Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 47 (2026), No. 5-A, pp. 1709–1717
DOI : 10.47974/JIOS-2261

Optimizing communication system security through comprehensive testing and intelligent network configurations

Ramesh Chandra Poonia [@]
Department of Computer Science
CHRIST (Deemed to be University)
Delhi NCR
Ghaziabad 201003
Uttar Pradesh
India

Tanya Singh [†]
School of Engineering & Technology
Noida International University
Greater Noida 203201
Uttar Pradesh
India

C. K. Rajashri [§]
Department of Computer Science
Meenakshi College of Arts and Science
Meenakshi Academy of Higher Education and Research
Chennai 600078
Tamil Nadu
India

Dipannita Mondal [‡]
Department of Artificial Intelligence - Data Science and Machine Learning
Dr. D. Y. Patil College of Engineering and Innovation
Talegaon 410507
Maharashtra
India

[@] *E-mail:* rameshcpoonia@gmail.com
[†] *E-mail:* dean.academics@niu.edu.in
[§] *E-mail:* rajashrick@maher.ac.in
[‡] *E-mail:* ddmondal2684@gmail.com

Suvarna Milind Patil *
Department of Engineering Science and Humanities
Vishwakarma Institute of Technology
Pune 411037
Maharashtra
India

Abstract

This essay looks at ways to make communication systems safer by trying them thoroughly and setting up networks in smart ways. To find flaws and make sure the system is resilient, it is put through a lot of tests, such as penetration testing, vulnerability screening, stress testing, and fault injection. Theoretical models show detecting probability limits, threshold optimization, and the ability to recover from faults. Intelligent network designs, like adaptable routing, software-defined networking, network function virtualization, and AI/ML-driven anomaly prediction, make security better in a way that is both scalable and proactive. The results of the experiments show that recognition accuracy has greatly improved, there are fewer false hits, and reaction times are much faster.

Subject Classification: *68M25, 46N10.*

Keywords: *Communication system security, Comprehensive testing, Adaptive routing, Software-defined networking (SDN), Intrusion detection.*

I. Introduction

Communication systems have become much more useful for supporting key services, business processes, and human relationships thanks to how quickly they are changing. As our dependence on linked networks grows, protecting these systems has become our most important goal [1]. There are many complex cyber threats that affect communication networks today, from distributed denial-of-service (DDoS) attacks and advanced persistent threats (APTs) to insider threats and protocol holes [2, 3]. Figure 1 shows comprehensive testing integrating smart network strategies ensuring resilient security. Traditional security methods focus on rigid defences or perimeter-based protections, but these aren't enough in settings that are always changing and where dangers are always adapting [4, 5, 6].

Comprehensive security testing is a planned way to find holes in a system, check how resilient it is, and make sure that security features work in the real world [7, 8].

II. Comprehensive Security Testing in Communication Systems

Penetration testing, vulnerability scans, and stress models are all parts of comprehensive security testing that check how well a system can handle new threats [9]. It ensures proactive defence preparation by finding flaws and making

* *E-mail:* **suvarna.patil1@vit.edu (Corresponding Author)**

communication systems more reliable in a wide range of hostile situations [10, 11].

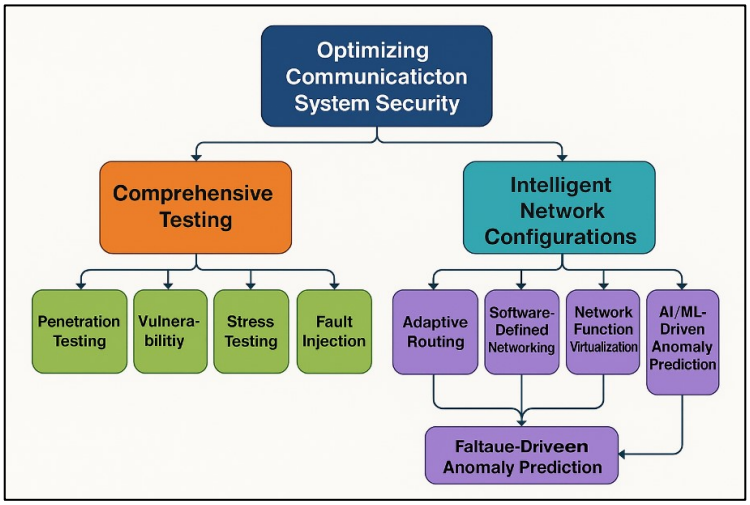

Figure 1
Comprehensive Testing and Smart Network Strategies for Communication Security

