[*Gautam *, Vol.5 (Iss.2: SE): February, 2018*] ISSN: 2454-1907
[*Communication, Integrated Networks & Signal Processing-CINSP 2018*] DOI: 10.29121/ijetmr.v5.i2.2018.617

IJETMR

International Journal of Engineering Technologies and Management Research
A Knowledge Repository

SECURING MOBILE ADHOC NETWORKS AND CLOUD ENVIRONMENT

Divya Gautam [*1]
[*1] Amity University, Gwalior, India

Abstract:
Securing mobile adhoc networks and cloud environment in opposition to denial of service attack by examine and predict the network traffic. DDoS attacks are most important threats next to the accessibility of cloud services. Prevention mechanisms to protect next to DDoS attacks are not forever efficient on their own. Unite dissimilar method (load balancing, throttling and Honey pots) to build hybrid defense method, in meticulous with dissimilar cloud computing layers, is extremely recommended. In this paper, a variety of DDoS attacks have been presented. We as well highlighted the defense methods to counter attack dissimilar types DDoS attacks in the cloud environment. This paper proposes SVM-based algorithm to anomaly intrusion detection. A multiclass SVM algorithm with parameter optimized by PSO (MSVM-PSO) is accessible to find out a classifier to detect multiclass attacks. This paper will extend the proposed techniques to new computing environments Mobile Ad-Hoc Networks to detect anomalous physical or virtual nodes.

Keywords: *Securing Mobile; Network; Cloud Environment.*

Cite This Article: Adekanmbi .M, Abumere.E.O, and Amusan J.A. (2018). "GENERATION OF LIGHT THROUGH PLASMA USING RADIO FREQUENCY SOURCE IN DISUSED FLUORESCENT TUBE." *International Journal of Engineering Technologies and Management Research*, 5(2:SE), 1-8. DOI: https://doi.org/10.29121/ijetmr.v5.i2.2018.617.

1. Introduction

Mobile Ad-Hoc Networks is a group of wireless nodes that can dynamically form a network to exchange information without using fixed network infrastructure. As we know that setup a new network is a costly and non-convenient task. Here Mobile Ad-Hoc Networks comes into the picture; it has capability to be setup easily and not too expensive. A network also requires costly and complex component while being established. Mobile ad-hoc network can be setup using any node supporting basic wireless facility. Since this network is easy to be setup and does not require any specific support so it is very popular among users. Nodes require to forward data among each other by using routing protocol. These protocols are designed to select best path to provide transmission. Nodes in mobile ad-hoc network are required to select trusted node from their neighbor. In this approach we have describe an approach to find the trusted nodes into Mobile Ad-Hoc Networks and select the path from these trusted node to provide better trusted path. We have developed a mechanism to monitor the behavior of their neighbors and exchange information about other nodes. Our system is able to select the optimized route to reduce the

network performance's degradation challenge. The proposed system selects the best routing protocol using an intelligence support vector classification feedback mechanism according to the networking requirement. We have given tested set to our classifier to judge the nodes behavior and find the trusted node in selection of path. We have performed simulation and compare our approach to other exiting protocol and it is proved that our approach is improving the network performance. To propose a new detection method based on Particle Swarm Optimization (PSO) - Support Vector Machine (SVM) for distributed denial of service attack on mobile adhoc networks and cloud environment.

We make the following assumptions for the proper operation of the proposed architecture:

1) Each mobile node in the network has a unique ID and can join or leave the network freely.
2) Each packet is of equal size, although packet may vary in size according to their contained data. Packet sending rates are also constant.
3) Initially, all nodes have equal computational and storage capability, although a node may have more resources than others during the communication process.

2. Related Work

Intrusion detection systems (IDS) defend computer networks from illegal users, counting possibly insiders. The intrusion detector (i.e a classifier) learns to construct a extrapolative replica which is accomplished of distinguishing among bad acquaintances (called intrusions or attacks) and good standard connections. IDS can be realized by misuse base or anomaly-based intrusion detection approach. By with Bayesian networks, [3] implements a misuse-based IDS, Basset (Bayesian System for Intrusion Detection), which is comprehensive from Snort. The definitive purpose of Basset is to give enhanced detection ability and less possibility of false alarms during assess Snort alerts by Bayesian networks. Though, the natural limitations of Bayesian networks and misuse-based approach create Basset hard to detect novel attacks, i.e., the miss rate are comparative high. study anomaly-based IDS. They complicated the basics of usually adopt irregularity intrusion detection techniques next to with their prepared architectures. They as well categorize these approach based on the type of dispensation that is associated to the behavioral model for the intention systems. Propose a narrative hybrid intrusion detection model, i.e., equivalent misuse and irregularity detection. The earlier approve C4.5 based binary decision trees, and the concluding adopts CBA (Classification Based Association) based classifier. The model's performance is assess on KDD Cup 99 benchmark. Though, the comparable nature of the proposed replica makes it hard to be deploy upon network systems. Intrusion detection and equivalent method are forever incessantly disturbed issues in literature; despite that new compute paradigms e.g., cloud computing have emerge. Survey dissimilar intrusions disturbing accessibility, discretion and honesty of Cloud resources and services. They inspect Intrusion Detection Systems (IDS) and Intrusion avoidance Systems in Cloud, and suggest equivalent proposals. Survey intrusion discovery research for Cyber Physical Systems. Pervasive healthcare scheme, smart grids. They categorize current CPS Intrusion Detection System (IDS) method based on two intend dimensions: discovery technique and audit substance.

