Journal of Information Assurance and Security.
ISSN 1554-1010 Volume 11 (2016) pp. 340-347
© MIR Labs, www.mirlabs.net/jias/index.html

Plant based Biologically Inspired Intrusion Response Mechanism : An insight into the proposed model PIRIDS

Rupam Kumar Sharma[1], Hemanta Kr. Kalita[2] and Biju Issac[3]

[1] School of Technlogy, North Eastern Hills University,
Shillong,Meghalaya, India
sun1_rupam1@yahoo.com

[2] School of Technology, North Eastern Hills university,
Shillong, Meghalaya, India
kalita.hemanta@gmail.com

[3] School of Computing,Teesside University,
England
bijuissac@gmail.com

***Abstract*: Intrusion Detection Systems (IDS) are one of the primary components in keeping a network secure. They are classified into different forms based on the nature of their functionality such as Host based IDS, Network based IDS and Anomaly based IDS. However, Literature survey portrays different evasion techniques of IDS. Thus it is always important to study the responsive behavior of IDS after such failures. The state of the art shows that much work have been done on IDS on contrary to little on Intrusion Response System (IRS). In this paper we propose a model of IRS based on the inspiration derived from the functioning of defense and response mechanism in plants. The proposed model is the first attempt of its kind with the objective to develop an efficient response mechanism in a network subsequent to the failure of IDS, adopting plants as a source of inspiration.**

Keywords: Intrusion Detection System, Intrusion Response System, Bio-inspired, nature, biologically inspired, Learning, KDD99, Anomaly Detection, Host Intrusion System , Network Security, bot nets , bot, SAR, plants defense.

I. Introduction

Biological Thinking has been a source of inspiration to engineers and researchers across the globe to explore possible solutions to the complex problems. In computer network biological inspirations have been used to design strategies both for attack and defense[27,28]. Human Immune System(HIS)/Artificial Immune System(AIS) has been extensively used as inspiration by researchers to model a robust intrusion detection system because of high level of protection exhibited even to most of the unseen pathogens. Arisytis is an example of Artificial Immune System Toolkits [1]. Current AIS research includes Negative Selection, clonal selection and immune network theory as the most popular underlying theories. The defense life cycle can be demonstrated as follows. Prevention phase consists of training phase whereupon a classifier is built using machine learning algorithm such as ANN(Artificial Neural Network), Bayesian Network , decision trees etc. Network traffic are then monitored for probable anomaly . If any traffic successfully by pass the preventive rules , there presence are detected on the network by different host based and network based intrusion detection techniques. The last phase mitigation complements the entire life cycle by responding to already performed attacks on the network , such as triggering a response mechanism to slow down or eradicate the malicious activity from further proliferation in the network [2]. However, much research have been done on IDS(Intrusion Detection System) in comparison to limited work on Intrusion response systems owing to the complexity of developing and developing an automated response.

Prevention ---> Monitoring ---> Detection ---> Mitigation

Figure 1. Defense Life Cycle

Till today much of the existing IDS have the response in form of an alert generated to bring into notice the administrator of certain activity otherwise restricted in the network. A generic taxonomy of intrusion response system is presented by stakhonova.et.al [3]. The authors have broadly classified the intrusion response system into two types , by (a) degree of automation and by (b) activity of triggered response. (a) is further classified into -Notification systems , Manual Response systems and Automatic Response systems . (b) is classified into -passive response and active response. Automatic Response systems again classified as per -ability to adjust(static, adaptive),by time of response(proactive , delayed),by cooperation ability(autonomous,cooperative),by response selection method(static, dynamic,cost-sensitive map-ping). Malware programs such as worms, virus, bots etc. can cause considerable impact on a network rendering the network vulnerable. In most cases a particular host is compromised and a zombie is created on the network. Computer worms are programs that self propagate in a network exploiting vulnerabilities with limited or no human intervention whereas, virus are programs that need human intervention to abet their propagation. The mode of propagation of worms sometimes can render the detection mechanisms impossible. The contagion strategy is an example of passive worm that uses embedded propagation. In such cases the worm appends or replaces a normal message. Today one of the biggest concerns in security is the rising bots and bot-net in networks. Bots are computer programs designed to perform predefined functions remotely, automatically and repeatedly once they are initiated by a victim's system or by an end user of the network [4]. In this paper we propose a bio-inspired method of detection and response to intrusion in a Network. The portrayed model is designed taking inspiration from the defense model in plants. The outline of the paper is as follows. Section II gives an overview of the defense and response mechanism in plants and an insight into the proposed bio-inspired model . Section III discuss the pylogenetic tree generation for signature set and Section iV discuss the mathematical foundations underlying the response time in plants and infection time by a malicious program in a Network. Section V marks the conclusion of the paper.

