A Novel Adaptive Coding Technology for Reliable Transmission in Cross-Datacenter Networks

Jinbin Hu[1], Rui Yang[1], Xuchong Liu[2], Fayez Alqahtani[3], Jin Wang[4]*

[1] School of Computer & Communication Engineering, Changsha University of Science & Technology, China
[2] Department of Information Technology, Hunan Police Academy, China
[3] Software Engineering Department, King Saud University, Saudi Arabia
[4] School of Computer Science and Engineering, Hunan University of Science and Technology, China
jinbinhu@csust.edu.cn, hjshyangrui@stu.csust.edu.cn, 14117874@qq.com,
fhalqahtani@ksu.edu.sa, jinwang@hnust.edu.cn

Abstract

More and more service providers deploy applications in data centers connected by the wide area network (WAN). WAN makes these data center networks (DCNs) interconnected to a certain extent, but the security problems within the network are increasingly prominent. Especially when a malicious attack occurs, data transmission across data center network may lead to packet loss, resulting in adverse effects such as data transmission delay, low throughput and network bandwidth waste. In order to ensure the reliability of cross DCN traffic transmission under malicious traffic attack, a coding method is proposed to achieve low delay and high throughput of cross DCN information under malicious traffic attack. This method uses forward error correction (FEC) coding based on the traditional fountain code. Specifically, senders encode the original data into more coded packets than the original data, while receivers can recover the complete effective data even in the case of packet loss. In addition, the coding module will dynamically adjust the number of redundant packages according to the network conditions to alleviate congestion. NS-3 simulation results show that under malicious traffic attack, FEC coding can reduce the transmission delay by 35% and improve the throughput by 30% compared with the existing schemes.

Keywords: Data center network, FEC coding, Adaptive, Redundancy control

1 Introduction

Due to the rapid development of big data and cloud computing, many service providers have invested a lot of money in the construction of data centers around the world. In addition, with the increasing demand for applications from users around the world, many service providers deploy services on cross DCNs connected through WAN [1-2]. These data centers store a large amount of data and use it for transmission, replication, query and calculation purposes [3].

As these data centers are connected by WAN, the increasing volume and complexity of business operations on wide area network application information systems have led to many security threats [4]. On one hand, security issues may arise from internal network devices such as switches and routers (e.g., routing information leakage, network device configuration risks). On the other hand, security issues stem from numerous hacker attacks on the external network. Hackers exploit eavesdropping, probing, scanning, and other sniffing programs to discover potential security vulnerabilities in the network, thereby launching attacks.

Recent researches have focused extensively on malicious attacks. One aspect of researches involves identifying, classifying, and filtering malicious attack flows, including encrypted malicious traffic [5], using various methods such as Convolutional Neural Network (CNN) [6-7] and Deep Neural Network (DNN) [8-9], to mitigate attacks at their source. Another area of researches involves manipulating transmitted data, employing techniques like backup [10], retransmission, and TCP tail loss recovery mechanisms [11], to duplicate data packets or transmit them multiple times to prevent data loss. However, both the methods for detecting malicious traffic and those for operating transmitted data have certain shortcomings and limitations.

In this article, we propose a FEC coding [12] method based on fountain code to encode and transmit streams across data centers. This method aims to reduce the impact of packet loss caused by malicious attacks on networks across DCs and diminish the latency introduced by packet loss, thus achieving rapid convergence. The key of this approach is the sender that using Error Correcting Code (ECC) to redundantly encode the message. Even in the event of a malicious attack, the receiver can recover the lost message as long as it receives sufficient encoded messages, eliminating the need for retransmission. This effectively avoids congestion caused by malicious attacks and delays due to data return. Additionally, the transparent coding layer only requires deployment between the TCP and IP layers of the terminal host without modifying the existing TCP/IP protocol.

The main work of this paper is as follows:

*Corresponding Author: Jin Wang; Email: jinwang@hnust.edu.cn
DOI: https://doi.org/10.70003/160792642026032702006

1. The paper empirically demonstrates the various adverse effects caused by malicious attacks during data transmission across DCNs. Then a FEC coding method based on fountain codes is proposed to mitigate the adverse effects of attacks generated by malicious traffic. The sender redundantly encodes messages using error correction codes, so that even in the presence of malicious attacks, the receiver can recover lost packets as long as a sufficient number of encoded packets are received, thus avoiding the detrimental effects of packet loss.

2. We theoretically analyze the probability of successful decoding at the receiver and demonstrate, through network simulation, that the performance of the FEC coding method is significantly better than existing schemes, including DCTCP [13], GTCP, and GEMINI.

3. We discuss the effects of different grouping strategies of FEC coding on traffic transmission across DCNs.

The sections of this paper are organized as follows: Section 2 outlines the motivation for this study, Section 3 discusses the coding design, Section 4 presents the experimental results, Section 5 provides the conclusion and future work.

