ISSN 2394-739X

IJRSET MARCH Volume 9 Issue 3

International Journal for Research in Science Engineering & Technology (IJRSET)

https://www.doi.org/10.5281/zenodo.6355160

PARTICLE SWARM OPTIMIZATION THREAT VALUE OF ATTACK ALGORITHM (PSO-TVA) FOR NETWORK SECURITY

[1] Mrs. S. Anusuya, [2] Dr. G. A. Mylavathi, [3] Dr. N. M. Mallika, [4] Dr. S. Prabhu, [5] Dr. M. Shanmugapriya,
[1] Research Scholar, [2, 3, 4] Assistant Professor, [5] Associate Professor,
[1, 3, 5] Department of Computer Science, [2] Department of Computer Technology, [4] Department of Information Technology,
[1, 3] Sri Vasavi College, [2, 4] Gobi Arts & Science College, [5] Park's College,
[1, 3] Erode, [2, 4] Gobichettipalayam, [5] Chinnakarai Tirupur,
[1, 2, 3, 4, 5] Tamil Nadu, India.

ABSTRACT - To assess the security situation of hierarchical network, a particle swarm optimization algorithm in light of the method of building a security hazard work is proposed. To work with going to proactive lengths to decrease the harm level of network security occasions model takes care of the security assessment issue for hierarchical network just and productively. This paper plans a hierarchical security situation evaluation method in light of the attributes of attack diagram engineering and the security occasions in the attack chart information plane. Then, at that point, the situation evaluation results are broke down, and the relationship in time arrangement is tapped. Then, at that point, a security situation prediction model in view of Particle Swarm Optimization Threat Value of Attack algorithm (PSO-TVA) is proposed to understand the security situation prediction for the attack chart information plane. The reproduction results show that the prediction model has higher prediction accuracy on the test set and is feasible in practical applications.

Keywords: [Network Security, Situation, Hierarchical, Attack, TVA, PSO.]

1. INTRODUCTION

Network security is an expansive term that covers a multitude of technologies, gadgets and processes. In its most straightforward term, it is a bunch of rules and arrangements intended to safeguard the honesty, privacy and availability of computer networks and data utilizing both programming and equipment technologies. Each association, paying little mind to measure, industry or foundation, requires a level of network security arrangements set up to safeguard it from the steadily developing scene of digital threats in the wild today. The present network design is perplexing and is confronted with a threat climate that is continuously changing and attackers that are continuously attempting to find and take advantage of weaknesses. These weaknesses can exist in a wide number of regions, including gadgets, data, applications, clients and locations. Therefore, there are much network security the board devices and applications being used today that address individual threats and exploits and furthermore administrative rebelliousness. At the point when only a couple of moments of personal time can make inescapable interruption and enormous harm an association's primary concern and notoriety, it is fundamental that these insurance measures are set up.

Network security comprises of the policies, processes and practices took on to forestall, distinguish and screen unapproved access, abuse, adjustment, or forswearing of a computer network and network-open assets. Network security includes the approval of admittance to data in a network, which is constrained by the network head. Clients pick or are relegated an ID and secret phrase or other confirming data that permits them admittance to data and projects inside their power. Network security covers an assortment of computer networks, both public and private, that are utilized in regular positions: going through with exchanges and interchanges among organizations, government offices and people. Networks can be private, for example, inside an organization, and others which may be available to public access. Network security is associated with associations, ventures, and different sorts of organizations. It does as its title clarifies: it gets the network, as well as safeguarding and managing tasks being finished. The most well-known and straightforward approach to safeguarding a network asset is by appointing it an exceptional name and a comparing secret key.

Network Security

In the present hyper-associated world, network security presents a more prominent test as more business applications move to private and public clouds. Besides, the actual applications presently will more often than not be virtualized and conveyed across numerous locations, some of which are outside the actual control of IT security groups. With the number of attacks on organizations climbing ever higher, safeguarding network traffic and foundation is basic.