II. OVERVIEW OF DEFENSE AND RESPONSE MECHANISM IN PLANTS

Plants are constantly exposed to various pathogens all the time. However, the strong defense mechanisms that plants constantly expose against these pathogens have been significant in keeping plants alive. The immune system in plants can be broadly classified into two types; one uses trans membrane pattern recognition receptors (PRR). PRR responds to microbial or pathogen-associated molecular patterns (MAMPs or PAMPS) such as flagellin. The second acts inside the cell using the polymorphic NB-LRR protein products encoded by most R-genes [5]. The first layer of defense plants exhibits is the plasma membrane. Microbes must first breach this cell wall in order to intrude inside host cell. The plasma membrane of plants has undergone a regular evolution both in mechanical properties and receptors capable of sensing cellular damage. Such breaches of cell wall should alarm the host about possible invasions. Pathogens which overcome these defensive layers are counterfeited by two response mechanisms in plants, namely; microbial-associated molecular patterns (MAMP/PAMP) trig-gered immunity (MTI/PTI) and effector-triggered immunity (ETI). Whenever PAMPSs (or MAMPs) are recognized by PRR, results in PAMP-triggered immunity (PTI). However, successful pathogens that could breach PTI deploy huge number of effectors to render pathogen virulence. Such effectors change the usual functionality of PTI resulting in effector-triggered susceptibility (ETS) [7]–[9].

A given effector is recognized by plants specifically by one of the NB-LRR proteins , resulting in effector-triggered immunity(ETI) [5]. The consequence of ETI sometimes is also in form of hypersensitive response resulting in programmed cell death (PCD) of the infected cells and production of antimicrobial molecules such as - 1,3-glucanase in the surrounding tissues resulting in local resistance. Early MAMP response triggers ROS, NO ,ethylene and a later deposition of callose and synthesis of antimicrobial components. Modification of self proteins of plants by the effectors triggers activation of R proteins in plants. Most commonly R protein RPM1 or RPS2 guards RIN4(RPM1-INTERACTING PROTEIN 4).

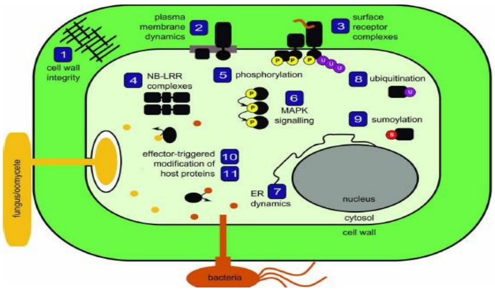


Figure 2. Mechanisms regulating immunity in plants [6]

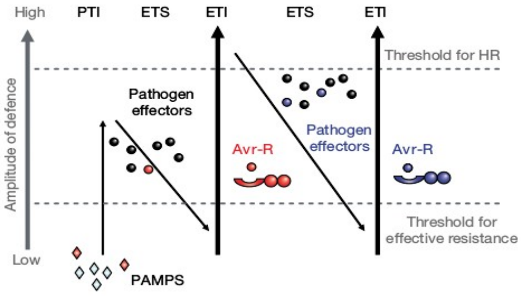


Figure 3. A zig-zag model illustrates the quantitative output of the plant immune system [5]

RIN4 are targeted and modified by three distinct pathogen effectors from P.syringae(AvrRpm1, AvrB and AvrRpt2). RIPK(RPM1-INDUCED PROTEIN KI-NASE) , was shown to phosphorylate RIN4 in response to pathogen effectors AvrRpm1 and AvrB. Phosphorylation of RIN4 is important for activation of R proteins. Such activity of pathogens in fact has portrayed the substantial decrease in pattern triggered immunity (PTI). The regulation of stomata after interaction of RIN4 with plasma membrane-associated H+-ATPases is also discovered , which are primary site of pathogen entry. Pathogenic bacteria swim towards open stomata. To prevent such activity stomata close to Pst and to Escherichia coli [10]. Literature study indicates that plant immune system uses R proteins to monitor effector-triggered modification of self-molecules , rather than to monitor presence of non-self molecules. The mobile signal generated in the infected tissues should travel to distal parts carrying vital information about the primary pathogen infection. The onset of SAR(Systemic Acquired Resistance)[Fig 4] is accompanied by increased accumulation of the signaling hormone salicylic acid in the phloem. Salicylic acid methyltransferase activity , which converts salicylic acid into methylsalicylic acid(MeSA) is required in the tissue that generates the immune signal. Conversely , MeSA esterase activity , which converts MeSA back into salicylic acid, is required for signal perception in systemic tissues. Experiments also demonstrates that defective in induced resistance 1-1(dir1-1) gene transports a lipid-based immune signal to systemic tissues. Organophosphate compound glycerol-3-phosphate(G3P) is a signal generated in the infection site and transmitted to distal tissues to induce systemic immunity. Likewise Azelaic acid induced 1(AZI1) is also involved in production and /or translocation of a mobile immune signal [11], [12]. Indirect recognition of effectors indicates that some R-proteins might not directly bind avirulence effectors but monitor host targets and observe their perturbation[Fig 5]. This phenomenon is described as the guard hypothesis. Loss or perturbation of the guardee by effectors leads to R-protein dependent HR based resistance. Flg22 recognition leads to several plant defense reactions , such as production of reaction oxygen species(ROS), activation of mitogen-activated protein kinases(MAPK), ethylene production , callose deposition at the cell wall and expression of defense related genes leading to enhanced immunity as well as growth arrest [8]. Recent Studies [9] indicate that at least some NB-LRR proteins enter nucleus to activate defenses, probably as a consequence of effector recognition. Most NB-LRR proteins detect effector proteins indirectly by associating with host proteins that are targeted by effectors. AvrRpm1 and AvrB trigger RPM1 resistance probably by inducing the phosphorylation of RIN4. The p. syringae effector HopAO1 modifies host chloroplast , suppress the production of defense hormone salicylic acid etc. Taken together , pathogenic bacteria use effectors to modulate diverse host response to their advantage. AvrPto directly interacts with several receptor kinases , including FLS2 and EFR in Arabidopsis and LeFLS2 in tomato plants to block PAMP/MAMP induced defenses and enhances bacterial virulence [13], [14].

