Design and Deployment of Network Testbed for Web Data Security

Shishir Kumar Shandilya

*School of Data Science and Forecasting, Devi Ahilya University,
Indore – MP, India
School of Computing Science & Engineering, VIT Bhopal University,
MP, India
E-mail: shishir.sam@gmail.com*

Received 30 April 2021; Accepted 04 June 2021;
Publication 23 December 2021

Abstract

In recent years, the cyber security scenario has transformed predominantly from conventional response-based security mechanisms to proactive security strategies. And this transformation is still continuing which is shifting it from proactive security strategies to cyber immunity which eliminates the cyber threats by introducing stringent and adaptive security measures. In the process of developing new security algorithms/procedures, accurate modelling and effective simulation play a vital role for the robustness and effectiveness of proposed system. It is also necessary to analyze the behaviour of proposed system against multiple types of known cyber attacks. This paper focuses on the existing network testbeds for an effective analysis and monitoring while proposing a new network testbed for examining new security concepts like cyber immunity. The proposed network testbed is designed to incorporate the methods and procedures of Nature-inspired Cyber Security to accommodate the adaptive responses against the sophisticated and ever-advancing cyber attacks. The proposed testbed provides customizable analytical tool to design,

Journal of Cyber Security and Mobility, Vol. 11_2, 127–140.
doi: 10.13052/jcsm2245-1439.1121

test and examine the new security algorithms through a rich set of attack scenarios. It also allows developers to design, implement, and evaluate their defensive techniques with library support.

Keywords: Nature-inspired cyber security, adaptive cyber defense, network monitoring, network simulation, performance tuning.

1 Introduction

Due to the advent of advanced methods in e-commerce and web development and its integration with artificial intelligence (AI), cyber security and data mining (DM) technologies, web data security is of paramount importance and thereby gaining attraction by recent researches. New standards, open source development tools and variety of formats makes the issue more complex for formulating a secured mechanism of web data transfer. Along with this, the rapid developments in AI and cyber security are making the web data more vulnerable against the sophisticated threats. Fortunately, the defensive researches are also progressing with time and they are countering the latest cyber attacks on web data with good predictive ratio and performance. While, the efficiency and efficacy both the factors are important to test and revise the proposed defensive mechanism, an appropriate test bed also plays vital role in modelling development and testing process. Such testbeds facilitates the developers to run and test the proposed algorithm/system on variety of attack scenarios under controlled network conditions [1-4].

There are other alternatives as well like cyber ranges and virtual machines but unfortunately they failed to provide a quick and intelligent solution as they require a detailed configuration and fine tuning of proposed method before simulating the network environment. This makes the entire development process complex and time-consuming which is certainly not the ideal condition when the attacks are continuously evolving and assisted by high-performance machines. Therefore, a flexible network testbed is required which not only facilitates the quick modelling but also provide rick library support to develop a precise defence system while testing it on multiple types of attack scenarios without much programming efforts.

More advanced defensive methods like adaptive or AI-assisted methods require more accurate and customized network testbeds. Nature-Inspired Cyber Security (NICS) is receiving a lot of attention due to better adaptability, multi-objective optimization and quick learning [5–8]. The nature-inspired defence system can proactively detect and mitigates the attacks, but they are often more complex to simulate and build and also requires a lot of simulation to verify its adaptability and correctness [9–11]. Therefore, a cohesive, highly customizable and feature rich testbed is required to design such defence system based on various network conditions like sudden decline in throughput, status misinformation, or excessive bandwidth usage.

This paper introduces a comprehensive network testbed for testing and analysis of a suitable defensive mechanism specifically for web data security, by taking all important modelling and development aspect into the account, while especially focusing on adaptive defence methodologies like Nature-inspired Cyber Security. The proposed testbed includes many functions written in libraries for implementing adaptive security techniques, to provide quick and easy setup of network by selecting the number of nodes, clusters and communication protocols rather than designing them, which save a lot time of researcher to focus on analysis.