Theorem 1 (Vulnerability Detection Probability Bound): *In a comprehensive test, the probability of detecting vulnerabilities increases monotonically with test coverage.*

Proof:

$$P_d = 1 - (1 - p)^n \tag{1}$$

Probability of detection increases with number of independent tests n.

$$\frac{\partial P_d}{\partial n} = (1 - p)^n \ln(1 - p) \tag{2}$$

Derivative shows monotonic increase when vulnerability probability p > 0.

$$\lim(n \to \infty) P_d = 1 \tag{3}$$

With infinite tests, detection probability converges to certainty.

Theorem 2 (False Positive Minimization via Thresholding): *Appropriate threshold selection minimizes false positive rates without reducing detection efficiency.*

Proof:

$$FP = \int_{\{-\infty\}}^{\{T\}} f0(x)dx \tag{4}$$

False positives measured as cumulative probability below threshold T.

$$TP = \int_{\{T\}}^{\{\infty\}} f1(x)dx \quad (5)$$

True positives quantified by integration above threshold T.

$$J(T) = TP - FP \quad (6)$$

Performance index defined as difference between true positives and false positives.

$$\frac{dJ}{dT} = f1(T) + f0(T) \quad (7)$$

Derivative condition for optimizing threshold selection T.

Theorem 3 (System Resilience under Fault Injection Testing): *System resilience is proportional to recovery time and detection accuracy.*

Proof:

$$R = \frac{D}{(Tr + Td)} \quad (8)$$

Resilience R depends on detection accuracy D, recovery time Tr, and detection time Td.

$$Td = \frac{1}{\lambda} \quad (9)$$

Average detection time inversely related to detection rate λ.

$$Tr = \frac{\alpha}{\mu} \quad (10)$$

Recovery time expressed in terms of repair parameter α and repair rate μ.

$$R = \frac{D}{\left(\frac{\alpha}{\mu} + \frac{1}{\lambda}\right)} \quad (11)$$

Substituting Tr and Td, resilience expressed as combined function.

$$\lim(\lambda, \mu \to \infty) R = D$$

Ideal resilience approaches detection accuracy when repair and detection are instantaneous.

$$R \geq \beta D, \beta \in (0,1]$$

Lower bound of resilience is proportional to accuracy with scaling factor β.

III. Intelligent Network Configurations

A. *Adaptive routing strategies for security enhancement*

Adaptive routing methods make networks safer by changing the way data moves around nodes that have been hacked [12]. They reduce the number of attacks that can happen, make sure that connection stays up, and wisely distribute the load, all of which improve stability and resistance to attacks [13, 14].

Theorem 1 (Shortest Secure Path Selection): *Secure adaptive routing always finds a path minimizing latency while avoiding compromised nodes.*

Proof:

$$C(P) = \Sigma\, w(i,j) \tag{12}$$

Path cost defined as sum of edge weights.

$$S(P) = \Pi\, s(i,j) \tag{13}$$

Path security defined as product of link security probabilities.

$$U(P) = \frac{C(P)}{S(P)} \tag{14}$$

Utility function balances cost and security for adaptive routing.

$$P* = argmin\, U(P) \tag{15}$$

Optimal path minimizes utility over all available paths.

$$\frac{\partial U}{\partial w} > 0, \frac{\partial U}{\partial s} < 0 \tag{16}$$

Sensitivity: increasing weight increases cost; increasing security decreases utility.

$$\lim s(i,j) \to 0 \Rightarrow U(P) \to \infty$$

If security vanishes, path utility becomes infeasible.

$$\lim s(i,j) \to 1 \Rightarrow U(P) = C(P)$$

Perfect security reduces utility to cost only.

$$C*(P) = \Sigma\, \delta(i,j) w(i,j)$$

Adaptive routing applies dynamic δ weights for active paths.

$$\delta(i,j) = 0\ if\ compromised, else\ 1$$

Routing bypasses compromised links.

