A lightweight security framework for network coding enabled mobile small cells

Vipindev Adat, Ilias Politis, and Stavros Kotsopoulos
Wireless Communications Laboratory
University of Patras, Greece
{vipindev, ipolitis, kotsop}@ece.upatras.gr

***Abstract*—Future wireless networks are expected to serve a dense network of mobile devices with high quality of service using the available bandwidth efficiently. Towards this end, the concept of small cells and cooperative networks are extensively studied in the 5G and beyond era of wireless communication. Network coding can be used to achieve high performance throughput as well as energy saving in wireless networks. However, efficient integrity schemes are necessary for a network coding environment to counter security challenges like pollution attacks and thus to exploit the benefits of network coding. In a network coding enabled mobile small cells, the security schemes can be optimised depending on the security conditions of the small cell deployment. Existing integrity schemes can be modified and optimised to reduce the latency and computational overheads using these conditions. This paper proposes a lightweight security framework for network coding enabled mobile small cells where the integrity check is limited to specific nodes considering the trustiness of the nodes in a small cell.**

I. Introduction

The fifth generation of wireless technology is already being rolled out in experimental and pilot studies around the globe. This new generation of wireless communication technology comes with a massive change in the perspective of communication networks than mere improvements in the bandwidth capacity. With the 5G networks, digital world is witnessing a paradigm shift in the technologies and architecture of the communication systems. 5G systems are expected to provide not just high data rate as enhanced mobile broadband (eMBB) compared to 4G, but also introduce new use cases including ultra reliable low latency communication (URLLC) and massive machine type communication (mMTC). To address these multiple use cases, the 5G systems are also expected to see paradigm shifts in the underlying technologies and radio access networks. Even the wireless infrastructure is redesigned and the base station centric cell structure that we are currently familiar with has been modified to a user-centric small cell environment and multi-layered cell structure which will also support device to device communication without the intervention of base stations. Furthermore, the 5G networks will also benefit from multiple novel concepts like artificial intelligence, blockchain, software defined networks, and network coding. Network coding proves to be very useful in the cooperative small cell environment where coded packets can be transmitted in the network to achieve high throughput and reliability. Possibilities of network coding enabled mobile small cells to cater efficiently the needs of future networks with reduced energy consumption and efficient bandwidth usage is under evaluation and showing promising results [1].

Network coding implementations help to achieve high throughput efficiency and resilience in a wireless environment, but they also suffer from multiple security challenges. On top of the generic security issues like denial of service and eavesdropping, the core idea of network coding enabling the intermediate nodes to code the packets, introduce new security challenges like pollution attacks and entropy attacks to the scenario [2]. Pollution attacks, in particular, are significantly challenging due to its high contagious probability and difficulty to identify the polluted packets. A polluted packet may not be different from the genuine packets in terms of packet size or characteristics. Generic integrity schemes also fail in the scope of network coding since the packets in transmission are linearly coded at the intermediate nodes. Thus homomorphic integrity schemes are being used in network coding environments to identify pollution attacks. Homomorphic message authentication codes (MACs) are extensively used in this aspect and provides secure network coding schemes with relatively smaller overheads compared to homomorphic signature or hashing schemes. A series of studies have been focused on secure network coding enabled mobile small cells and proposed integrity schemes suitable for such dense environments. However, most of these integrity schemes focused on identifying the polluted packets at the earliest genuine node.

