A Comprehensive Study on the Advancements of Man and Machine in Network Security and Coding Theory

[1]Hye Jin Kim and [2]Rhee Jung Soo
[1,2]Department of Smart Convergence Security, Busan University of Foreign Studies, Busan,South Korea.
[1]20225432@office.bufs.ac.kr, [2]rhee@bufs.ac.kr

Correspondence should be addressed to Rhee Jung Soo : rhee@bufs.ac.kr

Article Info
Journal of Machine and Computing (http://anapub.co.ke/journals/jmc/jmc.html)
Doi: https://doi.org/10.53759/7669/jmc202303021
Received 05 November 2022; Revised from 20 February 2023; Accepted 18 April 2023.
Available online 05 July 2023.

Abstract – The article offers a comprehensive analysis of network coding, communications security, and coding theory, examining their applications and advancements. It evaluates the fundamental concepts and methodologies utilized in these fields while shedding light on current progress and potential future research directions. The implications of the study discussed in this article extend widely across the communication sector, with immediate practical applications across various disciplines. One of the key areas covered in the article is the development of novel error-correcting codes and coding algorithms, which contribute to enhancing communication reliability. Additionally, the integration of machine learning and artificial intelligence (AI) techniques into network communications security is explored, highlighting their potential to bolster safeguarding measures. Furthermore, the incorporation of security controls into connected devices and Internet of Things (IoT) networks is addressed, acknowledging the need to ensure security in these interconnected systems. To ensure the reliability and security of network communications and foster innovation and growth within the communication sector, the article concludes that coding theory and network communications security must continue to evolve and progress. By pushing the boundaries of these fields, researchers can address emerging challenges, improve existing systems, and pave the way for future advancements in communication technology.

Keywords – Coding Theory, Network Coding, Network Security, Error-Correcting Codes, Cryptography.

I. INTRODUCTION

The generation and evaluation of error-correcting codes as well as their use in communication systems and data storage are the focus of the mathematical and computer science field known as coding theory. The objective of coding theory is to create techniques for error detection and correction in data transmission and storage. To make the data more redundant and enable error detection and correction, error-correcting codes are used. Error-correcting codes come in a variety of forms, including convolutional codes, turbo codes, and linear block codes. Convolutional codes are frequently used in wireless communication systems, whereas linear block codes, such as Reed-Solomon codes, are widely used in digital communication systems and storage devices. Performance nearest to the Shannon limit is attained using turbo codes, a type of concatenated code that is iteratively decoded. Wireless systems, digital communication systems, storage devices, and other fields all benefit from the use of coding theory.

Coding theory is employed in digital communication systems to increase the accuracy of data transmission over noisy channels [1]. The coding theory is used in storage devices to shield data from errors brought on by disk failures and other kinds of hardware malfunctions. By minimizing the implications of interference and fading, coding theory is used in wireless networks to boost the performance of wireless communication systems. Coding theory has recently been expanded to include issues like wireless networks, distributed storage systems, and network coding. By enabling intermediary nodes to analyze and convey data, the concept of network coding makes it possible for networks to communicate more effectively. Data protection in distributed storage systems makes use of coding theory to guard against storage node failures. By minimizing the impacts of fading and interference, wireless networks apply coding theory to enhance the performance of wireless communication systems. Modern network communications need the use of coding theory. It focuses on the creation, evaluation, and use of codes that may be used to send data through erratic and noisy channels.

In recent years, network communications have seen an increase in the use of coding theory, which has sparked the creation of novel methods and protocols known as network coding. Utilizing intermediary nodes to process and transfer data in a network, network coding is a method that makes effective use of network resources. The throughput, latency, and dependability of networks might all be improved by using this strategy. The necessity to get beyond the restrictions of conventional routing is one of the primary drivers behind the study of coding theory in network communications. It is assumed that data packets are sent from one node to the next based on their destination addresses in traditional routing techniques like hop-by-hop routing. This method, however, has a number of drawbacks, including the need for several routing tables and the incapability to handle multicast and broadcast broadcasts. By enabling intermediary nodes to mix and process data packets rather than just forwarding them, network coding overcomes these limits.

This article will primarily focus on network coding, network security, and communications security. This article will also provide a comprehensive understanding of coding theory as well as its applications in network communications, with a particular focus on network coding as well as the security of networks and communications. This paper will provide an in-depth understanding of the fundamental ideas and procedures of coding theory, as well as how these things are used in network coding. Additionally, it will provide you with an in-depth understanding of the many security concerns that are faced by networks, as well as the techniques and protocols that may be employed to address these difficulties.

The article is organized into the following sections: Section II presents a discussion of coding theory and application. Section III focuses on network coding, where key concepts are discussed: in introduction to network coding and its advantages over traditional routing; network coding for multicast and broadcast transmissions; network coding for cooperative communications; network coding for distributed storage systems; and network coding for wireless networks. Section IV reviews network and communications security. Lastly, Section V draws final remarks to the paper.

