ISSN: 0974-2115
www.jchps.com Journal of Chemical and Pharmaceutical Sciences

Modeling of detection of camouflaging worm using epidemic dynamic model and power spectral density

G Michael[1*], A Chandrasekar[2]
[1]Department of Computer Science and Engineering, Bharath University, Chennai, India
[2]Department of Computer Science, St.Joseph College of Engineering, Chennai, India
***Corresponding author: E-mail: micmgeo@yahoo.co.in**

ABSTRACT

A worm consequently repeats itself crosswise over systems and might contaminate a huge amount of servers in a brief time frame. It is possible that the digital terrorists might utilize a broad worm to bring about significant disturbance to the Internet economy. Camouflaging Worm has an capability to astutely direct its scan traffic amount eventually, so it is unique in relation to existing worm. The C-Worm covers its engendering from existing worm identification frameworks taking into account examining the spread activity created by worm. Its engendering don't have any example in time area, However, their refinement is clear in the recurrence space, because of the repeating manipulative nature of the C-Worm. Power Spectral Density allocation of the scan congestion amount and its consequent Spectral uniformity compute to differentiate the C-Worm congestion from background congestion.

KEY WORDS: C-Worm, PDF, PRS, PSD.

1. INTRODUCTION

The C-Worm has a self-inducing conduct like traditional web worms; it arrangements to rapidly taint however numerous powerless PCs as could sensibly be normal. Then again, the C-Worm is exceptionally interesting in connection to standard web worms in which it covers any detectable examples in the amount of polluted PCs definitely. The cover is finish by control the take a gander at development volume of worm polluted PCs. Such a control of the scope action volume turns away presentation of any exponentially growing inclinations or existing in order to despite crossing point of edges that are taken after acknowledgment arranges.

The C-Worm channel advancement shows no perceptible samples in the time locale, it exhibits a particular representation in the rehash space. In particular, there is an unquestionable fixation inside of a confined degree of frequencies. This middle inside of a confined degree of frequencies is unavoidable, since the C-Worm adjusts to the segments of the Internet in a repeating way to deal with control and controlling its general expansiveness activity volume. The above reiterating controls consolidate proceeding with advancement, trailed by a diminishing in the yield activity volume, such that the developments don't show up as any illustrations in the time zone or such that the yield activity volume does not cross limits that could uncover the C-Worm extension. Thusly by tolerating rehash range examination routines and add to an affirmation game plan against wide spreading of the C-Worm. Especially, a novel degree based affirmation plot that uses the Power Spectral Density transport of extension improvement volume in the rehash area to see the C-Worm activity from non-worm advancement. Consequently the C-worm is perceived utilizing PSD.

Problem description: The worm propagator models the worm such that it makes low movement in the system to maintain a strategic distance from recognition from the current framework. On the off chance that worm propagator sends the worm to any of the hub, the server recognizes the worm utilizing Power Spectral Density. In the wake of recognizing the worm, the worm conduct is examined physically and patch document is made to erase the worm. The server sends the patch document to the influenced hub and slaughters the worm.

System analysis:

Existing System: In C-Worm, conduct is camouflaged and its development is vivaciously put aside puzzle. So this advancement of see the C-Worm is dicey utilizing the standard Traditional Worm Detection Techniques and in addition IP Trace Back Systems. The Major great position of the C-Worm is that it investigates all the IP Present in the Network first then perceives the measure of new hit and number of copy.

C-Worm rather thinking all the IP, rather it concentrates just the new hits, in light of the way that these frameworks are the Target of C-Worm. The principle reason for C-Worm is the general yield improvement ought to be about move and assortment enough to cover any striking developing cases after some time for C-worm. Then again, a moderate development of the C-Worm is likewise not enchanting, since it defers snappy sullying fiendishness to the Internet. Thusly, the C-Worm necessities to change its spread with the goal that it races to be enough perceived, nor too move to surrender brisk harm on the Internet. The Detection framework is Spectrum strategy based system to dependably screen the Traffic Process. Despite the way that more humble measure of Traffic is essentially going to convey the Spectrum based technique will see the C-Worm in context of the conduct.

