An IDLP Mechanism for Network Coding-enabled Mobile Small Cells based on Broadcast Nature of Wireless Communication

Reza Parsamehr
Instituto de Telecomunicações
Aveiro, Portugal
Universidad Politécnica de Madrid
Madrid, Spain
parsamehr.r@av.it.pt
r.parsamehr@alumnos.upm.es

Vipindev Adat
Wireless Communications Laboratory
University of Patras
Patras, Greece
vipindev@ece.upatras.gr

Georgios Mantas
Instituto de Telecomunicações
Aveiro, Portugal
University of Greenwich
London, UK
gimantas@av.it.pt

Ilias Politis
Wireless Communications Laboratory
University of Patras
Patras, Greece
ipolitis@ece.upatras.gr

Jonathan Rodriguez
Instituto de Telecomunicações
Aveiro, Portugal
University of South Wales
Wales, UK
jonathan@av.it.pt

Jose-Fernán Martínez-Ortega
Universidad Politécnica de Madrid
Madrid, Spain
jf.martinez@upm.es

***Abstract*—Network Coding (NC) technology can be foreseen as a promising solution for mobile small cell technology problems existing in the 5th generation of mobile networks. NC-enabled mobile small cells increase network throughput and improve their performance in a cost-effective and energy-efficient manner. However, NC-enabled mobile small cells are vulnerable to pollution attacks. Although there have been some works done on pollution attack detection, the attackers may continue to pollute packets in the next transmission of coded packets from the source to the destinations. Therefore, in this paper, we present an intrusion detection and location-aware prevention mechanism to not only detect the pollution attacks and drop them but also detect the attacker's exact location in order to block them from making pollution in the next transmissions. In the proposed mechanism, the detection scheme is based on a homomorphic MAC scheme, and we make use of the advantages within broadcast nature in the wireless communication medium to find the source of the pollution attacks. The proposed mechanism, SpaceMac proposed in [1] and the IDLP mechanism proposed in [2] have been implemented in Kodo and their performance has been evaluated in terms of decoding probability.**

***Index Terms*—Network Coding, pollution attacks, IDPS, locating attacks, 5G**

I. Introduction

The fifth generation of wireless networks is expected to bring in significant changes in the mobile and digital world. To expect anything from these upcoming 5G networks regarding high data rates and quality of services, significant paradigm shift in technology and communication are required. An example of this paradigm change is the concept of small cell which provides a better coverage area and ensures the quality of service both efficiently and cost-effectively [3], [4]. Ensuring resilient and reliable communication over the wireless channels using the bandwidth efficiently in mobile small cell communication has been one of the significant challenges in this 5G era. Network coding is considered to be one of the best solutions to address this challenge. Network coding [5] improves the bandwidth efficiency of a network through mixing and recoding the packets at intermediate nodes and allowing the destination nodes to decode these coded packets. SECRET [6] studies and proposes a secure network coding enabled mobile small cell environment that addresses the challenges of future networks, as shown in Figure 1.

However, network coding enabled environment also requires adequate security and IDPS schemes to harness network coding benefits. Compared to the traditional store and forward networks, network coding-enabled networks suffer from more specific attacks like pollution. Since the intermediate nodes are allowed to recode the packets, a malicious user can insert a corrupted packet into the transition. This corrupted packet can pollute the communication flow, and if it goes undetected, it can spread across the network as the polluted packet mixes with other genuine packets attacks [7]. Pollution attack leads to a significant reduction in network throughput. Identifying the polluted packet at the earliest point and locating the adversary node polluting the channel are equally important to achieve secure and efficient communication. To achieve this, there exist many integrity schemes which detect pollution attacks in network coding [8]–[14], However, effectively locating

This work was partly supported by the European Union's Horizon 2020 Research and Innovation Programme under Grant H2020-MSCA-ITN-2016-SECRET-722424.

