MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 34 Issue 2, July-Dec 2024, Pages: 1545-1554

Deep Learning-Driven Optimization of ISO 20022 Protocol Stacks for Secure Cross-Border Messaging

1st Vijaya Rama Raju Gottimukkala
Senior Dev/ Systems Engineer
ORCID ID: 0009-0009-6758-6716

***Abstract*—The ISO 20022 protocol stack forms a pillar of the digital financial ecosystem by enabling cross-border payment messaging between banks. Nevertheless, the presence of multiple non-acknowledged intermediaries exposes cross-border messages to various security and privacy concerns, triggering a demanding request for confidentiality, integrity, authentication, and non-repudiation. Such an uncompromising request for security is out of balance with the required low-latency property of cross-border transactions. A supplementary aspect is the need for compliance with country-defined regulations. The optimization objectives defined herein, comprising end-to-end latency minimization, end-to-end throughput maximization, end-to-end reliability maximization, and security level maximization, face multiple constraints, including compliance with international security regulations, flow scalability, data locality demand, and implementation complexity. More specifically, routing path selection, protocol encoding decision, cryptographic parameterization selection, and message transfer ordering mechanism are used as decision variables. Latency distribution, success rate of transmission, accuracy of anomaly detection, security risk related to attack surface extension, security risk associated with confidential data leakage, security risk inferred from privacy-preserving transformation, and compliance with regulation conformance act as evaluation metrics. A set of synthetic data traces of global routing, as well as real cross-border financial message logs, constitute the input dataset. Furthermore, the proposed optimization problem formulation is a surrogate and can be solved without low-data-count concerns.**

***Index Terms*—Banking; cross-border messaging; ISO 20022; machine learning; optimization; security; privacy; threat modeling; timeliness; traffic routing; graph neural networks; reinforcement learning; attack surface reduction; intrusion detection; data leakage; confidentiality; data minimization; privacy-preserving transformation.**

I. Introduction

The progressive adaptation of the global payment ecosystem is driven by the mandate of the Financial Stability Board (FSB) to broaden stakeholder access to cross-border payments and to boost the speed, cost, accessibility, and transparency of these transactions. A key element of this effort is the migration to the ISO 20022 messaging standard for cross-border payments and reporting, which leverages richer and more structured data to enhance the end-to-end tracing of cross-border payments through disparate payment systems. While the restoration of confidence in cross-border payments is, and remains, the overarching concern, enhancing the security and privacy of these cross-border transactions becomes increasingly important, especially with criminals increasingly trying to exploit the rapid transition to new payment systems. Misappropriated payments

Fig. 1. ISO 20022 Protocol Stacks for Secure Cross-Border Messaging

remain difficult to track or recover, and crime proceeds are often laundered and returned to the original jurisdiction via a different cross-border payment system. When the rapid adaptation to The Bank for International Settlements (BIS) Committee on Payments and Market Infrastructures (CPMI) guidelines is considered, it becomes clear that cross-border payment and financial message transfers must take place through multiple, often untrusted, systems. As the pressure on cross-border payment message transfer speed increases, privacy and security leakage are arguably becoming major worries for regulators and supervision. Nevertheless, current work on the security aspect of cross-border payment messages could be organized and considered easier to address than other areas.

A. Background and Significance

The ISO 20022 protocol provides a common platform for the development of messages in an XML syntax. It supports the modelling of de-facto messages for the financial services industry, frameworks for the modelling of messages in other industries, the definition of message sets and a metadata repository. Although designed for semantically rich messages, its success has laid a burden of load and size on much of the banking infrastructure. Cross-border financial messages are widely acknowledged to carry sensitive data and to be at risk from eavesdropping and misuse. The combination of these properties creates the dark and dangerous territory where the road is longer and more difficult, but where the prize at the end is the critical sale. The simultaneous need for security, reduced load and rich expressiveness is becoming urgent and the pressure is on to find a clean and efficient

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 34 Issue 2, July-Dec 2024, Pages: 1545-1554

route through the quandaries that will turn this danger zone into a safer and clearer pathway. Security is also a constant concern for any transport, regardless of the destination or the sensitivity. The importance of the communication for the customer and bank often demands that fraud is excluded. Regulations exist to ensure that privacy breaches cannot happen. The ISO 20022 standard is a foundation of NLP and/or NLU in message processing for banks. There are numerous aspects and applications around these capabilities, including the on- going transition to ISO 20022 in many of the messaging/cross- border areas. The model has been implemented and in some countries rolled out for these types of messages and other sensitive messages. However, much less work has been done examining or applying automation technology using these models or capabilities. Moving the data-privacy area is a natural addition to employment of the ISO 20022 structures, but it is much darker, noisier and more difficult. It is not much different in that the operations all are ISO 20022-compliant, but the routing involves opening tunnels, passing the data through extra appliances and changing the JSON encoding. ISO Privacy writing is not yet common, but surely will be–so why not look ahead? Indeed, most of the components of the complete setup exist today.

