IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Ingénierie des Systèmes d'Information
Vol. 27, No. 1, February, 2022, pp. 29-39
Journal homepage: http://iieta.org/journals/isi

# A Comprehensive Review on Intrusion Detection and Prevention Schemes for Network Coding Enabled Mobile Small Cells

Chanumolu Kiran Kumar*, Nandhakumar Ramachandran

School of Computer Science & Engineering, VIT-AP University, Andhra Pradesh 522237, India

Corresponding Author Email: mounikakiran.138@gmail.com

https://doi.org/10.18280/isi.270104

**Received:** 6 November 2021
**Accepted:** 12 January 2022

***Keywords:***
*intrusion detection, intrusion prevention, network coding, mobile small cells, DDoS attacks, pollution attacks, entropy attacks, jamming attacks, network security*

**ABSTRACT**

With technological breakthroughs and increasing network technology reliability in daily life, it is vital to provide robust network-based system operations. According to the Comprehensive Error Rate Test Report, as network attacks become more common, the number of attacks nearly doubles or triples every year. The fifth-generation mobile communication is going to provide a connecting world with almost zero Latency. Network coding has emerged as a viable answer to the mostly efficiency, secure network needs for coming-generation networking technology. A small cell environment with network coding allows an effective system to communicate with the high rate of data. A significant countermeasure for several forms of network attacks is the Intrusion Detection Systems (IDS). Unique IDS solutions which are lightweight but also provide a high level of security are therefore demanded. The main security concerns in collaborative networks are Distributed -Denial- of- Service (DDOS) attacks, pollution attacks etc. While the network efficiency of non-DDOS attacks is also impaired, the impact of DDOS attacks is severe. In DDOS attacks, the specific node as a victim floods and mass traffic jams occurs, affecting the entire network performance. However, small, NC-enabled mobile cells, due to the essential NC vulnerabilities, are susceptible to pollution attacks. This article presents a brief survey on intrusion detection and mitigation schemes for Network Coding environment Mobile Small Cells.

## 1. INTRODUCTION

Since the early 1970s, mobile wireless industry has begun to develop, revolutionise and evolve technology. In recent decades, 4 or 5 generations of technological innovation and development have experienced mobile wireless technologies [1]. In recent years the world's telecommunications service has made a big leap. It is therefore necessary to explore the diverse generations of cellular networks as examined in mobile communications evolution from the first generation to the present Generation (5G) [2]. The digital world is undergoing a paradigm change in networking systems technology and design with the 5G networks. Cell traffic is explosively rising recently, higher data rates have continued to be sought and mobile communications have increased constantly, leading to the 5G mobile communications [3]. The ways of using cell phones in very high bandwidth have changed with 5G mobile technology.

Mobile consumers now have a lot of mobile technology knowledge. 5G technologies provide all kinds of innovative functionality, making 5G mobile technology the most effective and demanding in the short term. 5G communications aim at achieving bandwidth in big data, limitless networking capabilities and extensively covered signalling to support a wealth of high quality, customised service to customers while reducing mobile operators' equity and operating costs [4].

Mobile small cell technology is well-thought-out a 5G technology that provides cost-efficiency and energy efficiency in providing pervasive 5G services. Reliable wireless connectivity with good performance is a main goal of the coming generation of communication technologies. In a cooperative environment, networking will considerably increase the network's throughput performance. Network coding is the perfect option for better efficiency in the fifth generation of communication networks recognitions to cell technology and system for device communication.

In this regard, a large range of enabling technologies would be included in 5G Communication Systems. The 5G systems are likely to see changes in the paradigm of the underlying technology and radio access networks in order to solve these multifaceted scenarios [5]. Even the wireless infrastructure is revamped and a human-focused small cell network and multi-layered cell structure which currently has also been changed for the central cell station to facilitate device connectivity without the involvement of the base stations [6].

In addition, 5G networks would benefit from many new concepts, such as artificial intelligence, block chain and Network Coding (NC) [7]. In the collaborative small-cell setting, network coding is very useful because coding packets can be transmitted over the network for high performance and reliability [8].

### 1.1 Characteristics of 5G technology

The characteristics of 5G Technology are given as:

- 5G technology has a wide bandwidth and a low

latency.

- The technology provides 5G carrier delivery gateways with unrivalled full stability.
- 5G data transmission information delivers more precise and consistent results.
- 5G also supports a private virtual network.
- The downloading and uploading speeds of 5G technologies are extremely fast.
- 5G is a very fast network that establishes a trusted network.
- Every day, customers have quick access to the internet with high band 5G technology for sharp, passionate cellular phones.
- Mobile phone users can also download cell phone recording 5G technology.

A network with high service quality is expected to be effectively served by future wireless networks utilising the available bandwidth. In the 5G and beyond wireless networking, the idea of small cells is studied extensively [9]. The technology for small cells is regarded as an important 5G technology that enables reliable and economical delivery of ubiquitous 5G services. Small cells are cellular radio access nodes with very less power that has a small range. In reality, mobile small cells can be installed on demand anywhere, in any unit, which cover the urban landscape.

At the core, small cells are wireless senders and receivers designed to provide network coverage to very small areas. So, whereas big, high power "MACRO" towers keep the signal stronger throughout long distance, small cells are suitable for more closely developed environment like cities. Mobile small cell hotspots provide a host of 5G wideband networks at low cost, with a lower effect on mobile battery life. As wireless senders/receivers are looking for to "densify" present available wireless networks to provide data requirements of 5G, then small cells are presently observed as a solution to provide quality, improve network capacity, Re-using the same frequencies. The small cells don't penetrate walls, and don't travel too far, so these are important for in-build coverage such as buildings and offices -Mm wave signals.

Network coding can be used for high efficiency and wireless network energy saving. unlike the traditional coding systems, which can simply store/forward the packets, the network coding provides coding at the intermediate nodes. An effective network-coding environment requires an efficient integration scheme to address security issues such as pollution attacks and thus take advantage of network coding [10]. Network coding is a part of information theory and coding theory and it is a method of getting maximum data flow in a network. Network coding can be a successful solution for wireless networks because of limited transmission capacity, packet loss and energy usage restrictions. Network Coding is commonly divided as State-aware protocols and state-less protocols. Every node has some or whole network state details such as the network topology and packets available in neighbours' buffer in state-aware network code protocols. On the basis of this knowledge, a network code that can be decoded by the neighbouring nodes is created. The stateless network coding protocols, on the other hand, do not depend on network state data to determine when and how the packets can be mixed at each intermediate node. Thus, dynamically evolving topologies do not impact stateless network coding protocols.

