Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 8, pp. 3001–3009
DOI : 10.47974/JDMSC-2637

P4-assisted context-aware encryption framework for secure packet transmission in active SDN networks

Prashant Vats [#]
Department of Computer Science and Engineering
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Sandeep Kumar Budhani [†]
Department of Computer Applications
School of Computing
Graphic Era Hill University
Bhimtal Campus
Bhimtal 263136
Uttarakhand
India

Surabhi Shanker [§]
Centre of Excellence - Cyber Security
School of Engineering & Technology
K. R. Mangalam University
Gurugram 122103
Haryana
India

Devesh Kumar Srivastava [‡]
Department of Information Technology
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

[#] *E-mail:* prashant.vats@jaipur.manipal.edu
[†] *E-mail:* sandeepbudhani13@gmail.com
[§] *E-mail:* surabhi.shanker@krmamgalam.edu.in
[‡] *E-mail:* devesh.srivastava@jaipur.manipal.edu

Madan Lal Saini [@]
Department of Computer Science and Engineering
Apex Institute of Technology (AIT)
Chandigarh University
Mohali 140413
Punjab
India

Ashok Kumar Saini *
Department of Computer Science and Engineering
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Abstract

The rapid evolution of Software-Defined Networking (SDN) has transformed modern communication systems by enabling centralized and adaptive control of data flows. However, the increasing dynamism of SDN environments poses new challenges to maintain data confidentiality and cryptographic integrity. This paper presents a discrete cryptographic framework for Context-Aware Packet Encryption in Active SDN Networks Using P4-Based Code Injection. The proposed model employs selective, context-driven encryption at the packet level, utilizing discrete mathematical structures to dynamically determine encryption paths and security mappings. By integrating cryptographic primitives directly within the data plane, the framework achieves fine-grained protection while reducing redundancy and latency commonly observed in network-wide encryption mechanisms. Analytical evaluation demonstrates that the proposed approach ensures robust confidentiality, efficient key utilization, and optimal resource allocation under varying network conditions. The results affirm that discrete cryptographic methods can substantially enhance the efficiency and resilience of SDN-based communication systems against evolving security threats.

Subject Classification: *Primary 94A60, Secondary 68M12.*

Keywords: *Discrete cryptography, Context-aware encryption, Software-defined networking (SDN), Information security, Packet-level confidentiality, Active networks, Cryptographic key management.*

1. Introduction

As modern network infrastructures evolve toward high-speed and adaptive communication environments, Software-Defined Networking (SDN) has emerged as a foundational architecture that enables centralized control, flexible configuration, and efficient resource management. However, the separation of

[@] *E-mail:* **madan.e13485@cumail.in; mlsaini@gmail.com**
* *E-mail:* **ashok.saini@jaipur.manipal.edu (Corresponding Author)**

the control and data planes in SDN introduces inherent vulnerabilities that can be exploited for packet manipulation, traffic interception, and injection attacks, thereby compromising data confidentiality and integrity. These evolving threats necessitate robust cryptographic frameworks capable of securing dynamic and context-dependent network communications. Traditional encryption techniques, although mathematically sound, are often static in nature, applying uniform encryption policies regardless of the network context or traffic sensitivity. Such mechanisms impose significant computational and communication overhead when deployed across large-scale, heterogeneous network environments. Consequently, there is a growing need for Context-Aware cryptographic methods that can provide fine-grained, packet-level protection based on discrete, rule-driven conditions derived from network state and security policies. To address this challenge, this paper introduces a Discrete Cryptographic Framework for Context-Aware Packet Encryption (CAPE) in active SDN environments. The proposed framework utilizes a mathematically structured encryption model that selectively encrypts packets based on contextual triggers, flow metadata, and predefined security mappings. The remainder of this paper is structured as follows: Section 2 reviews existing cryptographic and SDN-based security models, highlighting the gaps in Context-Aware encryption. Section 3 describes the proposed Discrete Cryptographic Framework and the context-driven Diffie–Hellman enhancement. Section 4 presents simulation results and performance evaluation. Section 5 provides analytical discussions on cryptographic strength and computational efficiency, and concludes the paper with future research directions in adaptive and discrete cryptographic network design.

