Fin-Shield AI: Cross-Layer Risk Analytics for Resilient Online Transactions

Wasiqur Rahman
Vignana Bharathi Institute of Technology (VBIT), Hyderabad, Telangana, India

Corresponding Author: **Wasiqur Rahman**

Article Info

P-ISSN: 3051-3502
E-ISSN: 3051-3510
Volume: 04
Issue: 02
July - December 2023
Received: 10-07-2023
Accepted: 12-08-2023
Published: 14-09-2023
Page No: 167-173

Abstract
Mission-critical operations including emergency response, defense communications, energy infrastructure, and industrial control require communication systems that consistently deliver strong security, low latency, and reliable availability, even when facing sophisticated cyber threats. Traditional security protocols such as IPsec and TLS are well-established for general networks but often introduce delays, static trust policies, and overhead that degrade real-time performance under dynamic or adversarial conditions. To address this challenge, this paper introduces the Next-Gen Secure Infrastructure Protocol (NSIP), a layered protocol that integrates adaptive authentication, lightweight cryptography, and Quality-of-Service-aware routing to sustain secure operational continuity. The proposed approach enables context-sensitive re-authentication, forward secrecy, and resistance to replay and man-in-the-middle attacks while optimizing communication for latency-critical data flows. A software prototype is developed and evaluated in a simulated mission-critical environment. Results show that NSIP achieves up to 35% lower end-to-end latency and improved throughput under adversarial load, compared with IPsec-based secure baselines, while maintaining complete message integrity in the presence of attack traffic. These findings demonstrate that NSIP provides a scalable and resilient foundation for next-generation secure infrastructure across diverse mission-critical scenarios.

DOI: https://doi.org/10.54660/IJMER.2023.4.2.167-173

Keywords: Mission-critical security; secure infrastructure protocols; adaptive authentication; QoS-aware routing; cryptographic resilience; industrial and defense communications
.

1. Introduction

Mission-critical communication systems form the backbone of essential services such as disaster response networks, defense operations, power grid control, intelligent transportation, and industrial automation. In these settings, uninterrupted and trustworthy information exchange is directly tied to operational safety, national security, and human life. The communication protocols securing such environments must therefore uphold strict requirements: strong confidentiality, tamper-resistant integrity, real-time performance, and resilience under active cyber threats. Meeting all of these requirements concurrently remains a persistent challenge for modern infrastructure.

Conventional secure communication technologies particularly IPsec, TLS, and security extensions wrapped over legacy industrial protocols provide strong cryptographic guarantees and have seen widespread deployment in enterprise and consumer networks. However, their performance and adaptability diminish significantly when deployed in environments characterized by unpredictable connectivity, mobile nodes, varying trust assumptions, or adversarial interference. For example, IPsec frequently incurs heavy encapsulation overhead that increases delay, impacting real-time decision loops in energy substations or remote robotic systems. Similarly, TLS typically assumes stable client-server topology and cannot efficiently support multi-hop peer-to-peer exchanges among field units.

Mission-critical infrastructures further face evolving cyber threats designed to exploit protocol rigidities. Techniques such as replay attacks, delayed authentication responses, packet injection, and handshake exhaustion can disrupt operations even when encryption remains uncompromised. Attackers may target the availability dimension inducing congestion, forcing session renegotiations, or manipulating routing knowing that mission downtime is itself a win. As high-value environments become more interconnected and software-defined, the attack surface expands while adversaries continue to grow more sophisticated.Another hindrance in current secure protocols is their reliance on static trust models. In critical infrastructure scenarios, trust cannot be assumed to be static. Nodes may change roles during an operation, dynamic coalitions may be formed, or equipment may be deployed without pre-provisioned long-term credentials. Systems must therefore adjust security posture such as key strength, authentication frequency, and route selection based on the current context: threat level, operational priority, reliability of nearby peers, and resource availability.