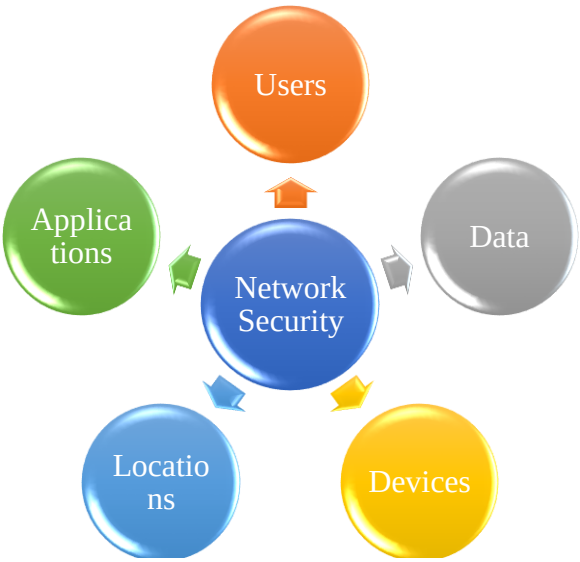

Figure 1.Network Security

The network security arrangements safeguard different weaknesses of the computer frameworks displayed in figure 1. The most essential illustration of Network Security is secret phrase insurance where the client of the network oneself picks. In the new times, Network Security has turned into the focal subject of digital protection with numerous associations welcoming applications of individuals who have abilities around here.

2. EXISTING SYSTEM

1. Y. Wang, J. Lu, Z. Wu and Y. Lu et.al proposed Component Based Security Control for Information Network. It proposes security control engineering in light of security control necessities of info-net. In the security control system in light of components of info-net, network substances are the makers, yet in addition the purchasers of security control components. SCC has the qualities of capacity specialization, interface standardization, reproducibility, update and propagability. The security control management system schedules SCCs consistently and it understands the circulated control on request of network security. Simultaneously, they additionally work on the flexibility and reliability of security control. The control design and thought is particularly appropriate for security control of the dynamic, mobile and private network, for example, space information network, strategic C3I, etc.

2. Zhiyong Lu, Yunyan Zhou et.al proposed the Evaluation Model for Network Security. Subsequent to dissecting and measuring the network information security components: confidentiality, integrity and accessibility, this paper characterizes the network security confidentiality vector, the network security integrity vector and the network security accessibility vector, and furthermore constructs the hierarchical marker system of network security evaluation. These paper progresses meanings of network security confidentiality vector, network security integrity vector and network security accessibility vector, lays out a hierarchical pointer system of network security evaluation, proposed a multilayer linear weight comprehensive evaluation model for network security evaluation which is both subjective and quantitative. Tests demonstrate that this model is judicious, logical and simple to work.

3. Shadi R. Masadeh, Shadi Aljawarneh, Nedal Turab et.al proposed a comparison of data encryption algorithms with the proposed algorithm: Wireless security. Encryption algorithms assume a principle part in wireless network security systems. In any case, those algorithms consume a lot of computing assets, for example, CPU time, and parcel size. While trying to cure the wireless network security issue, an original work has been sent to get the communicated data over wireless network, called a solid WiFi (sWiFi) algorithm. The sWiFi algorithm depends on created HMAC cryptography algorithm. Recreation results are given to show the adequacy of every algorithm. The created sWIFI algorithm is worked around a 64 bit encryption/decryption and may be additionally extended to cover 128 to reach up to 512 pieces and then some, will in any case be proficient in both Speed and size which could be executed into an equipment arrangement. In piece of future work, we will lead similar concentrate among sWiFi and other encryption algorithms on various stages and different battery power utilization.

3. PROPOSED METHODOLOGY

Threat value of an attack (TVA)

Threat value of an attack (TVA) is utilized to quantify the threat value of an attack step in a subnet that is in a specific state. TVA to evaluate network security level their estimation for TVA is like that for another boundary annihilates value of climate. It would be better for an evaluation model to have two totally unique evaluation lists. In this way, unique in relation to, propose TVA in view of attack reaction span, since the more top to bottom an attack step is, the more opportunity to reaction. Network intrusions are partitioned into have based intrusion and server-based intrusion. To server-based intrusion, we were unable to tackle the issue just by closing down the server or turning off the network cable. In the case of doing that, business will be intruded, and it isn't allowed. So the reaction here doesn't go to these lengths after all other options have run out into account.