Even though the computational and latency overheads due to this extensive integrity checks are very less, in a dense small cell environment, these overheads are cumulative leading to high computational power requirements and increased end to end latency. On the other hand, the probability of an attacker intruding to the network can be controlled and monitored by the small cell head. Moreover, the security and trust levels of each small cell will vary depending on different aspects like location and authentication policies. Thus a cooperative and adaptive security scheme will be more beneficial in the scope of energy efficient low latency communications. Towards this end, this paper proposes a lightweight security framework for network coding enabled small cell environment. This lightweight and adaptive framework is built on the blockchain enhanced integrity scheme [3], [4] where a cooperative en-

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie grant agreement No 722424

978-1-7281-6339-0/20/$31.00 ©2020 IEEE

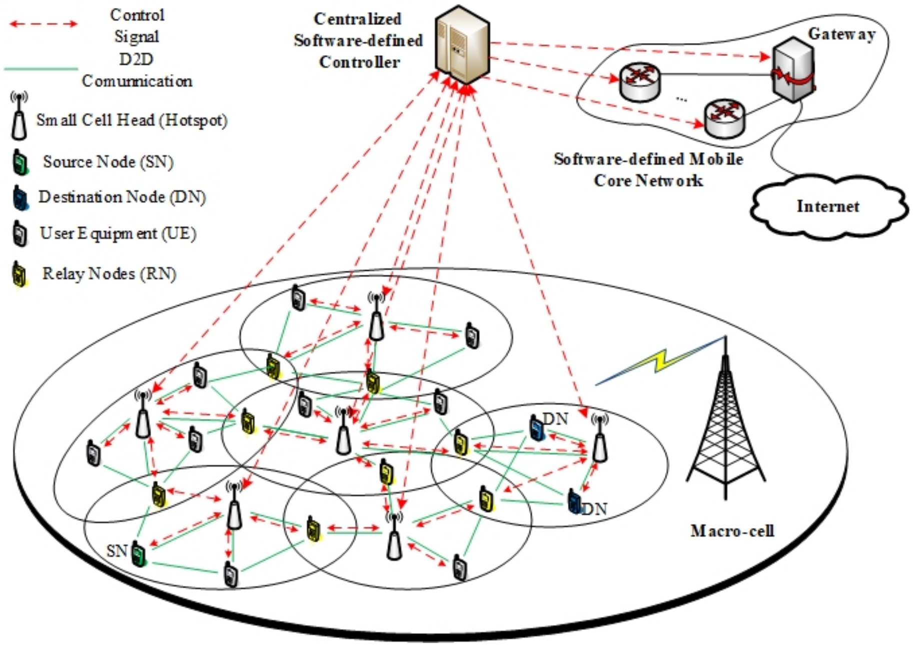


Fig. 1: Network coding enabled small cell environment

vironment of small cell heads and core network decides the security parameters and reduces the number of integrity checks to be done during the transmission. The remaining sections of the paper are arranged as follows. Section II discuss the important literature regarding existing solutions against pollution attacks in the backdrop of network coding enabled small cell environment. Section III explains the system model of the proposed lightweight integrity scheme and section IV discusses different scenarios and the adaptive security mechanism. Section V concludes the paper by discussing the possible extensions of the scheme.

II. Background and Related Works

Network coding was initially presented as an idea to optimize the bandwidth in a communication network by allowing the intermediate nodes to code the packets in transmission [5]. Further researches started to explore other benefits of network coding such as energy efficiency, latency, resilience and inherent weak security. The random linear network coding (RLNC) [6] shown the suitability of network coding to create a resilient wireless multicast and [7] showed the throughput and energy benefits of network coding in a device to device communication environment. The recent studies on secure network coding for reduced energy next generation mobile small cells (SECRET) [1] explores the idea of network coding in a small cell environment to serve a dense heterogeneous mobile network efficiently. The SECRET small cells also envision a dense network of mobile devices capable of sidelink communication as well as monitored and supported by small cell hotspots and an SDN based core network as shown in Fig. 1 [8]. The SECRET small cells also support cooperative radio resource management between the small cells to ensure all the relay nodes and edge nodes are provided with the best possible quality of service [9], [10]. These relay nodes can act as the gateway between different small cells for D2D communication and are controlled by both the small cell heads. In this proposed scheme these relay nodes also act as a security checkpoint for the incoming packets.