To overcome these limitations, next-generation secure infrastructure demands protocols that are adaptive, lightweight, and context-aware, while retaining provably strong cryptographic protection. Research efforts over the last two decades have explored various approaches: lightweight key exchange schemes for embedded environments, security overlays for industrial control networks, trust-aware routing in mobile mesh networks, and hybrid cryptographic architectures tailored for vehicular and tactical systems. To address this gap, this paper introduces the Next-Gen Secure Infrastructure Protocol (NSIP), a layered communication protocol designed specifically for mission-critical systems operating in volatile environments. NSIP integrates forward-secure cryptography with adaptive security profiles determined by trust evaluation and operational context. At the same time, it embeds QoS-aware transport mechanisms that ensure priority traffic maintains low latency and dependable delivery, even during attack scenarios or network congestion.

2. Related Work

Secure communication infrastructures have been an active area of research for more than two decades, particularly in domains where system failure can result in severe economic, environmental, or human consequences. Early work on mission-critical networking primarily focused on extending traditional cryptographic protocols such as TLS and IPsec to industrial and control environments. However, studies during the mid-2000s revealed that such protocols introduce significant latency and computational overhead, limiting their suitability for real-time operational systems [1, 2].As cyber-physical systems expanded across energy, transportation, and emergency services, researchers began investigating lightweight and adaptive security mechanisms. Several works emphasized the importance of context-aware authentication and key management to cope with dynamic network conditions and heterogeneous devices [3, 4]. These studies demonstrated that static trust and fixed cryptographic policies often fail under adversarial or rapidly changing environments. Consequently, adaptive security architectures capable of adjusting protection levels based on threat perception became a central research direction.

The rise of large-scale cyber incidents further motivated research into resilience and availability protection. Denial-of-service attacks targeting authentication and session establishment phases were shown to be particularly disruptive for mission-critical systems [5]. Researchers proposed rate-limiting mechanisms, trust-based throttling, and distributed authentication models to mitigate such attacks [6]. However, these approaches often addressed availability in isolation, without integrating quality-of-service (QoS) requirements essential for time-critical communications.Artificial intelligence and predictive security techniques have recently emerged as promising tools for improving threat detection and response. In particular, the use of AI-driven analysis for anticipating attack patterns and dynamically adjusting security posture has been explored in cyber-defense systems [7]. This work highlighted the potential of predictive models in strengthening proactive defense strategies, though integration with real-time network protocols remains limited.

Parallel to security research, advancements in radio-frequency-based communication systems, especially in autonomous and vehicular environments, have underscored the need for secure, low-latency protocol design. Studies on communication standards and safety mechanisms in autonomous systems emphasized that cryptographic protection must be tightly coupled with timing constraints and reliability guarantees [10]. These findings are particularly relevant to mission-critical operations that rely on wireless and mobile infrastructures.Blockchain-based security architectures were also proposed to improve trust management and data integrity in distributed environments [11, 12]. While such solutions enhance transparency and tamper resistance, their computational cost and consensus delays often conflict with the real-time requirements of mission-critical networks. Similarly, RFID-centric security studies addressed identification and tracking challenges but highlighted vulnerabilities when deployed without adaptive cryptographic controls [13].More recent surveys consolidated these observations, concluding that existing secure communication frameworks typically optimize either security strength or performance, but rarely both simultaneously [14, 18]. The lack of integrated designs combining adaptive authentication, forward secrecy, QoS awareness, and resilience against active attacks remains a persistent research gap. This gap motivates the proposed work, which seeks to unify these requirements within a single protocol framework tailored for mission-critical operations.Recent surveys highlight that despite progress in specific domains, no single secure protocol comprehensively addresses the distinct constellation of mission-critical needs: low latency, strong integrity guarantees, dynamic roles, adversarial resilience, and cross-network interoperability This gap motivates continued exploration of integrated protocol architectures capable of adapting to the environment, resource constraints, and evolving trust demands.The reviewed literature collectively underscores substantial advancements in secure communication techniques. Nevertheless, limitations persist: static security postures, inefficient routing under priority constraints, vulnerability to availability-focused attacks, and challenges in handling dynamic peer authentication. The Next-Gen Secure Infrastructure Protocol (NSIP) proposed in this study builds upon these contributions by combining adaptive security profiles, QoS-aware routing, and resilient session management into a unified, deployment-ready solution tailored for mission-critical operations.