2 Adaptive Defense and Security

Cyber attacks are evolving rapidly while effectively utilizing the AI-based methods to breach the networks of target organizations. And this is getting worse day-by-day especially in pandemic situation and work-from-home culture. Therefore, there is an utmost need of more intelligent and adaptive defensive system to safe-guard the personal networks and critical infrastructures [12, 13]. AI-based defence solutions which are generally trained on labelled dataset occasionally fail to recognise the potential threats in case the cyber attackers use polymorphic or metamorphic malwares which are server-assisted attack to generate a large of morphed malwares to get access one way or other. It is high time to consider other methods to make the defence system more robust against these high-end cyber attacks while guaranteeing active resilience. Nature-inspired Cyber Security is able to provide such security mechanism while attempting to achieve the ultimate cyber immunity. While attempting to provide adaptability, self-awareness and resilience, NICS methods are currently at the initial investigation by the researchers. Along with many attractive benefits, NICS also suffers relatively slow response as compared to AI-based solutions, due to the multi-objective functions [14, 15].

An ideal defence system must provide a proactive mechanism for threat identification, containment and resolution and while doing so, the system must also attempt to gain cyber immunity. Cyber Immunity is a condition where the cost of implementing a successful attack should be higher than the benefit to the attacker(s) [16].

3 Related Works

It is imperative to have the best defensive system for the organization, and therefore it is one of the most critical decisions which are to be taken after a detailed analysis. Every organization is having different setup of network and machines; and therefore requires a customised defensive system. These customised defence systems requires to be tested thoroughly on various operational parameters. A testbeds are therefore used to compare available defensive system on various attack scenarios and fine-tune the selected defensive system. Testbeds are also useful in threat analysis and vulnerability assessment of existing networks to avoid loss of data and network downtime. An effective defensive mechanism is to be tested thoroughly on various attack-defence simulations to identify the realistic parameters and most optimum configuration with respect to investment cost and response time [17].

Many testbeds are available but none is a generalised enough to be suited for all types of requirements [18]. But, for implementation of the latest security mechanisms like AI and NICS on the testbed and perform the various attack scenarios is a complex and time-consuming process. Designing a new testbed as per the requirement is also not a feasible solution as it requires a lot of time and also expensive. Many existing testbeds like University of Utah's Emulab [19], DETER [20], and Virtualised CR [21] are flexible, and offer ease of configuring and tuning the network parameters. Another remarkable testbed was UltraScienceNet which was an experimental WAN (Wide Area Network) testbed by providing on-demand and high bandwidth channels for large data transfers and high-precision channels for fine-tuning the control operations, to facilitate the development of networking technologies specifically for the next-generation large-scale scientific applications [22]. Zheng et al. proposed CHEETAH which was a high-speed WAN network solution for large file transfers and remote visualizations, which was having end-to-end transport architecture [23]. Recently, Minakhmetov et al. proposed a dynamic network resource allocation using software-defined networking optical controller on the COSMOS testbed [24].

In year 2021, Xiang et al. proposed another SDN and NFV based network emulation environment called communication Networks Emulator (ComNetsEmu) which is community-embraced open source packages. It also facilitates the replicable research [25]. Other quality testbeds which are commercially available are SoftFIRE and Emulab. SoftFIRE is a federated testbed consists of multiple independent testbeds to experiment in software defined networks [26]. Emulab is a network testbed, giving researchers a wide range of environments in which to develop, debug, and evaluate their systems [27]. But, the adaptive defence mechanisms like AI and NICS requires extra features like multi-objective optimization and intermediate performance evaluation. Therefore, a specific test-bed is required specifically for adaptive defensive strategies for design, test and develop a robust defensive system.

4 Proposed System

The proposed system is a testbed to facilitate the validity and efficiency of proposed defence system against the variety of attack scenarios. The testbed takes the preliminary configuration inputs from the user and formulate the proposed network layout by selection of nodes and clusters (Figure 1). The provision of including the pre-coded defence strategies is also possible. This initial setup will be scaled up automatically if the results are promising. Then, the pre-determined attack parameters are applied on the system. The proposed system has multiple attack scenarios of Ping of Death, Distributed Denial of Service (DDoS), Low-Rate Transmission Control Protocol Denial of Service (LRTCPDoS), and Evil Handshake attacks etc.

The proposed system integrates the input parameters and attack parameters along with NICS/AI based algorithm in the customized network setup and generate tcl script (by via Python3) for Network Simulator 2 (NS2).