NC technology can be perceived as a promising way to increase its throughput and boost its capacity for the wireless network with mobile small. From history NC technology is an emergent paradigm for communiqué that can provide significant network benefits by reducing packet transmission in wireless multi-casting model, improving network capacity, and ensuring packet loss robustness and low energy consumption. Despite NC technology's important benefits, NC enabled networks are however susceptible to different types of attacks. In light of this issues and since the safety of coming versions of 5G networks, NC enabled mobile small cells is analytically important for the success of identification of several types of attacks, novel protection mechanisms are required. To that end, the first move is to identify security threats in these networks.

New security problems, such as pollution attacks and entropy attacks, jamming attacks are present. In particular, pollution attacks are considerably challenging as infected packets are highly transferrable and difficult to detect [11]. A polluted packet has the same size and characteristics as a real packet [12]. There are various types of pollution attacks, such as data pollution attacks, in which the data in the packets is modified to disrupt the system's integrity, and tag pollution attacks, in which the tags appended to the packets, are modified without disturbing the data in the packet to confuse the receiver. Because the packets being forwarded are linearly coded at the intermediate nodes, generic integrity schemes are frequently scrapped in the field of network coding [13]. In network coding environments, homomorphic integrity schemes are used to detect pollution attacks. Malicious clients attempting to disrupt the system's diversity and tit-for-tat exchange balance are referred to as malicious attackers. In pollution attacks a malicious node injects polluted packets where as in entropy attacks the malicious node creates non-innovative packets in both cases the result is a severe degradation of the system performance. Malicious clients trying to inject bogus blocks in the content distribution process is called Jamming attack.

Ito design a cost-effective and energy-efficient method of delivering ubiquitous 5G services, small cell technology is the way to go. Indeed, movable tiny cells can be set up at any location at any time on any gadget to cover the metropolitan environment. In order to experience a wide range of 5G internet services at low cost and with minimal influence on mobile battery life, mobile small cell spots are the ideal vehicle.

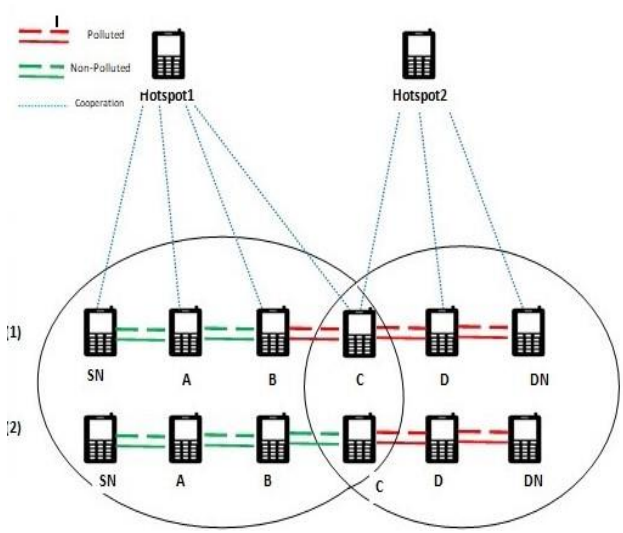


**Figure 1.** Pollution attack detection in nodes

The network design of 5G and beyond will be hybrid and multi-tiered by necessity, with ultra-dense small cells, to achieve the expected 1000-fold capacity. With self-organization, configuration, and maintenance, future wireless networks will be more resilient. This will involve collaboration among different nodes, tiers, and transmission layers.

The attacker's location can be found by using hotspots as shown below in Figure 1.

Here the adversary node is C. in case (1) attacker is fake, i.e., it is lying but in later case attacker cannot lie.

### 1.2 Homomorphic message authentication codes (HMACs)

HMACs are mostly used and are smaller in overhead associated to homomorphic signature or hashing techniques [14, 15] Homomorphic encryption means performing computations on its encrypted data even before decrypting it, so now, there is no need to use the secret key. While the results of this calculation are encoded, the user of the private key has access to them. Next, we will decrypt it and obtain the desired output. The important note here is that in both cases we got the same output. There are different types of homomorphic encryption, PHE (partial), SHE (somewhat), FHE (fully) based on circumstances we can use them.

Homomorphic message authentication codes allow to validate the computation on a previously signed data, the main advantage is that the validity of this tag can be tested without knowing the original dataset. Homomorphic signature scheme is a digital signature scheme which allows you to verifies that the calculation of signed data is correct or not. Whereas HMAC is a private verification scheme, H-Signature is a public verification scheme.

### 1.3 Peer-to-peer networks (P2P)

P2P networks computations facilitated are very important to the research community because of the enormous unused potential of the P2P concept in addition, P2P architectures have the potential to adjust to failures and the rapidly evolving network topology with an adequate communication and efficiency with a temporary population of nodes and devices [16]. Therefore, P2P systems display a high level of autonomy and failure tolerance. The P2P idea is a paradigm change between the client or node models and a more decentralised user to a device model.

The peer model permits end users to communicate directly to other internet users, to create communities and to cooperate, to produce virtual supercomputers, huge systems of files that can possibly be stored unlimited, user-created search engines and other new applications. P2P researchers and developers focused primarily on content delivery and file share systems, with particular emphasis on algorithms for improving query processing efficiencies and data search accuracy on P2P networks [17-26], resulting in a community that understands problems, techniques and solutions. The next generation of P2P systems will increasingly focus on enabling peers not only to exchange information safely and confidently, they will also enable peers to offload tasks for other peers and enable the development and deployment of commercial software systems that allow advanced P2P interactions and collaborations.

### 1.4 Cooperative communications (CC)

CC provide better utilization of communication resources, by allowing nodes in a network to collaborate with each other. It is auspicious technique for next generation communication systems. In network coded cooperative environment, we can take the benefits from mobile clouds and the random linear network coding to decrease the energy usage in the devices, which are participating in the communication. Normally nodes can cooperate to distribute data, but here they can save themselves by altering all other nodes when a malicious activity happens in the network.

Because of NC's intrinsic weaknesses, NC-enabled mobile small cells are susceptible to pollution attacks. In spite of numerous attempts to detect pollution attacks, the attackers may still infiltrate coded packets sent from the source node to the destination nodes in the next transmission.

The NC enabled small cell environment is depicted in Figure 2.