2 Motivation

(1) Analysis of limitations of current methods: There are many methods currently used to handle malicious attack flows in cross-DCNs. Whether filtering malicious attack flows from the source to avoid disrupting the transmission of normal flows, employing common retransmission measures to ensure data integrity at the expense of time, or adopting congestion control schemes between data centers to regulate reasonable transmission speeds and avoid packet loss [14], all of these approaches have their limitations.

First, in terms of malicious traffic detection methods, the detection success rate is a core indicator. Many mature commercial firewall products [15] have emerged at home and abroad, but they all have the disadvantages of limited protection rule state, poor readability and high maintenance cost. In addition, the traditional machine learning algorithm has relatively strict requirements on data sets, and needs to enumerate a large number of traffic characteristics, and it is easy to fall into local optimal solution [16-17]. In addition, in recent years, when the types and forms of malicious traffic are becoming more and more diverse and complex, CNN prediction methods are still limited to identifying a few types of attacks and cannot fully cover all scenarios [18]. Finally, in the high-speed DCN, it is challenging to achieve the required detection and feedback time [19].

On the other hand, backup may lead to excessive resource consumption and a large amount of bandwidth waste. Retransmission regards loss as congestion signal and controls the size of congestion window [20]. However, when a large number of retransmissions occur due to continuous packet loss, network congestion will be aggravated. The TCP tail loss recovery mechanism only reducing the time interval of retransmission timeout (RTO) cannot solve the delay problem caused by frequent error timeout and window reduction.

At the same time, in the research of congestion control between cross DCNs, whether GEMINI [21-22] dynamically adjusts windows and maintains low buffer occupancy through system integration of explicit congestion notification (ECN) [23] and delay signals to achieve high throughput, or latest suggestions of GTCP [24] on the difficulty of coordinating high utilization inter data center flows and low latency intra data center flows, these methods cannot effectively solve the problem of packet loss caused by malicious attacks. When a large number of malicious data packets pour in, Gemini's response time is very short, which makes it difficult to achieve reasonable dynamic window adjustment, and even leads to more serious link congestion. In addition, when malicious attacks occupy the entire link and packet loss occurs, the receiver driven mode adopted by GTCP will lead to more serious bandwidth waste and higher delay. Similarly, DCTCP is also a congestion control protocol specially designed for the DCN. By using ECN to provide more timely and accurate congestion feedback, it can realize the efficient utilization of network resources and reduce delay, so as to solve these challenges [25]. However, DCTCP has the problem of head end line blocking. As with the traditional TCP variant, the loss or delay of a single packet in the stream will lead to the suspension of subsequent packets, resulting in performance degradation and delay increase. Although DCTCP aims to alleviate this problem by quickly responding to congestion signals, it may not fully alleviate line congestion in all cases. Therefore, when malicious attacks lead to continuous packet loss, DCTCP will be in the congestion avoidance stage for a long time, significantly increasing the completion time of effective flow and reducing the throughput of effective flow within a certain period of time.

Finally, FEC code contains many codes, such as LDPC code, RS code, etc. Among them, the redundant encoding of LDCP code is in bits and its main function is to correct errors in transmitted data. Therefore, when packet loss occurs, LDPC code cannot reduce the number of retransmissions. RS codes are only suitable for short code units with a total number of bits less than 1000 and are not suitable for large-scale data transmission across data centers. Therefore, fountain codes in data packet units are the most suitable choice for cross data center transmission encoding in FEC codes.

(2) The impact of malicious traffic attack: To assess the harmfulness of malicious traffic attacks, NS-3 simulation was employed for experimentation. NS-3 simulation is a network simulator used to model network topology and execute various network protocols, thereby simulating the operational mechanisms of computer networks. Experiments were conducted on a double leaf-spine topology network, as depicted in Figure 1. This network comprises 2 hosts, 2 leaf switches, 3 spine switches, and 1 central switch.

The buffer size of each switch is set to 256 packets. Among them, S1 to S4 are sending nodes, and C1 to C4 are receiving nodes. The bandwidth of each path is 1Gbps, and the round-trip propagation delay is 100μs. In this

experiment, the FPT flow is set as the legitimate flow, while the CBR flow is set as the attack flow. The intensity of the malicious attack is controlled by adjusting the ratio of CBR flow size to FPT flow size.