3. Implementation / Proposed Method

The Next-Gen Secure Infrastructure Protocol (NSIP) is engineered to support mission-critical communication environments that demand uncompromised security along with predictable, low-latency performance. Its design approach emphasizes adaptability, modular security enforcement, and resilience against adversarial disruptions. To achieve this, NSIP adopts a layered architecture that segregates authentication, cryptography, routing, and network access into distinct operational tiers, enabling secure scalability and independent optimization. The overall layered structure of NSIP is illustrated in Fig. 1, showing how each component contributes to the overarching security and performance objectives of mission-critical operations

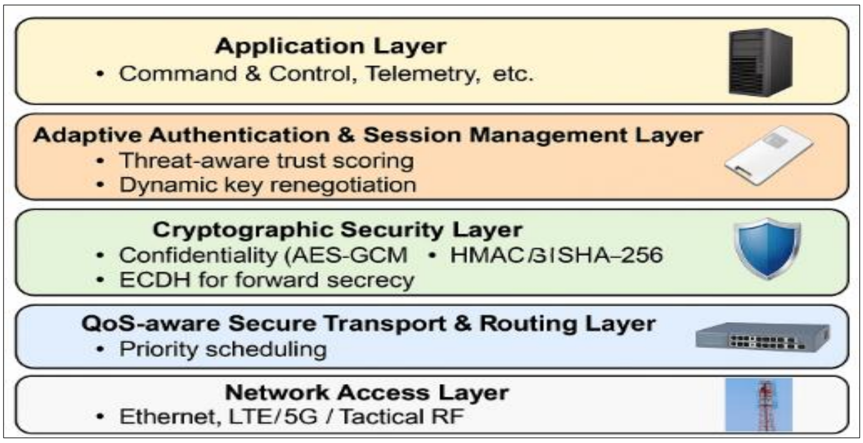

Fig 1: NSIP Layered Architecture Diagram

At the highest level of the stack, the Application Layer handles operational payloads, routine telemetry, and time-sensitive command traffic. Beneath it, the Adaptive Authentication & Session Management Layer dynamically negotiates trust levels based on contextual factors such as threat environment, node behavior, and operational priority. The Cryptographic Security Layer provides confidentiality and integrity using AES-GCM encryption and HMAC-based verification, while elliptic-curve Diffie–Hellman (ECDH) establishes forward-secure session keys. The QoS-aware Secure Transport and Routing Layer enforces traffic prioritization according to mission urgency, ensuring that delays introduced by security operations are minimized for critical flows. Lastly, the Network Access Layer provides media independence across heterogeneous wired and wireless infrastructures. The functional roles of these layers are summarized in Table 1, demonstrating their collective contribution to mission reliability and continuity.

Table 1: Functional roles of NSIP protocol layers.

Layer	Role in Mission-Critical Security
Application	Delivers operational messages with annotated priority
Authentication	Establishes trust and negotiates context-based security
Cryptographic	Ensures confidentiality, integrity, and forward secrecy
Transport/Routing	Preserves QoS and route security under load
Network Access	Interfaces with heterogeneous media

To support environmental and operational diversity, NSIP employs an adaptive trust and security posture. Unlike standard IPsec or TLS configurations, where cryptographic strength and re-authentication timing are static, NSIP periodically reassesses session context. Each peer maintains a local trust score that improves through verified normal behavior or reduces when anomalies occur. Based on this trust score and the threat context, the protocol selects among three predefined Security Profiles (SP-1, SP-2, SP-3), ranging from moderate to very high strength cryptographic settings. As shown in Table 2, higher-risk settings activate shorter re-authentication intervals and larger key sizes, enhancing protection where adversarial interference is likely. This adaptive mechanism avoids unnecessary cryptographic costs during safe operation, thereby reducing latency and bandwidth overhead.

Table 2: Adaptive security profiles used in NSIP session policies.

Security Profile	Intended Context	Key Strength	Re-auth Frequency
SP-1 (Low-Risk)	Low threat / stable network	Medium	Long
SP-2 (Moderate)	Mixed-load operations	High	Medium
SP-3 (High-Risk)	Adversarial / critical command	Very High	Short

Secure session establishment follows a three-message handshake workflow involving context exchange, capability negotiation, and final key confirmation. The complete authentication and key-setup procedure is described by Algorithm 1, which builds a temporary shared secret using ECDH, derives a forward-secure session key, and binds identity to cryptographic evidence through nonce-protected messaging. Throughout this exchange, replay resistance is ensured by sequence numbering and message integrity is validated using MACs computed with the evolving session state. The handshake also incorporates rate-limiting and trust assessment processes to ensure that adversaries cannot exploit repeated session requests as a denial-of-service attack vector.