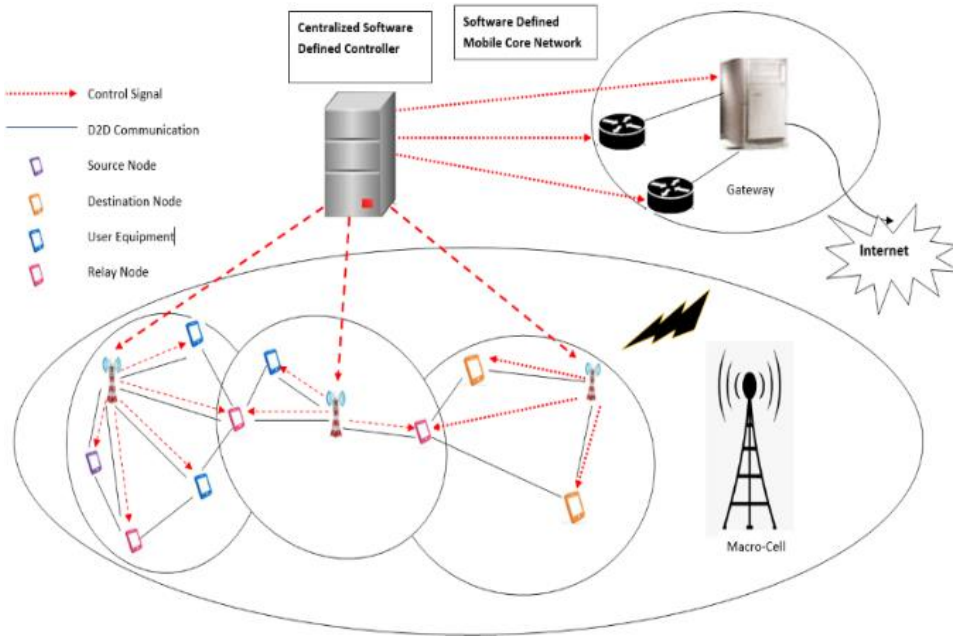


**Figure 2.** Network coding enabled small cell environment

## 2. LITERATURE SURVEY

The initial concept of network coding was to improve bandwidth and information flow in a communication network by enabling the transitional nodes to code the packets in the transmission. Additional investigations have begun to investigate other advantages of network coding, such as energy efficiency, latency, durability, and poor safety.

For NC-enabled mobile small cells, Parsamehr et al. [1] devised a new intrusion detection / prevention technique. In the proposed scheme, pollution attacks are detected and mitigation steps are performed to reduce the chance of an intrusion incident in a zero-space Homomorphic Message Authentication Code (HMAC) scheme. For small mobile NC-enabled cells to reach their full potential, intrusion prevention systems are crucial for identifying and reducing pollution attacks. The proposed scheme drops the polluted data packets and the attacker has no possibility of distributing the corrupted packet on the network without identifying, to protect NC-enabled mobile cells against waste of energy and network resources. The attack identification and labelling of the attacker nodes is also not concentrated in the proposed model.

### 2.1 Intrusion detection models

Parsamehr et al. [2] Suggested an Intrusion Detection and Location-aware Prevention (IDLP) system that doesn't just locate and dump corrupted packets, but also identifies the correct position of the attacker to block/suspend them and avoid or limit the pollution of packets in future transfers. Identification and localization are accomplished via the IDLP technique, which utilises a MAC system with a homomorphic null-space for identification. The proposed model identifies the location of attackers but because of mobility nature, the attackers move from one location to the other which represents that the proposed model takes much time to find the perfect location of the intruder. To analyse the contents much care, need to be taken for identifying and avoiding malicious nodes in the network. Otherwise, the totally network performance will be degraded if any node is compromised.

Adat et al. [3] proposed a scheme to classify and locate adversaries in a network, network coding environment that enables mobile nodes. It also addresses a protocol to prevent adversaries from misleading the network. Identifying pollution attacks and avoiding further attacks is a priority for ensuring a high output in an environment allowed by network coding. The network efficiency can be significantly improved by adapting network coding to a huge small cell environment that identifies malicious nodes and makes their existence known to other nodes until malignancies are carried out. The proposed model provides a malicious network coding identifier for mobile small cells. The proposed model does not concentrate on identification of all kinds of attacks. The proposed model can identify a limited attack type that does not achieve better performance levels.

Roychoudhury et al. [7] presented a hierarchical framework that focuses Mutual authentication and key agreement (HGMAKA) protocol to enable the small cell-based heterogeneity architecture consistent with 5G networks to deliver MTC services. Because of this, it has been proved that the Message Authentication Code-based technique is both robust and flexible to heterogeneous network architecture while still using minimal resources. This model introduces HGMAKA, a hierarchical group-dependent shared authentication system, for machine-type interaction over the LTE network. This architectural model uses a heterogeneous femtocell system, which will be in line with future 5G networks, as well as a mobile femtocell network. A big network group intrusion detection is not the focus of the model.

Lawrence et al. [8] propose using the HMAC authentication technique. Systems for NC-supporting networking that not only identify and drop compromised packets but also recognise hostile nodes that launched the attack are now used as authentication. In order to enhance the efficiency of an NC-enabled network, nodes that detect malformed packets should be able to repair (solve) the mistakes they find. As a result, the number of attacks is reduced, and connectivity performance improves as a result. As a result, retransmission communication costs are eliminated, and throughput is increased. Now we have a system that can detect pollution attacks, repair corrupted nodes, and identify the sources of pollution assaults.

A novel homomorphic MAC-based wireless sensor network system known as Dual Homomorphic MAC was introduced by Esfahan, Alireza et al (Dual HMAC). This proposed approach would incorporate two tags: one to protect against data pollution assaults, and the other to identify pollution nodes. Because a few contaminated messages can ruin a bundle of genuine messages, network coding-activated intermediary pollution attacks are common. Data pollution assaults and partially tag pollution assaults in this scheme are both resisted by using two sorts of tags. The main redistribution model relates to partial defence against tag emissions. In addition, the system proposed experience low overhead communication and low overhead computing compared with other current systems. The proposed does not concentrate on tagging the pollution attacks to improve system performance.

Adversary network nodes can conduct pollution attacks on network coding because of this inherent vulnerability. Because even a good or authentic node's output is corrupted if even one of the receiving packets is malformed, packet pollution blows out very quickly. In order to detect pollution assaults, Charles et al. [12] proposed a new homomorphic signature method for the network coding environment. Any linear grouping of received packets can be signed using the homomorphic signature feature without addressing the validation authority. This research is based on an elliptic curve, which increases performance while also detecting assaults and authenticating data.

Yu et al. [13] suggested a homomorphic signature feature to allow the relay nodes to generate and validate received messages (signatures) and prohibit them from generating signatures for polluted nodes without the involvement of signing entities (source). Where as in other schemas the validation process is done at sink node only, but in this proposed method relay nodes can also validate. in this scheme, no extra safe communication channel is needed. The experimental findings indicate that their efficiency of verification is up to 10 times higher than other related works. Here we are using the source authentication and batch verification technique. Because each intermediate node's encoding operation can affect the original source's signatures, signatures are a preferable alternative in this approach.

Network Mobile small cells enabled for coding are

regarded as prospective 5G networks, which can cover the urban environment on demand anywhere and in any devices at all times. Irrespective of the advantage of network coding in these networks, pollution attacks should be tackled prior network coding in small mobile 5G cells that reaches full potential. The intrusion detection and prevention technique proposed by Parsamehr et al. [20] is capable not only of detecting and preventing contaminant attacks but also for detecting the actual position of adverse nodes that cause pollution attacks. In the future, the author planned to expand the proposed IDPS to a collaborative IDPS which not only identifies the pollution attacks' source(s), but also to protect mobile small cells from being depleted on resources by mobile network coding when exposed to those attacks (such as CPU power, memory and battery level. The following Table 1 shows the limitations of intrusion detection models using H-MAC technique.