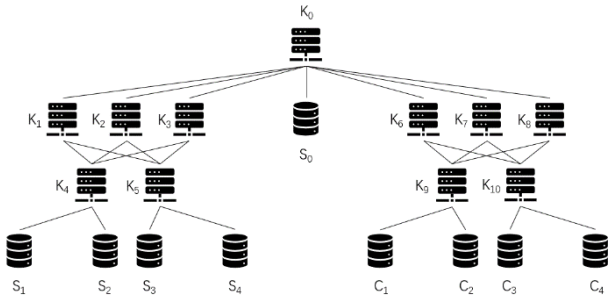

Figure 1. Double leaf-spine topology

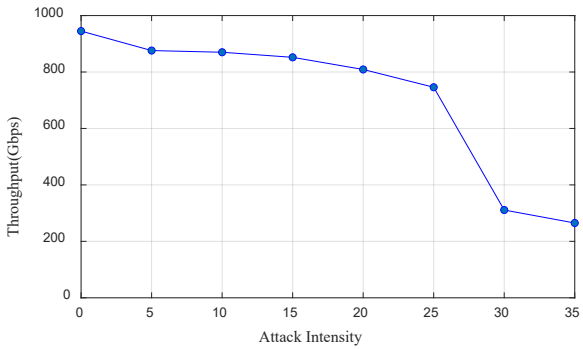

Figure 2. Relationship between throughput and attack intensity

From Figure 1, it can be seen that double leaf-spine topology networks are connected by switch K0. These two networks represent 2 DCNs, and the switch K0 and the links connected to it represent the wide area network connecting the data centers. Host S0 is connected to switch K0, representing the attacking host in WAN. In this experiment, the sending hosts S1 to S4 send legitimate data flows to the receiving hosts C1 to C4 respectively, with each flow size set to 100MB and each packet size set to 100KB. At the same time, host S0 randomly sends attack flows to the receiving hosts C1 to C4, with the intensity of the malicious attack increasing over time.

To demonstrate the adverse effects of malicious traffic attacks on DCNs, corresponding data collection and statistics were conducted at the senders, switches, and receivers. The number of packets sent at the senders was collected, the queuing rate of packets was monitored at the switches, and the throughput of legitimate flows was measured at the receivers. Since there are multiple senders, switches, and receivers, the collected statistical data are averaged by each flow. And these statistics are also averaged in the time dimension.

Figure 2 shows that the effective throughput at the receiving end continuously decreases with the increase in the intensity of malicious attacks. Throughput refers to the amount of data transmitted through the network per unit time [26]. It can be seen that as the attack intensity continues to increase, network congestion worsens, resulting in a decrease in the amount of legitimate traffic received by the recipient, thus leading to a reduction in effective throughput. When the attack intensity reaches 35, throughput decreases by approximately 78% compared to before the attack.

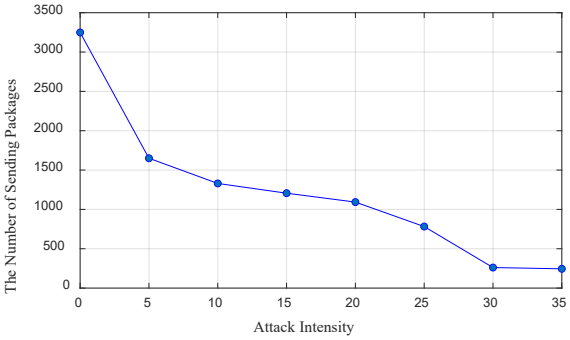

Figure 3. Variation of packet sending volume with attack intensity

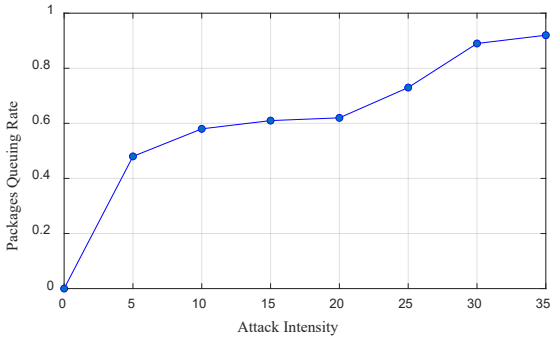

Figure 4. Variation of packet queuing rate with attack intensity

As shown in Figure 3, when the intensity of malicious attacks reaches 35, the number of packets sent by the sender significantly decreases, with the packet count dropping to around 200. That is because the sender to dynamically adjust the sending rate during data transmission to adapt to the network conditions while ensuring the reliability and efficiency of the network [27].

Similarly, Figure 4 reflects the relationship between malicious traffic attacks and packet queuing ratio, where the packet queuing ratio refers to the ratio of packets in the switch buffer to the packets being sent. From the figure, it can be observed that as the attack intensity increases, the packet queuing ratio sharply rises. When the intensity reaches around 35, the packet queuing ratio is very close to 1, indicating that the entire network is approaching a paralyzed state.

Based on experimental observations and systematic analysis, we conclude that both methods based on source-based malicious traffic detection and existing congestion handling methods have certain limitations.

3 System Design

3.1 Design Overview

FEC can timely recover lost packets by employing redundant packets, thereby enhancing transmission performance. Generally, adding a reasonable number of redundant packets can improve transmission reliability. Specifically, in the event of a malicious attack in the ross DCN leading to the loss of effective packets, the FEC coding method with redundant packets does not immediately trigger the retransmission mechanism. As long as the number of lost packets is smaller than the number of redundant ones, the original packets can be recovered, enabling the receiver to successfully receive the data. The framework of FEC coding is depicted in Figure 5.