II. CODING THEORY AND APPLICATIONS

Overview of Coding Theory and its Role in Network Communications

The study of codes and their suitability for various uses is known as "coding theory." Compressing data, encrypting it, detecting and correcting errors, transmitting it, and storing it all rely on codes. Information theorists, electrical engineers, mathematicians, linguists, and computer scientists all study codes so that they might create more effective and trustworthy means of transmitting information. This is done by reducing data repetition and fixing or finding faults in the sent information. Four distinct encoding methods exist: Line coding (also known as data compression or source coding) Error correction coding (also known as channel coding) Cryptographic coding.

It is the goal of data compression to reduce the amount of redundant information in a data set before transmission. ZIP data compression, for instance, makes files smaller, which may be useful for things like lowering network load. In certain cases, it makes sense to look at both data compression and error correction at the same time. When there are transmission channel interruptions, error correction provides beneficial redundancy to the data from a source, making the transmission more resilient. An average user probably isn't aware of all the places mistake correction is used. The Reed-Solomon algorithm is used by standard audio CDs to compensate for surface noise like scratches and dust. The CD itself acts as the transmission medium in this context. The fading and noise of high-frequency radio transmission are also compensated for by coding methods used in cell phones. Channel coding methods such as the turbo code and LDPC codes are used by data modems, telephone communications, and the NASA Deep Space Network to ensure that data is sent successfully [2].

As a two-part paper for the July and October editions of the Bell System Technical Journal in 1948, Claude Shannon presented "A Mathematical Theory of Communication." The issue of how to most efficiently encrypt the data a sender wishes to convey is the subject of this effort. In this seminal study, he made use of Norbert Wiener's probability theory techniques, which were only beginning to be applied to the field of communication theory. While effectively inventing the subject of information theory, Shannon created the concept of information entropy as a measure for the degree of uncertainty in a communication. Created in 1949, the binary Golay code is a form of communication. It's an erroneous data detection and correction algorithm that can identify and fix up to four faults per 24-bit word. The 1968 Turing Award went to Richard Hamming for his work at Bell Labs on numerical techniques, error-detecting and error-correcting codes, and automated coding systems. Hamming is credited for creating the fields of information theory and cryptography as well as the Hamming distance, Hamming codes, Hamming numbers, and Hamming windows. With the help of T. Natarajan and K. R. Rao, Nasir Ahmed introduced the discrete cosine transform (DCT) in 1972, and it was first implemented in 1973. JPEG, MPEG, and MP3 all employ the DCT as its foundational lossy compression technique.

The study of mathematical techniques for transmitting data via erratic or noisy channels is known as coding theory. Coding theory is used in network communications to create, evaluate, and put into practice codes that may be utilized to send data across a network. These codes may be used to compress data to lower the bandwidth needed for transmission or to remedy transmission faults that may happen. The potential to boost network performance in terms of throughput, latency, and dependability is one of the key benefits of utilizing coding theory in network communications. Utilizing intermediary nodes to process and transfer data in a network, network coding is a method that makes effective use of network resources. The throughput, latency, and dependability of networks might all be improved by using this strategy. The conventional routing and network coding are compared in **Table 1** below.

Table 1. Comparison of Traditional Routing and Network Coding

Traditional Routing	Network Coding
Forwarding based on destination address	Intermediate nodes can forward and process data
Large number of routing Tables	Minimal overhead
Inability to deal with broadcast and multicast transmissions	Can handle broadcast and multicast transmissions

Network coding is superior to conventional routing in a number of ways, as **Table 1** above illustrates. Network coding enhances network efficiency, enables more effective use of network resources, and can handle multicast and broadcast broadcasts that standard routing cannot. The source, channel, and destination are shown in the block diagram of a communication system in **Fig 1** below. Data is produced by the source, transmitted via the channel, and received at the destination. To boost the effectiveness of the communication system, coding and decoding are used at both the source and the destination.

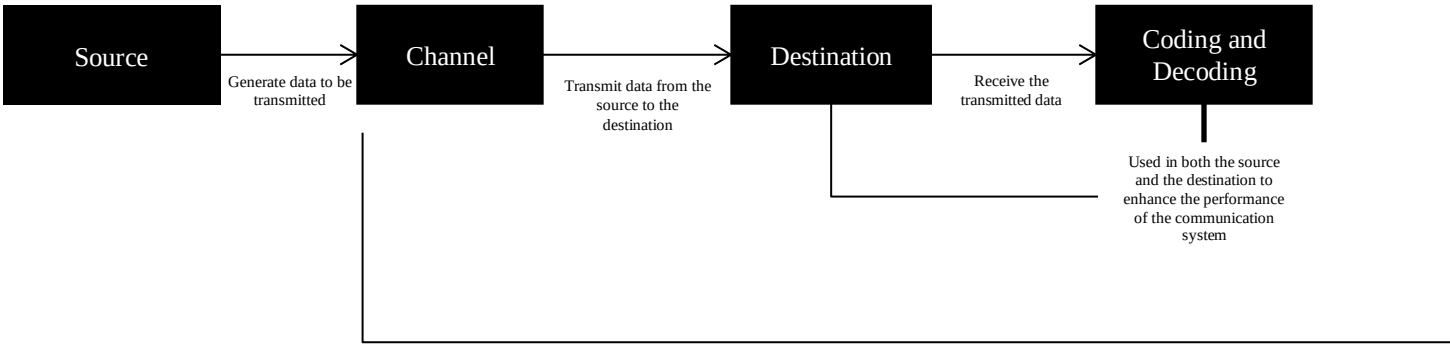

Fig 1. Block Diagram of a Communication System

Error-Correcting Codes and Their Applications in Network Coding

Error-correcting codes are a type of coding technique used to find and fix mistakes that could happen while transmitting data. These codes can be used to fix errors that may happen as a result of channel interference or other noise. Block codes and convolutional codes are two examples of different error-correcting codes. A description of each type of error-correcting code is provided in **Table 2** below.