**Table 1.** Intrusion detection models

| Ref No. | Proposed Method | Limitation Observed |
|---|---|---|
| [1] | Zero-space, Homomorphic Message Authentication Code (HMAC) scheme, for identifying pollution attacks and measures to mitigate the risk of an intrusion incident. | Not made any attempt to correct it or to retransmit the corrupted packets to improve the packet delivery rate. The attack identification and labelling of the attacker nodes is also not concentrated. |
| [2] | Intrusion Detection and Location-aware Prevention (IDLP) mechanism not only detects and drops polluted packets, but also identifies the correct location of the attacker. | Due to mobility nature, it takes much time to identify the correct location. The packet size of the polluted attack is won't change. We have to analyse the polluted packets for identifying correct one. |
| [3] | Classify and locate adversaries in a network coding environment that enables mobile nodes. It also addresses a protocol to prevent adversaries from misleading the network. | Does not concentrate on the methods of removing the malicious behaviour nodes from the network, and not allowing them for further communications. only can identify limited attack types. |
| [7] | Hierarchical group based Mutual authentication and key agreement (HGMAKA) protocol. MAC based approach, for communication over the LTE network. | Due to cell based heterogeneous architecture, it is very efficient in resource use, and good choice for 5g communications, but, does not concentrate on detection of intrusions in a large network group. |
| [8] | HMAC authentication scheme. Current authentication systems for NC-supporting networks that not only detect and drop compromised packages, but also recognise malicious nodes that initiated the attack. | Identifies the rogue (malicious) node and recover the node which is affected, finds the root node causing the attack, but does not concentrate on identification of various attacks on the network. |
| [9] | New homomorphic MAC-based system called Dual Homomorphic MAC (Dual HMAC). Two tags would be included to resist attacks on data pollution and tag pollution nodes. | Does not concentrate on tagging the pollution attacks to improve system performance. Even with 2 tags we reduce the tag pollution attacks' partially only. It is good if it identifies both data and tag pollution attacks effectively. |
| [12] | New homomorphic signature scheme to detect the polluted packets. This will provide the authentication of data as well. | An adversary can forge the signatures or produce new one without knowing the points on the elliptic curve. Computations involves polynomials, discrete -logs. |
| [13] | The author suggested a homomorphic signature feature to allow the relay nodes to validate received messages without the signing entities. In this scheme, no extra safe communication channel is needed. | The homomorphic signature proposed model increases the load in the network as the instructions are complex and time consuming. The energy consumption is also high in the proposed model. |

### 2.2 Network code analysis models

Ho et al. [14] explained how the random network coding is utilised to detect pollution assaults in an environment where it is random where it is distributed. In this case, no encryption functions are being applied. Randomly distributed nodes can choose from a finite field of random linear mappings on their own here. The packets can be verified with data and a hash symbol provided at the beginning of transmission by employing a packet-based randomised network coding technique. a good packet is one that a receiver receives with no changes made to the data and whose contents are unknown to anyone else. Network coding's distributed randomization and path diversity lend support to this hypothesis. Since no cryptographic function is used here, the computational complexity will be relatively large.

A MAC homomorphic system randomised linear network coding subspace features and zero verification keys were suggested by Kehdi and Li [15]. Redundancy in the space domain improves the performance of randomised network coding. The author also suggested a novel and computational efficiency security approach known as Null Keys to discover pollution threats based on random linear network coding's subspace features. The participating nodes examine if a block is part of the subspace covered by the source blocks to ensure its integrity. A vector orthogonal to all possible permutations of the source blocks must be present at every node in order for this to be achievable. Null keys are vectors that are part of the source blocks' null space and are dispersed in a random manner by the source. Through simulations, he also shows that the Null Keys strategy is more effective in controlling the pollution spread than collective security using homomorphic hashing.

Torre et al. [22] presented an advanced Network Code (NCC) network content distribution frame, which benefit from the interplay of Mobile Clouds (MC) and Random Linear Networks (RLNC) coding, which reduces total energy consumption in the communication devices. Unknowns remain outside the scope of this research and have to be researched further. Examples include the construction of the MC, maximum nodes per cloud, the investigation of MC-interference, mobility and handover. Another problem is that UEs have active mobile antennas and Wi-Fi. The latest generation of mobile high-end gadgets presents this feature.

The network would be clogged with redundant, low-value packets that give no added value, and a lack of substitutes would leave it vulnerable to packet loss. The Newton-

Raphson technique was used by Torre et al. [24] to develop a novel formal model that predicts how many losses a system will experience if the RLNC is implemented. The sender can select the minimum number of RLNC redundancies needed to keep packet loss to a manageable level. This research may examine a more complex architecture or a number of RLNC procedures for error correction. In addition, this research opens up fresh comparisons in similar situations across different optimization strategies.

They found that the chance of effective achievement was lower than the literature's approximation (Tsimbalo et al. [25] estimated it to be). The RLNC version also received a fresh performance evaluation, which was given by the researchers. This performance methodology is tested using extensive Monte Carlo simulations that look at how network and code parameters affect performance. Particularly for non-systematic RLNC, they demonstrate that the average square bound error for a 10-user network may be reduced to 910. It is possible to use the assumed limitation to the chance of good delivery for additional performance indicators, such as the mean decoding delay or energy efficiency. In addition, the findings can be applied to other network topologies, such as relays. To increase the boundaries' usefulness in non-systemic circumstances, it may be possible to reduce their complexity even further.

Error correction codes are employed to provide packet robustness. In particular, one of the most successful is random linear network coding. The network coding interaction with mobile clouds generates a mesh network in which nodes can receive information from different sources. RLNC was however optimised to enable D2D communications with an in-order delay. A new heterogeneous mesh network where nodes receive packets from various pathways has to be adapted by RLNC. In this study, Torre et al. [27] proposed a mechanism for enabling the simultaneous management of traditional RLNC protocols through several generations. Higher complexity studies must be developed which vary from sub-decoder to sub-decoder numbers, network conditions, code ratio, generation size, or packet size, among other parameters. In addition, it is also necessary to consider the capability of changing the optimum amount of sub decoders on the fly.

Pandi et al. [28] developed a new PACE RLNC approach that paces coded redundant package transmission throughout source symbols generation and evaluated it. The paced encoded packets can be used without waiting for the finishing of the generation to recover dropped source symbols. Compared to tail RLNC, rigorous simulation assessments show PACE-Uniform considerably reduces the average source symbolic latency while reaching almost the same chance of loss. The authors show additionally that the PACE-Burst generalises the pacing notion in redundant packet transmission and that the number of encoded packets in a burst can be controlled flexibly between the PACE-Uniform and the traditional tail RLNC. In conjunction with sparse RLNCs, another path is to consider the PACE technique, which can further speed up RLNC processing. The following Table 2 shows the limitations of network code analysis models using XOR and RLNC techniques.