3. Comparative Study

S No.	Author	Year	Strength	Weakness
1	Markku Antikainen, Tuomas Aura, and Mikko Särelä	[2014]	present DoS attacks against broad classes of Bloom-filter-based protocols and conclude that the protocols are not ready for deployment on open networks	The protocol variants that do not implement these security mechanisms suffer from distributed DoS vulnerabilities comparable to the current Internet.
2	Andreas Papalambrou in at al[2014]	2014	novel SHIELD secure architecture being developed, which aims at providing interoperability with other secure components as well as metrics to quantify their security Properties..	it is expected that accuracy can be further increased by field trials in real-world scenarios.
3	RajyaLakshmi G.V 1, Anusha [2013]	2013	propose effective anomaly based model analyzed by extracting more network features from the MANET and used fuzzy logic for classify the network traffic that is attack traffic or legitimate traffic.	compare many machine learning based algorithm with this and propose best classification algorithm
4	Adnan Nadeem Michael Howarth	2009	reduced overhead and increased throughput. algorithm performs well at an affordable processing overhead over the range of scenarios tested.	AIDP exhibits a high success rate and very low false alarm , isolate the nodes from the network to prevent intrusion.
5	Imad Aad, Jean-Pierre Hubaux, *Senior Member, IEEE*, and Edward W. Knightly, *Senior Member, IEEE*	2008	study the key performance factors for attack scalability of DoS attacks in ad hoc networks.	overhead of deploying a counter-strategy is merited given the damage that an attack can inflict
6	Mohamed Nidhal MEJRI , Jalel BEN-OTHMAN	September 21–26, 2014,	Proposed system intend to be used for simulation is collected of several nodes (vehicles) which	expecting validate the eefficiency of our dened metric for other DOS attack such as jamming.

			Form a WIBSS (Wave Independent Basic Service Set).	be expecting as well the design of a narrative reaction technique against these attacks.
7	Rodrigo do Carmo, Marc Werner, and Matthias Hollick	October 24–25, 2012	metric is lightweight yet effective for anomaly detection in both stationary and mobile wireless multihop networks	the difference rate of neighbor nodes can help us classify anomalies somewhat then depending on the complete number of nodes at present within transmission range
8	Wenjia Li, Tim Finin	2011	Trust Classification based several dimension	Introduced additional communication overhead
7	Zygmunt J. Haas	2011	distributive prioritization of transmission based on nodes coverage	Unstable behavior in the presence of multiple simultaneous broadcast
8	Jawwad Shamsi and Monica Brockmeyer	2010	demonstrate the effectiveness of QoSMap in providing QoS-compliant overlays which are resilient to DoS attacks. studying the effect destructive network perturbations on their performance	This approach can not work to incorporate the effect of different traffic models in our study
9	Jui Chi Liang	2010	Enhanced Services discovery with low overhead	Inefficient resources Utilization
10	Khabbazian M	2009	Guaranteed end to end Qos delivery	Qos reduced on high Mobility
11	Stephen Mueller	2009	Enhanced overall throughput by TCP connection in AD HOC network	Introduces additional communication delay in multipath routing

4. Proposed Methodology

In organize to resolve the shortage in Support Vector Machines, this paper suggest novel memory Genetic Algorithm optimization for Support Vector Machine. In this algorithm, Support Vector Machines era utilizes because the representation of the classification and Genetic Algorithms are accept in solve the problems of a hyper-plane optimization. The alternative of consequence factor c parameter for SVM and the kernel purpose parameter have a huge weight on the classification accurateness and simplification aptitude for SVM. Algorithm parameter optimization is revealed as follows:

1) System instatement, including SVM parameters and the beginning counter acting agent bunches,
2) The objective parameter streamlining for SVM capacities as an Antigen,
3) To figure every Antigen and counter using so as to act agent for their enthusiasm the objective capacity.
4) To log down the presence of the cells and record the incredible immune response during the time spent development. Given the ideal parameters are found, the development process closes and ideal parameters yield. At that point skip to strategy 5.
5) To ascertain every immune response of its focus and survival rate, and to suitably supply Immunizer choice and its safe framework.
6) The new gathering redesigns. New gatherings can be produced by method for selecting, recuperating and transforming, and after that expel the new kid on the block individual from the memory base to constitute another era, and afterward rehash from step 3.