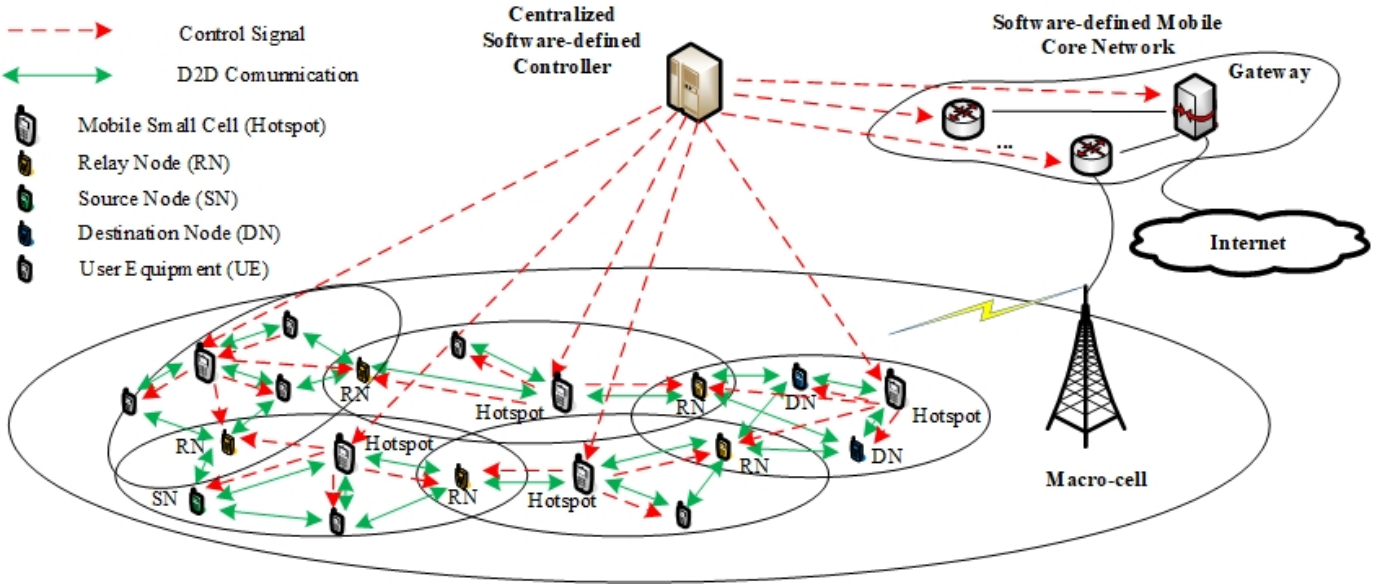

Fig. 1. SECRET Scenario Architecture.

the adversary node is a comparatively less explored research direction [1], [2], [15]–[18].

In this work, we propose an Intrusion Detection and Location-aware Prevention Mechanism based on Broadcast Nature of Wireless Communications (IDLP-BNWC) to detect and prevent pollution attacks and to detect the attacker's location. We use the null space based homomorphic MAC scheme [9], [10] for the detection scheme. This mechanism allows us to detect pollution attacks efficiently at the earliest possible node and drop the detected polluted packets. However, this course of action is generally not sufficient since the attackers can continue to pollute packets in the next transmission of coded packets from the source to the destinations, which leads to a waste of the network's throughput. Therefore, in this work, we focused on identifying the exact location of attackers and blocking them in order to protect our network from future pollution attacks. We make use of the advantage within the broadcast nature of the wireless communication medium. Thus, when a node sends the packet using the wireless communication medium, all the nodes and Hotspots on its coverage will receive its packets. So, neighbor nodes, by receiving the polluted packets, detect the pollution, and report it to the Hotspots. The Hotspots forward the reports to the SDN controller in order to make a suitable decision about blocking the attackers and to prevent the network from future attacks.

This paper is organized as follows: Our IDLP-BNWC mechanism is proposed in Section II. In Section III, we provide the performance evaluation of the proposed mechanism and compare it with IDLP in [2] and SpaceMac in [1]. Finally, Section IV concludes the paper.