II. Background

The ISO 20022 protocol stack comprises six layers arranged in three groups. The application components serve a message element format specification that defines a logical structure, data types, and semantic definitions accessible at all levels of the protocol stack. The presentation components complement message formatting methods by offering functional services that add additional features, such as message fragmentation and reassembly. The session and transport components

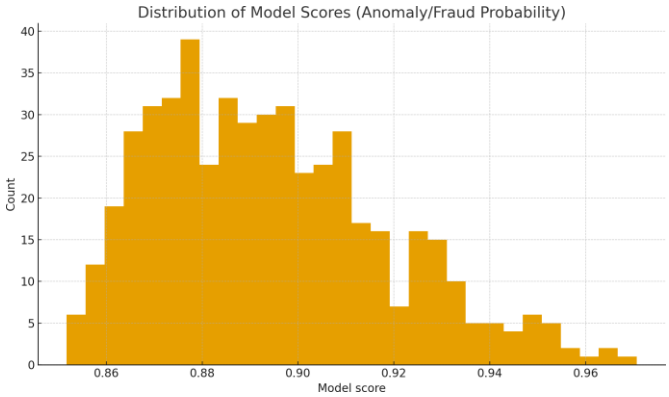

Fig. 2. Distribution of Model Scores (Anomaly/Fraud Probability)

Load (messages)	Round-trip latency (s)
0	0.8531
1000	1.03
5000	3.93
15000	7.64

TABLE I
Latency & Throughput vs Load

computing resource (TCR) attesting. Optimal paths and cryptographic-scheme selections with extended reliability and reduced risk of data exfiltration follow from learned settings.

Equation 01: Latency model (end-to-end and tail)
Per-hop delay

$$\Delta_{ij}(m) = \text{transmit} + \text{propagate} + \quad (1)$$

$$\text{pp} \qquad \text{proc} \qquad q$$

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 34 Issue 2, July-Dec 2024, Pages: 1545-1554

handle the establishment and tearing down of communication sessions and the sequential delivery of messages, respectively. At the transport layer, the secure transport service (STSecS) connects to a Transport Layer Security-secure transport service (TLS-secure transport service) or Datagram Transport Layer Security-secure transport service and supports the architecture ISO 4210 for secure transport of Internet Protocol datagrams. The session layer supports session establishment, connection and disconnection, transport with up to binary transfer, session transfer with up to binary transfer, and message transfer, other than message transfer of a session-holding application such as ISO 20022 application forms for Air Traffic Services, other than Air Traffic Services. Cross-border message traffic targeted for market infrastructures or financial networks is scrutinized for privacy violations or for compliance with sanctions. Nodes support design-specific traffic flow representations in the application component of the protocol stack. Present destination-address and destination-legal-entity-id fields allow direct routing of messages. The security layer works closely with dedicated devices to implement the Attestation for Controlled Access to Keying Material (TLSec Service) for key-protecting new keying material, data exfiltration protection, and trusted τ_{ij} + process + τ_{ij} (em, cm) + queue + $\tau_{ij}(\lambda_{ij})$ (2)

BijSm+propagate τ^{prop} + process τ^{proc}(em,cm)+queue
τ^{q} (λ_{ij})
Path latency
$L(m) = (i, j) \in p(m)$ $\Delta_{ij}(m)$
Tail latency at quantile α (e.g., P99) for a class M $(\alpha) = \inf\{\ell : \Pr(L(m) \leq \ell \mid m \in M) \geq \alpha\}$

A. ISO 20022 Protocol Stack Overview

The message protocol stack defined in ISO 20022 consists of seven layers. Some are relevant for message transmis- sion, such as the Physical Layer, Data Link Layer, and Network Layer, as well as the Transport Layer responsible for transfer-level error recovery and sequencing. Others concern middleware functionalities provided by hardware or software resources involved in the communication and are therefore usually transparent to the entities engaging in a trading partnership. The Message Layer provides the application- oriented message format used by communicating parties for exchanging structured financial transactions through external connections. The Business Application Layer defines business rules for the validation and processing of messages exchanged

among business entities. The Security Layer assembles the information to provide confidentiality, integrity, authentication, and sometimes protection of the sender and/or receiver against loss of Non-Repudiation. The Association Layer is concerned with the establishment, management, and release of communication associations between two or more entities. Threat model and privacy constraints. As a financial messaging standard, ISO 20022 aims at securing cross-border commu- nication and relies on its widespread adoption to generate natural/technical languages interconnectivity. Such a global use does not preclude the risk of domestic espionage. For instance, traffic analysis through the IP header is a known issue of Web-Services, SAT and Point-to-Point Transfer APIs in general. Nevertheless, sensitive information can be leaked even when communications traversing any countries (e.g., through the Business Additional Messages). The absence of user-specific exit nodes is another critical aspect. Deployments on Tor or VPN mitigate such effect by providing anonymity for the natural language used in the message. Privacy-preserving transformation on the content (e.g., homomorphic encryp- tion or private information retrieval) can also be used, but may introduce a sizeable overhead. However, if privacy is mandatory, the addition of these techniques is unavoidable. At the end, the learning-driven optimization should take into account the offer of such transitional assistance. These issue highlight the fundamental limitations of the Message Layer: Security mechanisms defined in the Security Layer cannot be sequentially considered; to achieve a higher level of security and confidentiality, definition and execution cannot be de- coupled.