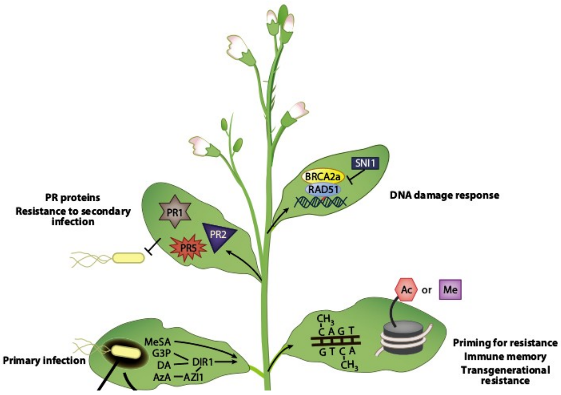


Fig 4: Mechanism of Systemic Acquired Resistance in Plants.

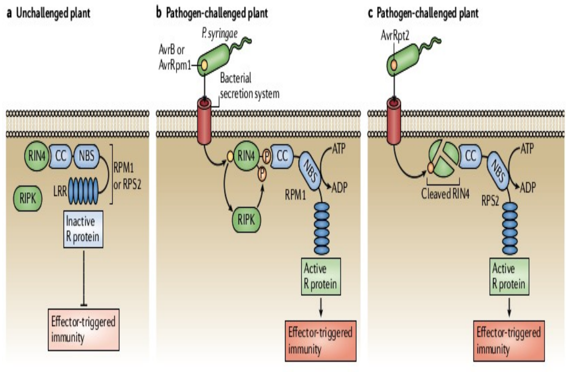


Figure 5. The guard model, surveillance of the host immune regulator by RIN4 by the R proteins RPM1 and RPS2.

I. PIRIDS(PLANT BASED INSPIRATION OF RESPONSE IN INTRUSION DETECTION SYSTEM)

Section II outlines in brief the mechanism in plants as response to pathogen attacks. In this section we try to derive an analogy between response mechanism in plants and a similar derived automatic response mechanism in a computer network whenever an end system in the trusted network is target for compromise. Fig 6 shows the architecture of an extended bus topology. Each end system in the topology behaves like a leaf in a plant. Figure 4 shows the sequence of events in SAR.

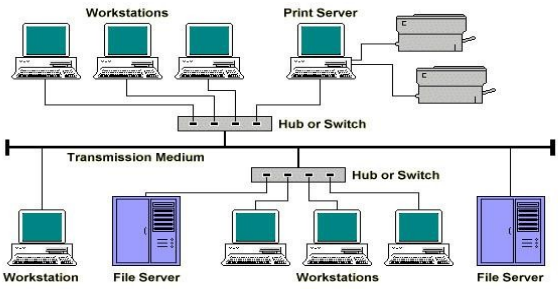


Figure 6. Structural similarity between an extended bus topology and plant

The “nodes” in our terminology are the systems repository of different information and services. Nodes implementing signature based intrusion detection might subject to failure to previously unseen signature [15].Such system is proved to fail detection against traffic framed intelligently simulating behavior similar like camouflage [15] in plants. Malicious programs breaching such security measures might succeed in creating havoc in the network. We therefore ,propose a multi-layered defense mechanisms based on the inspiration derived from plants. The structure of the proposed model can be described by the diagram below.