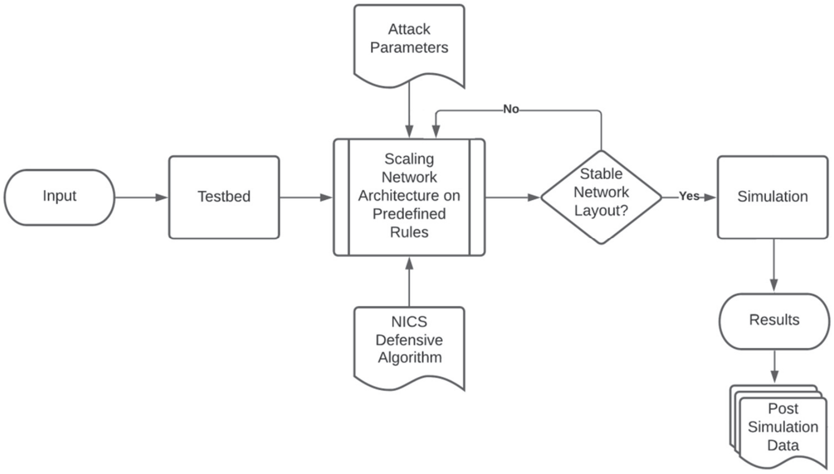


Figure 1 Proposed testbed.

This script is then used for simulating the network scenario and process data to be saved as post-simulation data for further analysis and fine-tuning of setup with respect to the major objective of simulation. The proposed system constantly monitor and check the stability of network layout in presence and absence of an attacks and records the important network parameters for further analysis.

4.1 Experimental Setup

The proposed testbed provides a dense and scalable network having variety of communication protocols (Figure 2). It is dynamic and flexible also i.e. the user can also select the number of nodes and cluster for the network along with other parameters like cluster-level communication protocol parameters, network topology, number and position of malicious node(s), and inter-cluster communication type & frequency.

The network is having *m* clusters namely C_x where $x = 1, 2, 3 \ldots m$ and each C_x is having *n* nodes denoted by C_xN_y where $y = 1, 2, 3 \ldots n$. E.g. C2N3 denotes the third node of second cluster in the network. Each cluster is connected via three routers R_z where $z = 1, 2, 3$, however it can be extend up

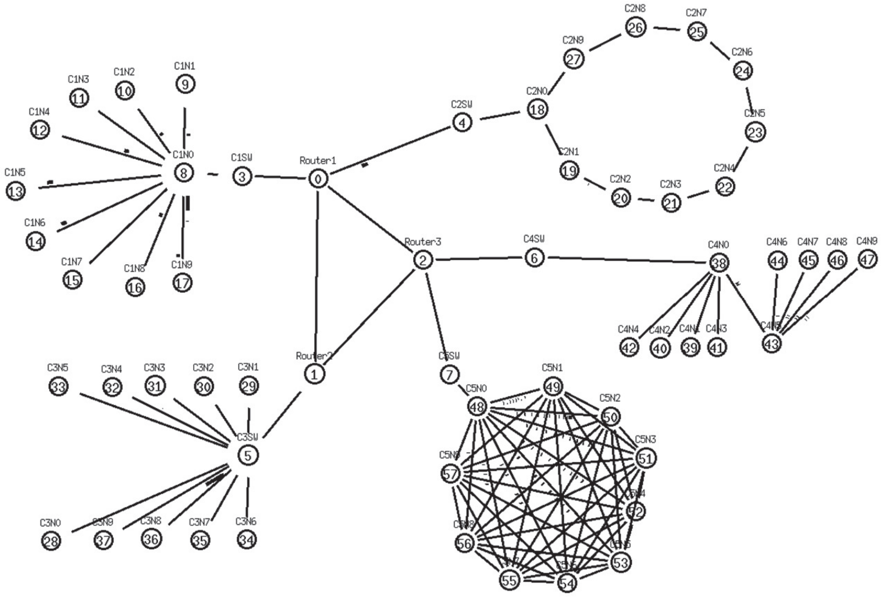


Figure 2 Proposed network.

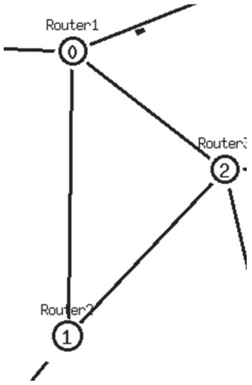


Figure 3 Router triangle.