Table 2. Different types of error-correcting codes and their characteristics

Types of Code	Characteristics
Block codes	Correct errors in blocks of data
Convolutional codes	Correct errors in continuous streams of data
Reed-Solomon codes	Can correct multiple errors in a block of data
Low-density parity-check codes	Can correct errors with high probability

To increase the network's performance in terms of dependability and error correction, error-correcting codes may be utilized in network coding. An error-correcting code encoder and decoder are shown in block diagram form in **Fig. 2** below. Before transmission, the encoder applies the error-correcting code to the data, and after transmission, the decoder fixes any transmission problems that may have happened.

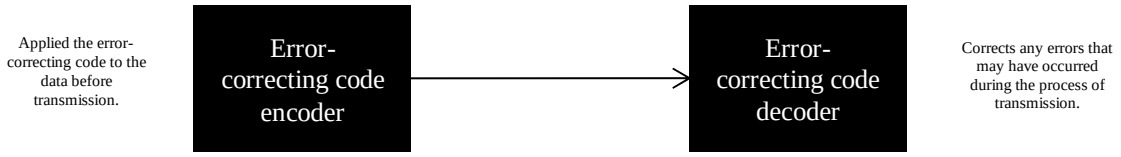

Fig 2. An Error-Correcting Code Encoder and Decoder Flow

Linear Block Codes and Their Applications in Network Coding

Block codes of the kind known as linear block codes may be used to fix faults in data blocks. These codes, which are based on linear algebra, may be used to fix faults that might be brought on by channel noise or other interference. Hamming and Reed-Solomon codes [3] are a few of examples of linear block codes. Examples of linear block codes are shown along with their parameters in **Table 3** below.

Table 3. Examples of Linear Block Codes and Their Parameters

Code	Parameters
Hamming codes	n, k, d
Reed-Solomon codes	n, k, t
BCH codes	n, k, d

In order to increase the network's reliability and error-correction capabilities, linear block codes can be used in network coding. The linear block code's encoding and decoding are shown in **Fig 3** below. Prior to transmission, the data is encoded using a linear block code, and any transmission errors are then fixed by the decoder.

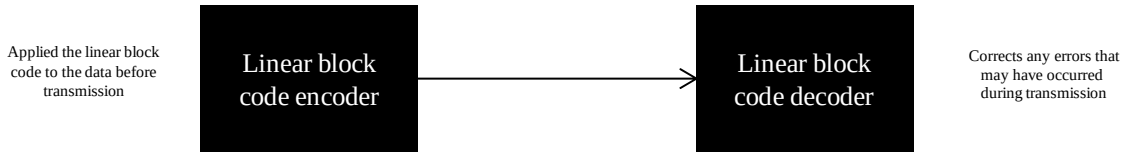

Fig 3. Linear Block Code's Encoding and Decoding Flow

Convolutional Codes and Their Applications in Network Coding

An error-correcting code called a convolutional code may be used to fix faults in data streams that are continuously flowing. These codes, which are based on convolutional processes, may be used to fix faults that may happen as a result of noise or other channel interference. Communications across wireless and mobile networks often use convolutional coding. Convolutional codes and linear block codes are contrasted in **Table 4** below.

Table 4. Comparison of Convolutional Codes and Linear Block Codes

Convolutional Codes	Linear Block Codes
Correct errors in continuous streams of data	Correct errors in blocks of data
Complex decoding process	Simple decoding process
Suitable for wireless and mobile communications	Suitable for wired communications

Network coding can make use of convolutional codes to increase the network's reliability and error-correction capabilities. The method of encoding and decoding a convolutional code is shown in **Fig. 4** below. Convolutional coding is applied to the data by the encoder prior to transmission, and any transmission errors are then fixed by the decoder.

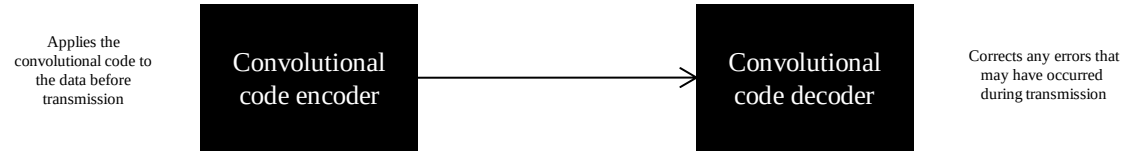

Fig 4. Encoding and Decoding a Convolutional Code Flow

Turbo Codes and Their Applications in Network Coding

Digital communications [4] may utilize turbo codes, a sort of error-correcting code, to fix mistakes. These codes, which may be used to repair mistakes brought on by noise or other interference in the channel, are based on the concatenation of two or more convolutional codes. Digital communications now often employ turbo codes, which were initially suggested in 1993. **Table 5** contrasts turbo codes with various error-correcting codes.