2. MATERIALS AND METHODS

Proposed System: The modification that we propose is by modeling the C-worm to delete potential files of the system (for Example - .exe files). Worm scans the system to find the potential file and destroy those information that

has a high economic value. All nodes connected to server, periodically sends the traffic log to server. Server performs the PSD analysis and if server detect any node affected by worm, server analyze it behavior. After analyzing its behavior, server deletes it by sending the patch file.

Architecture of worm detection system:

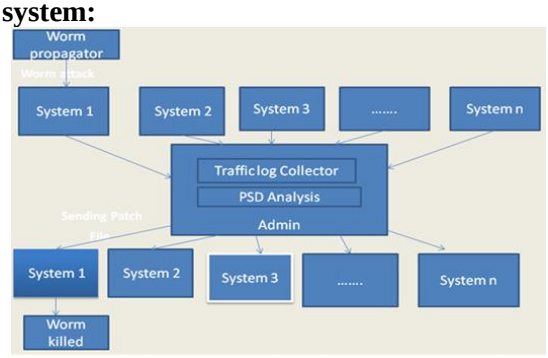

Figure.1. Architecture Diagram of C-Worm Propagation and Detection

In the network, all the n systems are inter-connected with each other and with server. Each node communicates with each other by sending and receiving packets as shown in figur1.

The server monitors each and every system in the network for any malicious activity. The server periodically collects the traffic log and performs the PSD analysis. If the PSD value is less than the historical value, the system is alerted to detect worm. When the worm Propagator attacks any one of the system, Server detects the worm and analyze its behavior. After analyzing, it deletes the worm by sending the patch file.

Module description: The proposed system consists of four modules:

- Network Construction
- Worm Propagator
- Modeling Of C-Worm
- Worm Propagation
- Worm Detection
- Dynamic Patch Distribution

Network Construction: In this module, the Graphical User Interface is illustrated with a particular deciding objective to make a dynamic framework. A worm aggressor may use an open-circle control framework by picking a randomized and time-related case for the checking and pollution in order to refrain from being recognized. Coincidentally, the open-circle control approach raises a couple issues of the impalpability of the attack. To begin with, worm multiplication over the Internet can be seen as a dynamic structure. Right when an attacker dispatches worm multiplication, it is to a great degree striving for the aggressor to know the accurate parameters for worm inducing movement over the Internet. Given the mistaken learning of worm causing over the Internet, the open-circle control system won't have the ability to offset the yield development. This is a known result from control structure speculation.

Subsequently, the general worm channel development volume in the open-circle control structure will reveal a much higher probability to show an extending design with the progression of worm inducing. As more frameworks get defiled, they, hence, tune in separating diverse PCs. From this time forward, the C-worm as a most skeptical situation attacking circumstance that uses a close hover control for dealing with the spread rate in perspective of the feedback expansion status. In a system, all hubs are interconnected with one another and server, which is observing the various hubs. All hubs are sending so as to impart their data to one another and getting bundles. Server occasionally gathers the IP address, port number, procedures and System Traffic of a framework.

Worm Propagator: Worm propagator is the aggressor who spreads the worm in a system. When all is said in done a worm propagator has two targets:

- One is to taint however many PCs as could be expected under the circumstances inside of a given timeframe.
- Other is to abstain from being influence which is as of now influents.