However, the security challenges inherent to network coding need to be addressed to exploit all these benefits. The security aspects of network coding were first studied in [11] to show how network coding provides weak security against wiretapping in general. However, more security challenges specific to network coding were identified later which includes pollution attacks and entropy attacks. Pollution attacks are inherent to network coding and it spreads quickly in the network since a single undetected polluted incoming packet can pollute the outgoing packets at a genuine node. There have been both cryptographic and information-theoretic approaches to address pollution attacks. Most of the information-theoretic approaches require time synchronization and the cryptographic schemes are more compatible with the low latency applications. Among the different cryptographic integrity schemes, the homomorphic MAC-based integrity schemes generally create smaller overhead compared to signature or hashing schemes as explained in [12], a detailed study of integrity schemes against pollution attacks. The homomorphic MAC-based integrity schemes are first proposed in [13] and extensively studied there onwards. Integrated schemes including homomorphic MACs and signatures were also proposed to prevent data pollution and tag pollution attacks [14], [15]. However, most of these integrity schemes are vulnerable to colluding attackers and requires a large number of tags attached to each packet and specific key distribution schemes to achieve security against multiple adversaries. This makes it practically difficult to employ in a dense and mobile network. To address these challenges, Adat et al. proposed a blockchain-based integrity scheme suitable for secure network coding enabled small cell environment [3], [4] where homomorphic MACs are shared through a blockchain overlay to efficiently defend pollution attacks without inducing impermissible overheads. An integrity scheme which identifies the exact location of the malicious user and notifies other participant nodes in the network about the attacker with the help of a central controller is presented in [16]. Other parallel works in this direction to address security challenges in a network coding enabled mobile small cell environment are based on a null space-based homomorphic MAC schemes [17], [18] which not only detect the pollution attack but also identify the adversary's location.

III. Security Framework

The blockchain enhanced integrity scheme explained in [3], [4] ensures that a polluted packet will be correctly detected by the immediate genuine node it reaches with a probability of $1/q^L$, where q is the field size and L is the number of tags. This integrity scheme performs the verification of tags in two steps. The tags received along with the packet are compared with the tags that can be retrieved from the blockchain and then verified against the received packet to ensure there are no tag pollution and data pollution attacks. However, this process involves verification of the L tags attached to them at every node. In a cooperative and monitored environment, this may be considered as an unnecessary overhead. All the participating devices need to be authenticated by the small cell head to be part of the network. The strict and regular authentication methods [19] ensure that every node in a small cell head has a level of trust by the small cell head. In a cooperative network, this trust factor can be considered to reduce security overheads. Considering this factor we define the security framework as follows.

A. System Design

The system architecture is a three layer architecture as shown in Fig.2. The base layer consists of the end nodes, including source, destination and intermedate nodes which are capable of sidelink communication. The nodes existing in the edge and connected to multiple small cells are called relay nodes. The small cell heads (hotspots) form the second layer and the third layer is the SDN controlled core network. The small cell heads and the central controller in the core network are considered as trusted entities with higher computational and storage capacities compared to the end nodes. The blockchain overlay that provides a secure distributed database for tag sharing is hosted by the small cell heads. The end nodes are connected to the hotspots in their corresponding small cell and there exists a dedicated control channel to provide controlling and security signals. Further, the small cell heads and SDN controller closely monitor the network and work in a cooperative manner to ensure the security of the network. In this cooperative security framework, the integrity check is initially performed only on the relay nodes instead of all the intermediate nodes. That is once a packet is generated, it will be only checked at the points where it may be transmitted to another small cell. The relay nodes act as a gateway node in these situations. If an attack is detected at the relay node, it will be reported to the central controller through the small cell head (hotspot) in the small cells serving the relay node. In this security framework, we assume the small cell heads and central controller are trusted agencies, and all the participating nodes have a secure control channel with the small cell head for control and security purposes. The blockchain-based database forms an integral part of the integrity scheme and it is distributed over the small cell heads as full nodes and other participating nodes as light nodes. The key distribution for the integrity scheme is performed in a decentralized fashion as explained in [20]. Only the full nodes are capable of verifying the blocks in the network, thus taking the computational overhead of verification process solely to them and the light nodes can only send a possible transaction to be included in the blockchain read the verified blocks. Whenever a pollution attack is detected, it will be informed to the small cell head and then to the central controller and they hold a record of reported pollution attacks. Depending on the security level required by the application, after a threshold number of attack detection, the integrity check will be made mandatory to all the participating nodes. The detailed description of the framework is explained in the next subsection.