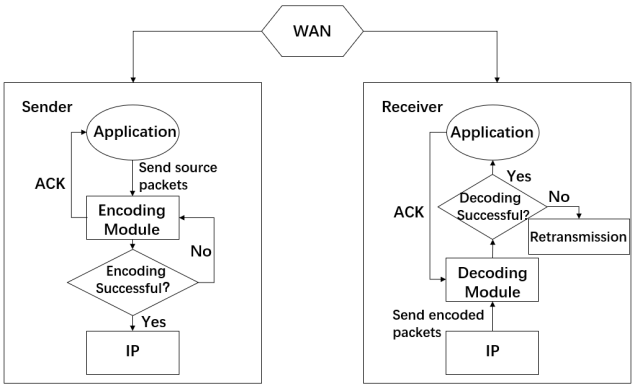

Figure 5. FEC coding framework

For senders, the source packets are passed to the encoding module for encoding. Within this module, an ACK is sent to notify the sender of successful receipt of the source packet. Upon receiving the ACK packet, the sender removes it and forwards it to the transmission layer. Subsequently, the senders generate $k + r$ encoded data packets through operations such as XOR summation on the k original data packets within the encoding module before transmitting them. It's noteworthy that in the coding process, r is not fixed, indicating that the number of redundant packets dynamically adjusts based on the real-time state of network traffic.

For receivers, the decoding module receives coded packets from senders and decodes $k + s$ (where $s \leq r$) coded packets. After successful decoding, the decoded packets are handed over to the upper layer. Simultaneously, receivers send an ACK to confirm the successful reception of the packet.

Figure 6 illustrates the detailed process of FEC encoding. From the figure, it can be observed that both the encoding layer at the sender and the decoding layer at the receiver are deployed between the TCP/IP protocol layers, without the need to modify the existing TCP/IP protocol. Therefore, the application of this encoding/decoding layer to both the sender and receiver is transparent, greatly reducing the deployment complexity of this encoding and being relatively hardware-friendly. Additionally, it is worth noting that the equal cost multi-path (ECMP) mechanism is deployed on all switches. This mechanism ensures that when there are multiple forwarding paths available, the switch will sequentially send the received data packets to these paths. The ECMP mechanism in switches ensures a certain degree of load balancing on the links, improving the utilization of each link and helping alleviate network congestion issues.

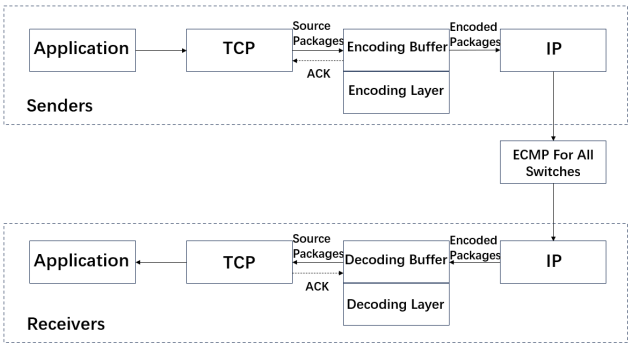

Figure 6. FEC encoding and decoding process

3.2 Design Details

In the encoding process, encoding redundancy affects both decoding latency and communication overhead, making it difficult to strike a balance between two aspects. For instance, to expedite the decoding operation, the sender should dispatch more redundant packets, inevitably incurring unnecessary traffic overhead and constraining the sender's own transmission rate. However, if too few redundant packets are transmitted, decoding speed is hampered as the receiver must wait for a sufficient number of encoded packets to conduct decoding operations. In essence, careful adjustment of encoding redundancy is necessary to achieve a favorable trade-off between decoding latency and traffic overhead. In this paper, the number of redundant packets is determined by the following rules.

Before sending data, as illustrated in Figure 7, the sender needs to divide the flow to be sent into k equally sized data packets. These data packets are further subdivided into m groups of equal length. Subsequently, the sender obtains the packet receiving rate $p_i (i = 1, \ldots, m)$ from the sender to the receiver by sending test packets.

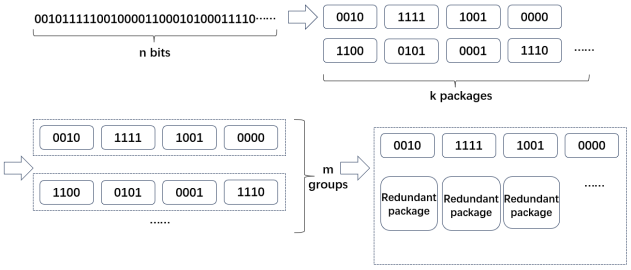

Figure 7. Redundant packages generation process

Let x_i denote the total number of test packets sent for the i-th group, and y_i denote the number of packets received by the receiver for the i-th group. Then p_i can be determined by the following equation:

$$p_i = \frac{y_i}{x_i} \tag{1}$$

Each group of packets requires testing for packet loss rate once, so there is a total of m groups and m tests need to be conducted. For each group, r_1, r_2, …, r_m redundant packets are generated respectively. Since the necessary condition for successful decoding is that the number of packets received by the receiver is greater than or equal to the number of source packets, r_i must satisfy the following equation:

$$\left(k + r_i\right) p_i \geq k \tag{2}$$

Further derivation from equations (1) and (2) yields that r_i should satisfy the following condition:

$$r_i = \left\lceil k\left(\frac{1}{1-p_i} - 1\right)\right\rceil \tag{3}$$

This ensures that the receiver can, on average, receive at least as many encoded packets as the number of source packets. Further analysis reveals that if the total number of packets sent by the sender in each group is denoted as h, then we have:

$$h = k + r_i \tag{4}$$

Therefore, in the case where the packet receiving rate is p_i, the probability that the receiver receives y packets is:

$$p\left(y\right) = C_h^y \left(p_i\right)^y \left(1 - p_i\right)^{h-y} \tag{5}$$