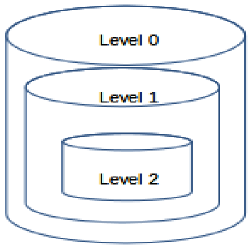


Figure7: Three level defense mechanism of a node

In the proposed model each node have three layers of defense. Level 0, level 1 and level 2 respectively. Level 0 Defense behaves similar like the PRR(Pattern Recognition Receptors) in plants and is the outermost level of defense. It is the most generic defense response mechanism of the model. There will be different receptor agents active on a given node repository. These receptor agents behaves like the PRR in plants. Different malicious programs might intend to harm a given node in a network. The functioning of receptor agents in analogy to plant PRR is shown below. In figure 8 it is shown that in the absence of pathogen , XA21 forms complex with XB24. But in presence of pathogen AxY^{5}22 induces dissociation of XA21 from XB24 and activates XA21, triggering auto phosphorylation which subsequently triggers downstream MAPK cascade. Figure 9 below shows the working principle of receptor agents running in a system. The different receptor agents are marked as RA1, RA2...etc. Different receptor agents have the responsibility of detecting different generic intrusion attempts into the node of the network. For example in the above figure , RA1 corresponds to the detector set against incoming connections. The detector set will be generated by the following mechanism.

◆ False services which are not actively required will be hosted such as to attract malicious bots and attackers. The connection details corresponding to those services will be recorded.

Source Address	**Destination Port**	**False Service**	**Future Status**
202.40.5.1	20/21	yes	Blocked
14.5.4.2	25	yes	Blocked

Figure 10: A Typical Detector set[Receptor Agent 1:RA1]

The above approach would avoid the application payload signature matching from those connections otherwise. In future when an extracted address from the incoming packets match the detector set , that particular connections will be no longer entertained.

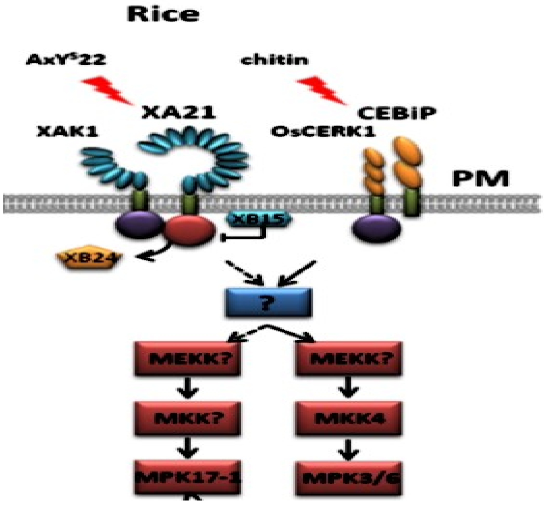


Figure 8. Pathogen mediated phosphorylation of PRR in plants

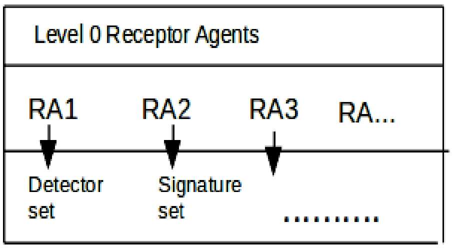


Figure 9: Block representation of Receptor Agents on a node

◆ RA2 might correspond to HTTP SQL injection set of attacks. The URL(Uniform Resource Locator) corresponding to any HTTP Post/Get request would be parsed for possible SQL Injection attempt comparing it against a stored sql injection database . If the HTTP request signature match any in the database the corresponding address against the connection is retrieved and stored in the detector set of RA1. It is noteworthy that any request coming from a node that match an entry in the detector set is thereby immediately rejected and no further application layer parsing takes place.

◆ Other receptor agents such as RA3,RA4...etc would be discovered in the course of further study. As for example RA3 could correspond to the signature set of MACRO virus , which often is being carried across email attachments.

◆ Once a particular Receptor Agent is activated as a result of intrusion attempt, the corresponding set against the Receptor Agent is distributed across different nodes.
In the following diagram on activation of RA1, the detector set is distributed across the File Servers.

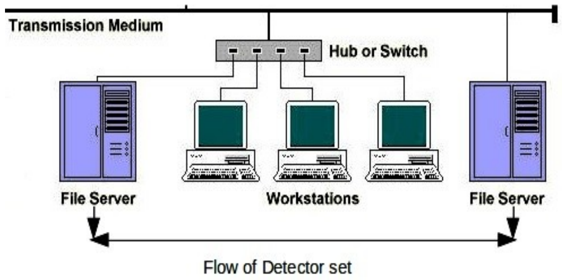


Figure 11: Demonstrates the flow of database set against a RA from one node to another

◆ Different Mobile Agents [MA] are activated for accomplishing different roles in the network. Three categories of MA are triggered for defense signaling in the network. The D-agent, A-agent and SM-agent. The D-agent in analogy to DIR1 in plants would trigger local response. The D-agent would update the signature database corresponding to a receptor agent [RA] with the new signature vector generated by the A-agent. On a remote system as well the D-agent on receiving immune signaling would update the receptor database, such that on secondary intrusion attempt, a high and quick response could be triggered. The A-agent in analogy to AZI1 in plants, would generate the signature of the foreign program using evolutionary method. The SM-agent in analogy to the defense signaling (SA-> Mesa)in plants ,would encrypt the signature generated by the A-agent using light symmetric key and than distributes it to other nodes on the network. Apart from the above mentioned three agents , another agent the S-agent in analogy to Salicylic Acid in plants will also have role in defense signaling. Every time a guard agent is activated, results in activation of the S-agent. Greater accumulation of S-agent exceeding thresholds would result in the Hypersensitive response of the node in the network.