### 2.3 Network communication models

These systems use a homomorphic hashing algorithm that the source applies to the communications. When sending the determined hash values between nodes, these systems frequently use additional secure channels. To verify midway nodes instantly, Krohn et al. [10] developed a well-known homomorphic hash method.

**Table 2.** Network code analysis models

| Ref No. | Proposed Method | Limitation Observed |
|---|---|---|
| [14] | Proposed how the distributed randomized network coding is used to detect the pollution attacks in a randomly distributed network coding environment. | Performance levels are poor for checking the integrity levels in the network. Here no cryptographic function is used, so computational complexity will be high. |
| [15] | MAC homomorphic system for detecting pollution attacks based on random linear network coding subspace characteristics using zero verification keys. | Because numerous zero keys are used in every generation, a high overhead bandwidth can arise. And computationally expensive. no mitigation after detecting the attack. |
| [16] | Multiple MACs are attached to each packet from the source. This concept can be used for XOR coding networks, but it is susceptible to tag pollution attacks. | Even though XOR coding networks can make use of this technique, tag pollution attacks can compromise the security of the system. |
| [22] | Because mobile clouds and Random Linear Network Codes (RLNC) are both used in this system, the total power consumption on the devices participating in communication can be reduced. | Unknowns about the power consumption have yet not been made available and will be further examined. There is another difficulty when EUs are supplied with active mobile antennas and Wi-Fi. |
| [24] | A new model to forecast how many packet losses a system will have when RLNC is used, in this architecture the sender can specify the minimum number of redundancies in RLNC required to keep packet loss below a certain threshold. | This work can be focused on a broader topology in the proposed model is unable to identify the root cause for packet pollution and the similar applications in this work opens new opportunities for additional comparisons of different modes of optimisation. |
| [25] | Proposed a lower limit on delivery success, which would be more accurate than the previous upper limit. In addition, a new performance evaluation was added to the RLNC systemic edition by the author. | The findings can be applied to various network topologies, including such relay networks, for analysis. In the non-systematic scenario, further reducing the complexity of the boundaries could improve their usefulness. |
| [27] | a method to improve conventional RLNC protocols by the simultaneous administration of multiple generations. They also identified potential trade-offs between the innovative technique and standard RLNC protocols. | The RLNC protocols improve the latency of the packet delivery and the transmission rate is also high in this model that reduces the system performance. |
| [28] | Proposed and tested a unique RLNC PACE technique to pace redundant coded packet transmissions throughout source symbol production. | In combination with the sparse RLNC, a further technique will be examined, which can expedite the processing of RLNC further that improves the accuracy of the model. |

The decentralisation key administration method built expressly to guarantee security in a network that benefits from NC-MSCs has been introduced by de Ree et al. [18]. They spread the Certificate Authority (CA) functions using secret thresholds in the key management scheme. A share of the master private key is delivered to each network node so that key management facilities are offered 'any time, everywhere.' Finally, the self-generated certification paradigm is used by the distributed CA. Thus, certificates may be issued and updated without the CA's dispersed interactions that decrease overhead transmission.

Liu et al. [19] Presented a D2D communication environment network-coding video distribution strategy. The H.264 video transmission uses network coding technology which can also provide safety for important video information. This allows recipients, especially in networks with interference, to decrypt the original video that is highly likely. Results from simulation reveal that after network coding, video quality is improved. The clinical and oncological translation potential of suggested protocols and algorithms should be excellent. In future study the author wants to examine and undertake task-based assessment of the proposed approaches on real patient data sets.

Device-to-device communication is a versatile technique which can discharge heightened traffic into 5G networks. There are, however, significant security problems due to its open nature. The LTE-A standard introduced methods for security and safety, including mutual authentication between EUs and the eNB. D2D communications, unfortunately, confront different threats: jamming, change of data, free retention and breach of privacy. Haus et al. [21] proposed architectures with a variety of security threats and needs for the LTE-D2D system and its applications. Furthermore, with the use of cellular networks, social trust and reputation should be brought into the system. It is also interesting to examine how device mobility in channel-based main agreement methods impacts key rates and entropy.

If mobile devices are close to one another and engaged in the same content, D2D networks such as Wi-Fi direct can be used opportunistically to establish a collaborative (and cooperating) cellular and D2D network infrastructure. However, understanding, quantifying, and leveraging the network coding potential for collaborating mobile devices in a cellphone/D2D arrangement is critical. It was studied by Keshtkarjahromi et al. [29] who came up with a solution that included two parts: (1) a network coding structure designed for cooperative portable devices in joint cellular/D2C settings, where the link capacity is identical, and (2) a network code achievement framework designed to restore the proposed system coding framework's packet completion times (i.e., the number of transmission slots).

Li et al. [30] suggested an adaptive RNC (ARNC)-based hybrid multicast and D2D transmission system to boost the network performance of a packet erasure channel. The suggested approach optimises the packet encoding structure in accordance with the network status such that User Equipment (UEs) can still decode meaningful data and regenerate new packets encoded to the D2D communications, although only a partial set of encoded packets are received. In this hybrid mode the effect of an erasure channel can be successfully eliminated and the total network output improved. The simultaneous broadcast of the multicast and D2D communications is considered for further investigation. Thus, the system model considers the signal interference noise ratio (SINR). In this case, the new scheduling and the RNC decoding strategy are being studied to maximise network performance. The following Table 3 shows the limitations of network communication models like D2D communication techniques.

**Table 3.** Network communication models

| Ref No. | Proposed Method | Limitation Observed |
|---|---|---|
| [10] | Well-known homomorphic hash system that enables on-the-fly verification of midway nodes. Verification time is very less and more accurate. | The process of key generation is complex in the proposed model and the nodes for verification are also limited. As the network size increases, the time for verification is high. |
| [18] | DISTANT, A decentralized key management scheme. Provides network security that takes advantage of NC-MSCs. | The safety of the key management system will have to be evaluated on the basis of a contradictory model that is practical and appropriate for NC-MSC and safety evidence that is nor observed in the model. |
| [19] | A video distribution strategy based on network coding for D2D communication has been proposed. | In video processing it is complex that improves the load on the model. It impacts the performance of the system. The complexity can be reduced by using the symmetric encoding technique. |
| [21] | latest security and privacy solutions for D2D communication in order to gain a better knowledge of the fundamental issues and possible remedies for D2D security and privacy. | D2D security and privacy solutions to be designed and implemented that is not considered here is a major drawback of this model. |
| [29] | For cooperative mobile devices, we developed an open-source code network infrastructure with the same capability for cellular and D2D communications. | Results of simulation confirm the considerable reduction in package completion times for NCMI-Batch and NCMI-Instant but the time complexity is high that need to be reduced. |
| [30] | To boost network capacity under packet erasure channels, proposed a multicast hybrid and D2D Transmission Scheme based on adaptive RNC (ARNC). | It takes account of the signal interference noise ratio (SINR). In this circumstance, the new scheduling and RNC decoding scheme are studied to maximise network performance for better results. |