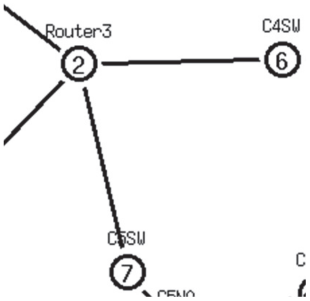


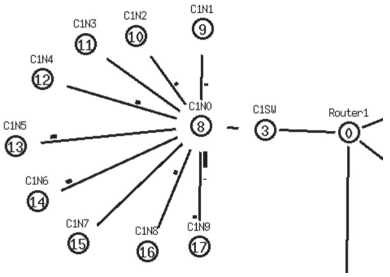
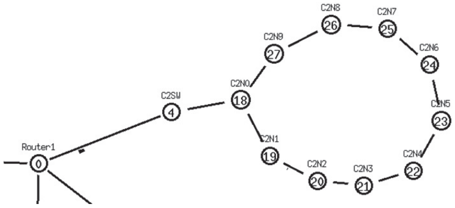
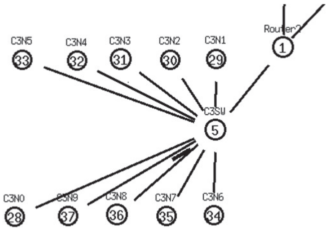
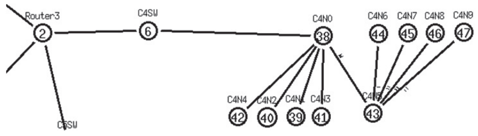
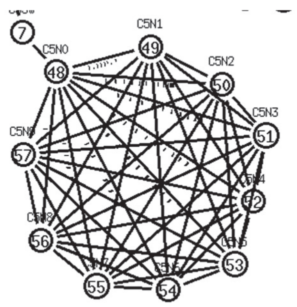
Figure 4 Router to switch connection.

to any number (Figures 3 and 4). Likewise, switches are also used as S_p where $p = 1, 2, 3 \ldots$ to inter connect clusters to the routers. Attack scenarios can be designed by selecting the malicious nodes $MALN_x$ or malicious clusters $MALC_y$.

The proposed system facilitates easy network setup as per the customization needed and variety of simulation to execute to test and verify the efficiency of the proposed network. Multiple clusters are placed based on variety of communication protocols and topologies. Following are the details of various clusters of the network which can be further scaled and reconfigured as per the need,

Once configured, the proposed testbed simulates the network with dummy traffic and records various parameters for further analysis. The results can be obtained as network animation (NS2) and comparative graphs based on recorded statistics, which can be modified as per the objectives.

Table 1 Cluster details

Cluster	Details
 C1N3 11 C1N2 10 C1N1 9 C1N4 12 C1N0 8 C1SW 3 Router1 0 C1N5 13 C1N6 14 C1N7 15 C1N8 16 C1N9 17	**Name:** Cluster 1 **Initial Set of Nodes:** 10 (can be selected or not selected). **Setup:** All nodes are connected to one node which is in turn connected to switch. **Scalable:** Yes
 C2N8 26 C2N7 25 C2N9 27 C2N6 24 C2N0 18 C2SW 4 C2N5 23 Router1 0 C2N1 19 C2N2 20 C2N3 21 C2N4 22	**Name:** Cluster 2 **Initial Set of Nodes:** 10 (can be selected or not selected). **Setup:** Ring Topology **Scalable:** Yes
 Router2 1 C3N5 33 C3N4 32 C3N3 31 C3N2 30 C3N1 29 C3SW 5 C3N0 28 C3N9 37 C3N8 36 C3N7 35 C3N6 34	**Name:** Cluster 3 **Initial Set of Nodes:** 10 (can be selected or not selected). **Setup:** All nodes are directly connected to switch. **Scalable:** Yes
 Router3 2 C4SW 6 C4N0 38 C4N6 44 C4N7 45 C4N8 46 C4N9 47 C4N4 42 C4N2 40 C4N1 39 C4N3 41 C4N5 43 C5SW	**Name:** Cluster 4 **Initial Set of Nodes:** 10 (can be selected or not selected). **Setup:** Hybrid Arrangement **Scalable:** Manual configuration required
 7 C5N1 49 C5N0 48 C5N2 50 C5N3 51 C5N9 57 C5N4 52 C5N8 56 C5N5 53 C5N7 55 C5N6 54	**Name:** Cluster 5 **Initial Set of Nodes:** 10 (can be selected or not selected). **Setup:** Ring Topology **Scalable:** Manual configuration required

5 Results Analysis

After setting up the testbed for adaptive defensive mechanism for securing web data, we have simulated it with 10 nodes per cluster, and having all five clusters active. The network data is to be recorded in base files. We have selected the R2 to initiate the Low-Rate TCP-Targeted Denial of Service Attack. This should affect the performance of other routers and eventually other inter-communication.