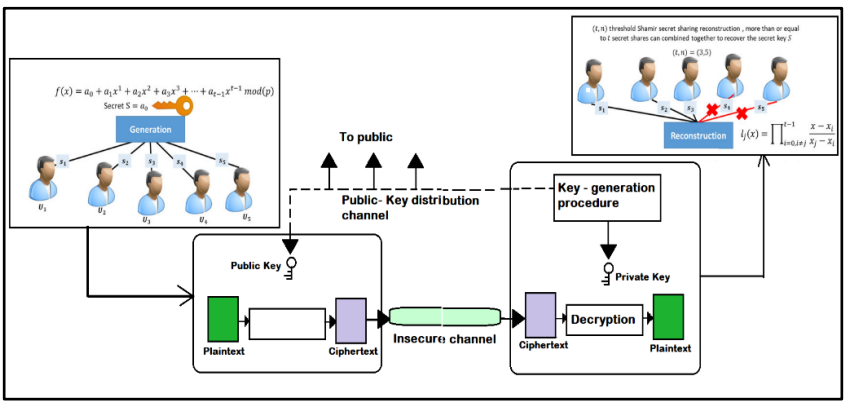

Figure 1
Secure Shared Secret Generation over an Insecure Channel.

2. Related Work

Several studies have explored secure medical image transmission using encryption, authentication, and optimization techniques. Lightweight encryption methods have been emphasized for real-time applications [1]. Wavelet and

chaotic-based schemes improve integrity and attack resistance [2, 3], while watermarking ensures verification [4]. Deep learning in IoMT frameworks supports accurate analysis and secure transmission [5, 6, 7]. Hasan et al. [8] introduced a lightweight IoMT encryption technique, and Li et al. [9] CLU-CNNs support secure transmission via semantic accuracy. Natarajan et al. [10] offered an energy-efficient healthcare security framework. Despite advances, many solutions impose high costs or lack scalability. The proposed cryptography-aware Diffie–Hellman approach offers a balanced solution for secure, efficient, and scalable multicast transmission [11, 12, 13, 14].

3. Proposed Work

Stage 1: Data Preparation and Route Optimization

As shown in Figure 1**,** the process begins with the source node performing entropy-based compression on the original dataset to minimize redundancy and optimize bandwidth utilization. Concurrently, the network initializes key operational parameters, including node energy levels, link reliability indices, and receiver group configurations.

For discrete random variable $X \propto$ with alphabet $X = \{x1, x2, \dots, xn\}$

&

corresponding probabilities $\rightarrow P(X = x^i) = p_i,$ where $\sum_{i=1}^{n} p_i = 1.$

Shannon entropy $H(X) = -i \sum_{i=1}^{n} p_i log_2 p_i$

(lower bound for lossless data compression.)

For entropy encoding $\rightarrow L = \sum_{i=1}^{n} p_i \,.\, l_i$ with $H(X) \leq L < H(X) + 1$

Network Parameter Initialization $\rightarrow$

For a directed graph $G = (V, E),$ where

$V\exists$ source $S \in V$ and receivers $R \subset V,$ and

$E \subseteq V \times V; E \rightarrow$ set of communcation links

For every node v$\rightarrow v \in V \aleph$:

Residual energy $Ev \geq 0$

A set of neighboring nodes $N(v) = \{ u \in V \mid (v, u) \in E \}$

cost of transmitting a packet over link $(u, v) \rightarrow cuv = \alpha \cdot ruv1 + \beta \cdot Ev1$

Total Cost $\rightarrow C(T) = \sum_{(u,v)\in ET} c_{u,v}$

Minimum Cost Steiner Tree on graph G connecting s

$\rightarrow$ all nodes in R with edge costs $c_{u,v}$

$$T \subseteq GminC(T) = \sum_{(u,v)\in ET} c_{uv}$$

Stage 2: Secure Encryption and Key Management

Before transmission, the compressed data undergoes lightweight symmetric encryption using algorithms such as SPECK or SIMON, both

designed to achieve an optimal balance between security robustness and computational efficiency.