Level 1 Defense :- The Guard Model

The Guard model is inspiration drawn from the guard model in plants. If Level 0 defense fails to recognize any critical intrusion attempts or attacks, Level 1 defense should come to rescue before the network of the organization collapse. Every critical program in the system will be guarded by a Guard Agent.

Permitted Address	**Permissions**
210.4.5.1	Read, Write, Execute
45.6.2.1	Read, Write
Others	Read

Figure 12: Reference Table

Whenever an external program from a remote user tries to interact with a critical program being guarded, the guard agent looks into the Reference Table and performs the following actions.

◆ The reference table stores address of those systems which are permitted to do manipulation of the resources on the server. All other addresses only might have READ accessibility. If an unknown remote program succeeds to fail Level 0 defense and interacts with a critical program of the system , then this particular connection will be immediately picked up the Guard Agents.

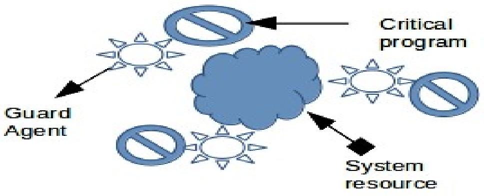


Figure 13: Guard Model as second layer of defense in Node.

◆ Guard Agents will match the connection details with the Reference Table. If the entry is not found in the reference table, immediately the remote program is blocked from further infection of the critical program and triggers the next action.

◆ If Guard Agents fails to find a match in the Reference Table, it activates A-agent provided the foreign program interacting with the critical program/resource is residing on the server itself as that of the critical resource.

◆ The A-agent is a special program who is responsible of finding the foreign program interacting with the critical program/resource. Once identified the A-agent will send the interacting program to Quarantine. The signature of the foreign program would be generated and hand it over to the SM-Agent. SM-Agent is responsible to carry it across the network and hand it over to the D-Agent Receptors of the various servers. The D-Agent would then accordingly update the RA Database of the node.

◆ If Guard Agents finds that the foreign program interacting with the critical resource is from a remote machine , then subsequent activation of A-agent would mean generating the detector element corresponding to that particular connection.

◆ With every trigger of a Guard Agent a S-agent counter would be increased. If on a particular system the threshold level of the S-agent exceeds , the third level of defense which is in analogy to HR(Hyper Sensitive) in plants, would be triggered.

Level 2 Defense : The Hyper Response

Level 3 defense is the extreme response of the system. The analogy is like that of HR(Hyper Sensitive Response) in plants. The Threshold value met by the S-Agent indicates changes in high number of critical resources guarded. The activation of this level will trigger the following response

◆ Initiate a cooling time. Cooling time is an approximate time for which the system is going off from the network.

◆ Broadcast the status of the critical resources being infected. This broadcast message is intended for other servers in the network to find a possible duplicate copy.

◆ Trigger self destructive programs which shuts the system off the network such that further propagation of malicious programs is restricted in the network from the infected system.

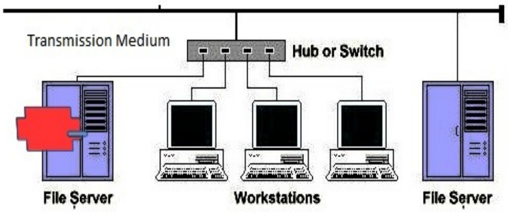
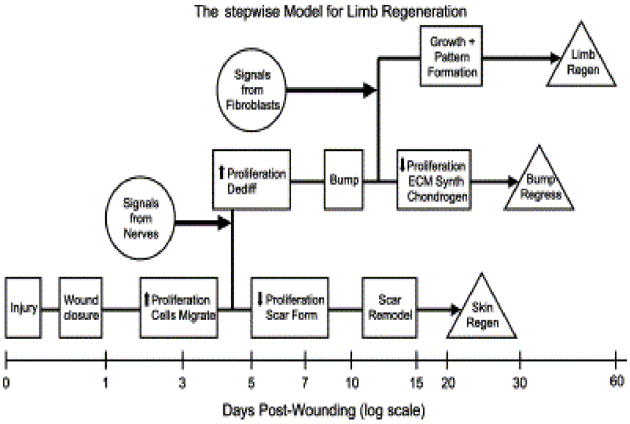


Figure 14: The File Server on the Left is temporarily shutdown from the network. Consequence of HR Response

◆ Once the cooling time is out , the system waits for its recovery by behavior of collaborative effort from the neighbors. The infected program will be deleted and the new one's received automatically from the neighbors will be re-installed. Collaborative effort from neighbors is designed based on the inspiration of self regeneration on salamanders.



The detail of the model is not discussed in this paper. However, the steps of regeneration in salamanders is shown below.