Thus, it can be concluded that the probability of successful decoding by the receiver, denoted as p_c, is:

$$p_c = 1 - \sum_{y=0}^{k-1} p(y) \tag{6}$$

Similar to fountain codes, the encoding module at the sender generates redundant packets from source packets through XOR operations. As depicted in Figure 7, during transmission, in addition to sending the source packets, the sender also needs to transmit these redundant packets. This approach is more favorable for decoding at the receiver compared to traditional fountain codes. Meanwhile, the ECMP mechanism is deployed on switches. By using the same metric standards, ECMP distributes traffic reasonably across multiple paths with equal costs to improve network performance and fault tolerance. Through the ECMP mechanism, traffic in the network can be more evenly and efficiently distributed, avoiding congestion and failure risks on a single path. This helps enhance network throughput and response speed, thereby improving user experience and system performance.

4 Experimental Results and Analysis

4.1 Experimental Setup

The experiment will be carried out on the double leaf-spine topology based on Figure 1, with network parameters set according to Section 2. But, compared to Figure 1, there are 1 additional sender and receiver, which means 3 senders and receivers are activated in the network topology. Similar to Figure 1, during the transmission, 6 senders send packages to the corresponding receiver respectively. Every switch is equipped with the ECMP mechanism to distribute received packets sequentially across each link, ensuring the utilization of each link. when collecting statistical data, we obtain the flow completion time (FCT) for 6 flows and the throughput for 6 receiving host machines, and then take the respective average values of these two metrics as overall indicators.

4.2 Experimental Results

(1) Comparison between FEC encoding and other schemes under normal intensity attack: In this experiment, the intensity of malicious attacks ranged randomly from 0 to 40, with a variation period set at 1000μs. Each sender transmitted a flow of 1000MB to the receiver, dividing the flow into 100 groups before transmission. Each group contained 10 data packets, making each packet size 1MB.

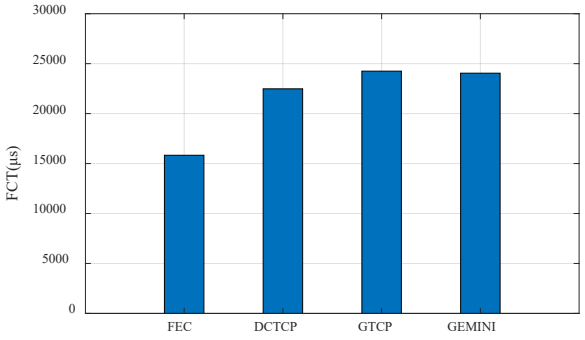

Figure 8. Comparison of FCT of each method

Figure 8 clearly demonstrates the comparison of FCT among FEC, DCTCP, GTCP, and GEMINI under specific experimental conditions. From the graph, it can be observed that the FEC encoding scheme proposed in this paper performs exceptionally well in reducing FCT. Its average FCT is reduced by approximately 35% compared to the other three methods. This significant advantage indicates the excellent performance of FEC encoding in traffic transmission across DCNs.

Figure 9 intuitively presents the significant advantage of FEC encoding proposed in this paper in terms of throughput compared to DCTCP, GTCP, and GEMINI methods. From the graph, it can be seen that among these four methods, FEC encoding exhibits the most

prominent throughput performance, increasing throughput by approximately 20% to 30%. This result once again demonstrates the effectiveness of FEC encoding in improving data transmission efficiency.

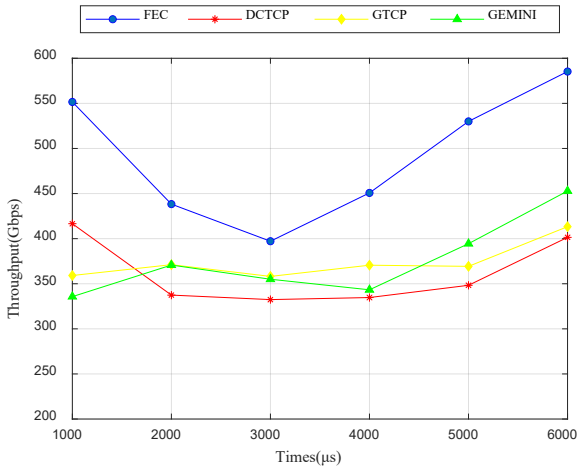

Figure 9. Throughput comparison of various methods

(2) Comparison between FEC encoding and other schemes under high intensity attack: To demonstrate the universal advantage of the FEC encoding scheme proposed in this paper, in the following experiments, we will continue to increase the intensity of malicious attacks to observe the performance of each method in extreme situations. Therefore, we will increase the intensity of malicious attacks from 0 to 40 to a range of 40 to 100, indicating a worse network condition and more severe packet loss.