### 2.4 Collaborative models

To detect Firecol-based flood DDOS attacks and block attacks using Dynamic Growing Self-Organizing Tree, Poongodi and Bose [4] created an intrusion detection and prevention system (DGSOT). Firecol and DGSOT were used to detect and prevent processes in the proposed model's IDPS system, which was unique at the time. There are also comparisons between the conventional IDS and the delays and efficiency output measures. Distributed Denial of Service

(DDoS) is the primary security threat in collaborative networks (DDOS). DDOS attacks aren't to blame for the poor performance of the network. Simulated outcomes suggest that the proposed technology enhances flood DDOS attack safety. According to the findings of the simulations, DGSOT is superior to Firecol for the identification and avoidance of intrusions (DGSOTFC). The proposed model concentrates on the DDoS attacks and not concentrated to identify attacks of other categories. The performance of the model is high in detecting DDoS attack but if any other attacks are identified in the network, the performance levels will be decreased.

Gkantsidis and Rodriguez [11] introduced an addition to Network Code-enabled Networks and by allowing cooperation verification further reduces the costs of the calculation of Hash Functions at each intermediate node. The homomorphic character of these signatures enables nodes to sign the receiving packets without touching the signing entity on a linear basis. The signature calculation covers the entire message increased.

Vasudevan et al. [17] examined network coding protection vulnerabilities and the subsequent countermeasures, in particular those imposed by pollution attacks. Due to the nature of coding and spreading through the entire network, specific attacks in network coding such as pollution attacks are extremely harmful. They harm the efficiency of bandwidth and even interrupt the correct decoding at receipt of any message. In addition, the authenticity of intermediate nodes in a wireless environment cannot be easily guaranteed and makes it easier for an intruder to join the network. There is a lot of research interest in the direction of secure network coding that leads to some interesting approaches. Most schemes, however, do not meet the necessary requirements or incur high device overheads. Schemes that effectively solve dense heterogeneous networks are still required for achieving better outcomes.

Network-coded cooperative systems for various cloud sizes were evaluated for their latency overhead, as described by Torre et al. [23]. Network traffic in 5G networks consists primarily of video data, with 5G networks containing heterogeneous data. The base station (BS) currently establishes one unicast connection to each user, which is inefficient because the BS sends repeated data to co-located users when users are close to one another and demand the same information (e.g., streaming services in stadiums, connecting information in trains, slide dissemination in conferences, etc.). Using Random Linear Network Coding (RLNC) and Mobile Clouds, Network-Coded Cooperative (NCC) networks improve network performance in the aforementioned circumstances. We have two things to provide in this paper: First, we describe a new approach for measuring latency that does not require synchronising the clocks within the computers. This approach as well as traditional timestamps is used to determine the latency in the NCC testbed. According to the findings, the average latency for three clients is 200 ms, whereas the average delay for four clients is 400 ms. In addition, we discovered a connection between packet loss and the number of clients in the MC.

Pandi et al. [26] demonstrated the combination of cooperative network coding and Random linear network coding, which allows for the use of dependable huge video cross-casting over regular LTE lines. The bulk of LTE traffic is discharged via Wi-Fi, enhancing the efficiency and size of the use of LTE canals. It shows how RLNC may be used to strengthen the stadium experience by broadcasting different user-choiced immediate playback systems. However, because of the logistical considerations, the stadium cannot be carried to CCNC's venue, but the demo includes all technical aspects. In the case of LTE receiving problems at the cited point, the demonstration is designed to reuse Ethernet connections and imitate the LTE connection with suitable loss models. The following Table 4 shows the limitations of co-operative/collaborative models

**Table 4.** Collaborative models

| Ref No. | Proposed Method | Limitation Observed |
|---|---|---|
| [4] | A new approach for detecting and preventing intrusions based on Firecol-based flood DDOS attacks and Dynamic Growing Self-Organizing Tree attacks to identify and prevent such attacks. | concentrates on the DDoS attacks only and not on other attacks. The performance is high in detecting DDoS attacks but it will be low for other attacks. |
| [11] | The homomorphic character of these signatures enables nodes to sign the receiving packets without touching the signing entity on a linear basis. | The proposed model hash functions are complex and the load of the system will increase thus results in poor network performance. |
| [17] | The author examined network coding protection vulnerabilities and the subsequent countermeasures, in particular those imposed by pollution attacks. | It does not meet the necessary requirements or incur high device overheads. Schemes that effectively solve dense heterogeneous networks are still required for achieving better outcomes. |
| [23] | Network-Coded Cooperative (NCC) networks A new latency measurement approach is presented where no clocks need to be synced inside the computers. | The overhead of the model is still not reduced to a satisfactory level. Based on the cloud sizes, the model has to balance the load for achieving better performance. |
| [26] | Showed how to perform reliable massive video multicasting over standard LTE links by integrating the Random Linear Network Coding and the Cooperative Networking principle. | In the case of problems with the LTE reception, the demo will revert to Ethernet connections and imitate the LTE connection by means of appropriate loss models that increases time complexity. |

### 2.5 Block chain enables small cells

It was proposed by Adat et al. [5] that the upgraded block chain small cell environment may be protected from pollution attacks by using a network coding model instead. An introduction of overhead transmission and latency issues is provided, as well as the tiny SECRET block chain's design. Due to network coding, small mobile cells can play an important role in enhancing overall network performance. Small SECRET cells must be protected against pollutant attacks at all costs. Assailants can readily breach the conceptual model cryptography algorithms, which weaken the system's security levels. Digital signatures, hashing, and encryption techniques can all be used in conjunction with the proposed architecture to increase security levels, and polluted

packets can be easily identified using HMAC and hashing techniques.

The SDN-based mobile cells were used by Adat et al. [6] to implement a secure network coding mobile cell that reduces overhead and time. This Security Scheme is modified by using this central unit as a security solution by some current approaches including Dual HMAC and Homo MAC. The proposed scheme follows similar message authentication systems, but uses the centralised controller's availability to cut computational and coordination costs across the networks. As the security problems must be addressed in advance, the work will focus specifically on security issues and examine an SDN based mobile small cell ecosystem enabled by network coding. In particular, the model addresses a message authentication code-based protection scheme against small cell SDN pollution attacks.