Figure 15: Stepwise model for limb regeneration[24]

In the above figure the points of divergence of three pathways which are wound healing , bump formation and limb formation are represented by vertical lines. Fig 16 represents the full diagrammatic flow of the entire model.

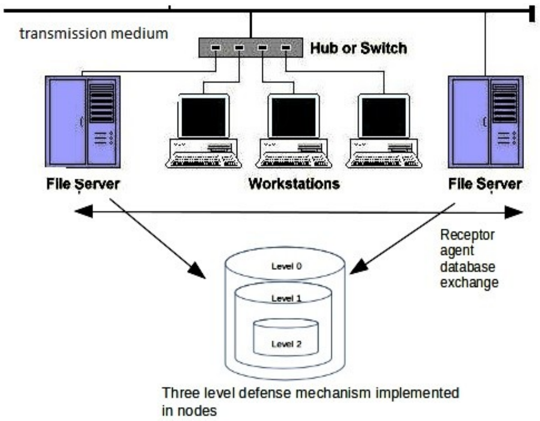


Figure 16: Diagrammatic flow of the model.

Phylogenetic Tree Construction from the signature set to identify candidates for evolution of new signatures:-

Phylogeny is the evolution of a genetically related group of organisms[25,26]. Phylogenetic tree represents the evolutionary relationship between organisms, species or genomic sequence. The most closely related sequence are grouped nearby followed by grouping of more distantly related ones.

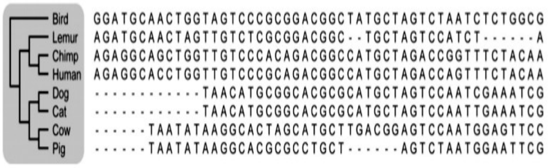

Bird GGATGCAACTGGTAGTCCCGCGGACGGCTATGCTAGTCTAATCTCTGGCG
Lemur AGATGCAACTAGTTGTCTCGCGGACGGC--TGCTAGTCCATCT------A
Chimp AGAGGCAGCTGGTTGTCCCACAGACGGCCATGCTAGACCGGTTTCTACAA
Human AGAGGCACCTGGTTGTCCCGCAGACGGCCATGCTAGACCAGTTTCTACAA
Dog ------------TAACATGCGGCACGCGCATGCTAGTCCAATCGAAATCG
Cat ------------TAACATGCGGCACGCGCATGCTAGTCCAATTGAAATCG
Cow ------TAATATAAGGCACTAGCATGCTTGACGGAGTCCAATGGAGTTCC
Pig ------TAATATAAGGCACGCGCCTGCT------AGTCTAATGGAATTCG

Figure 17: Phylogenetic Tree generation corresponding to the sequences.

The above diagram shows the phylogenetic tree corresponding to the amino-acid sequence. The amino-acid sequence can be thought of as a similar analogy to signature set of virus and worms.

A typical signature of Klez.E worm looks like below in hexadecimal format.

Worm/Klez.E=33be732d4000bd08104000e89eeaffff80bd08104000be7d2d4000e849eaffff6a00e83500000064756d6d792e65786500653a5c77696e646f77735c53795374656d33325c644c6c63616368655c6464642e65786500ff254c404000ff25544040

Algorithmic Representation of the Phylogenetic Tree Generation for the signature set of virus/worms from the signature database.

Step 1: Normalize the length of each signature equal to the longest signature in the database say 'L'

Step 2: Concatenate with special padding character '-' to each signature whose size is less than the 'L'.

Step 3:Prepare a Distance Matrix such that the size of the matrix is 'n x n' , where 'n' is the number of signature in the database.

Step4:The value of the Distance is equal to number of exact matches divided by the sequence length ignoring gaps.

Step5:Repeat Steps 6 and 7 until there are only two clusters.

Step6: Cluster a pair of leaves by shortest distance

Step7: Recalculate a new average distance with the new cluster and other 'signature/cluster' and make a new distance matrix.

A Typical Phylogenetic tree for signature 'A','B','C','D', & 'E' might look as below

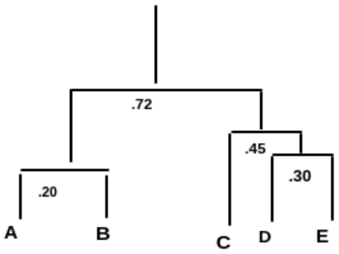


Figure18: Phylogenetic Tree for Signature A,B,C,D & E

The above Phylogenetic Tree demonstrates that signature 'A' and 'B' are literally derived from a common ancestor and have much more resemblance amongst themselves than compared to 'C' ,'D' and 'E'. The right subtree can be candidate of evolution for further generation of new signature as possible detectors for future unseen attacks.