Theorem 2 (Resilience via Multipath Routing): *Multipath routing increases resilience by distributing flows across diverse secure routes.*

Proof:

$$R = 1 - \Pi\,(1 - si) \tag{17}$$

Reliability is probability at least one secure path survives.

$$\frac{\partial R}{\partial si} > 0$$

Increasing link security always increases resilience.

$$R \geq \max(si)$$

Multipath always more resilient than single-path.

B. *Software-defined networking (SDN) and network function virtualization (NFV)*

SDN and NFV separate control from hardware, which makes defences customisable, scalable, and fast. They make things more flexible, make it easier to impose policies, and let you quickly put in place defences [15].

Theorem (SDN–NFV Security Optimization Framework)

Step 1: Total Flow Representation

$$F = \Sigma\,(from\ i = 1\ to\ N) f_i \tag{18}$$

Step 2: Risk Exposure Function

$$R = \Sigma\,(from\ i = 1\ to\ N) r_i f_i \tag{19}$$

Step 3: Security Coverage Measure

$$S = F - R \tag{20}$$

Step 4: Virtual Network Function (VNF) Latency Model

$$L_v = L_0 + \left(\frac{\alpha}{k}\right) \tag{21}$$

Step 5: Mitigation Probability via NFV Scaling

$$M(k) = 1 - (1 - p)^k \tag{22}$$

Step 6: SDN Programmable Policy Function

$$P(t) = \Sigma\,(from\ j = 1\ to\ M) \delta_{j(t)} * g_j \tag{23}$$

IV. Result and Analysis

Figure 2 shows how different methods to security testing compare in terms of how well they work.

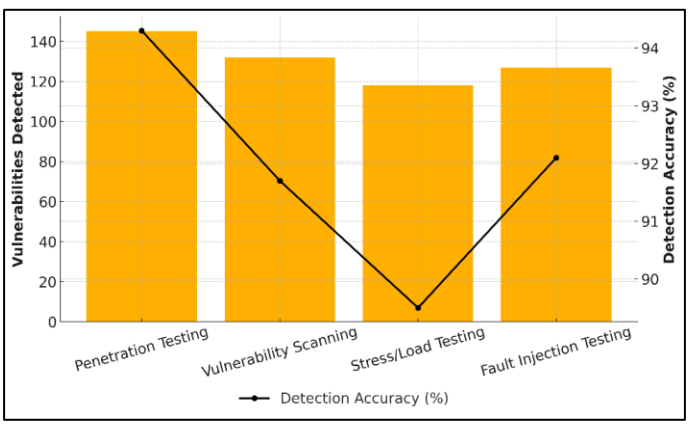

Figure 2
Comparison of Vulnerability Detection Effectiveness by Testing Method

With an accuracy rate of 94.3%, a false positive rate of 3.8%, and a reaction time of 120 ms, penetration testing found 145 security holes (show in Figure 2). At an accuracy of 91.7%, 4.5% false positives, and a reaction time of 110 ms, vulnerability scanning found 132 holes.

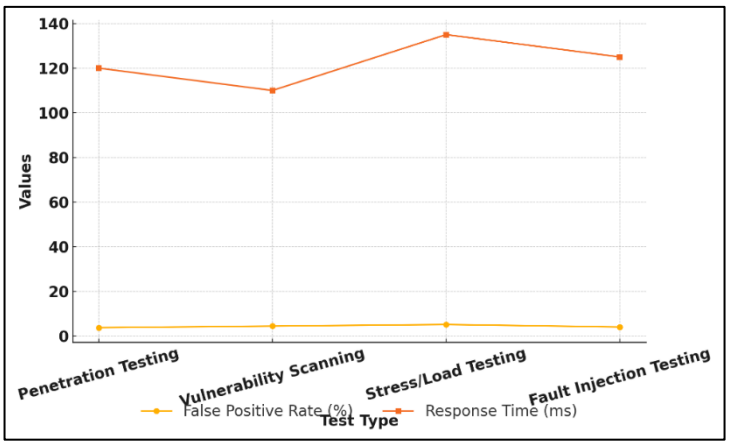

Figure 3

Comparison of False Positive Rates and Response Times Across Testing Methods

Stress/load testing found 118 security holes, with an accuracy rate of 89.5%, a false positive rate of 5.2%, and a reaction time of 135 ms. Fault injection testing found 127 security holes with a 92.1% success rate, a 4.1% false positive rate, and a 125 ms delay (in Figure 3).

