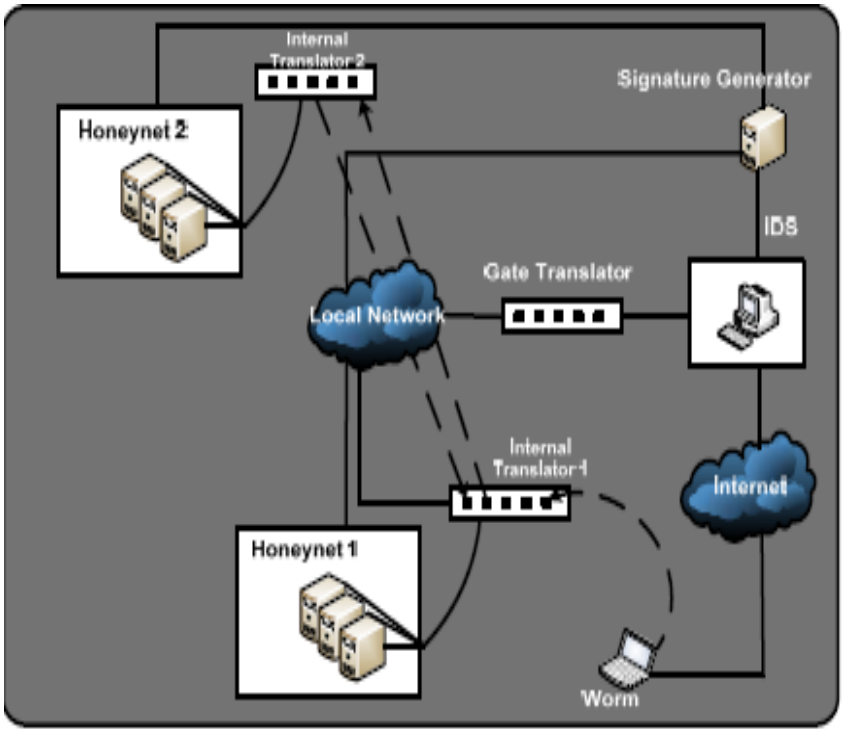

Fig. 4 Double Honeypot Architecture

Kreibich & Crowcroft. [2004] proposed an approach called "Honeycomb approach aims to generate signature for malicious network traffic automatically and it uses pattern-detection techniques and packet header similarities tests on traffic captured from Honeypots" which has disadvantage like "Fail to match all polymorphic network worm instances".

Autograph proposed by [19] is a distributed system for automatically generating network worm signatures for Bro [20] and Snort [21-29]. Autograph aims to mechanically engender signatures for unknown worms that spread using Transmission Control protocol transport.

Autograph produces signatures by analyzing the prevalence of portions of flow payloads, and thus uses no knowledge of protocol semantics above the TCP level [30-37]. It is designed to manufacture signatures that display elevated sensitivity (high true positives) and huge specificity (low false positives).

Singh, Estan, Varghese, & Savage,[2004] Proposed an "Earlybird system for generating signatures to detect network worms based on the assumption that the network worms must generate significant traffic to propagate [38-45]. This traffic will contain common substring which will transfer from source (attacker) to destinations". But it fails to detect polymorphic worm instances. As polymorphic worm changes its appearances with every instance.

Approach	Description	Disadvantage
Kreibich & Crowcroft, 2004	Honeycomb approach aims to generate signature for malicious network traffic automatically and it uses pattern-detection techniques and packet header similarities tests on traffic captured from Honeypots	Fail to match all polymorphic network worm instances
Kim & Karp, 2004	Proposed an Autograph which aims to automatically generate signatures for unknown network worms that propagate using TCP transport. Autograph generates signatures by analyzing the prevalence of portions of flow payloads, and thus uses no knowledge of protocol semantics above the TCP level	Fail to match all polymorphic network worm instances
Singh, Estan, Varghese, & Savage, 2004	Proposed an Earlybird system for generating signatures to detect network worms based on the assumption that the network worms must generate significant traffic to propagate. This traffic will contain common substring which will transfer from source (attacker) to destinations	Fail to match all polymorphic network worm instances

Fig. 5 Automating Signature Generating Techniques of Worm

Conclusions

In this review article, we have discussed the strategies to sense and avert Internet worms in a computer network. This work has highlighted the harshness of presence the Internet worm in the network. Then the lively approach for worm signature automations are discussed and advantages and drawbacks for each approach are tinted.

References

Spitzner, L. (2002). *Honeypots: Tracking Hackers.* Addison Wesley Pearson Education: Boston.

Bidgoli, H. (2006). *Handbook of information security, information warfare, social, legal, and international issues and security foundations.* John Wiley & Sons.