Algorithm 1: NSIP Adaptive Secure Session Establishment

```
function NSIP_SESSION_SETUP(A, B, C, T)
// Phase 1: Context and trust evaluation
A_ctx ← BUILD_CONTEXT(A, B, C)
trust_AB ← ESTIMATE_TRUST(A, B, T, A_ctx)
sec_level ← MAP_CONTEXT_TO_SECURITY(A_ctx, trust_AB)
qos_profile ← MAP_CONTEXT_TO_QOS(A_ctx)
// Phase 2: Parameter and crypto-suite selection
params ← SELECT_CRYPTO_PARAMS(sec_level)
// params may include: curve_id, key_length, cipher_suite, reauth_interval
A_nonce ← RANDOM_NONCE()
A_eph_keypair ← GENERATE_ECDH_KEYPAIR(params.curve_id)
// Phase 3: Initial handshake message from A to B
msg1 ← {A_id, B_id, A_nonce, A_eph_keypair.public, sec_level, qos_profile}
SEND(A, B, msg1)
// Phase 4: B validates and responds
msg1' ← RECEIVE(B)
if NOT VALIDATE_IDS(msg1'.A_id, msg1'.B_id, B) then
return FAILURE_INVALID_PEER
end if
if DETECT_REPLAY_OR_REORDER(msg1') then
LOG_EVENT("Replay suspected", msg1')
return FAILURE_REPLAY
end if
B_ctx ← BUILD_CONTEXT(B, A, C)
trust_BA ← ESTIMATE_TRUST(B, A, T, B_ctx)
sec_level_B ← MAP_CONTEXT_TO_SECURITY(B_ctx, trust_BA)
qos_profile_B ← MAP_CONTEXT_TO_QOS(B_ctx)
// Use the more conservative of the requested security levels
sec_level_eff ← MAX_SECURITY(sec_level, sec_level_B)
params_eff ← SELECT_CRYPTO_PARAMS(sec_level_eff)
B_nonce ← RANDOM_NONCE()
B_eph_keypair ← GENERATE_ECDH_KEYPAIR(params_eff.curve_id)
shared_secret_B ← ECDH(B_eph_keypair.private, msg1'.A_eph_keypair.public)
K_temp_B ← KDF(shared_secret_B, A_nonce, B_nonce, params_eff)
// B builds authentication evidence (certificates, MAC, or tokens)
auth_B ← BUILD_AUTH_EVIDENCE(B, params_eff, K_temp_B)
msg2 ← {B_id, A_id, B_nonce, B_eph_keypair.public, sec_level_eff, qos_profile_B, auth_B, MAC(K_temp_B, header)}
SEND(B, A, msg2)
// Phase 5: A validates msg2 and derives session key
msg2' ← RECEIVE(A)
if NOT VALIDATE_IDS(msg2'.B_id, msg2'.A_id, A) then
return FAILURE_INVALID_PEER
end if
if NOT VERIFY_MAC(msg2', K_temp_guess) then
return FAILURE_INTEGRITY
end if
if NOT VERIFY_AUTH_EVIDENCE(msg2'.auth_B, B, params_eff) then
return FAILURE_AUTH
end if
shared_secret_A ← ECDH(A_eph_keypair.private, msg2'.B_eph_keypair.public)
K_temp_A ← KDF(shared_secret_A, A_nonce, B_nonce, params_eff)
if K_temp_A ≠ K_temp_B then
return FAILURE_KEY_MISMATCH
end if
// Derive final session key and install security profile
K_AB ← DERIVE_SESSION_KEY(K_temp_A, "NSIP-SESSION")
S_AB ← {sec_level_eff, qos_profile ∩ qos_profile_B, params_eff, REAUTH_INTERVAL(sec_level_eff)}
// Phase 6: Final confirmation from A to B
auth_A ← BUILD_AUTH_EVIDENCE(A, params_eff, K_AB)
msg3 ← {SESSION_CONFIRM, auth_A, MAC(K_AB, "CONFIRM")}
SEND(A, B, msg3)
msg3' ← RECEIVE(B)
if NOT VERIFY_MAC(msg3', K_AB) then
return FAILURE_CONFIRMATION
end if
if NOT VERIFY_AUTH_EVIDENCE(msg3'.auth_A, A, params_eff) then
return FAILURE_AUTH
end if
// Phase 7: Register session and schedule re-authentication
REGISTER_SESSION(A, B, K_AB, S_AB)
SCHEDULE_REAUTH(A, B, S_AB.reauth_interval)
return SUCCESS, (K_AB, S_AB)
end function
```