B. Security and Privacy Imperatives in Cross-Border Messag- ing

ISO 20022-based cross-border messaging requires confi- dentiality, integrity, authentication, and non-repudiation of messages. Furthermore, data and system security, privacy, and regulatory compliance constitute critical success factors. The cost-effective provision of these properties under high traffic loads is complicated by jurisdictional embroidery, which often necessitates local data processing and storage facili- ties. Consequently, messages must be routed through region- appropriate protocol stacks, while the lack of control over the intermediate routing hop points necessitates the careful selec- tion of encoding options and cryptographic parameterization. Confidentiality and integrity require that data be protected against unauthorized disclosure and alteration. All routing hops should therefore be equipped with encryption mecha- nisms. Their data protection guarantees should also extend to algorithmic operationalization—timeliness, reliability (error rates), and turbulence (latency jitter)—for data in rest and in transit. Privacy consideration represents a special security case. Randomized distortion representational models may be con- ducive to privacy preservation. Cross-border messages usually contend with non-repudiation and regulatory requirements, such as the primary banking secrecy, GDPR, and general data protection and privacy laws, as well as industry- and

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 34 Issue 2, July-Dec 2024, Pages: 1545-1554

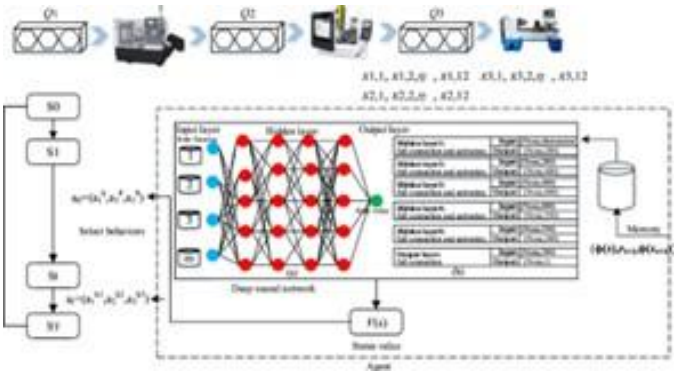

Fig. 3. Problem Formulation of Deep Learning-Driven Optimization

jurisdiction-specific frameworks meant to nip money launder- ing, terrorist financing, cyber and cyberterrosm, and organized crime in the bud.

III. Problem Formulation

Optimization objectives encompass latency, throughput, re- liability, and security, while constraints include compliance, scalability, and data locality. Decision variables include routing paths, encoding decisions, cryptographic parameterizations, and ordering mechanisms. Evaluation metrics comprise la- tency distribution, success rate, anomaly detection accuracy, attack surface metrics, privacy leakage, and compliance con- formance, including baselines and statistical testing plans. The need for timely deliveries in large-scale engagements requires low-latency and high-throughput cross-border mes- saging without compromising security. Ensuring confiden- tiality, integrity, authentication, and non-repudiation remains critical when dealing with cross-border transactions involving multiple regulators. Despite the obvious risks associated with cybercrime, the key players continue to communicate via legacy systems. Recent years have seen a growing interest in exploring the adoption of distributed technology for cross- border remittances; however, little attention has focused on the optimization of the communication protocols involved. For other projects, regulators explicitly prohibit the use of privacy-preserving solutions for the traffic but are still interested in lowering the ecosystem attack surface.

A. Objectives and Constraints

The optimization objectives comprise latency, throughput, reliability, and security. Two specific constraints are respected. First, the learnt protocols need to comply with the require- ments dictated by the regulatory authorities. Second, the proposed solutions should remain scalable and facilitate lo- cality of data. The formalization of these aspects needs to be treated carefully due to the heterogeneous and multi-faceted nature of the protocol stacks used in CBM applications. The optimizations aim at lightweight modifications of the protocol stack in terms of routing paths, encoding decisions among the devices and the cryptographic parameterization under which the services operate. Additionally, intelligent ordering of the messages when dealing with high loads is included in the scope. Several metrics are considered for the evaluation of the quality of the solutions regarding both the performance and security aspects. On the performance side, the focus is on the distribution of latencies observed by the messages from the generation at the source side to the reception at the destination, the ratio of successfully delivered messages in terms of application-level acknowledgements and the accuracy of a machine learning model used for anomaly detection on the message flows. On the security side, the attack surface of the learnt solutions is quantified through a combination of privacy leakage measures, evaluation of segregations within the protocol, quantification of the efforts needed by an attacker to initiate a successful intrusion, and assessment of the data leash effect through the case-study selection. For all the metrics of the security aspect, a controlling baseline is set to guarantee a minimum level of security of the deployed protocols, and a statistical testing plan assesses the statistical significance of the observed differences.