For $Lightweight\ Symmetric\ Encryption \rightarrow$

$M \in \{0,1\}^m$; m = packet length/bits;

$\forall\ ciphertext\ C: C = E_K(M), where$

$K \in \{0,1\}^k$; $secret\ symmetric\ key\ shared$

$for\ decryption\ function\ D \rightarrow M = D_K(C)$

For a sequence $(a0_0, a_1, a_2 \ldots\ldots a_n)$

$\{$

$Hashed\ Chain$

$-\ Based\ Key\ Distribution\ \forall source\ generates\ a\ secret\ seed\ s_0 \in \{0,1\};$

Hash Function: $H: \{0,1\}^k \rightarrow \{0,1\}^k$;

$key\ chain \rightarrow\ s_i = H(s_i - 1), i = 1,2, \ldots, N;$

$For\ each\ session\ i \rightarrow k: K_i = s_{N-1}$

$Challenge - Response\ Authentication\ Protocol:$

$random\ nonce\ challenge\ Ch \in \{0,1\}^l \rightarrow\ R = h(Ch \parallel Sec)$

$source\ verifies\ RRR\ by\ computing\ the\ expected\ response \rightarrow$

$R' = h(Ch \parallel Sec);$

$\beth\ source\ verifies\ R\ using\ the\ receiver's\ stored\ secret.$

If R=R′, the receiver is authenticated; otherwise, the connection is rejected.

Stage 3: Scheduled Multicast Transmission and Reception

The encrypted packets are transmitted through a slot-based multicast scheduling scheme, designed using discrete time-slot allocation to minimize channel collisions and optimize bandwidth utilization across the network.

Multicast Scheduling Model: Assume Multicast group $N=\{n_1,n_2,\ldots,n_k\}$ *and fixed-length intervals* $T=\{t_1,t_2,\ldots,t_m\}$.

- P_i: *encrypted packet scheduled for transmission.*

- $S(n_i,t_j) \in \{0,1\}$: *scheduling variable, where S=1 if node* n_i *transmits during time slot* t_j, *otherwise 0,*

- *The scheduling constraint:* $\sum_{n_i \in N} S(n_i, n_j) \leq 1 \qquad \forall j$

minimize total transmission time $min\, T_{total} = \sum_{j=1}^{m} \delta j$

Packets PiP_iPi follow optimized paths computed in Stage 1. Each node maintains:

Routing Table: contains next-hop information for each destination.

ACK Timer τ *: if acknowledgment not received within* $\tau|tau\tau$, *a retransmission is triggered.*

Let:

Pij→ probability of packet loss on link between nodes n_i *and* n_j

$$Rij = \frac{1}{1 - \rho ij} - 1$$

$$Latency_{avg} = (dij + Rij \cdot dij)$$

$For\ Decryption, Authentication, and\ Reconstruction\ at\ Receiver$:

Authentication $h(M \parallel Ki) \triangleq MAC$*; (Upon packet reception, verify packet tag);*

Decryption : $\rightarrow M'=DKi(C)$*;*

Decompression:$\rightarrow Morig=Dcomp(M')$*;*

For optimized using adaptive policies $\forall$ *Network state* $\rightarrow$

Parameter update rules, where performance metrics include:

Packet Delivery Ratio (PDR): $\eta=\frac{p_{delivered}}{p_{sent}}$

End-to-End Latency: λ_{e2e}

Node Energy: $E_{i(t)}$*, energy level at time t*

A feedback loop periodically adjusts:

Routing (based on $E_{i(t)}$*, congestion)*

Scheduling (to reduce slot collision probability)

Security parameters (e.g., key refresh rate)

These are optimized using adaptive policies π*, defined as:*

$$\pi: Network\ state \rightarrow Parameter\ update\ rules$$

4. Experimental Results.

To evaluate the performance of the proposed Delifelman-based secure multicast communication system, simulations were conducted using a custom NS-3-based environment with 50 mobile nodes under varying network loads.