Table 5. Comparison of Turbo Codes and Other Error-Correcting Codes

Turbo Codes	Other Error-Correcting Codes
High error-correction capability	Lower error-correction capability
Complex decoding process	Simple decoding process
Suitable for high data rate applications	Suitable for low data rate applications

In order to increase the network's dependability and error-correction capabilities, turbo codes may be utilized in network coding. A turbo code encoder and decoder's block diagram is shown in **Fig 5** below. Prior to transmission, the encoder applies the turbo code to the data, and any transmission faults are then fixed by the decoder.

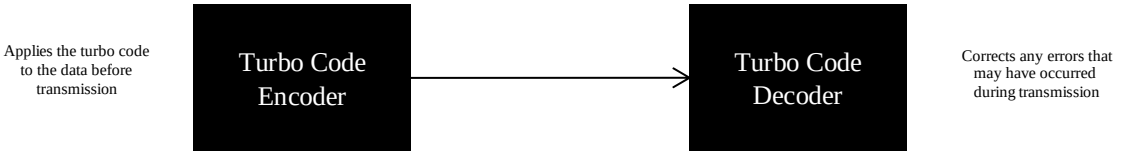

Fig 5. A Turbo Code Encoder and Decoder's Block Diagram

III. NETWORK CODING

Introduction to Network Coding and its Advantages Over Traditional Routing

Network coding technology [5] allows for data integration and processing at intermediary nodes before data is sent. Unlike in conventional routing, where intermediate nodes simply transfer incoming packets to their destination, this technique allows them to execute data manipulation that improves the system's overall speed. System coding's key advantage is its ability to make more efficient use of network resources. To improve network capacity and decrease transmission latency, network coding allows intermediary nodes to integrate and analyze the data. As an additional perk, network coding may strengthen the network's resilience. By letting intermediary nodes analyze and integrate the information, network coding may decrease the consequences of system failures and increase the network's fault tolerance. **Table 6** presents the advantages of network coding over traditional routing.

Table 6. Advantages of Network Coding Over Traditional Routing

Advantages	Description
Efficient use of network resources	Allow intermediate nodes to effectively process and integrate data, increasing network capacity and reducing delay
Improved robustness	Reduces the impacts of network failures and enhances fault tolerance

For cooperative communications, multicast and broadcast transmissions, distributed storage systems, and wireless networks, network coding has been proven to be very helpful. The intricacy of the encoding and decoding process as well as the need for exact network synchronization provide certain difficulties, however. To solve these issues and fully realize the potential advantages of network coding, further study is required.

Network Coding for Multicast and Broadcast Transmissions

Ergodic error processes in link networks are often where the capacity of a network is discussed. For certain of these networks, such multiple access channels, broadcast channels, and relay channels; there are channel coding theorems and capacity areas that may be identified. Error-free network capacity has received fresh study in recent years. In particular, multicast connection transmission using error-free network coding has been investigated. See authors in [6] for a more up-to-date explanation of network coding. Wang, Karande, Sadjadpour, and Garcia-Luna-Aceves in [7] analyzed multicast networks' capacity and how it relates to cutsets. Coding across a network helps increase capacity. We provide a novel, surprisingly simple, and useful approach for investigating the capabilities of networks. There is a direct mapping between a specific network information flow issue and an algebraic variety over the closure of a finite field inside this framework, which is fundamentally algebraic. There are algebraic components in the findings of the Wachter-Zeh and Sidorenko in [8] (i.e., linear coding and a comment on convolutional codes), but the proposed link to ideas from algebraic geometry allows for the application of highly powerful theorems in well-developed mathematical areas.

We discover necessary and sufficient requirements for any set of connections to be realizable across any given network, for which the use of linear codes is constrained (we subsequently make explicit the meaning of linear codes, as these codes are not bitwise linear). In this paper, we use our framework to demonstrate that the feasibility of a multicast connection across a network can be verified in polynomial time since it has a very specific structure. Furthermore, we replicate the findings of Stasiak, Sobieraj, and Zwierzykowski [9] and demonstrate that any practical multicast connection may be realized using just network-wide linear codes. Giving the sufficient and necessary conditions for connections to be viable in a network when no multicasting is taking place is shown here to be comparable to the issue of locating a point in an algebraic variety, which is NP-complete in general. Furthermore, the cutset criteria are merely required but probably not sufficient in the case of universal connections, i.e., a random assortment of point-to-point connections, but they are essential and sufficient to show the viability of a specific collection of links for multicast connections.