B. Description

In the initial phase, all the authenticated nodes in a small cell are considered as trusted by the small cell head and thus trusted in that small cell. However, the relay nodes are connected to more than one small cell head and since these two small cell heads are not directly interacting with each other, the relay nodes have only partial trust compared to the other general nodes in the network. That is the relay nodes always act as a gateway node in the multihop D2D communications from one small cell to the other. Thus integrity checks are always performed before recoding or decoding the packets received at the relay nodes. This considerably reduces the number of integrity checks to be performed in the network and thus reduces the computational complexity of the system. Even though the tag verification process induces a very low latency, in a dense network with a large number of hops, it can accumulate to a distinguishable amount of delay. This reduction in integrity checks will be beneficial to achieve nearly real-time communication as well.

On the other hand, this lightweight scheme introduces a probability of pollution spread inside a small cell. If any of the nodes in the small cell is a malicious node that somehow passed the authentication process or an authenticated node is later compromised by adversaries, it can introduce a polluted packet to the information flow. However, it will only be detected in the next relay node. Till that time, the polluted packet will be in transit and possibly polluting multiple packets. Thus deciding whether to go for a lightweight scheme or to continue

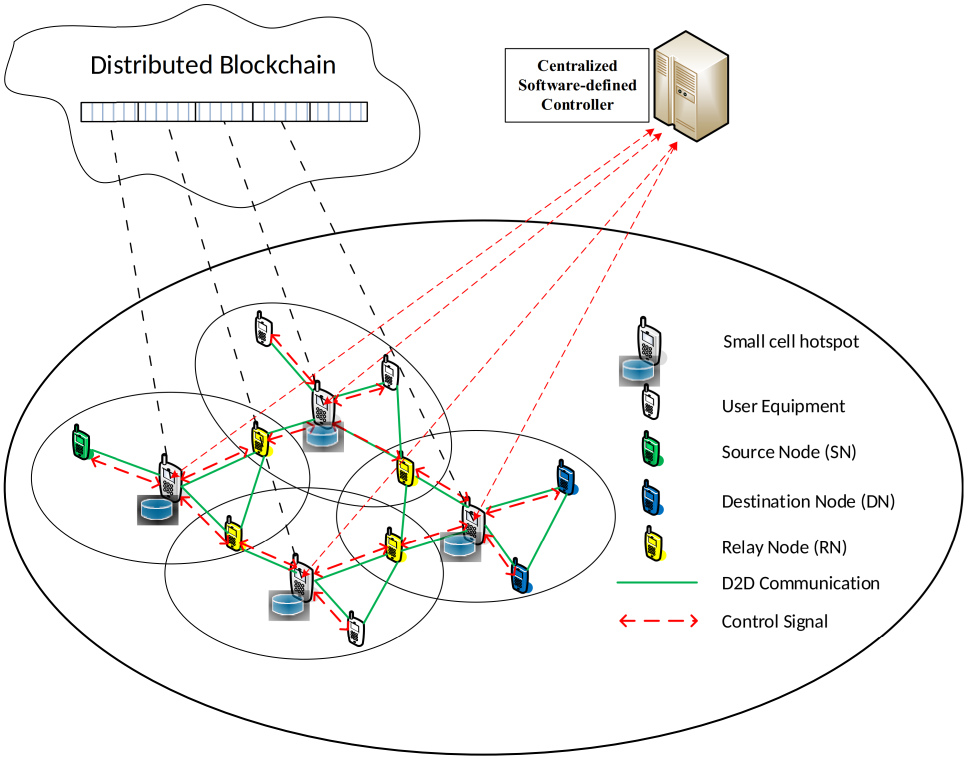
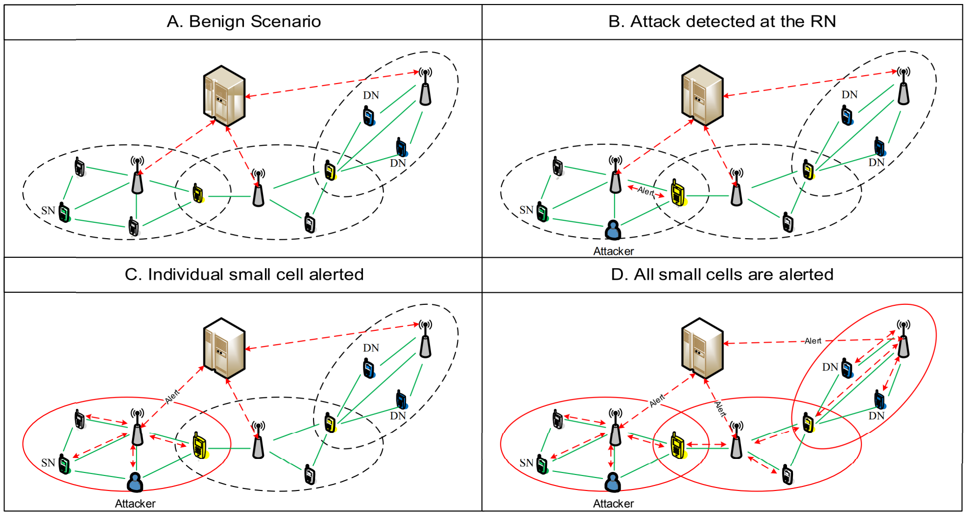