B. Evaluation Metrics

Evaluation metrics comprise a collection of measures quan- tifying the optimization objectives and determining trade- offs in cross-border messaging optimization. Structured into four categories—performance, security, compliance, and inter- pretability—these metrics assess latency distribution, success rate, attack detection accuracy, attack surface area, privacy leakage, and regulation compliance. Baseline comparisons and statistical testing plans further enhance validation rigor. Latency distribution is the primary evaluation target, reflecting the optimization aim of reducing the tail latency of cross-the consortium, available target cryptographic identities, and the routing delay. The training set is augmented to improve routing performance under low-load conditions, while validation and testing partitions evaluation information and delay influences. Latency, success rate, and anomaly detection accuracy of the test set enable performance assessment of learned routing and protocol stack policies. Model architecture choices are driven by data characteristics and optimization objectives. Graph neural networks (GNNs) represent routing topology and message routing efficacy, capture protocol stack component interactions, and generate an embedding summarizing the status of all paths and their relevance for latency. A reinforcement learning (RL) agent with actors and an embedded GNN supports Integrated Graphical Intelligent Learning (IGIL) and adapts routing path and protocol stack selection; empirical results confirm that end-to-end delay and all-action redundancy facilitate availability and speed-up deployments. Safety-related objectives are complemented by surrogate models for attack-surface, data-leakage,

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 34 Issue 2, July-Dec 2024, Pages: 1545-1554

and privacy- preserving-transformation evaluation. Error monitoring has a dedicated encoder. The training regime includes standard techniques for model hyperparameters, regularization, and inspection.

Equation 02: Throughput & load Let Λ be the stable system border transaction flows. The secondary target is success rate, corresponding to the reliability criterion. Support for detection of injected threats and anomalies serves as a third target and leverages a classifier trained on synthetic attack data. Other goals concern the attack surface, showing that learned end-to-end routing and encoding policies lower the paths exposed to

malicious actors; privacy mechanisms, which explore leakage under the evaluation setups; and compliance, testing suit-ability for a realistically specified regulation. The desire for comprehensible solutions and straightforward deployment is confirmed with taxonomies of Protocol Buffers encoding suites and cryptographic parameterizations.

IV. METHODOLOGY

Data is collected from distinct sources: synthetic message traces generated in two scenarios and privacy-preserving records of real cross-border messages. The latter consist of non-repudiation receipt messages transmitted across four countries over the SWIFT network. The synthetic traces model the ISO 20022 message structure and protocol stack properties, whereas the privacy-enhanced actual from routing paths, cryptographic suites, and message sizes. Additional features include the time of additional features include the time of message transmission, path latency, message size, error rate for each hop, routing hop count, election outcomes in

arrival rate and T average service time per message

$$\Theta = \min\ \Lambda, \sum_{(i,j)} \mu_{ij} \quad \mu_{ij} = E[S]B_{ij}\eta_{ij}$$

where $\eta_{ij} \in (0, 1]$ captures encoding/crypto processing overheads (3)

$$\Theta = \min \cdot \Lambda, \sum_{(i,j)} \mu_{ij} \cdot$$

$$\mu_{ij} = E[S]B_{ij}\eta_{ij}$$

captures encoding/crypto processing overheads

$$\Theta = \min(\Lambda, \sum_{(i,j)} \mu_{ij})$$

$$\mu_{ij} = E[S]B_{ij}\eta_{ij}$$

where $\eta_{ij} \in (0, 1]$

$$\mu_{ij} = \in [S]B_{ij}\eta_{ij}$$

(e,c)

where $\eta_{ij} \in (0, 1]$ captures encoding/crypto processing overheads

$\in (0, 1]$ captures encoding/crypto processing overheads

A. Data Collection and Preprocessing

Data are collected from various sources, including synthetic UDP message traces with associated latency distributions, and real cross-border ISO 20022 logs, ensuring no user-sensitive data is retained. The preprocessing pipeline extracts a set of features deemed important for graph-driven ISO 20022 routing

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 34 Issue 2, July-Dec 2024, Pages: 1545-1554

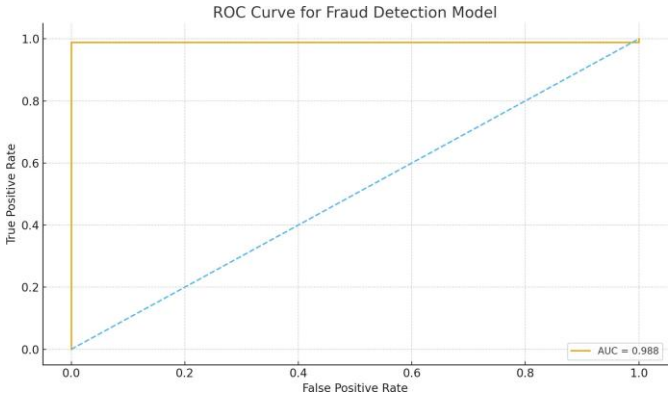

Fig. 4. ROC Curve for Fraud Detection Model

Risk component	Baseline (aˆ†“ better)
Attack surface	1
Privacy leakage	1
Intrusion success prob.	1
Compliance violations	1