We have then tested the system in presence and absence of attack to observe the impact of attack on overall performance and stability of network. We may also test the defensive methods at routers R1 and R3 routers to contain on resolve the attack. We have used the average of throughput with respect to the time to test the performance of each node.

The trace files can be then evaluated and plotted on various network parameters. In our experiment, we have implemented the adaptive defensive mechanism against the Denial of Service attack on R2 router.

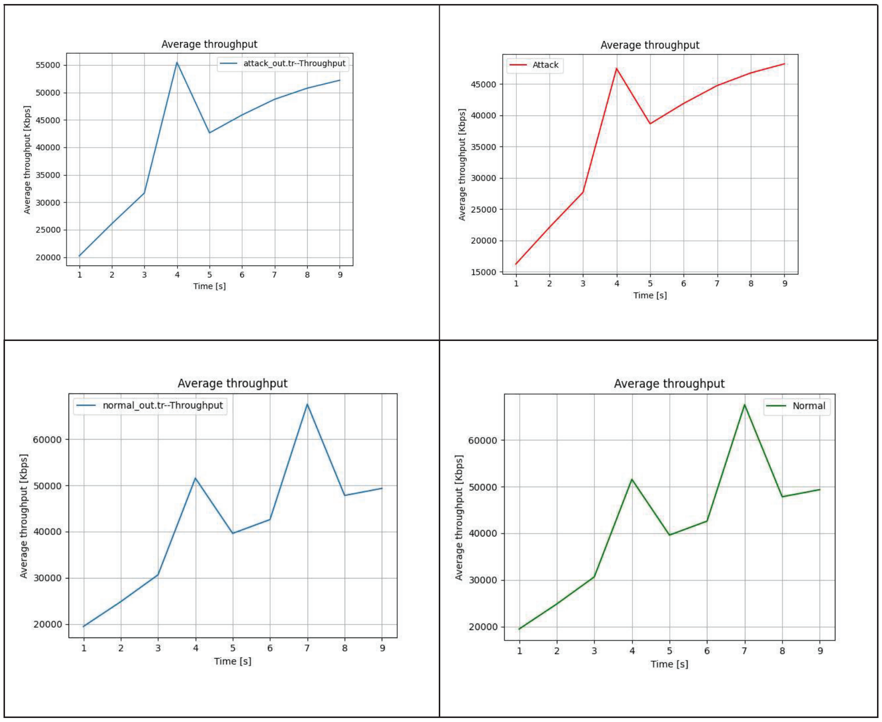


Figure 5 Network performance graphs.

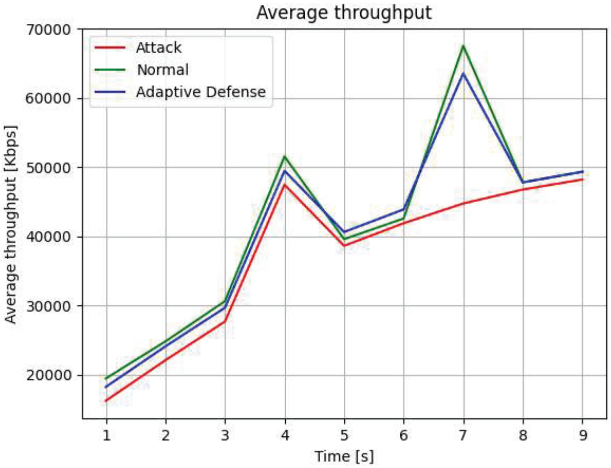


Figure 6 Performance evaluation on proposed testbed.

By observing Figure 6, we may conclude that the defensive method implemented on routers R1 and R3. One may observe that in the absence of any defensive mechanism the network performance is severely affected especially from 00:06 to 00:08. Such simulation can be repeated under vairous set of network parameter values and variety of attacks.