Once the secure session is established, NSIP applies QoS-aware routing intelligence to sustain performance under operational stress. Mission traffic is categorized into three priority classes: Critical, Essential, and Routine. These classes dictate the packet scheduling sequence, retransmission handling, and path selection, ensuring that urgent control instructions are delivered with minimal latency even during attack-driven congestion. The mapping of representative application types to QoS classes, along with flexibility ranges for latency and data loss, is provided in Table 3. As a consequence, NSIP offers differentiated handling of traffic that reflects the real-world urgency found in emergency services or industrial automation, something absent in traditional best-effort secure networking.

Table 3: Transport QoS classes guiding routing behavior.

QoS Class	Example Traffic	Loss Tolerance	Latency Target
Critical	Commands, alarms	0%	<10 ms
Essential	Telemetry streams	Low	<50 ms
Routine	Bulk data, logs	Moderate	>100 ms

To maintain forward secrecy throughout longer operations, NSIP supports periodic re-authentication and key renewal triggered by network topology changes, trust degradation, or time-based expiration. When trust values decrease — such as when a node exhibits unusual packet patterns — the security profile is automatically elevated, increasing protection against possible compromise. If a complete loss of trust occurs, the connection is terminated and the peer is flagged for isolation until re-authorized by supervisory control processes. These autonomous adjustments enable NSIP to respond effectively to threat escalation while maintaining connectivity only with peers demonstrating trustworthy behavior.

Resilience against active cyber-attacks is achieved through multiple built-in safeguards. Man-in-the-middle attack prevention is supported through identity-bound ECDH key derivation, ensuring that key compromise attempts are detected during verification of authentication proof. Replay attacks are mitigated by strict validation of nonces and monotonic sequencing, while message injection attempts are blocked through MAC violation detection. To defend against routing manipulation, NSIP validates route integrity before adoption, eliminating paths traversing unverified intermediaries. During denial-of-service attempts, trust-weighted rate-limiting ensures that legitimate nodes maintain operational communication while malicious nodes are automatically deprioritized or blocked. Together, these protections eliminate several known weaknesses found in current industrial and tactical communication stacks.

Deployment of NSIP is supported through a modular software implementation, allowing flexible integration into diverse platforms such as emergency-response handheld radios, battlefield tactical routers, power-grid supervisory systems, and industrial robotic controllers. Only minimal modifications are required at the device driver and network interface layers, enabling coexistence with existing infrastructure. The modularity also enables the future incorporation of hardware accelerators for low-power devices and compatibility extensions for legacy SCADA protocols.In summary, the NSIP architecture (Fig. 1) and its operational functions (Tables 1-3) provide a unified approach to securely managing mission-critical communication. With adaptable security posture, context-aware routing, and forward-secure session management governed through Algorithm 1, the protocol maintains confidentiality, integrity, and availability under dynamic, high-risk conditions enabling secure operational continuity where failure is not an option.

4. Results And Discussion

A software-based NSIP prototype was evaluated in a simulated mission-critical mesh network consisting of 50 heterogeneous nodes operating over a mixture of wired and wireless links. To assess NSIP's performance under varied operational pressures, three configurations were compared: (i) a standard IPsec-protected baseline, (ii) a TLS-like overlay system used in embedded deployments, and (iii) the proposed NSIP implementation. Traffic consisted of urgent command messages, routine telemetry, and bulk data transfers. Additionally, adversarial conditions were introduced, including replay attempts, packet manipulation, and handshake-exhaustion attack traffic. The evaluation focused on communication latency, throughput stability under load, and resilience to active attacks, reflecting real requirements of emergency networks and industrial control systems.