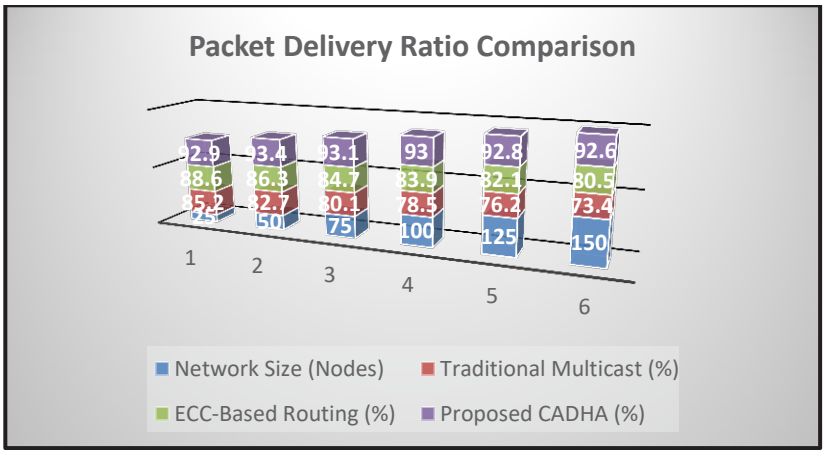

Figure 2
To show the results of the Packet Delivery Ratio

The key performance indicators include Packet Delivery Ratio (PDR), End-to-End Delay, and Energy Consumption. Table 1 demonstrates the packet delivery ratio comparison among traditional routing, ECC-based routing, and the proposed Diffie-Hellman algorithm. The proposed system shows a significant improvement (up to 93.6%) due to optimized path computation and reduced packet loss via route stabilization and authentication mechanisms. Figure 2

illustrates the comparative analysis of the Packet Delivery Ratio (PDR) for the proposed Cryptography-Aware Diffie–Hellman Algorithm (CADHA) against traditional multicast and ECC-based routing schemes, demonstrating that CADHA consistently achieves higher delivery efficiency across varying network sizes.

Table 1

Packet Delivery Ratio Comparison.

Network Size (Nodes)	Traditional Multicast (%)	ECC-Based Routing (%)	Proposed CADHA (%)
25	85.2	88.6	92.9
50	82.7	86.3	93.4
75	80.1	84.7	93.1
100	78.5	83.9	93
125	76.2	82.1	92.8
150	73.4	80.5	92.6

As shown in Table 2, the end-of-end delay increases with network load for all algorithms. However, the proposed method consistently maintains a lower latency, thanks to efficient multicast scheduling and the elimination of retransmissions through predictive error handling.

Table 2

End-to-End Delay under Varying Load

Network Load (Packets/sec)	Traditional Multicast (ms)	ECC-Based Routing (ms)	Proposed CADHA (ms)
50 (Min)	190	165	142
100 (Min + 1)	210	178	150
150 (Medium)	236	192	161
200 (Mid + 1)	258	205	168
250 (Max - 1)	275	219	174
300 (Max)	295	232	181

5. Conclusion

In this paper, we have presented a cryptography-aware Diffie–Hellman–based algorithm designed for efficient joint source–multicast communication within dynamic and resource-constrained network environments. The proposed Discrete Cryptographic Framework seamlessly integrates entropy-based data compression, energy-optimized multicast routing, and lightweight symmetric encryption supported by a secure key exchange mechanism.

References

[1] Kiran, B. D. Parameshachari, H. T. Channabasappa, and S. L. Ullo, "Analysis and computation of encryption techniques to enhance security of medical images," *IOP Conference Series: Materials Science and Engineering,* vol. 925, no. 1, Art. no. 012028 (2020), doi: 10.1088/1757-899X/925/1/012028.