Network coding allows for more effective use of prevalent network bandwidth during multicast and broadcast broadcasts. With the typical approach of routing, data for a multicast or broadcast is sent out to each individual node in the group, which may lead to unnecessary transmissions and a drain on the network's resources. Thanks to network coding, intermediate nodes may consolidate and evaluate the information they receive, therefore minimizing the number of data transfers required and increasing the network's overall throughput. In addition to reducing latencies in unicast and multicast broadcasts, network coding may improve latency in broadcast transmissions. With network coding, intermediary nodes may analyze and aggregate data, reducing the number of hops needed for the data to reach all of the receivers and

hence the latency. By reducing the quantity of transmissions, network coding also helps save power. In wireless networks, when power is scarce, this is particularly helpful. **Table 7** presents advantages of network coding for multicast and broadcast transmissions.

Table 7. Advantages of Network Coding for Multicast and Broadcast Transmissions

Advantages	Description
Increased throughput	Allows intermediate nodes to process and combine the data, reducing the number of transmissions needed and enhancing the general throughput
Reduced delay	Allows intermediate nodes to effectively process and combine data, minimizing the number of hops needed for the data to reach all receivers and reducing delay
Reduced energy consumption	Reduces the number of transmission needed, particularly beneficial for wireless networks

It should be mentioned, nonetheless, that network coding implementation in multicast and broadcast broadcasts may be difficult since it requires exact synchronization between the intermediary nodes and receivers. Furthermore, encoding and decoding might be difficult for certain network devices with little computing power due to their complexity. Overall, it has been discovered that network coding is a potential method for enhancing multicast and broadcast transmission performance. Many network coding systems have been developed by researchers, including Random Linear Network Coding (RLNC) [10] and Coded Cooperative Multicast (CCM) [11], which have been found to significantly reduce latency and increase throughput. To fully comprehend the potential advantages and difficulties of network coding in multicast and broadcast transmissions, more study is necessary.

Network Coding for Cooperative Communications

Cooperative communications, in which multiple nodes cooperate to transmit data, can also use network coding. Unlike network coding, which allows multiple nodes to combine and process data before forwarding it, traditional routing simply involves each node forwarding the packets it receives to its destination. This makes it possible to use network resources more effectively and can enhance the effectiveness of cooperative communications. Network throughput can be greatly increased by network coding, which is one of its main benefits in cooperative communications. Network coding can increase the volume of data that can be transmitted in a given amount of time by allowing multiple nodes to process and combine the data. Additionally, network coding can increase the reliability of cooperative communications. Network coding can lessen the impact of node failures and improve the network's fault tolerance by allowing multiple nodes to process and combine the data. **Table 8** presents advantages of network coding for cooperative communications.

Table 8. Advantages of network coding for cooperative communications

Advantages	Description
Increased throughput	Allows different nodes to process and integrate data, enhancing the amount of data that can be transmitted in a particular timeframe
Improved robustness	Allows different nodes to process and combine data, minimizing the effects of node failure and enhancing fault tolerance of the network

However, because it necessitates exact coordination between the cooperating nodes, network coding in cooperative communications can be difficult to implement. Furthermore, encoding and decoding might be difficult for certain network devices with little computing power due to their complexity. It has been discovered that network coding is a promising method for enhancing cooperative communications. Numerous network coding schemes have been proposed by researchers, including Coded Cooperative Relaying (CCR) and Coded Cooperation (CC), which have been shown to significantly increase throughput and robustness. To fully comprehend the potential advantages and difficulties of network coding in cooperative communications, more study is required.

Network Coding for Distributed Storage Systems

Distributed storage systems are used to store and retrieve data over a network of nodes. Network coding may also be employed with these systems. Unlike network coding, which encrypts the data and stores it across numerous nodes, standard distributed storage systems merely repeat the data over multiple nodes. This makes it possible to utilize network resources more effectively and may increase the availability and dependability of the data that is being stored. The ability to increase the dependability of the stored data is one of the key benefits of network coding in distributed storage systems. Network coding may minimize the effects of node failures and improve the fault tolerance of the system by encoding and storing the data across many nodes. The availability of the stored data may also be increased by network coding. Network

coding may speed up data retrieval times and boost data availability by encoding and storing the data across numerous nodes to cut down on the number of transfers needed. **Table 9** presents the advantages of network coding for distributed storage systems.

Table 9. Advantages of Network Coding for Distributed Storage Systems

Advantages	Description
Increased reliability	Encoding and storing data across multiple nodes, reduces the effects of node failure and enhances fault tolerance of the system
Improved availability	Encoding and storing data across multiple nodes, reduces the number of transmisions required to retrieve the data, improvides retrieval time and enhances the availability of data

However, since it requires exact coordination between the nodes and the encoding and decoding process may be complicated, the application of network coding in distributed storage systems might be difficult. Additionally, there are trade-offs between the network coding scheme's degree of availability and dependability and its storage expense. It has been discovered that network coding is a viable method for enhancing the performance of distributed storage systems. Different network coding systems, including Fountain codes and Coded Replication (CR), have been developed by researchers and have been demonstrated to significantly enhance reliability and availability. To fully comprehend the possible advantages and difficulties of network coding in distributed storage systems, as well as to determine the best trade-off between storage overhead and the degree of dependability and availability, additional study is nonetheless required.