Adat et al. [31] proposed an "on block chain based secure network coding for mobile small cell. "This paper investigates the existing security architectures and proposes a secure network coding architecture that incorporates block chains to support efficient integrity schemes against pollution attacks. This block chain structure supports a homomorphic MAC-based integrity scheme against pollution attacks. Further, to avoid overburdening the end nodes, the block chain network only comprises the small cell heads and the end nodes connects to the small cell nodes as a central controller to communicate the tags. This architecture helps to reach a balance between the number of communication channels and storage and computational overhead on the end nodes for the integrity schemes and thus ensuring the maximum benefit of SECRET small cells.

**Table 5.** Block chain enhanced models

| Ref No. | Proposed Method | Limitation Observed |
|---|---|---|
| [5] | Network coding model that allows the enhanced block chain small cell environment to avoid attacks by pollutants. | The proposed model cryptography techniques are easily cracked by the attackers that reduce the system performance in terms of security levels. |
| [6] | Implemented secure network coding mobile cells that reduces overhead and time. This Scheme is modified by using this central unit with Dual HMAC and Homo MAC. | MAC scheme considers only nodes with high energy levels. The low energy level nodes are not considered and precautions not provided that reduces the system performance. |
| [31] | Presents a network coding architecture with secure block chains to facilitate efficient integrity methods beside pollution attacks. | All nodes in the network must be linked to a single centralized authority for inter-small cell communication. As a result, there is a single point of failure, as well as a convoluted communication system. |

Shnaiwer et al. [32] have researched the cloud download improvements by using F-RANs to allow heterogeneous LTE and Wi-Fi technologies to enhance remote radio heads (eRRHs). They first define the problem of CBS as an optimization problem over a dual conflict graph, which has proven unworkable. Thus, as a weighted graphic colouring problem, they created an online variant of the CBS offloading issue in heterogeneous F-RANs. Then, they designed a new heuristic solution to this problem that supports Opportunistic Network Coding (ONC) which breaks it into two sub problems and individually addresses each under problem. The study can be extended in the formulation of CBS download problem by looking at the customer download rates from CBS. The joint problem of both completion time and CBS offloading could be further expanded. Table 5 shows the limitations of block chain enhanced models for intrusion detection.

## 3. PROPOSED MODEL

The effective use, security and seamless co-operation of heterogeneous network systems is evident as one of the fundamental criteria for future wireless networks with validation and testing of communications architectures of 5G. Network coding is a possible technology that can guarantee bandwidth efficiency and extremely long-term connectivity, in particular with adverse Wireless Conditions. Network coding, without a security policy to protect data and the identity of communicators, may however be proved as a significantly deteriorating factor in network performance. Although various encryption schemes have been used in recent years to guarantee secure network coding communication, none have specifically been designed to solve the next fifth-generation small mobile network access paradigm.

In reaction to pollution assaults, both cryptographic and information theoretical solutions were used. To avoid data pollution and pollution assaults, time synchronisation and cryptographic systems that are considerably more compatible with latency applications are required in the proposed integrated schemes. However, many integration initiatives are prone to collusion. Each model has different tags and key distribution mechanisms in place to defend it from several attackers. There is a pressing need to provide a centralized model with Homomorphic MACS and advanced block chain enhancements to accurately detects network breaches and improves network performance.

## 4. CONCLUSIONS

The evolution of the 5G network results in large-scale wireless cellular network production, connectivity, and processing. The smart grid is thought to be useful in both existing cellular and forthcoming 5G technology. In the current energy markets, 5G communication with networks is being reinforced, which will give energy providers with new business models. Small cells must be widely deployed in 5G networks to maximise capacity per unit area. The existing wireless capacity is approaching the theoretical limit. From the standpoint of an operator, the frequency distribution is preferable to the spectrum distribution because frequency resources are scarce and frequency resources are used more effectively; however, interferences between macro-base stations and smaller base stations will seriously affect the system's output. Small cells' spectrum efficiency can be boosted by making frequency reuse more flexible in one location. This study provides a quick overview of intrusion detection on small cells enabled by network coding. The Internet is expected to be useful in future 5G networks in order to deliver extremely high data rates, seamless coverage,

a large number of linked devices, minimal latency, and so on. The complicated reliability of 5G networks is an important aspect in dealing with dense and rapidly evolving communications.

## REFERENCES


[1] Parsamehr, R., Esfahani, A., Mantas, G., Radwan, A., Mumtaz, S., Rodriguez, J., Martínez-Ortega, J.F. (2019). A novel intrusion detection and prevention scheme for network coding-enabled mobile small cells. IEEE Transactions on Computational Social Systems, 6(6): 1467-1477. https://doi.org/10.1109/TCSS.2019.2949153

[2] Parsamehr, R., Mantas, G., Rodriguez, J., Martínez-Ortega, J.F. (2020). IDLP: An efficient intrusion detection and location-aware prevention mechanism for network coding-enabled mobile small cells. IEEE Access, 8: 43863-43875. https://doi.org/10.1109/ACCESS.2020.2977428

[3] Adat, V., Parsamehr, R., Politis, I., Tselios, C., Kotsopoulos, S. (2020). Malicious user identification scheme for network coding enabled small cell environment. In ICC 2020-2020 IEEE international conference on communications (ICC), Dublin, Ireland, pp. 1-6. https://doi.org/10.1109/ICC40277.2020.9148736

[4] Poongodi, M., Bose, S. (2014). Design of intrusion detection and prevention system (IDPS) using DGSOTFC in collaborative protection networks. Fifth International Conference on Advanced Computing, Chennai, India. https://doi.org/10.1109/ICoAC.2013.6921946

[5] Adat, V., Politis, I., Tselios, C., Kotsopoulos, S. (2019). Blockchain enhanced SECRET small cells for the 5G environment. In 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Limassol, Cyprus, pp. 1-6. https://doi.org/10.1109/CAMAD.2019.8858457

[6] Adat, V., Politis, I., Tselios, C., Kotsopoulos, S. (2018). Secure network coding for SDN-based mobile small cells. In International Conference on Broadband Communications, Networks and Systems, pp. 347-356. https://doi.org/10.1007/978-3-030-05195-2_34

[7] Roychoudhury, P., Roychoudhury, B., Saikia, D.K. (2017). Hierarchical group based mutual authentication and key agreement for machine type communication in LTE and future 5G networks. Security and Communication Networks, Article ID: 1701243. https://doi.org/10.1155/2017/1701243

[8] Lawrence, T., Li, F., Ali, I., Kpiebaareh, M.Y., Haruna, C.R., Christopher, T. (2021). An HMAC-based authentication scheme for network coding with support for error correction and rogue node identification. Journal of Systems Architecture, 116: 102051. https://doi.org/10.1016/j.sysarc.2021.102051

[9] Esfahani, A., Yang, D., Mantas, G., Nascimento, A., Rodriguez, J. (2015). Dual-homomorphic message authentication code scheme for network coding-enabled wireless sensor networks. International Journal of Distributed Sensor Networks, 11(7): 510251. https://doi.org/10.1155/2015/510251

[10] Krohn, M.N., Freedman, M.J., Mazieres, D. (2004). On-the-fly verification of rateless erasure codes for efficient content distribution. In IEEE Symposium on Security and Privacy, Berkeley, CA, USA, pp. 226-240. https://doi.org/10.1109/SECPRI.2004.1301326

[11] Gkantsidis, C., Rodriguez, P. (2006). Cooperative security for network coding file distribution. In Proceedings of the 25th IEEE International Conference on Computer Communications (INFOCOM '06), Barcelona, Spain, pp. 1-13.