Modeling of C-Worm: The C-Worm covers its extension by controlling expansiveness advancement volume amidst its instigating. The base complex approach to manage control break down improvement volume is to self-self-assuredly change the measure of worm cases driving port yield. With a specific choosing goal to suitably maintain a strategic distance from unmistakable confirmation, the general broadness improvement for C-Worm ought to be respectably move and assortment enough to not show any well-known amplifying plans after some time. Obviously, a moderate inducing of the C Worm is besides not enchanting, since it puts off quick pollution harm to the Internet. Thusly, the C-Worm necessities to change its extension with the goal that it hurries to be not effectively perceived, nor too move to yield speedy naughtiness on the Internet. To organize the C-Worm review development volume, we

demonstrate a control parameter called strike likelihood P(t) for every worm-sullied PC. P(t) is the likelihood that a C Worm occasion takes an interest in the worm augmentation at time t.

C-Worm model with the control parameter P(t) is level. It additionally decreases the improvement level by ruining assaulting the definitively affected PCs. The basic accepted is as indicated by the going with. A C-Worm could survey the rate of PCs that have beginning now been debased once again the aggregate number of IP regions and moreover, through checking a reach endeavor as another hit or a copy hit. This framework requires each worm event to be stamped exhibiting that this PC has been corrupted. As needs be, the point at which a worm case analyzes one sullied PC, then PC will perceive such an engraving, along these lines getting the opportunity to be careful that PC has been spoiled.

Worm Propagation: Worm uses epidemic element model for disease multiplication, which has been generally used for worm spread showing. Particularly, the scourge dynamic model acknowledges that any given PC is in one of the going with states: immune, weak, or spoiled. An immune PC is one that can't be debased by a worm. A feeble PC is one that has the ability of being corrupted by a worms, a debased PC is one that has been spoiled by a worm. The pandemic component model comparison is given in (Equation 1).

$$d(M(t))/dt = \beta.M(t).(N-M(t)) \quad \text{(Equation.1)}$$

where M (t) is the number of affect computers at time t

N is the number of computer at time t

β is the number of vulnerable computers at time t

The C-Worm has another causing model stood out from standard PRS worms because of its p(t) parameter. Henceforth, Epidemic component equation (formula 4.1) is changed in accordance with demonstrate the expansion of the C-Worm by introducing the P(t)- the ambush probability that a worm-spoiled PC shares in worm spread at time t is given in (Equation.2)

$$d(M(t))/dt = P(t).\ \beta.M(t).(N-M(t)) \quad \text{(Equation. 2)}$$

Worm detection: With a particular deciding objective to perceive the C-Worm expansion in the repeat territory, we use the scattering of PSD of the analyze movement. Overwhelmingly, PSD delineate how the effect of a period game plan is flowed in the repeat zone. Numerically, it is portrayed as the Fourier change of the autocorrelation of a period plan. For our circumstance, the time course of action identifies with the modification in the amount of worm events that successfully coordinate yields after some time. Therefore PSD is used to recognize the C-Worm.

To get the PSD, change information from the time area into the recurrence space. In the Spectrum Analysis, the worm's conduct is checked constantly for a timeframe, and afterward the information is changed from time area to recurrence space utilizing Discrete Fourier Transform.

Equation 3 demonstrates discrete fourier change used to change over information from time area to recurrence space. The extensive PDF estimations of typical non-worm filter movement can be clarified as takes after: The ordinary non-worm examine activity does not tend to assemble at a specific recurrence, since its arbitrary motion is not brought about by any repeating wonder. The little estimation of PDF can be considered by the way that the force of C-Worm take a gander at development is inside of a narrowband rehash range. Such fixation inside of a small degree of frequencies is unavoidable, since the C-Worm changes with the flood of the Internet in a repeating way to deal with control the general expansiveness activity volume.

In the event that the DFT estimation of the framework is not exactly the verifiable estimation of that framework, then framework will be cautioned to recognize the worm. The recurrence space examination will require more specimens in correlation with the time-area investigation, since the recurrence area investigation system, for example, the Fourier change, needs to determine power range adequacy for distinctive frequencies.

$$DFT\ (R_x(T)) = \sum_{n=0}^{N-1} (R_x(T))e^{-2j\pi kn/N} \quad \text{(Equation. 3)}$$

Where K =0, 1, . . .N - 1.