Network Coding for Wireless Networks

Wireless networks may benefit from network coding as well, since it can increase their throughput, latency, and energy economy. Network coding in wireless networks has many benefits, one of which is that it may boost the network's throughput. Network coding may enhance the amount of information that can be carried in a given amount of time by enabling intermediary nodes to analyse and combine the data. By lowering the amount of transmissions and hops necessary for the data to reach its destination, network coding may also decrease the latency in wireless networks. Applications that demand minimal latency in real-time may benefit the most from this. Wireless networks' energy efficiency may be increased via network coding since it requires fewer transmissions. This is especially advantageous for wireless networks as they have a limited supply of energy. **Table 10** presents the advantages of network coding for wireless networks.

Table 10. Advantages of Network Coding for Wireless Networks

Advantage	Description
Increased throughput	Allows intermediate nodes to process and combine data, enhance the amount to information being transmitted at a particular duration
Reduced delay	Minimizes the overall transmission needed and the hopes required for data to get to its destination
Improved energy efficiency	Minimizes the transmission needed, particularly advantageous for wireless networks where energy is considered a limited resource.

However, since it requires exact synchronization between the nodes and the encoding and decoding process might be complicated, the application of network coding in wireless networks can be difficult. Network coding may also improve wireless network security by making it more difficult for an attacker to capture and decode sent data. Overall, it has been discovered that network coding is a potential method for enhancing wireless networks' performance. Network coding approaches like Network Coded Cooperation (NCC) [12] and Network Coded Multiple Access (NCMA) [13], which have been found to significantly enhance throughput, latency, and energy efficiency, have been developed by researchers. To completely comprehend the potential advantages and difficulties of network coding in wireless networks, additional study is necessary. Additionally, it will be crucial to examine the trade-offs between the complicated encoding and decoding process, the synchronization that is necessary, and any possible gains in throughput, latency, and energy efficiency. Additionally, additional investigation is required to properly understand the security implications of network coding in wireless networks and the best ways to defend against future assaults.

IV. NETWORK AND COMMUNICATIONS SECURITY

Overview of Security Threats and Vulnerabilities in Network Communications

Network communications are susceptible to a variety of security risks and flaws, including malware, denial-of-service attacks, hacking, and data leaks. These dangers could have detrimental effects on people and organizations alike, including the leakage of private data, monetary loss, and reputational damage. One of the most prevalent security risks in network communications is hacking. Hackers can access a computer or network without authorization by using a number of methods, including phishing, social engineering, and exploiting software flaws. Once they have access, they can steal confidential data, put malware on the system, or stop the network from functioning normally.

Another frequent security risk to network communications is malware. Software that is intended to harm a computer or network is known as malware. Malware includes things like Trojan horses, worms, and viruses. Malicious websites, infected software, and email attachments can all spread malware. Attacks that cause a denial of service (DoS) are another frequent security risk. A DoS attack involves the attacker flooding a computer or network with traffic so that it is unavailable to the users for whom it is intended. This can be achieved in one of two ways: either by flooding the network with requests or by seizing control of numerous targets and employing them in the attack. Another frequent security risk in network communications is data breaches. A data breach happens when an unauthorized party has access to sensitive data, such as private information about an individual, money, or trade secrets. Serious repercussions from data breaches include reputational damage, legal liability, and monetary loss. **Table 11** presents a review of common security threats in network communications.

Table 11. Common Security Threats in Network Communications

Threat	Description
Hacking	Attempts to gain unauthorized access to computers or networks
Malware	Software designed to cause harm to computers or networks
Denial of Service (DoS)	Attempts to make computers or networks unavailable to its purposed users
Data breaches	Unauthorized access or theft to sensitive information

Cryptography and its Applications in Network Security

Through the use of encryption, cryptography is a method that may be utilized to secure network communications. Data may be shielded using encryption from being intercepted and viewed by unauthorized parties. In addition to ensuring the integrity of sent data, cryptography may be used to verify the sender and receiver's identities. The Advanced Encryption Standard is among the most widely used encryption algorithms for network communications (AES). AES is a symmetric-key encryption method that is often used to safeguard sensitive data, including credit card numbers and personal information.

Confirming the identification of a person or device is the process of authentication. Authentication may be used in network communications to guarantee that only authorized users or devices can access the network or its resources. Passwords are one of the most popular authentication techniques used in network communications. Passwords serve as a secret phrase or word that verifies the user's identity. However, passwords are vulnerable, and more sophisticated techniques like two-factor authentication, which calls for a second form of verification, such a fingerprint or security token, are gaining popularity. Making sure the data hasn't been altered with during transmission is the procedure of maintaining data integrity. Data integrity may be guaranteed using cryptographic methods like digital signatures and message authentication codes (MAC). **Table 12** presents the applications of cryptography in network security.

Table 12. Applications of Cryptography in Network Security

Application	Description
Data encryption	Protecting the data from being intercepted or read by unauthorized users
Authentication	Confirming the identity of the sender and the receiver
Data integrity	Ensuring that data has not been tampered with during transmission

Authentication and Access Control in Network Communications

Access control refers to the act of limiting who or what is permitted access to a network or network resource, while authentication refers to the process of verifying the identity of a person or device. Access control and authentication may be used in conjunction to stop unauthorized users from accessing a network or its resources. Role-based access control is one of the most widely used access control techniques in network communications (RBAC). According to a user's position or job function, RBAC controls access to resources. A user with the job of "administrator," for instance, may have access to private network resources, but a user with the role of "guest" might only have access to a small number of resources. **Table 13** presents a review of authentication and access control techniques.