5. Conclusion

In this paper of dissimilar technique for detecting and prevent DDOS Securing mobile adhoc networks system and the relative analysis amongst them has been converse is in advance attractiveness, but with the prevalent usage of, the issue of security is also surfacing. DDoS is the major threat to MANETs. Because of this device's battery can be depleted with in no time which is the most required thing in mobile devices. To overcome this, it is required to provide a Defence mechanism against DDoS attacks

In Intrusion Detection System Using Dempster Shafter Theory, exceptions are generated at which slow down performance. There is possibility if we develop such mechanism in which exception generated by are updated at Node/Cluster so that next time such exception should be entertained at cloud node or cluster level.

References

[1] Antikainen, Tuomas Aura, and Mikko Särelä ," Denial-of-Service Attacks in Bloom-Filter-Based Forwarding" IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 22, NO. 5, OCTOBER 2014.
[2] Andreas Papalambrou "Detection, traceback and filtering of denial of service attacks in networked embedded systems" New Delhi, India — October 12 - 17, 2014.
[3] Rajya Lakshmi G.V, Anusha.K" Detection of Anomaly Network Traffic for Mobile Ad-hoc Network Using Fuzzy Logic" September- 2013.
[4] Supriya Bamane, Rajesh Singh," AODV Based Improved Method for Detecting Good Neighbor Nodes" Volume 3, Issue 7, July 2013.
[5] Jiajia Liu, Student Member, IEEE, Xiaohong Jiang, Senior Member, IEEE, Hiroki Nishiyama, Member, IEEE, and Nei Kato, Senior Member, IEEE ," generalized two-hop relay for flexible delay control in manets" ieee/acm transactions on networking, vol. 20, no. 6, december 2012.
[6] Mohamed Nidhal MEJRI , Jalel BEN-OTHMAN ," Entropy as a New Metric for Denial of Service Attack Detection in Vehicular Ad-hoc Networks MSWiM'14, September 21–26, 2014, Montreal, QC, Canada.

[7] Rodrigo do Carmo, Marc Werner, and Matthias Hollick ," Signs of a Bad Neighborhood: A Lightweight Metric for Anomaly Detection in Mobile Ad Hoc Networks" Q2SWinet'12, October 24–25, 2012, Paphos, Cyprus

[8] Aminu mohammed, mohamed ould-khaoua, lewis m. Mackenzie and jamal abdulai," adaptive counter-based broadcasting scheme in mobile ad hoc networks" hp-mosys'12, october 25, 2012, paphos, Cyprus.

[9] Manikandan, S.P. and R. Manimegalai," Survey On Mobile Ad Hoc Network Attacks And Mitigation Using Routing Protocols " American Journal of Applied Sciences, 2012, 9 (11), 1796-1801.

[10] S.Ganapathy, P. Yogesh, and A.Kannan: "Intelligent agent based intrusion detection system using enhanced multiclass SVM", Computational Intelligence and Neuroscience, volume 2012, article ID 850259.

[11] Monita Wahengbam, Ningrinla Marchang: "Intrusion detection in MANET using fuzzy logic", 2012 IEEE. [15] QualNet Network simulator 5.0.2 "Programming guide".

[12] C. Kruegel, D. Mutz, W. Robertson and F. Valeur, "Bayesian event classification for intrusion detection", Proceedings of the 19th Annual Computer Security Applications Conference (ACSAC), (2003), pp. 14-23.

[13] S. Mukherjee and N. Sharma, "Intrusion detection using naive Bayes classifier with feature reduction", Procedia Technology, vol. 4, (2012), pp. 119-128.

[14] M. J. Wei, L. C. Xia, J. G. Jin and C. Chen, "Research of Intrusion Detection Based on Clustering Analysis", Proceedings of International Conference on Cybernetics and Informatics, (2012), pp. 1973 1979.

[15] W. Tylman, "Misuse-based intrusion detection using Bayesian networks", Proceedings of 3rd International Conference on Dependability of Computer Systems (DepCos), (2008), pp. 203-210.

[16] V. Jyothsna, V. V. R. Prasad and K. M. Prasad, "A review of anomaly based intrusion detection systems", International Journal of Computer Applications, vol. 28, no. 7, (2011), pp. 26-35.

[17] R. Goel, A. Sardana and R. C. Joshi, "Parallel Misuse and Anomaly Detection Model", International Journal of Network Security, vol. 14, no. 4, (2012), pp. 211-222.

[18] J. McHugh, "Testing intrusion detection systems: A critique of the 1998 and 1999 DARPA intrusion detection system evaluations as performed by Lincoln Laboratory", ACM Transactions on Information and System Security, vol. 3, no. 4, (2000), pp. 262-294. S. Hettich and S. D. Bay, "The UCI KDD Archive", http://kdd.ics.uci.edu/databases kddcup99/kddcup99.html, (1999)

*Corresponding author.
E-mail address: divyagautam06@ gmail.com