The proposed testbed is fully customizable and flexible to design and experiment the security mechanisms under various types of attacks.

6 Conclusions

In this paper, we have introduced a novel testbed which facilitates the designing and experimenting new security mechanisms especially AI/NICS based defence strategies. The proposed test-bed is fully capable of incorporating the peculiarities of adaptive defence techniques for an effective network simulation. We have presented the general architecture of the proposed test-bed and Low-Rate TCP-Targeted Denial of Service Attack scenario with experiment results on throughput. An adaptive defence system is also demonstrated, where we have compared the network performance in different scenarios namely, ‘normal’, ‘under attack’, and ‘under attack in presence of adaptive defence’ and achieved stable experimental results. Selection and appropriate defensive system for an organization is a critical decision. The proposed test-bed can be the solution that offers full-customization on various parameters under observation, a high degree of sensitivity analysis, and effective performance-tuning on various operational parameters, without the risk of losing data and integrity. The immediate future work can be a web application service of the proposed test-bed and establishing it as standard test-bed equipped with rich libraries for implementing the adaptive defence mechanisms on the proposed testbed.

References

[1] S. Bitam, S. Zeadally, A. Mellouk, Bio-inspired cyber security for wireless sensor networks, IEEE Communications Magazine 54(6) (2016) 68–74.

[2] U. Rauf, A taxonomy of bio-inspired cyber security approaches: existing techniques and future directions, Arabian Journal for Science and Engineering 43(12) (2018) 6693–6708.

[3] K. Demertzis, L. Iliadis, A bio-inspired hybrid artificial intelligence framework for cyber security, in: Computation, Cryptography, and Network Security, Springer, 2015, pp. 161–193.

[4] S. N. Mthunzi, E. Benkhelifa, T. Bosakowski, S. Hariri, A bio-inspired approach to cyber security, Machine Learning for Computer and Cyber Security: Principle, Algorithms, and Practices; CRC Press: Boca Raton, FL, USA (2019) 75.

[5] M. E. Kuhl, M. Sudit, J. Kistner, K. Costantini, Cyber attack modelling and simulation for network security analysis, in: 2007 Winter Simulation Conference, IEEE, 2007, pp. 1180–1188.

[6] D. S. Fowler, M. Cheah, S. A. Shaikh, J. Bryans, Towards a testbed for automotive cyber security, in: 2017 IEEE International Conference on Software Testing, Verification and Validation (ICST), IEEE, 2017, pp. 540–541.

[7] G. Apruzzese, M. Colajanni, L. Ferretti, A. Guido, M. Marchetti, On the effectiveness of machine and deep learning for cyber security, in: 2018 10th International Conference on Cyber Conflict (CyCon), IEEE, 2018, pp. 371–390.

[8] H. Jiang, T. Choi, R. K. Ko, Pandora: A cyber range environment for the safe testing and deployment of autonomous cyber attack tools, arXiv preprint arXiv:2009.11484.

[9] M. Atighetchi, P. Pal, F. Webber, C. Jones, Adaptive use of network-centric mechanisms in cyber-defense, in: Sixth IEEE International Symposium on Object-Oriented Real-Time Distributed Computing, 2003., IEEE, 2003, pp. 183–192.

[10] G. Cybenko, M. Wellman, P. Liu, M. Zhu, Overview of control and game theory in adaptive cyber defenses, in: Adversarial and Uncertain Reasoning for Adaptive Cyber Defense, Springer, 2019, pp. 1–11.

[11] Z. Hu, P. Chen, M. Zhu, P. Liu, Reinforcement learning for adaptive cyber defense against zero-day attacks, in: Adversarial and Uncertain Reasoning for Adaptive Cyber Defense, Springer, 2019, pp. 54–93.

[12] J. B. Fraley, J. Cannady, The promise of machine learning in cybersecurity, in: SoutheastCon 2017, IEEE, 2017, pp. 1–6.

[13] I. Ghafir, M. Hammoudeh, V. Prenosil, L. Han, R. Hegarty, K. Rabie, F. J. Aparicio-Navarro, Detection of advanced persistent threat using machinelearning correlation analysis, Future Generation Computer Systems 89 (2018) 349–359.