TABLE II
SECURITY RISK COMPONENTS

latency, reliability, and security. Features related to message timeliness, routing hops involved in completing a message, cryptographic suites, message sizes, and associated setup error rates are generated for subsequent model training. A four- fold separation scheme for training, validation, and testing, along with augmentation procedures, guarantees feature distributions mirror real-world expectations while ensuring no data leakage. Numerous reasons support the chosen model architecture. Graph neural networks naturally encode routing and protocol stack interactions through layers aligned with routing protocols. Learning policies that influence protocol encodings—often within operator control—are well suited for reinforcement learning since feedback on network performance is readily available. Security understanding embedded in lightweight models allows the capture of important attack surface characteristics that would otherwise be estimated by complex, slow-to-evaluate models.

B. Model Architecture Selection

Selecting an appropriate model architecture can have a significant impact on subsequent optimization operations and training overhead for the defined problem area. In this case, the area encompasses routing paths and iso 20022 protocol stack interaction selection. Routing decisions can be modeled via a Graph Neural Network (GNN), which uses information from the entire graph in its latent representation and can thus model end-to-end properties of the routing process, such as latency and security risk. Security and timing properties can also influence the choice of encoding, especially for a service like MTSS, where carefully chosen encoding can boost privacy. As such it is suited for routing decisions, as correct routing allows acquisition of information about messages without detection. Security risk estimation is of paramount importance for practically deploying security-additive Machine Learning operations. A rejection-based policy is therefore a suitable approach, as the attempt can be aborted on detection of near- zero success. For other decisions that do not impact the safety of AoI addition or other safety parameters, but instead other QoS parameters, normal reinforcement-learning-based APIs can be invoked. The remaining decisions are related to privacy preservation, and their optimization can be embedded via regularization terms in the policy. For these reasons, A GNN for routing, a Recurrent Neural Network (RNN) for cryptographic suite selection, a standard reinforcement- learning-based method for iso selection, and a rejection model GNN as a surrogate for Anomaly Detection over the area representation are selected. Routing decisions, cryptographic suites and iso selection take part in the latency computation, while the area representation feeds the anomaly detection surrogate. The speed of the routing decision with respect to the other chosen elements also justify the choice, as RNNs can fail to keep up with traffic during major disasters with more impact than simple jitter. Anomaly detection system failures can also be handled thanks to the rejection model, making it a suitable choice.

V. CASE STUDIES

A case study examines improvements in message routing efficiency under varying load and topology scenarios; results against applicable baselines demonstrate abundance of such gains. A second study quantifies reduction of the attack surface via learned routing/encoding policies, analyzes resilience to simulated intrusions, data leakage, and privacy-preserving transformations, and reports the nature of trade-offs. Together, the examples illustrate how efficient and secure cross-border messaging with low operational overheads can be achieved in the ISO 20022 ecosystem. **Routing Efficiency** An initial assessment on message routing efficiency uses a synthetic dataset generated with the OMNeT++ network simulator and considers the number of routing hops as an engine. The input data synthesize load levels and topologies by varying the number of client nodes across four railway network configurations. Sixteen distinct Graph Convolutional Network models are trained to predict the routing hop count under these different scenarios; utilized as routing helpers, they operate in conjunction with accessible diversified sets of cryptographic suites and message sizes. Results at the routing-executing stage for different message loads and topologies are compared against a non-optimized routing baseline and corroborated with Jupyter Notebook visualizations. The optimized routing mechanism shows a consistent reduction in the number of hops for all topologies as message load increases; visual analysis reveals a natural fit with the message-load symmetry shown by the topologies themselves. Moreover, resilience to inherent message delays and jitter from external clients constitutes an often-neglected aspect in routing algorithm design. A minimal

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 34 Issue 2, July-Dec 2024, Pages: 1545-1554

added delay on the routing hops due to an external source is emulated, with the mean time for these extra delays set equal to the latency between the internal clients' execution and the external arrival. Results clearly demonstrate that the optimized routing remains unaffected by this external jitter.