Table 13. Authentication and Access Control Techniques

Technique	Description
Passwords	Using a secret word or phrase to confirm identity
Two-factor authentication	Requiring a second form of authentication, such as a fingerprint or security token
Role-based access control	Restricting access to resources based on the users' role or job function

Intrusion Detection and Prevention in Network Communications

Systems for detecting and preventing intrusions into networks and their resources are known as intrusion detection and prevention systems (IDPS) [14]. In addition to alerting network managers to suspected security breaches, IDPS may be used to identify and prevent malicious traffic. Signature-based detection is one of the most widely used approaches for detecting intrusions. By comparing it to recognized signatures or patterns, signature-based detection finds malicious communication. Anomaly-based detection is another popular technique that finds malicious traffic by searching for patterns or actions that differ from typical network activity [15].

Since anomaly-based detection doesn't depend on established signatures, it may be more successful in identifying fresh or undiscovered threats. However, as typical network activity sometimes deviates from what is thought to be normal, it might also result in more false positives. Instead of just warning the administrator, intrusion prevention systems (IPS) actively block any malicious traffic that is discovered. This may offer another layer of security to the network. **Table 14** presents an overview of intrusion detection and prevention techniques.

Table 14. Intrusion Detection and Prevention Techniques

Technique	Description
Signature-based detection	Identifying malicious traffic by matching it to known signatures or patterns
Anomaly-based detection	Identifying malicious traffic by looking for patterns or behaviours that deviate from normal network activity

Firewalls and Their Role in Network Security

Firewalls (such as in **Table 15**) are a form of security mechanism that regulates the flow of data into and out of a network. In order to prevent unauthorized users from accessing a network and to let only authorized traffic through, firewalls may be deployed. There are several kinds of firewalls, including packet-filtering, stateful inspection, and next-generation firewalls (NGFW). Based on pre-established rules and protocols, packet-filtering firewalls filter traffic. Stateful inspection firewalls monitor the status of network connections and apply traffic filtering based on that data. Intrusion prevention, virus protection, and application management are just a few of the security features that the NGFW integrates.

Table 15. Types of Firewalls

Type	Description
Packet-filtering firewall	Filtering traffic basen on predefined rules and protocols
Stateful inspection fireway	Tracking the state of nework connections and filtering traffic based on that information
Next-generation firewall (NGFW)	Combining multiple security functions such as intrution prevention

In order to effectively secure networks and communications, one must use a multi-layered strategy that incorporates firewalls, intrusion detection and prevention systems, authentication and access control, encryption, and constant monitoring and maintenance. The efficiency of these security measures may also be increased by using cutting-edge methods and tools like machine learning and artificial intelligence.

V. CONCLUSION

Various facets of coding theory and its applications, network coding, and network and communications security have been critically surveyed in this article. We covered an overview of coding theory and its application to network communications in the first part. We also discussed the many forms of error-correcting codes, including turbo codes, convolutional codes, and linear block codes, as well as how they are used in network coding. The second section of this paper discussed the concept of network coding, a relatively new method, which has shown to be much more advantageous than conventional routing. We discussed several forms of network coding, including wireless networks, cooperative communications, distributed storage systems, and multicast and broadcast transmissions. We closely analyzed the many facets of network and communications security in the third portion. We discussed several network communication security risks and

weaknesses as well as ways to protect network communications using firewalls, authentication and access control, intrusion detection and prevention, and cryptography.

The security of network communications and coding theory are two quickly developing topics that are crucial to the communication sector. Although these sectors have made considerable strides recently, there is still a lot of potential for more study and improvement. The creation of new error-correcting codes that may provide even more reliability and efficiency is one of the main topics of future study in coding theory. This might include the creation of novel coding algorithms as well as the use of sophisticated mathematical methods, such as algebraic coding theory. The study of how coding theory is used in cutting-edge technologies like 5G networks and the Internet of Things (IoT) will also be a key topic of study. Researchers in the field of network communications security expect that machine learning and artificial intelligence (AI) will have a major influence in the years to come. Adopting these technologies may help boost the efficiency of security measures by providing real-time monitoring and threat detection. As the use of quantum computers grows more commonplace, efforts to develop cryptographic protocols that are immune to their effects will become more important. Network communications security will also need to be studied in the context of the increasing number of Internet of Things (IoT) networks and linked devices. Examples include the development of encrypted messaging standards and the addition of security functions to the hardware and software of these gadgets.

The study that is the subject of this article has broad ramifications for the communication sector as well as immediate applications in several disciplines. The improvement of novel error-correcting codes and coding algorithms may significantly affect the dependability and effectiveness of network communications, according to the discipline of coding theory. As a result, wireless networks, satellite communications, and other types of communication may function better. The use of coding theory in cutting-edge technologies like 5G networks and the Internet of Things (IoT) may potentially open up new prospects for development and expansion in the communications sector. Machine learning and artificial intelligence (AI) may be used to increase the efficacy of security measures in the area of network communications security. Better defense against cyberattacks and data breaches may result from this, which in turn may contribute to the security and dependability of network communications.