III. Mathematical Model and analogy of Plant response time to infection and Malicious Program spread in a Network

The transition from one system to another with with u(t) as control variable and x(t) as state variable can be defined as [18]

$dx/dt = f(t, x(t), u(t)), 0 \leq t \leq T$, (1) , with initial condition $x(0) = x_1$ where ,f(x,t,u) is the state function and T is the terminal time (assuming T is finite). Then there is an objective functional

$J(u)=\ln(g(t,x(t),u(t))dt$,where $g(x,t,u)$ is a given continuously differentiable function and x(t)follows as a reponse to u(t). The fundamental problem is to determine u(t) that maximizes J(u). Precise choice of u(t) will give very good control to stop spread infection from one system to another in the network. Under environmental conditions susceptible plants(S) might turn diseased (D), upon subjected to pathogen or are able to withstand the infection (R) via host defense mechanism. In such cases the sum total of the probability distribution is

$S + R + D =1$

Likewise if systems susceptible to attack in a network is (S’) from which (D’) systems are infected in a network and (R’) systems could withstand the attack then the above equation can be modified into

$S^{'} + R^{'} + D^{'} =1$

Giuseppe et.al [19] have derived the equation for the n of machines that will be

compromised in the interval of time dt(’a’ being constant) as $n = (N a).K(1 - a)dt$

where K=average initial compromise rate i.e the number of vulnerable hosts that an infected host can compromise per unit time at the beginning of the outbreak. a(t)= is the proportion of vulnerable machines which have been compromised at the instant t. N.a(t)= is the number of infected hosts, each of which scans other vulnerable machines at a rate K per unit time. But since a portion of a(t) of the vulnerable machines is already infected , only K.(1-a(t)) new infections will be generated by each infected host, per unit of time. If 'N' is constant in a network,

$N\,da = (N\,a).K(1 - a)dt$

thus, $da/dt = Ka(1 - a)$or

$a = e^{k}(t - T)/1 + e^{k}(t - T)$, where the above equation is a form of logistic curve and T is a time parameter representing the point of maximum increase in the growth. The guard agents used in level 1 defence can be a set of detectors.The overview of detectors as from [23] is a string that do not have any match with any of the protected data. The protected data with progress of time are monitored by detectors. If ever a change is known to occur the corresponding detector is activated. The change could be modification of the existing file , append of new contents to the existing file or deletion of contents or change in the permission rights of the file considered protected. However , it is important in such perspective that protected strings do not change frequently over time and are nearly stable strings(we do not often change the statements of a program frequently). Forrest et.al [23] have stated that the probability P M that two random strings match at least r contiguous locations if :m= the number of alphabet symbols. l= the number of symbols in a string (length of the string) r= the number of contiguous matches required for a match.

$$P_M = m^{r}\,[(l - r)(m - 1)/m + 1]$$

IV. CONCLUSION

The paper portrays a defense model based on the inspiration of the defense and signaling mechanism in plants. The implementation of the above model and the analysis of experimental results is undertaken and will be discussed in the near future. However, challenges such as effective receptor database set generation , proper signal transmission with memory from the infected node to other nodes, nature of cooling time and collaborative effort by the neighbors for self healing of the network will be considered in more depth. The proposed model designed from plants as source of inspiration could prove beneficial for implementing an effective intrusion detection and response mechanism capable of withstanding both known and unseen attacks.

References

[1] W. Ma, D. Tran, and D. Sharma, "Negative selection with antigen feedback in intrusion detection," in Artificial Immune Systems. Springer, 2008, pp. 200–209.

[2] A. Shameli-Sendi, M. Cheriet, and A. Hamou-Lhadj, "Taxonomy of intrusion risk assessment and response system," Computers & Security, vol. 45, pp. 1–16, 2014.[3] N. Stakhanova, S. Basu, and J. Wong, "A taxonomy of intrusion response systems," International Journal of Information and Computer Security, vol. 1, no. 1, pp. 169–184, 2007.

[4] N. Weaver, V. Paxson, S. Staniford, and R. Cunningham, "A taxonomy of computer worms," in Proceedings of the 2003 ACM workshop on Rapid malcode. ACM, 2003, pp. 11–18.

[5] J. D. Jones and J. L. Dangl, "The plant immune system," Nature, vol. 444, no. 7117, pp. 323–329, 2006.

[6] A. M. Jones, J. Monaghan, and V. Ntoukakis, "Editorial: Mechanisms regulating immunity in plants," Frontiers in plant science, vol. 4, 2013.

[7] V. Nicaise, M. Roux, and C. Zipfel, "Recent advances in pamp-triggered immunity against bacteria: pattern recognition receptors watch over and raise the alarm," Plant Physiology, vol. 150, no. 4, pp. 1638–1647, 2009.

[8] C. Zipfel, "Pattern-recognition receptors in plant innate immunity," Current opinion in immunology, vol. 20, no. 1, pp. 10–16, 2008.

[9] J.-M. Zhou and J. Chai, "Plant pathogenic bacterial type iii effectors subdue host responses," Current opinion in microbiology, vol. 11, no. 2, pp. 179–185, 2008.