[14] M. Breza, J. A. McCann, Lessons in implementing bio-inspired algorithms on wireless sensor networks, in: 2008 NASA/ESA Conference on Adaptive Hardware and Systems, 2008, pp. 271–276. doi:10.1109/AHS.2008.72.

[15] S. Mthunzi, E. Benkhelifa, T. Bosakowski, S. Hariri, A Bio-inspired Approach To Cyber Security: Principles, Algorithms, and Practices, 2019, pp. 75–104. doi:10.1201/9780429504044-4.

[16] N. Pankov, Applied cyberimmunity: What is it?, https://www.kaspersky.com/blog/applied-cyberimmunity/28772/, [Online; accessed 10-January-2020] (2019).

[17] V. D. Veksler, N. Buchler, B. E. Ho_man, D. N. Cassenti, C. Sample, S. Sugrim, Simulations in cyber-security: A review of cognitive modelling of network attackers, defenders, and users, Frontiers in psychology 9 (2018) 691.

[18] J. Davis, S. Magrath, A survey of cyber ranges and testbeds, Tech. rep., Defence Science and Technology Organisation, Edinburgh (Australia) (2013).

[19] C. Siaterlis, A. P. Garcia, B. Genge, On the use of emulab testbeds for scientifically rigorous experiments, IEEE Communications Surveys & Tutorials 15(2) (2012) 929–942.

[20] T. Benzel, The science of cyber security experimentation: the deter project, in: Proceedings of the 27th Annual Computer Security Applications Conference, 2011, pp. 137–148.

[21] J. Mayo, R. Minnich, D. Rudish, R. Armstrong, Approaches for scalable modeling and emulation of cyber systems: Ldrd final report, Sandia report, SAND2009-6068, Sandia National Lab.

[22] Rao, Nageswara, Wing, William, Carter, Steven, Wu, Chase. (2005). UltraScience Net: Network testbed for large-scale science applications. Communications Magazine, IEEE. 43. S12–S17. 10.1109/MCOM.2005.1541694.

[23] Zheng, Xuan, Veeraraghavan, Malathi, Rao, Nageswara, Wu, Chase, Zhu, Michelle. (2005). CHEETAH: Circuit-Switched High-Speed End-to-End Transport Architecture Testbed. Communications Magazine, IEEE. 43. s11–s17. 10.1109/MCOM.2005.1497551.

[24] Minakhmetov, Artur, Gutterman, Craig, Chen, Tingjun, Yu, Jiakai, Ware, Cédric, Iannone, Luigi, Kilper, Daniel, Zussman, Gil. (2020). Experiments on Cloud-RAN Wireless Handover using Optical Switching in a Dense Urban Testbed. Th2A.25. 10.1364/OFC.2020.Th2A.25.

[25] Xiang, Zuo, Pandi, Sreekrishna, Cabrera Guerrero, Juan, Granelli, Fabrizio, Seeling, Patrick, Fitzek, Frank. (2021). An Open Source Testbed for Virtualized Communication Networks. IEEE Communications Magazine. 59. 77–83. 10.1109/MCOM.001.2000578.

[26] https://www.softfire.eu/testbed/

[27] https://www.emulab.net/portal/frontpage.php

Biography

Shishir Kumar Shandilya is a research scholar of higher doctorate at Devi Ahilya University and the Division Head of Cyber Security and Digital Forensics at VIT Bhopal University. He is working as a Principal Consultant to the Govt. of India for Technology Development and Assessment in Cyber Security. He is also a Visiting Researcher at Liverpool Hope University-United Kingdom, a Cambridge University Certified Professional Teacher and Trainer, ACM Distinguished Speaker and a Senior Member of IEEE. He is a NASSCOM Certified Master Trainer for Security Analyst SOC (SSC/Q0909: NVEQF Level 7) and an Academic Advisor to National Cyber Safety and

Security Standards, New Delhi. He has received the IDA Teaching Excellence Award for distinctive use of technology in Teaching by Indian Didactics Association, Bangalore (2016) and Young Scientist Award for two consecutive years, 2005 and 2006, by Indian Science Congress and MP Council of Science and Technology. He has seven books published by Springer Nature-Singapore, IGI-USA, River-Denmark and Prentice Hall of India. His recently published book is on Advances in Cyber Security Analytics and Decision Systems by Springer.