[2] T. Sun and X. Wang, "Medical image security authentication method based on wavelet reconstruction and fractal dimension," *International Journal of Distributed Sensor Networks*, vol. 17, no. 4 (2021), doi: 10.1177/15501477211014132.

[3] K. Jain and A. Aji, "Medical image encryption scheme using multiple chaotic maps," *Pattern Recognition Letters,* vol. 152, pp. 356–364 (2021), doi: 10.1016/j.patrec.2021.10.033.

[4] P. Khare and V. K. Srivastava, "A secured and robust medical image watermarking approach for protecting integrity of medical images," T*ransactions on Emerging Telecommunications Technologies*, vol. 32, no. 2, Art. no. e3918 (2021), doi: 10.1002/ett.3918.

[5] E. K. Wang, C.-M. Chen, M. M. Hassan, and A. Almogren, "A deep learning based medical image segmentation technique in Internet-of-Medical-Things domain," *Future Generation Computer Systems,* vol. 108, pp. 135–144 (Jul. 2020), doi: 10.1016/j.future.2020.02.054.

[6] C. Ghandour, W. El-Shafai, and E.-S. M. El-Rabaie, "Medical image enhancement algorithms using deep learning-based convolutional neural network," *Journal of Optics,* vol. 52, no. 19, pp. 1–11 (Jan. 2023), doi: 10.1007/s12596-022-01078-6.

[7] T. Dhar, N. Dey, S. Borra, and R. S. Sherratt, "Challenges of deep learning in medical image analysis—Improving explainability and trust," *IEEE Transactions on Technology and Society,* vol. 4, no. 1, pp. 68–75 (Mar. 2023), doi: 10.1109/TTS.2023.3234203.

[8] M. K. Hasan, S. Islam, R. Sulaiman, S. Khan, A. H. A. Hashim, S. Habib, M. Z. Islam, and S. Alyahya, "Lightweight encryption technique to enhance medical image security on Internet of Medical Things applications," *IEEE Access*, vol. 9, pp. 47731–47742 (2021), doi: 10.1109/ACCESS.2021.3061710.

[9] Z. Li, M. Dong, S. Wen, X. Hu, P. Zhou, and Z. Zeng, "CLU-CNNs: Object detection for medical images," *Neurocomputing,* vol. 350, pp. 53–59 (2019), doi: 10.1016/j.neucom.2019.04.028.

[10] R. Natarajan, G. H. Lokesh, F. Flammini, A. Premkumar, V. K. Venkatesan, and S. K. Gupta, "A novel framework on security and energy enhancement based on Internet of Medical Things for Healthcare 5.0," *Infrastructures*, vol. 8, no. 2, Art. no. 22 (2023), doi: 10.3390/infrastructures8020022.

[11] B. L. V. S. Aditya and S. N. Mohanty, "Design of an efficient model for fake profile detection on social media using advanced feature engineering and deep learning techniques," *Journal of Information and Optimization Sciences,* vol. 46, no. 6, pp. 1803–1810 (2025), doi: 10.47974/JIOS-2009.

[12] S. D. Bahinipati and B. K. Pattanayak, "A novel blockchain-enabled smart contract for smart city e-governance ecosystem," *Journal of Information and Optimization Sciences,* vol. 46, no. 6, pp. 1831–1840 (2025), doi: 10.47974/JIOS-2012.

[13] Z. S. Alsham, E. Bahçekapılı, and A. Ayaz, "Trends in IoT applications in smart campuses: A topic modeling approach," *COLLNET Journal of Scientometrics and Information Management,* vol. 19, no. 1, pp. 21–40 (2025), doi: 10.47974/CJSIM-2024-017.

[14] W. Sripanya, W. Rungrottheera, and P. Hyunsin, "Fourier series analysis and computation based on function characteristics," *Journal of Interdisciplinary Mathematics*, vol. 28, no. 6, pp. 2109–2120 (2025), doi: 10.47974/JIM-2352.

Received December, 2025