Furthermore, the creation of quantum-resistant cryptographic techniques may boost data transmission security, which is essential in industries like banking and the military. Another significant practical application of the research covered in the paper is the incorporation of security controls into the hardware and firmware of connected devices and IoT networks. In order to safeguard these devices' security and guard against illegal access and data breaches, this might be helpful. The study covered in the article, taken as a whole, has important ramifications for the communication sector and real-world applications in several sectors. The reliability and security of network communications may be increased, and the communication sector can innovate and flourish, with the continuing study and progress of coding theory and network communications security.

Data Availability

No data was used to support this study.

Conflicts of Interests

The author(s) declare(s) that they have no conflicts of interest.

Funding

This research was supported by the MSIT(Ministry of Science and ICT), Korea, under the ICAN (ICT Challenge and Advanced Network of HRD) program (IITP-2023-2020-0-01825) and supervised by the IITP(Institute of Information & Communications Technology Planning & Evaluation) and This research was partly supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea Government(MSIT) and Korea Institute for Advancement of Technology(KIAT) grant funded by the Korea Government(MOTIE) (P0008703, The Competency Development Program for Industry Specialist)

Ethics Approval and Consent to Participate

The research has consent for Ethical Approval and Consent to participate.

Competing Interests

There are no competing interests.

References

[1]. D. Hurley and T. Hurley, "Coding theory: the unit-derived methodology," Int. J. Inf. Coding Theory, vol. 5, no. 1, p. 55, 2018.
[2]. E. Goh, H. S. Venkataram, M. Hoffmann, M. D. Johnston, and B. Wilson, "Scheduling the NASA deep space network with deep reinforcement learning," in 2021 IEEE Aerospace Conference (50100), 2021.
[3]. I. M. Boyarinov, "Self-checking circuits and decoding algorithms for binary hamming and BCH codes and Reed-Solomon codes over GF(2 m)," Probl. Inf. Transm., vol. 44, no. 2, pp. 99–111, 2008.
[4]. A. Khalid and P. Suksompong, "Application of maximum rank distance codes in designing of STBC-OFDM system for next-generation wireless communications," Digit. Commun. Netw., 2023.
[5]. M. AlaaEldin, E. Alsusa, and K. G. Seddik, "IRS-assisted physical layer network coding over two-way relay fading channels," IEEE Trans. Veh. Technol., vol. 71, no. 8, pp. 8424–8440, 2022.

[6]. **王**艺蒙 Wang Yimeng, **李蔚** Li Wei, 韩纪龙 Han Jilong, **姚海涛** Yao Haitao, **余少**华 Yu Shaohua, and 杨奇 Yang Qi, "Upstream date transmission based on wavelet packet transform coding in passive optical network," Zhongguo Jiguang (Chin. J. Lasers), vol. 41, no. 6, p. 0605001, 2014.

[7]. Z. Wang, S. S. Karande, H. R. Sadjadpour, and J. J. Garcia-Luna-Aceves, "On the multicast capacity of wireless ad hoc networks with network coding," J. Commun. Netw., vol. 13, no. 5, pp. 525–535, 2011.

[8]. A. Wachter-Zeh and V. Sidorenko, "Rank metric convolutional codes for Random Linear Network Coding," in 2012 International Symposium on Network Coding (NetCod), 2012.

[9]. M. Stasiak, M. Sobieraj, and P. Zwierzykowski, "Modeling of multi-service switching networks with multicast connections," IEEE Access, vol. 10, pp. 5359–5377, 2022.

[10]. J. Park and D.-H. Cho, "Separated random linear network coding based on cooperative medium access control," IEEE Netw. Lett., vol. 3, no. 2, pp. 66–69, 2021.

[11]. X. Wang, H. Li, M. Tong, K. Pan, and Q. Wu, "Network coded cooperative multicast in integrated terrestrial-satellite networks," in 2019 IEEE Symposium on Computers and Communications (ISCC), 2019.

[12]. K. Zhang, L. Yin, and J. Lu, "Feedback-based adaptive network coded cooperation for wireless networks," EURASIP J. Wirel. Commun. Netw., vol. 2011, no. 1, 2011.

[13]. S. Hong, K. Cheun, H. Lim, and S. Cho, "Performance of M-ary turbo coded synchronous FHSS multiple access networks with noncoherent MFSK under Rayleigh fading channels," J. Commun. Netw., vol. 15, no. 6, pp. 601–605, 2013.

[14]. F. Aliyu, T. Sheltami, M. Deriche, and N. Nasser, "Human immune-based intrusion detection and prevention system for fog computing," J. Netw. Syst. Manag., vol. 30, no. 1, 2022.

[15]. Anandakumar Haldorai, Shrinand Anandakumar, "An Design of Software Defined Networks and Possibilities of Network Attacks", vol.2, no.3, pp. 088-097, July 2022. doi: 10.53759/181X/JCNS202202012.