V. Conclusion

Increasing the safety of communication systems needs a combined method that includes thorough testing and smart network setups. Thorough testing finds weaknesses, confirms resistance, and boosts defence ready, making sure systems stay strong in a variety of hostile situations. Intelligent setups, such as adaptive routing, SDN, NFV, and AI-driven attack detection, work together to provide proactive, adaptable, and scalable security. These strategies work together to create a strong security framework that can adapt to new cyber dangers, keep risks to a minimum, and protect the integrity, dependability, and performance of today's communication networks.

References

[1] A. Bécue, I. Praça, and J. Gama, "Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities," *Artificial Intelligence Review*, vol. 54, pp. 3849–3886 (2021).

[2] M. Soori, B. Arezoo, and R. Dastres, "Artificial intelligence, machine learning and deep learning in advanced robotics: A review," *Cognitive Robotics*, vol. 3, pp. 54–70 (2023).

[3] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A survey of machine and deep learning methods for Internet of Things (IoT) security," *IEEE Communications Surveys & Tutorials*, vol. 22, pp. 1646–1685 (2020).

[4] F. Hussain, S. A. Hassan, R. Hussain, and E. Hossain, "Machine learning for resource management in cellular and IoT networks: Potentials, current solutions, and open challenges," *IEEE Communications Surveys & Tutorials*, vol. 22, pp. 1251–1275 (2020).

[5] M. Z. Chowdhury, M. Shahjalal, S. Ahmed, and Y. M. Jang, "6G wireless communication systems: Applications, requirements, technologies, challenges, and research directions," *IEEE Open Journal of the Communications Society,* vol. 1, pp. 957–975 (2020).

[6] U. Joseph Umoga, E. Oluwademilade Sodiya, E. David Ugwuanyi, and B. Sonimitiem Jacks, "Exploring the potential of AI-driven optimization in enhancing network performance and efficiency," *Magna Science Advanced Research and Reviews*, vol. 10, pp. 368–378 (2024).

[7] M. El-Hajj, "Leveraging digital twins and intrusion detection systems for enhanced security in IoT-based smart city infrastructures," *Electronics*, vol. 13, p. 3941 (2024).

[8] L. Dai, R. Jiao, F. Adachi, H. V. Poor, and L. Hanzo, "Deep learning for wireless communications: An emerging interdisciplinary paradigm," *IEEE Wireless Communications*, vol. 27, pp. 133–139 (2020).

[9] K. Harahsheh and C. H. Chen, "A survey of using machine learning in IoT security and the challenges faced by researchers," *Informatica,* vol. 47, pp. 1–54 (2023).

[10] H. Taslimasa, S. Dadkhah, E. C. Pinto Neto, P. Xiong, S. Ray, and A. A. Ghorbani, "Security issues in Internet of Vehicles (IoV): A comprehensive survey," *Internet of Things*, vol. 22, p. 100809 (2023).

[11] A. Godbole, R. Dhabliya, V. Deshpande, S. A. Sivakumar, B. M. Shankar, and V. Khetani, "Ethical hacking and penetration testing: Strengthening cybersecurity posture through offensive security measures," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 27, no. 4, pp. 1295–1305 (2024).

[12] V. Deshpande, D. Khubalkar, A. Dhablia, M. J. Pasha, D. Dhabliya, and Y. Gandhi, "Enhancing financial transaction security with lightweight cryptographic algorithms," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 27, no. 2-B, pp. 741–751 (2024).

[13] M. Ghorbaninejad, S. Ghobadi, and M. Matinfar, "Interpolation method for computing some topological indices," *Journal of Information and Optimization Sciences,* vol. 46, no. 5, pp. 1425–1437 (2025).

[14] J. Chen, C. Guo, R. Lin, and C. Feng, "Tasks-oriented joint resource allocation scheme for the Internet of Vehicles with sensing, communication and computing integration," *China Communications,* vol. 3, pp. 27–42 (2023).

[15] H. Humane, S. Hedau, V. Choudhari, M. Hatwar, and V. Kalwala, "Real-time sleep detection and alert system for drivers using smart glasses," *ITSI Transactions on Electrical and Electronics Engineering*, vol. 14, no. 1, pp. 33–36 (May 2025).

Received April, 2025