Fig. 2: System design for secure network coding enabled small cells

with the full integrity scheme as in [3] is a trade-off between various parameters including required security strength of the application, authentication mechanism of new users, trust factor of the small cell head and reported pollution attacks in the neighbourhood. Once a pollution attack is detected at a relay node, it should be reported to the small cell head and then to the central controller. Then the integrity check shall be performed at the nodes from the corresponding small cell and thus trace back to real adversary node. However, in the case of an intelligent adversary which modifies the packets only at regular intervals, the gradual increments in the integrity checkpoints will not be sufficient. Thus, if a particular small cell sees a considerable number of pollution attacks being reported, then the integrity check should be made mandatory to all the packet transmission originate or pass through that small cell. These decisions can be made by the cooperation of small cell heads and the central controller in the core network considering the security requirements of the application.

IV. Implementation Details and Analysis

The proposed security framework is based on a lightweight and adaptive version of the blockchain based integrity scheme. This integrity scheme is tested by simulations in a Linux based environment. The network coding implementations are based on the KODO library [21] and the blockchain overlay is facilitated by bigchainDB [22]. The integration of KODO based implementation with bigchainDB is done with the help of the collaboration platform, Postman API. As explained in the system description, the decision on when to extend the integrity check to all participating nodes depend on multiple factors like security requirement of the application, number of participating nodes, authentication scheme adapted by the small cells to accept a new node, frequency and history of pollution attack etc. The quantitative benefits of the security framework depend on the number of nodes in a small cell and the number of intermediate nodes in a particular information flow. Figure 3 shows major instances in the security framework. The blockchain overlay is not portrayed in the figure for simplicity. The benign scenario shows the situation of the network in the starting phase and till any node starts a malicious activity. In Fig.3.B, a node in the network is compromised and creates a pollution attack. It will be detected at the first relay node where the integrity check is performed. Once a pollution attack is detected, the relay node sends an alert to the corresponding small cell head. The small cell head informs all the participating nodes about the presence of an adversary and asks every node to perform the integrity check whenever a new packet is received. The small cell head also informs the central controller regarding the detected pollution attack. However, other small cells will continue to work as in the initial phase. However, repeated reporting of pollution attacks from a small cell will lead to the higher alert level and once a minimum number of pollution attacks are reported, then the central controller will alert all the small cell heads to enforce strict integrity checks. Once such an alert level is indicated, all the participating nodes will perform integrity checks to prevent the spreading of pollution attacks as shown in Fig 3.D. However, this alert level is temporary and will