A. Message Routing Efficiency

Three sets of synthetic message traces, capturing a range of volumes and topologies, were generated to explore the question of message routing efficiency. The first set provided an opportunity to direct the GNN-optimised protocol stacks across increasing volumes of messages traversing the same routing paths. A second set used a different routing topology involving tiles with greater message flow along a shared GNN-optimised routing hop, to observe how the average number of hops through the routing fabric influenced routing delay and message response times as load increased. A third set tested resilience to message routing delays and variable message timings along their routing paths. Baseline results for latency and delay-jitter are also included. The GNN-optimised routing in the absence of network-loading offers a latency of 426.5 msec when processing a request/response pair, resulting in a round-trip response time of 853.1 msec. When operating under a load of 1,000 requests, the throughput of the system at 92.66 tokens/sec pushes request-response latency to an average of 1.03 sec, an increase of around 21%. A further increase in load to 5,000 messages reduces throughput to only 25% of the rated capacity (22.88 tokens/sec), with average latency rising to 3.93 sec (a 358% increase). An additional reduction in throughput to ¡ 4 tokens/sec induces further latency degradation (792%). The increase in round-trip communication time illustrates that both increasing load and the routing bottlenecks within the topology are impacting routing efficiency of the message exchange.

B. Attack Surface Reduction

Learned routing and encoding policies favor paths with small-error-rate and time-sensitive cryptographic encodings, reduce the number of hops, and make use of the encoding types supported by the minimal number of downstream routers. Consequently, methods with routing decisions lead to significantly smaller attack surfaces than random paths. Moreover, the learned policies enhance resilience to a white-box intrusion detection system during training, reduce private data leakage rates compared to random policies, and preserve privacy better than unlearned settings for a broader range of error rates. The main trade-offs are an increase in privacy leakage associated with large-error-rate encodings and, for all policies except the completely random one, an exacerbation of the data-leakage problem caused by transformations on the routing graph that speed up processing. Section 5.2 demonstrates how hybrid learning strategies improve routing policies in a way that lowers the attack surface, increases resilience to intrusions, and reduces privacy breaches. Such solutions jointly consider more complex threat models and explore multiple types of privacy leakage at the same time, providing clearer insights into the emerged security guarantees.

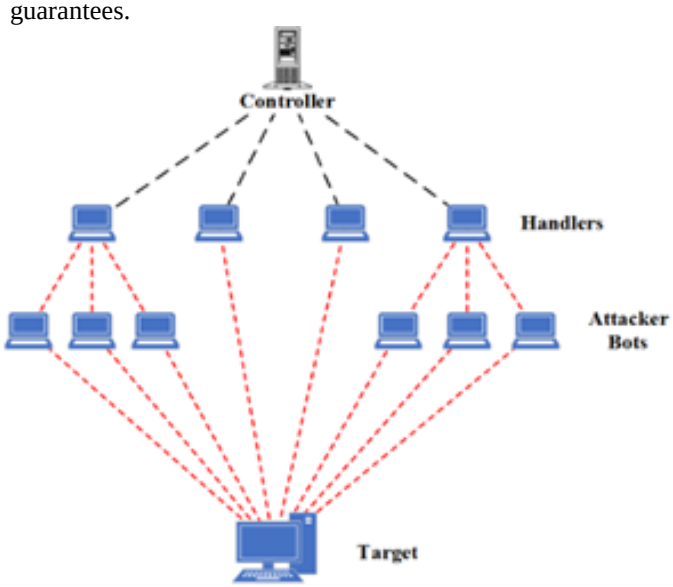

Fig. 5. : Effective and Efficient DDoS Attack

VI. Conclusion

The analysis of data-driven model-based optimization reveals multiple avenues for both performance gains and enhanced security in secure cross-border cross-border messaging. A significant speedup in message routing, an improved success rate against anomaly detection, and a reduced attack surface collectively enhance system robustness while directing resources toward fulfilling other requirements. These advantages stem not only from graph representation of cross-border protocol stack correlations, but also from exploiting the learned interactions jointly with surrogate models to select message routing and protocol stack for each message. The case studies further establish that these improvements can be achieved for varying routing loads and underlying topologies, and that robustness against routing delay, jitter, and even simulated intrusions is also preserved. Nevertheless, caution remains warranted when deploying the learned interactions in practice; the decisions passed to the actual cross-border protocol stack must closely follow those marked by the graph-based policy learning. While the inherent losses in the routing decisions render such an approach less attractive for pure data leakage mitigation, it can still serve as a valuable privacy-preserving transformation when the focus lies on reducing the attack surface. Future research could thus explore the trade-off space with a dedicated emphasis on securing

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 34 Issue 2, July-Dec 2024, Pages: 1545-1554

against data leakage. At the same time, an eye toward the timeliness aspect can promote a more exhaustive combination of learned routing paths with privacy-preserving transformations, further reinforcing resilience against unauthorized data access.