N=number of system connected to internet.

R_x (T) =Traffic log detail in time domain.

The recurrence space investigation will require more examples in examination with the time-area investigation, since the recurrence space investigation method, for example, the Fourier change, needs to determine power range plentifulness for diverse frequencies. With a specific end goal to produce the precise range plentifulness for generally high frequencies, a high granularity of information inspecting will be necessary.

Dynamic patch distribution: Server periodically collects all the information about the system and performs the PSD analysis. If server detects any system affected by C-worm, it will analyze the worm behavior and gives patch file to delete the worm.

System implementation:

General: The implementation provides the snapshots of the output for each and every modules and every single process. It also shows how the accuracy improves among the existing and proposed method.

Network construction:

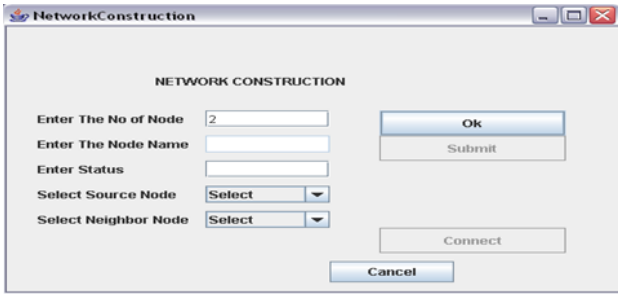

Figure.2. Describes the total number of nodes

Network construction is the first step in the propagation of C-worm. Fig 2 describes the total number of nodes to be connected for the worm to propagate. Here we enter the number of nodes that we want in a network.

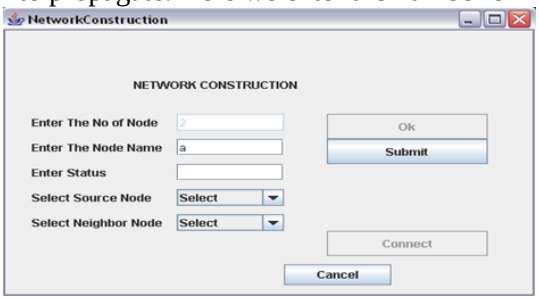

Figure.3. Presents the naming of individual nodes

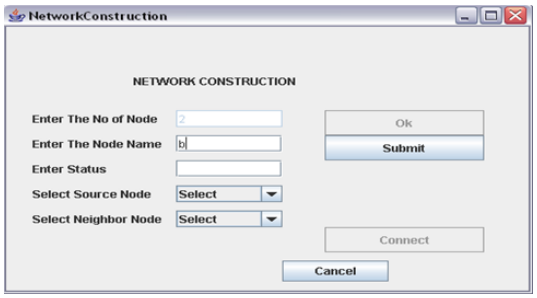

Figure.4. Similarly all other nodes are given a name

As the total number of nodes is mentioned, Fig.3, presents the naming of individual nodes. Each node is given a unique name and is updated in the server. Similarly all other nodes are given a name which is updated in the server as shown in above Fig 4

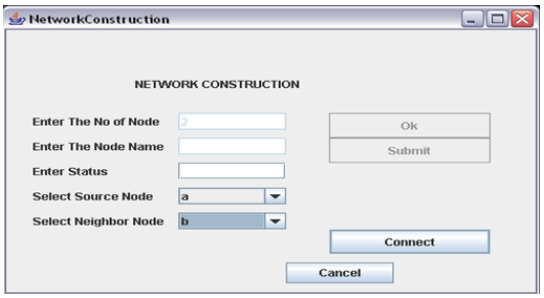

Figure.5. Indicates that a link between a source node and a destination node

Fig.5, indicates that a link between a source node and a destination node is given. The source node name and the destination node name is specified and then connect button is pressed.