Figure 10 and Figure 11 provide detailed comparisons of the performance of each method in terms of FCT and throughput under high-intensity malicious attacks. We can observe that the FEC encoding method proposed in this paper maintains relatively stable performance under high-intensity attacks. The increase in FCT and the decrease in throughput for FEC encoding are smaller compared to other methods, demonstrating the robust resistance and stability of FEC encoding against malicious traffic attacks.

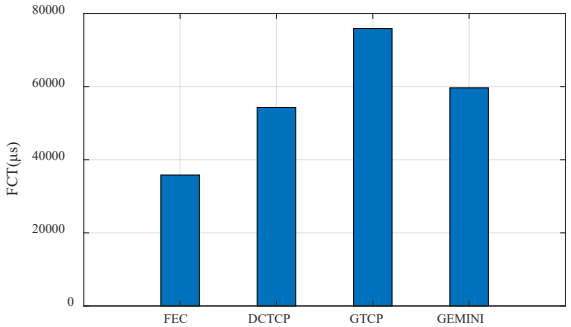

Figure 10. FCT of various methods under high intensity attack

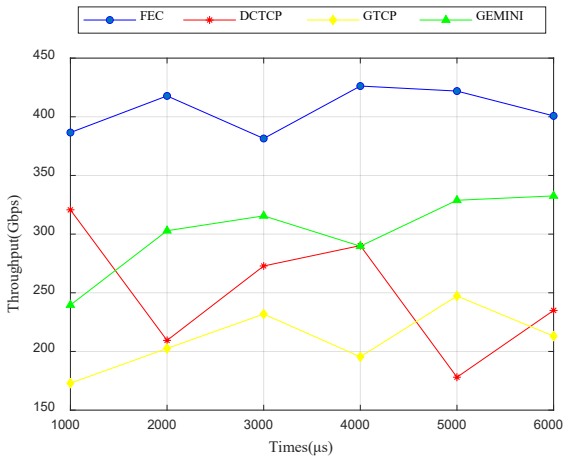

Figure 11. Throughput of various methods under high intensity attack

(3) The Influence of Different Groupings on the Encoding Performance of FEC: To further analyze and study the influence of groupings on the encoding performance of FEC, we divided the sender's flow into different numbers of groups, with each group containing a different number of data packets. Specifically, we divided them into four groups: 100 groups with 10 data packets each, 50 groups with 20 data packets each, 20 groups with 50 data packets each, and 10 groups with 100 data packets each. In this experiment, the variation period of malicious traffic attacks will be set to 1000μs, and the main metric selected is the average FCT of 6 flows.

Figure 12 shows the FEC encoding FCT under these four different groupings. It can be observed that the longer numbers of data packets in each group, the longer the FCT.

This is because, in the case of a long variation period of attacks, there is relatively less likelihood of a change in packet loss rate during the transmission of each group of data packets. This means that the packet loss rate obtained through previous testing data packets still has high accuracy, allowing the generated redundant codes to adapt well to the network conditions and ensure smooth data transmission.

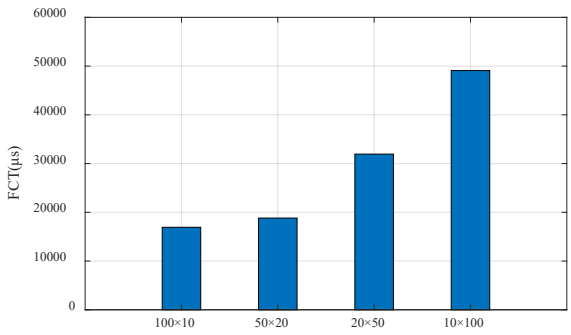

Figure 12. FCT of different groups

Conversely, when the variation period is short, there is a higher probability of significant changes in the packet loss rate during the transmission of data packets. At this point, the packet loss rate obtained through previous testing data packets is no longer applicable to the current network conditions.

Furthermore, when the number of data packets in each group is small, the corresponding number of redundant packets generated will also be smaller, and the impact of a small number of data packets on the network will be lower; On the contrary, when there are many packets in each group, the number of redundant packets generated will be higher. When a large number of redundant packets are generated and transmitted simultaneously, it is highly likely to make the network congestion worse, which goes against the design purpose of FEC coding in this paper.

It's also worth noting that if the number of data packets in each group is too small, the number of groups will increase accordingly. This means that before each data packet is sent, test data packets need to be sent to assess the current packet loss rate. With the increase in the number of groups, the frequency of sending test data packets will also rise sharply. Excessive sending of test data packets may also lead to wastage of network resources.