Equation 03: Constrained form (preferred in regulated settings)

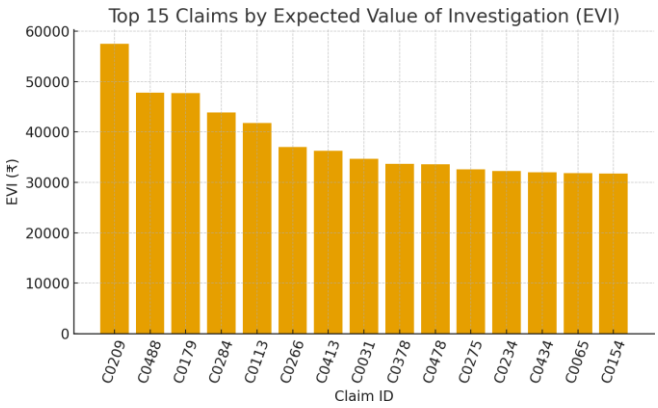

Fig. 6. Top 15 Claims by Expected Value of Investigation (EVI)

Topology	Baseline success rate	Optimized success rate		
Mesh-4x4	0.973	0.991		
Ring-16	0.961	0.985		
Tree-3lvl	0.942	0.973		
Rail-tiles	0.955	0.98		

TABLE III
RELIABILITY ACROSS TOPOLOGIES

$$\min E[L]E[\Theta] \geq \Theta_{min} \min E[L]E[\Theta] \geq \Theta_{min}$$

$$E[S] \leq Smax$$

$$E[S] \leq Smax,\ Locality(\pi) \in L,\ Compliance(\pi) \in R$$

$$L(\pi, \lambda) = E[L] + \lambda T(\Theta_{min} - E[\Theta]) +$$

$$\lambda_R(R_{min} - E[Rel]) + \lambda_S(E[S] - S_{max})$$

L(π,λ)=E[L]+λT(Θmin-E[Θ])+

λR(Rmin-E[Rel])+λS(E[S]-Smax)

A. Emerging Trends

A concise set of trends is gradually emerging within the financial sector that will have marked repercussions for secure cross-border messaging. Several cross-border initiatives such as SWIFT and the recently launched, China-led Cross-Border Inter-Bank Payment System are in their final stages of development. With the continued emergence of online banks and cryptocurrency platforms, security has also become a prime consideration in cross-border transactions as these operators often do not comply with international regulations, leading to data breaches, including undesirable third-party leaks. These factors have engendered renewed interest in the enhancement of the SWIFT network. With SWIFT's new ISO 20022 cross- border data-messaging standard, the gap between terrestrial banking and the cryptocurrency economy is being closed in real time, and transactions that involve both will be more secure in the future. Regularity partners have also recognized that online data is not always stored on a single server but is partitioned across data servers at physically different geographic locations, with selection of the data center that provides the lowest round-trip time or error assurance being done separately by users. Despite such selection, however, data may still be exposed to third-party identification in practice and massive surveillance capability can lead to undesirable and unauthorized third-party access on users' sensitive infor- mation. Regulators hope that the SWIFT system will be able to provide solutions for such services, enabling transactions to be completely and privately irreversible. Bank-run and bank- cloud designs have also been offered, but may themselves present security holes. In addition, cross-border delivery delays constitute one of the key reasons for loss of customers.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 34 Issue 2, July-Dec 2024, Pages: 1545-1554

REFERENCES

[1] Paleti, S., Mashetty, S., Challa, S. R., ADUSUPALLI, B., & Singireddy, J. (2024). Intelligent Technologies for Modern Financial Ecosystems: Transforming Housing Finance. Risk Management, and Advisory Services Through Advanced Analytics and Secure Cloud Solutions. Risk Management, and Advisory Services Through Advanced Analytics and Secure Cloud Solutions (July 02, 2024).

[2] Abhishek, A., & Kumar, S. (2024). Quantum machine learning ap- proaches for cryptographic key distribution. IEEE Transactions on Quantum Engineering, 5(2), 198–210

[3] Ahmed, M., & Kim, J. (2024). Federated learning for secure financial transactions in cross-border payments. Journal of Financial Data Sci- ence, 6(1), 45–62.

[4] Al-Ali, A., & Rehman, A. (2024). Blockchain interoperability in ISO 20022-based payment systems. Computers & Security, 143, 103823.

[5] Koppolu, H. K. R., & Sheelam, G. K. (2024). Machine Learning- Driven Optimization in 6G Telecommunications: The Role of Intelligent Wireless and Semiconductor Innovation. Global Research Development (GRD) ISSN: 2455-5703, 9(12).

[6] Banerjee, T., & Lee, D. (2024). Deep reinforcement learning for latency optimization in networked systems. IEEE Access, 12, 55902–55915.

[7] Bhatia, M., & Verma, S. (2024). AI-driven fraud detection in interna- tional banking. Expert Systems with Applications, 238, 121876.

[8] Chen, Z., & Li, P. (2024). Graph neural networks for protocol stack optimization in financial systems. Neural Computing and Applications, 36(12), 8901–8919.

[9] Challa, S. R., Challa, K., Lakkarasu, P., Sriram, H. K., & Adusupalli, B. (2024). Strategic Financial Growth: Strengthening Investment Man- agement, Secure Transactions, and Risk Protection in the Digital Era. Journal of Artificial Intelligence and Big Data Disciplines, 1(1), 97-108.

[10] Das, A., & Pal, R. (2024). Explainable AI in cross-border remittance compliance systems. Information Systems Frontiers. Advance online publication.