The numerical depictions about TVA are as per the following: When a subnet is in a state s_a of path p_k , the threat value of attack is denoted as $tva\ (s_a)^{p_k}$. Think about an extreme case: an attack step's TVA is somewhat low; however the following stage's TVA is high to such an extent that not enough time to deal with it. So move into account. Then, at that point:

$$\boldsymbol{tva(S_a)^{P_k} = \frac{1}{2}.(t(S_a,(S_a)^{P_k}_{next}) + t((S_a)^{P_k}_{next},((S_a)^{P_k}_{next})^{P_k}_{next}))} \quad \textbf{(1)}$$

And if s_a is the final state of p_k,

$$\boldsymbol{t((S_a\,{}^{P_k}_{next}),((S_a)^{P_k}_{next})^{P_k}_{next})) = (t(S_a,(S_a)^{P_k}_{next})} \quad \textbf{(2)}$$

Likewise with calculation of resources loss, s_a maybe middle state of n attacks. TVA at state is s_a is denoted as $tva\ (s_a)$:

$$\boldsymbol{tra(s_a) = max(tra(s_a)^{P_k} = \frac{1}{2}.max\left(t(S_a,(S_a)^{P_k}_{next}) + t((S_a)^{P_k}_{next},((S_a)^{P_k}_{next})^{P_k}_{next})\right), k \in [1,n]} \quad \textbf{(3)}$$

This paper makes upgrades to the PSO algorithm and proposes a Threat value of attack Swarm Optimization Algorithm (PSO-TVA). This algorithm changes the boundaries of the PSO algorithm nonlinearly so that the particle has continually changed search capacities at various

times to adjust the global and neighborhood search abilities of the particles. Simultaneously, it likewise changes the out-of-bounds particles so the out-of-bounds particles don't assemble at the limit to tackle the issue that the PSO algorithm is inclined to fall into the neighbourhood outrageous value, subsequently further developing the optimization execution of the algorithm,

The particular process of PSO algorithm to streamline the construction of TVA network is as per the following:

Step 1: *Initialize the algorithm's boundaries;*
Step 2: *Initialize the TVA network structure;*
Step 3: *Set the wellness capacity of the PSO as the loss function capacity of the network. In this paper, the mean square error function is utilized as the wellness work.*

$$fit_{MSE} = \frac{1}{n}\sum_{i=1}^{n}(\hat{y}_i - y_i)$$

In the equation, nn is the particle swarm size, and $\hat{y}_i$ and y_i are the predicted value and the true value respectively.
Step 4: *Calculate the wellness function value of each particle;*
Step 5: *update the nearby optimal place of each particle and the global optimal place of the particle swarm;*
Step 6: *update each particle's own speed and position;*
Step 7: *If the greatest number of iterations is not reached, go to step 4.*

4. EXPERIMENT RESULTS

Accuracy

Particle	SCCs	sWiFi	Proposed PSO-TVA
1	20	30	50
2	35	45	65
3	40	50	70
4	55	65	85
5	65	75	95

Table 1.Comparison of Accuracy

The table 1 describes Comparison of Accuracy values explain the different values of existing algorithms (SCCs, sWiFi) and proposed PSO-TVA. While comparing the Existing algorithm (SCCs, sWiFi) and proposed PSO-TVA, provides the better results.

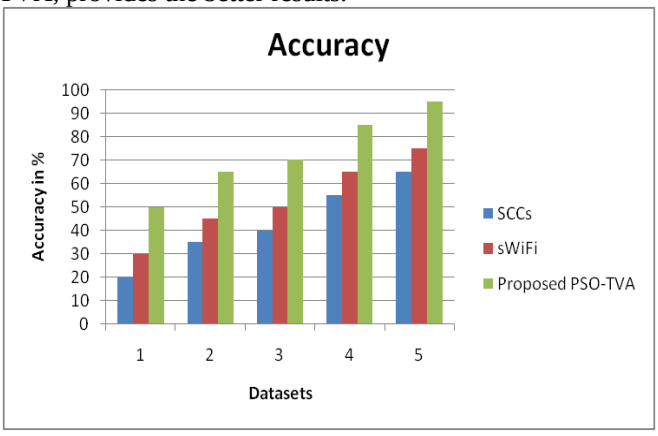

Figure 2.Comparison of chart Accuracy

The figure 2 shows Comparison chart of Accuracy values explain the different values of existing algorithms (SCCs, sWiFi) and proposed PSO-TVA. X axis denote the Nodes Accuracy in percentage and y axis denotes the Particles. While comparing the Existing algorithm (SCCs, sWiFi) and proposed PSO-TVA, provides the better results. The existing algorithm values start from 20 to 65, 30 to 75 and proposed PSO-TVA values starts from 50 to 95.