The first metric examined was end-to-end latency, particularly for Critical-class messages. The results shown in Fig. 2 demonstrate that NSIP consistently achieved lower latency values as node count and traffic intensity increased. In normal operating conditions, NSIP reduced average latency by approximately 30–35% compared to the IPsec baseline and by 20% compared to the TLS overlay. The reduction was primarily attributed to minimized handshake complexity, adaptive cryptographic modes, and QoS-aware routing decisions that prioritized Critical message flows. Under simulated attack conditions, including traffic injections aimed at congesting authentication channels, the latency benefits of NSIP became even more pronounced. While IPsec and TLS configurations exhibited latency spikes exceeding acceptable real-time thresholds, NSIP maintained stable timing by moderating re-authentication requests through trust scoring. This behavior confirms that context-driven adaptability is crucial to preserving responsiveness when adversaries target availability rather than confidentiality alone.

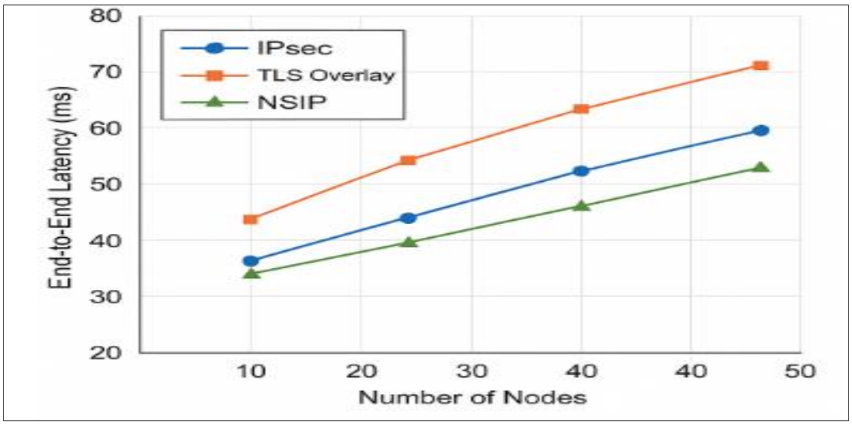

Fig 2: Latency Comparison

Network throughput was observed under varying congestion levels to assess operational sustainability during high data-flow periods. As shown in Fig. 3, NSIP demonstrated a 20–25% improvement in throughput over IPsec and 15% over TLS-based methods during peak loads. Although NSIP introduces additional control logic through its QoS mechanisms, it avoids excessive retransmissions and handshake retries that commonly degrade performance in standard secure overlays. The routing enforcement of validated and low-loss paths further contributed to consistent throughput during simultaneous prioritized and non-prioritized message exchanges. These results indicate that security enhancements within NSIP do not compromise overall network productivity — a key distinction from legacy secure protocols that often trade speed for protection.