A. Benign Scenario

B. Attack detected at the RN

C. Individual small cell alerted

D. All small cells are alerted

Fig. 3: Different events as described in the proposed framework

be removed if no attacks are detected for a duration. Again, this will be decided depending on the security conditions to be met by the network. We set a threshold of 10% of the total number of participating nodes as the number of attack instances to declare a high alert level and 10 times the average end to end latency as the timespan to remove the high alert level if no attack is detected during that period.

V. Conclusions

Energy efficient network coding enabled mobile small cells for next-generation communication networks promise to be an interesting concept to provide high throughput and serve low latency applications. Such cooperative networks can also cooperate to ensure the security of the network in a dynamic fashion with respect to security incidents happening over execution. This paper proposes a lightweight and adaptive security framework for such NC-enabled small cells. The security scheme starts with the assumption of all authenticated nodes being benign and limits the integrity checks to the relay nodes. This limits the security overhead to the minimum and limits the security threats, if any, to the corresponding small cells only. However, if any polluted packets are detected at this initial phase gradually the integrity check is expanded to the small cell and with repeated incidents of pollution attack, the whole network is put on a high alert and integrity checks are made mandatory to all participating nodes until no more pollution is detected for a definite period. This scheme reduces the computational overhead and latency compared to the more generic schemes in [3], [4] and then adaptively tightens the security measures. The threshold limits for high-security alert and period to refrain the alert level depends on various security-related parameters such as authentication scheme, application demands, number of participating nodes, and frequency of attack instances. The proposed integrity scheme is based on the blockchain enhanced integrity scheme proposed before. However, this security framework can be adapted to other similar integrity schemes with minor changes. This work can also be considered as an initial step towards security profiling of the network devices and an automated learning-based security framework for next-generation network coding enabled mobile small cells.

References

[1] J. Rodriguez, A. Radwan, C. Barbosa, F. H. Fitzek, R. A. Abd-Alhameed, J. Noras, S. M. Jones, I. Politis, P. Galiotos, G. Schulte *et al.*, "Secret—secure network coding for reduced energy next generation mobile small cells: A european training network in wireless communications and networking for 5g," in *2017 Internet Technologies and Applications (ITA)*. IEEE, 2017, pp. 329–333.

[2] V. N. Talooki, R. Bassoli, D. E. Lucani, J. Rodriguez, F. H. Fitzek, H. Marques, and R. Tafazolli, "Security concerns and countermeasures in network coding based communication systems: A survey," *Computer Networks*, vol. 83, pp. 422–445, 2015.

[3] V. Adat, I. Politis, C. Tselios, P. Galiotos, and S. Kotsopoulos, "On Blockchain Enhanced Secure Network Coding for 5G Deployments," in *2018 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2018, pp. 1–7.

[4] V. Adat, I. Politis, C. Tselios, and S. Kotsopoulos, "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)*. IEEE, 2019, pp. 1–6.

[5] R. Ahlswede, N. Cai, S.-Y. Li, and R. W. Yeung, "Network information flow," *IEEE Transactions on information theory*, vol. 46, no. 4, pp. 1204–1216, 2000.

[6] T. Ho, M. Médard, R. Koetter, D. R. Karger, M. Effros, J. Shi, and B. Leong, "A random linear network coding approach to multicast," *IEEE Transactions on Information Theory*, vol. 52, no. 10, pp. 4413–4430, 2006.

[7] N. J. Hernández Marcano, J. Heide, D. E. Lucani, and F. H. Fitzek, "Throughput, energy and overhead of multicast device-to-device communications with network-coded cooperation," *Transactions on Emerging Telecommunications Technologies*, vol. 28, no. 2, p. e3011, 2017.