Normalized Data Prediction

Particle	SCCs	sWiFi	Proposed PSO-TVA
1	0.73	0.80	0.91
2	0.74	0.83	0.92
3	0.76	0.85	0.95
4	0.77	0.87	0.97
5	0.79	0.88	0.99

Table 2.Comparison of Normalized Data Prediction

The table 1 describes Comparison of Normalized Data Prediction values explain the different values of existing algorithms (SCCs, sWiFi) and proposed PSO-TVA. While comparing the Existing algorithm (SCCs, sWiFi) and proposed PSO-TVA, provides the better results.

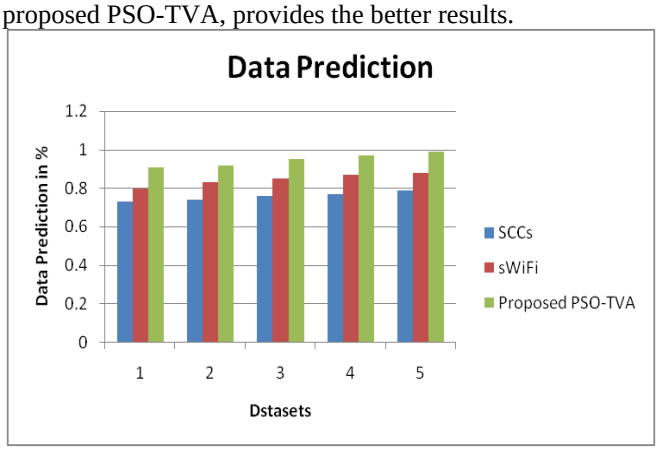

Figure 3.Comparison of chart Normalized Data Prediction

The figure 3 shows Comparison chart of Normalized Data Prediction values explain the different values of existing algorithms (SCCs, sWiFi) and proposed PSO-TVA. X axis denote the Normalized Data Prediction in percentage and y axis denotes the Particles. While comparing the Existing algorithm (SCCs, sWiFi) and proposed PSO-TVA, provides the better results. The existing algorithm values start from 0.73 to 0.79, 0.80 to 0.89 and proposed PSO-TVA values starts from 0.91 to 0.99.

Prediction Errors

Particle	SCCs	sWiFi	Proposed PSO-TVA
5	0.80	0.91	1.10
10	0.82	0.92	1.11
15	0.83	0.93	1.15
20	0.85	0.95	1.17
25	0.87	0.97	1.21

Table 3.Comparison of Prediction Errors

The table 3 describes Comparison of Prediction Errors values explain the different values of existing algorithms (SCCs, sWiFi) and proposed PSO-TVA. While comparing the Existing algorithm (SCCs, sWiFi) and proposed PSO-TVA, provides the better results.

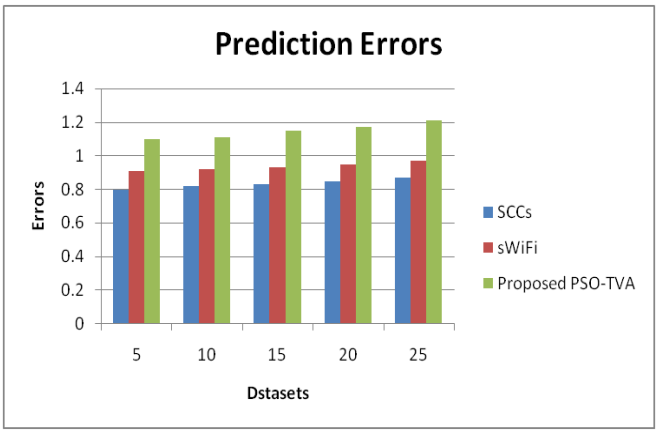

Figure 4.Comparison of chart Prediction Errors

The figure 4 shows Comparison chart of Prediction Errors values explain the different values of existing algorithms (SCCs, sWiFi) and proposed PSO-TVA. X axis denote the Errors and y axis denotes the Particles. While comparing the Existing algorithm (SCCs, sWiFi) and proposed PSO-TVA, provides the better results. The existing algorithm values start from 0.80 to 0.87, 0.91 to 0.97 and proposed PSO-TVA values starts from 1.10 to 1.21.