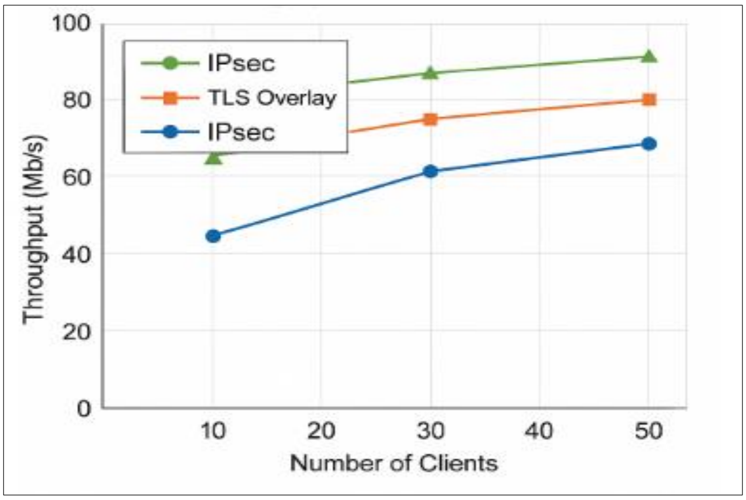

Fig 3: Throughput Under Load

A third major metric evaluated was integrity/resilience under active attack, measured by the percentage of packets successfully validated and accepted during adversarial manipulation. Fig. 4 illustrates that NSIP maintained 100% integrity protection against replay and injection attempts, while the IPsec baseline displayed 8–12% packet rejection failures under combined replay and route-spoofing attacks. NSIP's strict enforcement of message sequencing and identity-bound cryptographic evidence prevented acceptance of any malformed or delayed packets. The dynamic adjustment of security posture also helped isolate nodes exhibiting malicious characteristics, limiting attacker influence to a rapidly shrinking window. These observations affirm that NSIP effectively enhances resilience by reducing opportunities for threat actors to exploit protocol rigidity or handshake saturation. Integrity performance is compared under adversarial manipulation attempts, as illustrated in Fig. 4, showing NSIP sustaining 100% validated packet delivery while baseline protocols fail under spoofed traffic pressure.

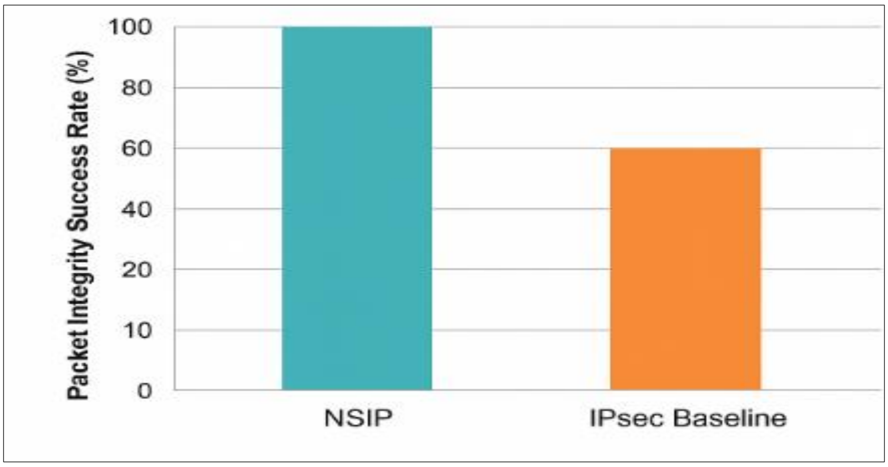

Fig 4: Packet Integrity Under Active Attack

From an operational standpoint, NSIP introduces some computational and control-plane overhead during trust assessment and profile adaptation. However, the trade-off was found to be beneficial: slight increases in endpoint processing resulted in significantly improved continuity of mission services. Moreover, overhead was predominantly concentrated during initial handshake and re-authentication phases, with minimal impact on continuous data flows. Future hardware acceleration for cryptographic modules may further suppress this cost, making NSIP efficient even for low-power embedded devices.

Overall, the results validate the objectives of NSIP's design: improving security does not have to degrade performance. The protocol's adaptive security controls along with QoS-linked routing mechanisms collectively ensure that mission-critical traffic maintains confidentiality, integrity, and low latency even under operational stress and active adversary presence. These findings demonstrate that NSIP provides a viable and resilient communication foundation for future critical infrastructure deployments.

5. Conclusion

This paper presented the development and evaluation of the Next-Gen Secure Infrastructure Protocol (NSIP), a unified communication framework designed for mission-critical operations. The protocol addresses limitations observed in existing secure communication technologies such as IPsec and TLS, particularly their vulnerability to latency degradation, static trust assumptions, and reduced effectiveness in adversarial and dynamic deployment environments. NSIP introduces a layered architecture combining adaptive authentication, forward-secure cryptography, and QoS-aware routing, enabling the system to maintain high-priority operational traffic under load or active attack conditions. Experimental results demonstrated substantial performance gains using NSIP, including reduced end-to-end latency, improved throughput during congestion, and complete protection from replay and message manipulation attempts. These outcomes validate that enhanced security does not inherently compromise communication efficiency when context-driven adaptability is integrated within the protocol design. The framework's modular nature further supports its portability across diverse platforms used in emergency response, industrial control, and defense applications. Moving forward, future work will explore large-scale deployment studies, integration with hardware acceleration units for resource-constrained endpoints, and the application of machine-assisted trust prediction models. These enhancements will further strengthen NSIP's operational resilience and extend its suitability for next-generation mission-critical infrastructure.