Figure.6. Established between the source node and the destination node

The dialog box indicates that a connection is established between the source node and the destination node. A message dialog box appears indicating that the connection is established between the nodes as shown in above Fig.6.

Node creation:

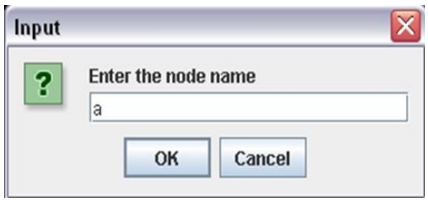

Figure.7. The node name is given as the input as shown

A input dialog box appears once the node.java file is executed. The node name is given as the input as shown above in Fig.7.

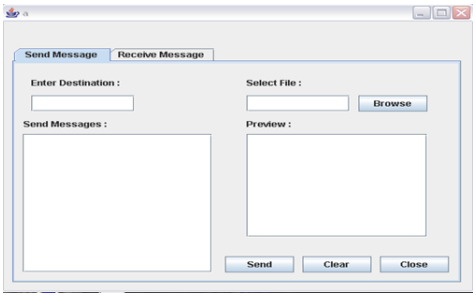

Figure.8. Indicates the sender receiver dialog box for node

Fig.8, indicates the sender receiver dialog box for node a. The C-worm file can be browsed and can be sent to the destination node that is specified.

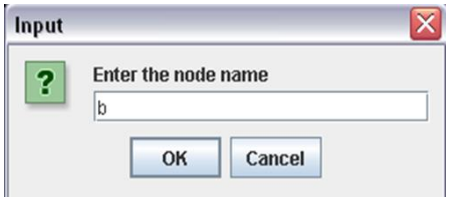

Figure.9. Node name is specified

Similarly as the node.java file is executed, another input dialog box appears where other node name is specified as shown in above Fig.9.

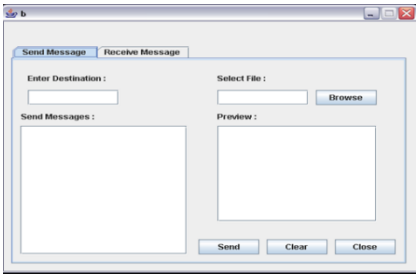

Figure.10. This is the destination node where the C-worm is received

Another sender receiver dialog box appears for node b. This is the destination node where the C-worm is received. This is described in Fig.10, as shown above.

Worm propagation:

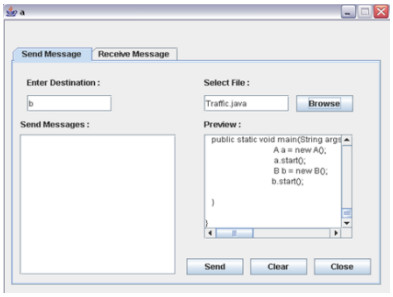

Figure.11. Describes the destination node for the worm file

Figure.11, describes the destination node for the worm file. The C-worm file is browsed and it is sent to the destination node where it starts running on its own.

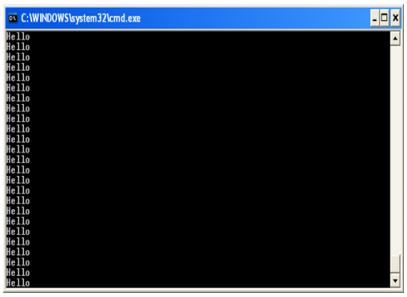

Figure.12. Indicated that the C-worm starts running on the destination node

Fig.12, indicated that the C-worm starts running on the destination node. It prints the word hello as soon as it reaches the destination.