[10] M. Melotto, W. Underwood, J. Koczan, K. Nomura, and S. Y. He, "Plant stomata function in innate immunity against bacterial invasion," Cell, vol. 126, no. 5, pp. 969–980, 2006.

[11] S. H. Spoel and X. Dong, "How do plants achieve immunity? Defence without specialized immune cells," Nature Reviews Immunology, vol. 12, no. 2, pp. 89–100, 2012.

[12] A. C. Vlot, D. F. Klessig, and S.-W. Park, "Systemic acquired resistance: the elusive signal (s)," Current opinion in plant biology, vol. 11, no. 4, pp. 436–442, 2008.

[13] S. T. Chisholm, G. Coaker, B. Day, and B. J. Staskawicz, "Host-microbe interactions: shaping the evolution of the plant immune response," Cell, vol. 124, no. 4, pp. 803–814, 2006.

[14] M. Muthamilarasan and M. Prasad, "Plant innate immunity: an updated insight into defense mechanism," Journal of biosciences, vol. 38, no. 2, pp. 433–449, 2013.

[15] P. De Boer and M. Pels, "Host-based intrusion detection systems," Amsterdam University, 2005.

[16] R. S. Boyer and J. S. Moore, "A fast string searching algorithm," Communications of the ACM, vol. 20, no. 10, pp. 762–772, 1977.

[17] M. I. Sharif, A. Lanzi, J. T. Giffin, and W. Lee, "Impeding malware analysis using conditional code obfuscation." in NDSS, 2008.

[18] A. Latif and N. Syaza, "Mathematical modelling of induced resistance to plant disease: a thesis presented in partial fulfilment of the requirements for the degree of doctor of philosophy in mathematics at massey university, albany campus, new zealand," Ph.D. dissertation, The author, 2014.

[19] G. Serazzi and S. Zanero, "Computer virus propagation models," in Performance Tools and Applications to Networked Systems. Springer, 2004, pp. 26–50.

[20] M. Khan, "A computer virus propagation model using delay differential equations with probabilistic contagion and immunity," arXiv preprint arXiv:1410.5718, 2014.

[21] B. K. Mishra and A. Prajapati, "Mathematical model on attack by mali- cious objects leading to cyber war," International Journal of Nonlinear Science, vol. 17, no. 2, 2014.

[22] "Cyber warfare: Worms transmission model," International Jour- nal of Advanced Science & Technology, vol. 63, 2014.

[23] S. Forrest, A. S. Perelson, L. Allen, and R. Cherukuri, "Self-nonself discrimination in a computer," in 2012 IEEE Symposium on Security and Privacy. IEEE Computer Society, 1994, pp. 202–202.

[24] Endo, Tetsuya, Susan V. Bryant, and David M. Gardiner. "A stepwise model system for limb regeneration." *Developmental biology* 270.1 (2004): 135-145.

[25] Schreiber, Fabian. "Phylogenetic Sequence Analysis."

[26] Satbhai, Santosh B., et al. "Pseudo-response regulator (PRR) homologues of the moss Physcomitrella patens: insights into the evolution of the PRR family in land plants." *DNA research* 18.1 (2011): 39-52.

[27]Sharma, Rupam Kumar, Hemanta Kr Kalita, and Biju Issac. "PIRIDS: A Model on Intrusion Response System Based on Biologically Inspired Response Mechanism in Plants." *Innovations in Bio-Inspired Computing and Applications*. Springer International Publishing, 2016. 105-116.

[28]Hamamoto, Anderson H., Luiz F. Carvalho, and M. L. Proenca. "ACO and GA metaheuristics for anomaly detection." *2015 34th International Conference of the Chilean Computer Science Society (SCCC)*. IEEE, 2015.

Author Biographies

Rupam Kumar Sharma The author is from Assam , India. The author has completed his MCA(Master of Computer Applications) in the year 2010 from NEHU , India and per suing his Doctoral research in the same university in the discipline of Bio-inspired Computation and Network Security. He is currently working as an Assistant Professor in the Dept. of CSE & IT in Assam Don Bosco University. He has a total of 5 years of academic and research experience and has published a number of papers in international conferences .

Hemanta Kumar Kalita The author is from Assam, India and presently working as an Associate Professor in the Dept. of IT in NEHU. He has completed his PhD from Jadavpur University, India. He has around 11 years of Teaching Experience and 6 years of R&D experience in industry. He also has a patent to his credit with application number Application Number: PCT/IB2010/002118. His research interest includes Big Data Analysis and Network Security. He has published several research papers in International Conference and Journals.

Biju Issac The author is from India and presently working as Senior Lecturer in Computing , School of Computing , Teesside University, UK. He has Bachelor of Engineering in Electronics and Communication Engineering (ECE),after which he completed Master of Computer Applications (MCA) with honours. He earned his PhD in Networking and Mobile Communications, by research and the thesis was 'Predictive Mobility Management using Optimized Delays and Security Enhancements in IEEE 802.11 Infrastructure Networks". His research interest includes Computer Network , Wireless Network , Ubiquitous Computing.