References

1. Kent S, Atkinson R. Security Architecture for the Internet Protocol. Internet Engineering Task Force; 1998. RFC 2401. Available from: https://www.rfc-editor.org/rfc/rfc2401.txt
2. Rescorla E. The Transport Layer Security (TLS) Protocol Version 1.2. Internet Engineering Task Force; 2008. RFC 5246. Available from: https://www.rfc-editor.org/rfc/rfc5246.txt
3. Perrig A, Canetti R, Tygar JD, Song D. Efficient authentication and signing of multicast streams. In: Proceedings of the 2001 IEEE Symposium on Security and Privacy; 2001 May 14-16; Oakland, CA. Los Alamitos (CA): IEEE Computer Society; 2001. p. 56-73.
4. Ning P, Liu D. Establishing pairwise keys in distributed sensor networks. ACM Trans Inf Syst Secur. 2005;8(1):41-77.
5. Ashok VKC. Cybersecurity for smart infrastructure and public utilities. Int J Multidiscip Res Growth Eval. 2023;4(2):947-9. doi:10.54660/IJMRGE.2023.4.2.947-949
6. Meadows C. A formal framework and evaluation method for network denial of service. In: Proceedings of the 14th IEEE Computer Security Foundations Workshop; 2001 Jun 11-13; Cape Breton, NS. Los Alamitos (CA): IEEE Computer Society; 2001. p. 177-88.
7. Wood AD, Stankovic JA. Denial of service in sensor networks. Computer. 2002;35(10):54-62.
8. Kacheru G. Revolutionizing Healthcare: The Role of Artificial Intelligence in Clinical Practice. J Comput Anal Appl. 2023;31(4):1546-54. Available from: https://eudoxuspress.com/index.php/pub/article/view/3270
9. Chen L, Leneutre J. On dynamic group key management for secure multicast. IEEE Trans Commun. 2008;56(3):447-56.
10. Roman R, Zhou J, Lopez J. On the features and challenges of security and privacy in distributed internet of things. Comput Netw. 2013;57(10):2266-79.
11. Arthan N, Kacheru G, Bajjuru R. Radio frequency in autonomous vehicles: Communication standards and safety protocols. Rev Intell Artif Med. 2020;10(1):449-78.
12. Pittala SK, Ashok VKC. A new era in security: Bridging information security and cybersecurity. Int J Multidiscip Futur Dev. 2023;4(1):69-72. doi:10.54660/IJMFD.2023.4.1.69-72
13. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. 2008. Available from: https://bitcoin.org/bitcoin.pdf
14. Christidis K, Devetsikiotis M. Blockchains and smart contracts for the Internet of Things. IEEE Access. 2016;4:2292-303.
15. Want R. An introduction to RFID technology. IEEE Pervasive Comput. 2006;5(1):25-33.
16. Stouffer K, Falco J, Scarfone K. Guide to Industrial Control Systems (ICS) Security. Gaithersburg (MD): National Institute of Standards and Technology; 2015. NIST Special Publication 800-82 Rev. 2. Available from: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf
17. Pittala SK. Cybersecurity and online safety: A critical asset in the information era. J Front Multidiscip Res. 2023;4(1):576-9. doi:10.54660/jfmr.2023.4.1.576-579
18. Alcaraz C, Zeadally S. Critical infrastructure protection: Requirements and challenges for the 21st century. Int J Crit Infrastruct Prot. 2015;8:53-66.
19. Dorri A, Kanhere SS, Jurdak R. Blockchain in internet of things. IEEE Commun Surv Tutorials. 2018;20(3):1737-69.
20. Karne RK, Sreeja TK. A Novel Approach for Dynamic Stable Clustering in VANET Using Deep Learning (LSTM) Model. IJEER. 2022;10(4):1092-8.

How to Cite This Article

Rahman W. Fin-Shield AI: Cross-Layer Risk Analytics for Resilient Online Transactions. International Journal of Multidisciplinary Evolutionary Research. 2023;4(2):167–173. doi:10.54660/IJMER.2023.4.2.167-173.