[8] V. Adat, I. Politis, C. Tselios, and S. Kotsopoulos, "Secure Network Coding for SDN-Based Mobile Small Cells," in *International Conference on Broadband Communications, Networks and Systems*. Springer, 2018, pp. 347–356.

[9] T. Akhtar, I. Politis, P. Georgakopoulos, and S. Kotsopoulos, "Efficient radio resource management scheme in cooperative network using coalition game," in *2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*. IEEE, 2019, pp. 1–6.

[10] P. Georgakopoulos, T. Akhtar, I. Politis, C. Tselios, E. Markakis, and S. Kotsopoulos, “Coordination multipoint enabled small cells for coalition-game-based radio resource management,” *IEEE Network*, vol. 33, no. 4, pp. 63–69, 2019.

[11] N. Cai and R. W. Yeung, “Secure network coding,” in *Proceedings IEEE International Symposium on Information Theory,*, 2002, pp. 323–.

[12] V. A. Vasudevan, C. Tselios, and I. Politis, “On security against pollution attacks in network coding enabled 5g networks,” *IEEE Access*, vol. 8, pp. 38 416–38 437, 2020.

[13] S. Agrawal and D. Boneh, “Homomorphic macs: Mac-based integrity for network coding,” in *International Conference on Applied Cryptography and Network Security*. Springer, 2009, pp. 292–305.

[14] P. Zhang, Y. Jiang, C. Lin, H. Yao, A. Wasef, and X. Shenz, “Padding for orthogonality: Efficient subspace authentication for network coding,” in *2011 Proceedings IEEE INFOCOM*. IEEE, 2011, pp. 1026–1034.

[15] A. Esfahani, G. Mantas, J. Rodriguez, and J. C. Neves, “An efficient homomorphic mac-based scheme against data and tag pollution attacks in network coding-enabled wireless networks,” *International Journal of Information Security*, vol. 16, no. 6, pp. 627–639, 2017.

[16] V. Adat, R. Parsamehr, I. Politis, C. Tselios, and S. Kotsopoulos, “Malicious user identification scheme for network coding enabled small cell environment,” in *ICC 2020-2020 IEEE International Conference on Communications (ICC)*. IEEE, 2020, pp. 1–6.

[17] R. Parsamehr, A. Esfahani, G. Mantas, A. Radwan, S. Mumtaz, J. Rodriguez, and J.-F. Martínez-Ortega, “A novel intrusion detection and prevention scheme for network coding-enabled mobile small cells,” *IEEE Transactions on Computational Social Systems*, vol. 6, no. 6, pp. 1467–1477, 2019.

[18] R. Parsamehr, G. Mantas, J. Rodriguez, and J.-F. Martinez-Ortega, “Idlp: an efficient intrusion detection and location-aware prevention mechanism for network coding-enabled mobile small cells,” *IEEE Access*, vol. 8, pp. 43 863–43 875, 2020.

[19] M. de Ree, G. Mantas, J. Rodriguez, and I. E. Otung, “Distributed trusted authority-based key management for beyond 5g network coding-enabled mobile small cells,” in *2019 IEEE 2nd 5G World Forum (5GWF)*. IEEE, 2019, pp. 80–85.

[20] V. Adat, T. Akhtar, I. Politis, C. Tselios, and S. Kotsopoulos, “Towards secure network coding enabled mobile small cells,” in *2019 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2019, pp. 1–6.

[21] M. V. Pedersen, J. Heide, and F. H. Fitzek, “Kodo: An open and research oriented network coding library,” in *International Conference on Research in Networking*. Springer, 2011, pp. 145–152.

[22] T. McConaghy, R. Marques, A. Müller, D. De Jonghe, T. McConaghy, G. McMullen, R. Henderson, S. Bellemare, and A. Granzotto, “Bigchaindb: a scalable blockchain database,” *white paper, BigChainDB*, 2016.