[12] Charles, D., Jain, K., Lauter, K. (2006). Signatures for network coding. In 2006 40th Annual Conference on Information Sciences and Systems, Princeton, NJ, USA, pp. 857-863. https://doi.org/10.1109/CISS.2006.286587

[13] Yu, Z., Wei, Y., Ramkumar, B., Guan, Y. (2008). An efficient signature-based scheme for securing network coding against pollution attacks. In IEEE INFOCOM 2008-The 27th Conference on Computer Communications, Phoenix, AZ, USA, pp. 1409-1417. https://doi.org/10.1109/INFOCOM.2008.199

[14] Ho, T., Leong, B., Koetter, R., Médard, M., Effros, M., Karger, D.R. (2008). Byzantine modification detection in multicast networks with random network coding. IEEE Transactions on Information Theory, 54(6): 2798-2803. https://doi.org/10.1109/TIT.2008.921894

[15] Kehdi, E., Li, B. (2009). Null keys: Limiting malicious attacks via null space properties of network coding. In IEEE INFOCOM 2009, Rio de Janeiro, Brazil, pp. 1224-1232. https://doi.org/10.1109/INFCOM.2009.5062036

[16] Yu, Z., Wei, Y., Ramkumar, B., Guan, Y. (2009). An efficient scheme for securing XOR network coding against pollution attacks. In IEEE INFOCOM 2009, Rio de Janeiro, Brazil, pp. 406-414. https://doi.org/10.1109/INFCOM.2009.5061945

[17] Vasudevan, V.A., Tselios, C., Politis, I. (2020). On security against pollution attacks in network coding enabled 5G networks. IEEE Access, 8: 38416-38437. https://doi.org/10.1109/ACCESS.2020.2975761

[18] de Ree, M., Mantas, G., Rodriguez, J., Otung, I.E. (2019). Distributed trusted authority-based key management for beyond 5G network coding-enabled mobile small cells. In 2019 IEEE 2nd 5G World Forum (5GWF), Dresden, Germany, pp. 80-85. https://doi.org/10.1109/5GWF.2019.8911711

[19] Liu, Y., Cheng, C., Li, Y., Wang, L. (2019). Network coding for reliable video distribution in device-to-device communications. In 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), Guilin, China, pp. 143-146. https://doi.org/10.1109/CyberC.2019.00033

[20] Parsamehr, R., Esfahani, A., Mantas, G., Rodriguez, J., Martinez-Ortega, J.F. (2019). A location-aware IDPS scheme for network coding-enabled mobile small cells. In 2019 IEEE 2nd 5G World Forum (5GWF), Dresden, Germany, pp. 91-96. https://doi.org/10.1109/5GWF.2019.8911650

[21] Haus, M., Waqas, M., Ding, A.Y., Li, Y., Tarkoma, S., Ott, J. (2017). Security and privacy in device-to-device (D2D) communication: A review. IEEE Communications Surveys & Tutorials, 19(2): 1054-1079. https://doi.org/10.1109/COMST.2017.2649687

[22] Torre, R., Leyva-Mayorga, I., Pandi, S., Salah, H., Nguyen, G.T., Fitzek, F.H. (2020). Implementation of

network-coded cooperation for energy efficient content distribution in 5G mobile small cells. IEEE Access, 8: 185964-185980. https://doi.org/10.1109/ACCESS.2020.3029601

[23] Torre, R., Salah, H., Nguyen, G.T., Fitzek, F.H. (2019). Evaluating the latency overhead of network-coded cooperative networks for different cloud sizes. In 2019 IEEE 2nd 5G World Forum (5GWF), Dresden, Germany, pp. 253-258. https://doi.org/10.1109/5GWF.2019.8911708

[24] Torre, R., Pandi, S., Nguyen, G.T., Fitzek, F.H. (2019). Optimization of a random linear network coding system with newton method for wireless systems. In ICC 2019-2019 IEEE International Conference on Communications (ICC), Shanghai, China, pp. 1-6. https://doi.org/10.1109/ICC.2019.8761304

[25] Tsimbalo, E., Tassi, A., Piechocki, R.J. (2018). Reliability of multicast under random linear network coding. IEEE Transactions on Communications, 66(6): 2547-2559. https://doi.org/10.1109/TCOMM.2018.2801791

[26] Pandi, S., Arranz, R.T., Nguyen, G.T., Fitzek, F.H. (2018). Massive video multicasting in cellular networks using network coded cooperative communication. In 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, pp. 1-2. https://doi.org/10.1109/CCNC.2018.8319324

[27] Torre, R., Pandi, S., Fitzek, F.H. (2018). Network-coded multigeneration protocols in heterogeneous cellular networks. In International Conference on Broadband Communications, Networks and Systems, pp. 357-366. https://doi.org/10.1007/978-3-030-05195-2_35

[28] Pandi, S., Gabriel, F., Cabrera, J.A., Wunderlich, S., Reisslein, M., Fitzek, F.H. (2017). PACE: Redundancy engineering in RLNC for low-latency communication. IEEE Access, 5: 20477-20493. https://doi.org/10.1109/ACCESS.2017.2736879

[29] Keshtkarjahromi, Y., Seferoglu, H., Ansari, R., Khokhar, A. (2018). Device-to-device networking meets cellular via network coding. IEEE/ACM Transactions on Networking, 26(1): 370-383. https://doi.org/10.1109/TNET.2017.2787961

[30] Li, B., Li, H., Li, X., Jiang, H., Tang, W., Li, S. (2018). Hybrid multicast and device-to-device communications based on adaptive random network coding. IEEE Transactions on Communications, 67(3): 2071-2083. https://doi.org/10.1109/TCOMM.2018.2882797

[31] Adat, V., Politis, I., Kotsopoulos, S. (2019). On blockchain based secure network coding for mobile small cells. In 2019 IEEE 2nd 5G World Forum (5GWF), pp. 274-279. https://doi.org/10.1109/5GWF.2019.8911729

[32] Shnaiwer, Y.N., Sorour, S., Al-Naffouri, T.Y., Al-Ghadhban, S.N. (2019). Opportunistic network coding-assisted cloud offloading in heterogeneous fog radio access networks. IEEE Access, 7: 56147-56162. https://doi.org/10.1109/ACCESS.2019.2913860