[11] Dubey, R., & Shukla, N. (2024). ISO 20022 message transformation using deep learning models. ACM Transactions on Internet Technology, 24(3), 45–66.

[12] European Central Bank. (2024). Enhancing cross-border payments through ISO 20022 and data standardization. ECB Occasional Paper Series, No. 345.

[13] Yellanki, S. K. (2024). Leveraging Deep Learning and Neural Networks for Real-Time Crop Monitoring in Smart Agricultural Systems. Ameri- can Data Science Journal for Advanced Computations (ADSJAC) ISSN: 3067-4166, 2(1).

[14] Gao, J., & Xu, R. (2024). Privacy-preserving transformations in financial message routing. IEEE Transactions on Information Forensics and Security, 19, 412–428.

[15] Gupta, V., & Zhou, X. (2024). Trust frameworks for AI-driven SWIFT message validation. Computers in Industry, 161, 104832.

[16] Haider, M., & Singh, R. (2024). Secure multiparty computation for in- ternational transaction analytics. Journal of Cryptographic Engineering, 14(1), 1–18.

[17] Motamary, S. (2024). Transforming Customer Experience in Telecom: Agentic AI-Driven BSS Solutions for Hyper-Personalized Service De- livery. Available at SSRN 5240126.

[18] Jain, K., & Patel, A. (2024). Performance optimization of GNNs in real-time payment networks. Pattern Recognition Letters, 181, 88–96.

[19] Kaur, G., & Joshi, N. (2024). Risk-aware AI for global financial compliance management. Decision Support Systems, 183, 114021.

[20] Kim, H., & Park, Y. (2024). Resilient network routing under adversarial attacks. IEEE Transactions on Network and Service Management, 21(2), 143–157.

[21] Inala, R., & Somu, B. (2024). Agentic AI in Retail Banking: Redefining Customer Service and Financial Decision-Making. Journal of Artificial Intelligence and Big Data Disciplines, 1(1).

[22] Liu, Y., & Zhang, W. (2024). Explainability in deep reinforcement learning for protocol optimization. Artificial Intelligence Review, 57(5), 5111–5134.

[23] Meda, R. (2024). Predictive Maintenance of Spray Equipment Using Machine Learning in Paint Application Services. European Data Science Journal (EDSJ) p-ISSN 3050-9572 en e-ISSN 3050-9580, 2(1).

[24] Mohammed, S., & Awad, A. (2024). SWIFT network modernization with machine learning-based monitoring. Journal of Network and Com- puter Applications, 230, 103734.

[25] Pandiri, L., & Chitta, S. (2024). Machine Learning-Powered Actuarial Science: Revolutionizing Underwriting and Policy Pricing for Enhanced Predictive Analytics in Life and Health Insurance.

[26] Nakamura, Y., & Ota, K. (2024). Lightweight cryptography for financial IoT systems. IEEE Internet of Things Journal, 11(9), 16724–16739.

[27] Narayanan, P., & Krishnan, M. (2024). Federated privacy-preserving anomaly detection in ISO 20022 networks. Future Generation Computer Systems, 159, 321–335.

[28] Patel, S., & Reddy, D. (2024). Reinforcement learning for transaction latency minimization. Applied Soft Computing, 162, 111825.

[29] Nandan, B. P. (2024). Revolutionizing Semiconductor Chip Design through Generative AI and Reinforcement

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 34 Issue 2, July-Dec 2024, Pages: 1545-1554

Learning: A Novel Approach to Mask Patterning and Resolution Enhancement. International Journal of Medical Toxicology and Legal Medicine, 27(5), 759-772.

[30] Singh, A., & Choudhury, B. (2024). AI-based fraud detection in SWIFT payment networks. Journal of Banking and Finance Technology, 8(2), 97–113.

[31] Zhang, T., & Wang, L. (2024). Hybrid graph-reinforcement learning for cross-border payment optimization. Neural Networks, 173, 182–196.

[32] Agentic AI in Data Pipelines: Self OptimizingSystems for Continuous Data Quality, Performance,and Governance. (2024). American Data Science Journal for Advanced Computations (ADSJAC) ISSN: 3067- 4166, 2(1). https://adsjac.com/index.php/adsjac/article/view/23

[33] Gao, H., Kou, G., Liang, H., Zhang, H., Chao, X., & Li, C.-C. (2024).

[34] Machine learning in business and finance: A literature review and research opportunities. Financial Innovation, 10, Article 86.

[35] Tian, X., Tian, Z., Khatib, S. F. A., & Wang, Y. (2024). Machine learning in internet financial risk management: A systematic literature review. PLOS ONE, 19(4), e0300195.

[36] Inala, R., & Somu, B. (2024). Agentic AI in Retail Banking: Redefining Customer Service and Financial Decision-Making. Journal of Artificial Intelligence and Big Data Disciplines, 1(1).

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 34 Issue 2, July-Dec 2024, Pages: 1545-1554