5 Conclusion and Future Work

In this paper, research on FEC encoding in the context of malicious attacks during cross data center traffic transmission is presented. This encoding is an adaptive coding technique that can dynamically adjust redundant settings based on network conditions, allowing the receiver to successfully recover the source data without receiving complete data. Due to its ability to make real-time adjustments based on network conditions, this encoding reduces unnecessary bandwidth wastage while meeting decoding requirements, thus avoiding additional congestion caused by redundant data packets. Moreover, this encoding maintains compatibility with existing transport layer protocols and does not require complex hardware modifications during actual deployment.

In the future work, it would be beneficial to consider integrating more practical network environments and business requirements for deeper simulation testing and field deployment verification of these methods. For example, incorporating artificial intelligence and machine learning techniques into the optimization of FEC encoding grouping could be explored. This would involve dynamically adjusting FEC grouping based on network conditions to prevent excessive packet loss triggering retransmissions due to mismatch between the rapidly changing attack variation period and the observed packet loss rate.

Acknowledgment

This work was funded by the Researchers Supporting Project Number (RSP2024R509), King Saud University, Riyadh, Saudi Arabia.

References

[1] Z. Wang, Z. Li, G. Liu, Y. Chen, Q. Wu, G. Cheng, Examination of WAN traffic characteristics in a large-scale data center network, *21st ACM Internet Measurement Conference*, Virtual Event, USA, 2021, pp. 1-14.

[2] Z. Wang, Z. Li, H. Pan, G. Liu, Y. Chen, Q. Wu, G. Tyson, G. Cheng, Large-Scale Measurements and Prediction of DC-WAN Traffic, *IEEE Transactions on Parallel and Distributed Systems*, Vol. 34, No. 5, pp. 1390-1405, May, 2023.

[3] J. Wang, Y. Yang, T. Wang, R.-S. Sherratt, J. Zhang, Big data service architecture: a survey, *Journal of Internet Technology*, Vol. 21, No. 2, pp. 393-405, March, 2020.

[4] J. Hu, H. Shen, X. Liu, J. Wang, RDMA Transports in Datacenter Networks: Survey, *IEEE Network*, Vol. 38, No. 6, pp. 380-387, November, 2024.

[5] Z. Wang, K.-W. Fok, V.-L. Thing, Machine learning for encrypted malicious traffic detection: Approaches, datasets and comparative study, *Computers & Security*, Vol. 113, Article No. 102542, February, 2022.

[6] N. Choudhury, D. Deka, A. Tewari, S. Gaur, S. Sarmah, V. Sharda, S. Gautam, Malicious Traffic Classification Using Convolutional Neural Network, *2023 14th International Conference on Computing Communication and Networking Technologies*, Delhi, India, 2023, pp. 1-7.

[7] B.-H. Tang, W.-X. Jiang, Y.-X. Ke, Research on CNN-based malicious traffic identification method, *2021 7th International Conference on Computing and Artificial Intelligence*, Tianjin, China, 2021, pp. 257-265.

[8] Y. Zhou, H. Shi, Y. Zhao, W. Ding, J. Han, H. Sun, X. Zhang, C. Tang, W. Zhang, Identification of encrypted and malicious network traffic based on one-dimensional convolutional neural network, *Journal of Cloud Computing*, Vol. 12, Article No. 53, April, 2023.

[9] T. Anitha, S. Aanjankumar, S. Poonkuntran, A. Nayyar, A novel methodology for malicious traffic detection in smart devices using BI-LSTM–CNN-dependent deep learning methodology, *Neural Computing and Applications*, Vol. 35, No. 27, pp. 20319-20338, September, 2023.

[10] S. Das, K.-G. Panda, D. Sen, W. Arif, Maximizing last-minute backup in endangered time-varying inter-datacenter networks, *IEEE/ACM Transactions on Networking*, Vol. 29, No. 6, pp. 2646-2663, December, 2021.

[11] M. Rajiullah, P. Hurtig, A. Brunstrom, A. Petlund, M. Welzl, An evaluation of tail loss recovery mechanisms for TCP, *ACM SIGCOMM Computer Communication Review*, Vol. 45, No. 1, pp. 5-11, January, 2015.

[12] V. K. Bhargava, I. J. Fair, Forward Error Correction Coding, in: S. S. Suthersan (Ed.), *The Mobile Communications Handbook*, CRC Press LLC, 1999, pp. 166-179.

[13] M. Alizadeh, A. Greenberg, D. A. Maltz, J. Padhye, P. Patel, B. Prabhakar, S. Sengupta, M. Sridharan, Data center tcp (dctcp), *ACM SIGCOMM 2010 Conference*, New Delhi, India, 2010, pp. 63-74.

[14] J. Hu, C. Zeng, Z. Wang, J. Zhang, K. Guo, H. Xu, J. Huang, K. Chen, Load Balancing with Multi-Level Signals for Lossless Datacenter Networks, *IEEE/ACM Transactions on Networking*, Vol. 32, No. 3, pp. 2736-2748, June, 2024.

[15] M. S. C. Pyke, W. Meng, B. Lampe, Security on Top of Security: Detecting Malicious Firewall Policy Changes via K-Means Clustering, *International Conference on Machine Learning for Cyber Security (ML4CS 2023)*, Yanuca Island, Fiji, pp. 145-162, 2023.