Gusfield, D. (1997). *Algorithms on Strings, Trees and Sequences.* Cambridge University Press: Cambridge.

Levine, J., La Bella, R., Owen, H., Contis, D., & Culver, B. (2003). The use of honeynets to detect exploited systems across large enterprise networks. *In IEEE Systems, Man and Cybernetics Society Information Assurance Workshop*, 92-99.

Kreibich, C., & Crowcroft, J. (2003). Honeycomb–creating intrusion detection signatures using honeypots. *Workshop on Hot Topics in Networks (Hotnets-II), Cambridge, Massachusetts.*

Kim, H.A., & Karp, B. (2004). *Autograph: Toward Automated, Distributed Worm Signature Detection.* In USENIX security symposium.

Singh, S., Estan, C., Varghese, G., & Savage, S. (2004). Automated worm finger printing. *Proc. of the 6th conference on Symposium on Operating Systems Design and Implementation (OSDI)*, 4-4.

Newsome, J., Karp, B., & Song, D. (2005). Polygraph: Automatically generating signatures for polymorphic worms. *In IEEE Symposium on Security and Privacy (S&P'05)*, 226-241.

Yegneswaran, V., Giffin, J.T., Barford, P., & Jha, S. (2005). An Architecture for Generating Semantic Aware Signatures. *In USENIX Security Symposium*, 97-112.

Tang, Y., & Chen, S. (2007). An automated signature-based approach against polymorphic internet worms. *IEEE Transactions on Parallel and Distributed Systems*, *18*(7), 879-892.

Li, Z., Sanghi, M., Chen, Y., Kao, M.Y., & Chavez, B. (2006). Hamsa: Fast signature generation for zero-day polymorphic worms with provable attack resilience. *In IEEE Symposium on Security and Privacy (S&P'06)*, 15.

Damon, J., & Marron, J.S. (2014). Backwards principal component analysis and principal nested relations. *Journal of Mathematical Imaging and Vision*, *50*(1-2), 107-114.

Allen, G.I., Grosenick, L., & Taylor, J. (2014). A generalized least-square matrix decomposition. *Journal of the American Statistical Association*, *109*(505), 145-159.

Qijun, G., Chistopher, F., & Rizwan, N. (2011). A study of self-propagating mal-packets in sensor networks: Attacks and defenses. *ELSEVIER, Computers & Security*, *30*(1), 13-27.

Tahan, G., Rokach, L., & Shahar, Y. (2012). Mal-ID: Automatic Malware Detection Using Common Segment Analysis and Meta-Features. *Journal of Machine Learning Research*, *13*(1), 949-979.

Yu, W., Wang, X., Clayam, P., Xuan, D., & Zhao, W. (2011). Modeling and Detection of Camouflaging Worm. *IEEE Transactions on Dependable and Secure Computing*, *8*(3), 377-390.

Chen, C., Chen, Z., & Li, Y. (2010). Characterizing and defending against divide-conquer-scanning worms. *Elsevier, Computer Networks*, *54*(18), 3210-3222.

Moskovitch, R., Elovici, Y., & Rokach, L. (2008). Detection of unknown computer worms based on behavioral classification of the host. *Elsevier, Computational Statistics & Data Analysis*, *52*(9), 4544–4566.

Snort. (2010). *A free lightweight network intrusion detection system for UNIX and Windows.*

Paxson, V. (1999). Bro: a system for detecting network intruders in real-time. *Computer networks*, *31*, 2435-2463.

Kim, H., & Karp, B. (2004). Autograph: Toward automated, distributed worm signature detection. *In USENIX security symposium*.

Rao, A.N., Vijayapriya, P., Kowsalya, M., & Rajest, S.S. (2020). Computer Tools for Energy Systems. *In International Conference on Communication, Computing and Electronics Systems, Springer, Singapore*, 475-484.

Gupta, J., Singla, M.K., Nijhawan, P., Ganguli, S., & Rajest, S.S. (2020). An IoT-Based Controller Realization for PV System Monitoring and Control. *In Business Intelligence for Enterprise Internet of Things, Springer, Cham*, 213-223.

Sharma, M., Singla, M.K., Nijhawan, P., Ganguli, S., & Rajest, S.S. (2020). An Application of IoT to Develop Concept of Smart Remote Monitoring System. *In Business Intelligence for Enterprise Internet of Things, Springer, Cham*, 233-239.

Ganguli, S., Kaur, G., Sarkar, P., & Rajest, S.S. (2020). An Algorithmic Approach to System Identification in the Delta Domain Using FAdFPA Algorithm. *In Business Intelligence for Enterprise Internet of Things, Springer, Cham*, 203-211.