Worm detection and deletion:

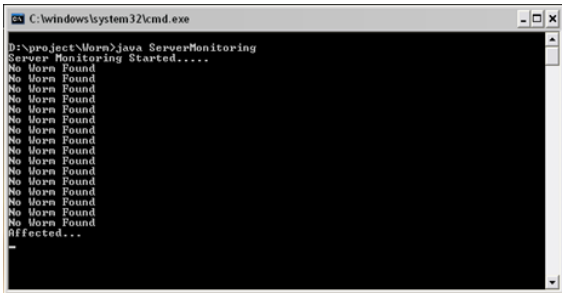

Figure.13. the server monitor that monitors the worm behavior such as the traffic, IP address, and port number

Figure.13, is the server monitor that monitors the worm behavior such as the traffic, IP address, and port number. When the server detects the presence of C-worm in a system, it compares the historical data with the present data. If it is greater the one then the server deletes the worm file.

3. RESULTS AND EVALUATION

General: Performance evaluation is a phase where we compare the performance of the PRS worm affected traffic with that of the C-worm affected traffic. We evaluate the performance with the help of a line graph.

Performance graph:

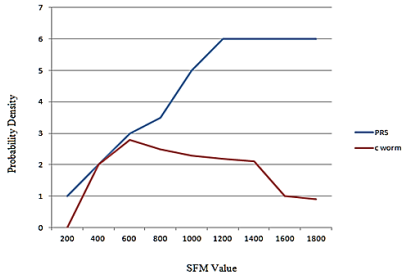

Figure.14.PDF of PRS worm and C-worm

Figure 14 shows the PDF of the PRS worm traffic and C-Worm traffic. whenever a worm enter the system, it become active and the worm code run continuously, so the traffic of the system goes up and traffic remains constantly high.. As you can see, the traffic of PRS worm goes up instantly and remains constantly high. So the PRS worm can be detected easily. The traffic of C-Worm is not either too high or too low. So the performance of C-Worm is better than the PRS worm.

4. CONCLUSION

Engendering and promote evade the discovery from the current recognition framework. In spite of the fact that the C-Worm effectively disguises its proliferation in the time space, its covering nature unavoidably shows as an unmistakable example in the recurrence area. Taking into account perception, we added to a novel range based identification plan to identify the C-Worm. It can viably distinguish the C-worm. Our assessment information demonstrated that our plan accomplished unrivaled recognition execution against the C-Worm in correlation with existing delegate existing discovery plans.

Future work: The major disadvantage of C-Worm is that it showed a distinct pattern in time domain. In future, the C-Worm can be modeled to overcome this disadvantage so that it cannot be detected using spectrum based analysis.

REFERENCES

Achudhan M, Prem Jayakumar M, Mathematical modeling and control of an electrically-heated catalyst, International Journal of Applied Engineering Research, 9 (23), 2014, 23013.

Chen ZS, Gao LX and Kwiat K, Modeling the Spread of Active Worms, Proc. IEEE INFOCOM, 2003

Christian Schallhart, Helmut Veith And Johannes Kinder, Proactive Detection Of Computer Worms Using Model Checking, IEEE Transactions On Dependable And Secure Computing, 2010

Cliff Zou C, Don Towsley And Weibo Gong, The Monitoring And Early Detection Of Internet Worms, IEEE/ACM Transactions On Networking, 2008

David Dagon, John Levine And Xinzhou Qin, Honeystat-Local Worm Detection Using Honeypots", IEEE Transactions On Dependable And Secure Computing, 2006

Gopalakrishnan K, Sundeep Aanand J, Udayakumar R, Electrical properties of doped azopolyester, Middle - East Journal of Scientific Research, 20 (11), 2014, 1402-1412.

Gopinath S, Sundararaj M, Elangovan S, Rathakrishnan E, Mixing characteristics of elliptical and rectangular subsonic jets with swirling co-flow, International Journal of Turbo and Jet Engines, 32 (1), 2015, 73-83.

Ilayaraja K, Ambica A, Spatial distribution of groundwater quality between Injambakkam-Thiruvanmyiur areas, south east coast of India, Nature Environment and Pollution Technology, 14 (4), 2015, 771-776.