[16] Z. Wang, K.-W. Fok, V. L. L. Thing, Machine learning for encrypted malicious traffic detection: Approaches, datasets and comparative study, *Computers & Security*, Vol. 113, Article No. 102542, February, 2022.

[17] J.-L. Guerra, C. Catania, E. Veas, Datasets are not enough: Challenges in labeling network traffic, *Computers & Security*, Vol. 120, Article No. 102810, September, 2022.

[18] P. Zhang, F. He, H. Zhang, J. Hu, X. Huang, J. Wang, X. Yin, H. Zhu, Y. Li, Real-time malicious traffic detection with online isolation forest over sd-wan, *IEEE Transactions on Information Forensics and Security*, Vol. 18, pp. 2076-2090, March, 2023.

[19] J. Hu, J. Huang, J. Wang, J. Wang, A Transmission Control Mechanism for Lossless Datacenter Network Based on Direct Congestion Notification, *Acta Electonica Sinica*, Vol. 51, No. 9, pp. 2355-2365, September, 2023.

[20] J. Hu, Y. He, W. Luo, J. Huang, J. Wang, Enhancing Load Balancing with In-Network Recirculation to Prevent Packet Reordering in Lossless Data Centers, *IEEE/ACM Transactions on Networking*, Vol. 32, No. 5, pp. 4114-4127, October, 2024.

[21] G. Zeng, W. Bai, G. Chen, K. Chen, D. Han, Y. Zhu, L. Cui, Congestion control for cross-datacenter networks, *IEEE/ACM Transactions on Networking*, Vol. 30, No. 5, pp. 2074-2089, October, 2022.

[22] G. Zeng, Congestion Control Mechanisms for Inter-Datacenter Networks, *arXiv preprint arXiv*: 2201.03734, January, 2022. https://arxiv.org/abs/2201.03734

[23] S. Yan, X. Wang, X. Zheng, Y. Xia, D. Liu, W. Deng, ACC: Automatic ECN tuning for high-speed datacenter networks, *Proceedings of the 2021 ACM SIGCOMM 2021 Conference*, Virtual Event, USA, 2021, pp. 384-397.

[24] S. Zou, J. Huang, J. Liu, T. Zhang, N. Jiang, J. Wang, Gtcp: Hybrid congestion control for cross-datacenter networks, *2021 IEEE 41st International Conference on Distributed Computing Systems*, DC, USA, 2021, pp. 932-942.

[25] M. Alizadeh, A. Javanmard, B. Prabhakar, Analysis of DCTCP: stability, convergence, and fairness, *ACM SIGMETRICS Performance Evaluation Review*, Vol. 39, No. 1, pp. 73-84, June, 2011.

[26] S. A. Jyothi, A. Singla, P. B. Godfrey, A. Kolla, Measuring and understanding throughput of network topologies, *SC'16 the International Conference for High Performance Computing, Networking, Storage and Analysis*, Salt Lake City, UT, USA, 2016, pp. 761-772.

[27] M. Fisk, W.-C. Feng, *Dynamic adjustment of TCP window sizes*, LANL Report: LA-UR 00-3221, July, 2000.

Biographies

Jinbin Hu received the B.E. and M.E. degrees from Beijing Jiao Tong University, China, in 2008 and 2011, respectively, and the PhD degree in computer science from Central South University, China, in 2020. She is currently a Post-Doc in the Department of Computer Science and Engineering, Hong Kong University ofScience and Technology, and working in the School of Computer and Communication Engineering, Changsha University of Science and Technology, China. Her current research interests are in the area of datacenter networks, RDMA networking and learning-basednetwork systems.

Rui Yang is currently pursuing the M.E. degree in the School of Computer and Communication Engineering at Changsha University of Science and Technology, China. His topics of research are in the area of datacenter networks and network reliable transmission.

Xuchong Liu, Doctor of Engineering, Professor, Doctoral Supervisor, Vice Dean of the College, and Second level Police Inspector. Hosted over 30 scientific research projects, including 13 projects at or above the provincial and ministerial level, and won 1 provincial and ministerial level scientific and technological progress award, 1 teaching achievement award, and 3 political and legal intelligent innovation awards.

Fayez Alqahtani is a full professor at King Saud University (KSU). He has been lecturing in the university since 2002, teaching several information technology subjects. In 2004 he was appointed Director of the Computer Division at the Deanship of Student Affairs. Currently, Dr. Alqahtani's has supervised number of projects, authoring number of research papers in the area of knowledge management Systemes, Web 2.0 Technologies & Application and so on.

Jin Wang received the M.S. degree from Nanjing University of Posts and Telecommunications, China in 2005. He received Ph.D. degree from Kyung Hee University Korea in 2010. Now, he is a professor at Changsha University of Science and Technology. He has published more than 400 international journal and conference papers. His research interests mainly include wireless ad hoc and sensor network, network performance analysis and optimization etc. He is a senior member of the IEEE and a Fellow of IET.