CONCLUSION

This paper plans a hierarchical security situation evaluation method in view of the attributes of attack graph engineering and the security occasions in the attack graph data plane. Then, at that point, the situation evaluation results are investigated, and the connection in time succession is tapped. Then, at that point, a security situation prediction model in view of Particle Swarm Optimization Threat Value of Attack algorithm (PSO-TVA) is proposed to understand the security situation prediction for the attack graph data plane. The recreation results show that the prediction model has higher prediction accuracy on the test set and is possible in practical applications.

REFERENCES

[1]. Dhenakaran S. S., Parvathavarthini A., An Overview of Routing Protocols in Mobile Ad-Hoc Network. International Journal of Advanced Research in Computer Science and Software Engineering. 2013; 3(2).
[2]. Dwivedi P., Gupta S., A Review of Routing Protocols & Techniques for Mobile Ad-Hoc Networks. International Journal of Scientific Research Engineering & Technology. 2015; 4(7): 782-788.
[3]. Gupta K. A., Sadawarti H., Verma K. A., Performance analysis of AODV, DSR and TORA Routing Protocols. International Journal of Engineering and Technology. 2010; 2(2).
[4]. Haihui Ge, Lize Gu, Yixian Yang and Kewei Liu, "An attack graph based network security evaluation model for hierarchical network," 2010 IEEE International Conference on Information Theory and Information Security, 2010, pp. 208-211, doi: 10.1109/ICITIS.2010.5688764.
[5]. J. Li and C. Dong, "Research on Network Security Situation Prediction-Oriented Adaptive Learning Neuron," 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing, 2010, pp. 483-485, doi: 10.1109/NSWCTC.2010.247.
[6]. Kaur A., Singh A., A Review on Security Attacks in Mobile Ad-hoc Network. 2014; 3(5): 1295-1299.
[7]. Kumar V., Tyagi A., Kumar A., Mobile Ad-hoc Network: Characterstics, Applications, Security Issues, Challenges and Attacks. IJARCSSE. 2015; 5(1).
[8]. Lalar S., Security in MANET: Vulnerabilities, Attacks & Solutions. IJMCR. 2014; 2(Jan-Feb).
[9]. M. H. Khyavi and M. Rahimi, "Conceptual Model for Security in Next Generation Network," 2016 30th International Conference on Advanced Information Networking and Applications Workshops (WAINA), 2016, pp. 591-595, doi: 10.1109/WAINA.2016.12.
[10]. M. Sheng, H. Liu, X. Yang, W. Wang, J. Huang and B. Wang, "Network Security Situation Prediction in Software Defined Networking Data Plane," 2020 IEEE International Conference on Advances in Electrical Engineering and Computer Applications(AEECA), 2020, pp. 475-479, doi: 10.1109/AEECA49918.2020.9213592.
[11]. M. Wu and X. Liu, "Research on Key Technologies of ship network security protection," 2021 2nd International Conference on Computer Communication and Network Security (CCNS), 2021, pp. 89-93, doi: 10.1109/CCNS53852.2021.00026.
[12]. Sahu S., Security Issues and Attacks in Mobile Ad-hoc Network. 2013; https://www.slideshare.net/xeon40/attacks-on-mobile-ad-hocnetworks-12619703?next_slideshow=1.
[13]. Shrivastava S., Jain S., A Brief Intoduction of Different Type of Security Attacks Found in Mobile Ad-hoc Network. IJCSET. 2013; 4: 222-224.
[14]. Shukla S., Sharma S., Study & Analysis of dsdv, aodv & dsr. International Journal of Advanced Research in Computer and Communication Engineering. 2013; 2(5).
[15]. T. Yin, L. Han, C. Wan, X. Qu and Y. Li, "The Probability of Trojan Attacks on Multi-level Security Strategy Based Network," 2010 International Conference on Multimedia Information Networking and Security, 2010, pp. 555-559, doi: 10.1109/MINES.2010.122.
[16]. Y. Kai, H. Qiang and M. Yixuan, "Construction of Network Security Perception System Using Elman Neural Network," 2021 2nd International Conference on Computer Communication and Network Security (CCNS), 2021, pp. 187-190, doi: 10.1109/CCNS53852.2021.00042.
[17]. Z. Qu and X. Wang, "Study of Rough Set and Clustering Algorithm in Network Security Management," 2009 International Conference on Networks Security, Wireless Communications and Trusted Computing, 2009, pp. 326-329, doi: 10.1109/NSWCTC.2009.47.