Kang .M.G, J. Caballero, and D. Song, "Distributed Evasive Scan Techniques and Countermeasures," Proc. Int'l Conf. Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA), 2007.

Kerana Hanirex D, Kaliyamurthie KP, Kumaravel A, Analysis of improved tdtr algorithm for mining frequent itemsets using dengue virus type 1 dataset: A combined approach, International Journal of Pharma and Bio Sciences, 6 (2), 2015, 288-295.

Lingeswaran K, Prasad Karamcheti SS, Gopikrishnan M, Ramu G, Preparation and characterization of chemical bath deposited cds thin film for solar cell, Middle - East Journal of Scientific Research, 20 (7), 2014, 812-814.

Nan Z Hang,Wei Yu And Wei Zhao"Self-Disciplinary Worms And Counter Measures: Modeling And Analysis" ,IEEE Transactions On Parallel And Distributed Systems, 2010

Premkumar S, Ramu G, Gunasekaran S, Baskar D, Solar industrial process heating associated with thermal energy storage for feed water heating, Middle - East Journal of Scientific Research, 20 (11), 2014, 1686-1688.

Shigang Chen And Yong Tang, Daw: A Distributed Antiworm System, IEEE Transactions On Parallel And Distributed Systems, 2008

Staniford S, Paxson V and N. Weaver, "How to Own the Internet in Your Spare Time," Proc. 11th USENIX Security Symp. (SECURITY), 2002.

Sundar Raj M, Saravanan T, Srinivasan V, Design of silicon-carbide based cascaded multilevel inverter, Middle - East Journal of Scientific Research, 20 (12), 2014, 1785-1791.

Thooyamani KP, Khanaa V, Udayakumar R, Application of pattern recognition for farsi license plate recognition, Middle - East Journal of Scientific Research, 18 (12), 2013, 1768-1774.

Thooyamani KP, Khanaa V, Udayakumar R, Efficiently measuring denial of service attacks using appropriate metrics, Middle - East Journal of Scientific Research, 20 (12), 2014, 2464-2470.

Thooyamani KP, Khanaa V, Udayakumar R, Partial encryption and partial inference control based disclosure in effective cost cloud, Middle - East Journal of Scientific Research, 20 (12), 2014, 2456-2459.

Thooyamani KP, Khanaa V, Udayakumar R, Using integrated circuits with low power multi bit flip-flops in different approch, Middle - East Journal of Scientific Research, 20 (12), 2014, 2586-2593.

Thooyamani KP, Khanaa V, Udayakumar R, Virtual instrumentation based process of agriculture by automation, Middle - East Journal of Scientific Research, 20 (12), 2014, 2604-2612.

Thooyamani KP, Khanaa V, Udayakumar R, Wide area wireless networks-IETF, Middle - East Journal of Scientific Research, 20 (12), 2014, 2042-2046.

Udayakumar R, Kaliyamurthie KP, Khanaa, Thooyamani KP, Data mining a boon: Predictive system for university topper women in academia, World Applied Sciences Journal, 29 (14), 2014, 86-90.

Vogt R, Aycock J and Jacobson M, Quorum Sensing and Self-Stopping Worms, Proc. Fifth ACM Workshop Recurring Malcode(WORM), 2007.

Wang X, Yu W, Champion A, Fu X and Xuan D, Detecting Worms via Mining Dynamic Program Execution, Proc. IEEE Int'l Conf. Security and Privacy in Comm. Networks (SECURECOMM), 2007.

Wright C, Coull S and Monrose F, Traffic Morphing, An Efficient Defense Against Statistical Traffic Analysis, Proc. 15th IEEE Network and Distributed System Security Symp. (NDSS), 2008.

Yu W, Wang X, Xuan D and Lee D, Effective Detection of Active Worms with Varying Scan Rate, Proc. IEEE Int'l Conf. Security and Privacy in Comm. Networks, 2006.