Singla, M.K., Gupta, J., Nijhawan, P., Ganguli, S., & Rajest, S.S. (2020). Development of an Efficient, Cheap, and Flexible IoT-Based Wind Turbine Emulator. *In Business Intelligence for Enterprise Internet of Things Springer, Cham*, 225-231.

Rajasekaran, R., Rasool, F., Srivastava, S., Masih, J., & Rajest, S.S. (2020). Heat Maps for Human Group Activity in Academic Blocks. *In Business Intelligence for Enterprise Internet of Things, Springer, Cham*, 241-251.

Kummara, H., & Gowd, D. (2014). Design and Fabrication of Plastic Injection Molding Tool for Pump Gaskets. *International Journal of Advanced Engineering Research and Science*, *1*(3), 38-45.

Pasha, R., Saxena, A., & Jindal, J. (2014). Comparison of Various Types of Algorithm for Target Coverage Problem in Wireless Sensor Network. *International Journal of Advanced Engineering Research and Science*, *1*(3), 46-49.

Kumar, M., Kumar, M., & Kumar, G. (2014). PCB Image Enhancement Using Machine Vision for Effective Defect Detection. *International Journal of Advanced Engineering Research and Science*, *1*(3), 50-53.

Sharma, A. (2015). Key Highlights of the Companies Act, 2013- Incorporation of the Companies. *International Journal of Advanced Engineering, Management and Science*, *1*(5), 01-04.

Mandal, D., & Hussain, A. (2015). An Insight into the Governance of Indian Universities since 20th Century. *International Journal of Advanced Engineering, Management and Science*, *1*(5), 05-09.

Babu, A., Haile, A., & Viswanath, C. (2015). Application of Load Following Control in Multi Area Hydrothermal Gas System under Reconstituted Scenario. *International Journal of Advanced Engineering, Management and Science*, *1*(5), 10-15.

Ahmed, E.R., Abdul Rahim, N.F., Alabdullah, T.T.Y., & Thottoli, M.M. (2019). An Examination of Social Media Role in Entrepreneurial Intention among Accounting Students: A SEM Study. *Journal of Modern Accounting and Auditing*, *15*(12), 577-589.

Alabdullah, T.T.Y., Ahmed, E.R., & Nor, M.I. (2018). New Ideas from Management, Finance and Accounting Perspective: The Research for A New Link Between A Company's Outcome and Risk Management. *5th International Conference on New Ideas in Management, Economics and Accounting*.

Manafe, J., Setyorini, T., & Alang, Y. (2018). Influence of implementation on mix promotion model strategy towards tourist visitation in Indonesia. *International Research Journal of Management, IT and Social Sciences*, *5*(6), 26-39.

Maimun, M., & Mandala, H. (2018). Ideology in tempo magazine advertising: a critical discussion analysis. *International research journal of management, IT and social sciences*, *5*(6), 40-51.

Pramanaswari, A.S.I., & Yasa, G.W. (2018). Graham & Dodd theory in stock portfolio performance in LQ 45 index at Indonesia stock exchange. *International Research Journal of Management, IT and Social Sciences*, *5*(6), 52-59.

Kasiselvanathan, M., Sangeetha, V., & Kalaiselvi, A. (2020). Palm pattern recognition using scale invariant feature transform. *International Journal of Intelligence and Sustainable Computing*, *1*(1), 44-52.

Selvaraj, J., & Mohammed, A.S. (2020). Mutation-based PSO techniques for optimal location and parameter settings of STATCOM under generator contingency. *International Journal of Intelligence and Sustainable Computing*, *1*(1), 53-68.

Rao, S.S. (2020). Semantic SPA framework for situational student-project allocation in education. *International Journal of Intelligence and Sustainable Computing*, *1*(1), 69-82.

Arulmurugan, R., & Anandakumar, H. (2018). Early detection of lung cancer using wavelet feature descriptor and feed forward back propagation neural networks classifier. *In Computational Vision and Bio Inspired Computing, Springer, Cham*, 103-110.

Suganya, M., & Anandakumar, H. (2013). Handover based spectrum allocation in cognitive radio networks. *In International Conference on Green Computing, Communication and Conservation of Energy (ICGCE)*, 215-219.

Anandakumar, H., & Umamaheswari, K. (2017). An efficient optimized handover in cognitive radio networks using cooperative spectrum sensing. *Intelligent Automation & Soft Computing*, 1-8.

Haldorai, A., Ramu, A., & Murugan, S. (2018). Social Aware Cognitive Radio Networks: Effectiveness of Social Networks as a Strategic Tool for Organizational Business Management. *In Social network analytics for contemporary business organizations*, *IGI Global*, 188-202.