II. Proposed IDLP-BNWC mechanism

In this section, we present the proposed IDLP-BNWC mechanism for network coding-enabled mobile small cells based on broadcast nature mechanism. This mechanism consists of a) a detection scheme based on the Null Space homomorphic MAC scheme [9], [10] and uses it to detect pollution attacks; and b) a locating scheme which is part of the prevention mechanism and is supported by the detection scheme which allows us to identify the exact location of the adversary nodes (i.e., the source of pollution attacks). The locating scheme uses the broadcast nature of wireless communication for identification.

In this mechanism, by taking advantage of the broadcast nature of the wireless communication medium, when a mobile device is sending out a coded packet, all its neighbors (e.g., hotspot, downstream and upstream mobile devices) can receive this packet. Each neighbor can verify the received packet using the detection scheme and report the pollution attack to the hotspots if there exists any. Then, the hotspots forward the report to the SDN Controller. The SDN Controller identifies the exact location of the adversary based on the reports received from different hotspots as described in the "locating scheme" subsection.

Here, we discuss the detection scheme and locating scheme of the proposed IDLP-BNWC mechanism for network coding-enabled mobile small cells based on broadcast nature mechanism.

A. Detection Scheme

The detection scheme of the location-aware IDPS mechanism is based on the null space-based homomorphic MAC scheme presented in our previous works [10] and [9] and makes use of the orthogonality to verify the tags appended to the end of each packet. According to [10], the source node

divides the message into a generation of native packets denoted as $\underline{\mathbf{b}}_1, \underline{\mathbf{b}}_2, ..., \underline{\mathbf{b}}_m$, where m is generation size and each packet $\underline{\mathbf{b}}_i$ consists of n symbols (i.e., $\underline{b}_{i,1}, \underline{b}_{i,2}, ..., \underline{b}_{i,n}$) in the finite field $\mathbb{F}_p^n$. Therefore, the source node will generate a coded packet $\mathbf{b}_i$ according to RLNC principles and sends it to the next intermediate nodes.

$$\mathbf{b}_i = (\overbrace{\underbrace{0, \cdots, 0}_{i-1}, 1, 0, \cdots, 0}^{m}, \underline{b}_{i,1}, \cdots, \underline{b}_{i,n}) \in \mathbb{F}_p^{m+n} \quad (1)$$

For simplicity, (1) can also be written as follows:

$$\mathbf{b}_i = (b_{i,1}, \cdots, b_{i,m+n}) \in \mathbb{F}_p^{m+n} \quad (2)$$

Then, each intermediate node combines h received coded packets $(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_h)$ and creates a new coded packet x and sends it to its neighbors. As shown in (3), the new coded packet is a liner combination of all the received coded packets belonging to the same generation, where β is randomly selected from $\mathbb{F}_p$ and all arithmetic operations are done over the finite field $\mathbb{F}_p$.

$$x = \sum_{i=1}^{h} \beta_i \mathbf{b}_i \quad (3)$$

As we mentioned in previous work [10], when an SN creates the coded packet, it also generates L tags, based on null space properties [19], which are used to detect pollution attacks. There are five steps to create the tags and verify the orthogonality of the received coded packets with the tags appended to them:

1) Key distribution to the source node: A key distribution center creates a set of keys $(\mathcal{C}_1, \mathcal{C}_2, ..., \mathcal{C}_L)$ in the finite field $\mathbb{F}_p^{m+n+L}$ and distributes them to the source node.
2) The source node creates L tags (i.e., $t_1, t_2, ..., t_L$) using L keys, distributed by KDC in the previous step, for each coded packet according to (4). Each coded packet contains $m+n$ symbols and the L generated tags (i.e., t_{SN}) are appended to the end of each coded packet, as shown in Figure 2.

$$\begin{bmatrix} \mathcal{C}_{1,1} & \ldots & \mathcal{C}_{1,m+n} \\ \vdots & \vdots & \vdots \\ \mathcal{C}_{L,1} & \ldots & \mathcal{C}_{L,m+n} \end{bmatrix}_{L*(m+n)} * \begin{bmatrix} \mathbf{b}_{i,1} \\ \mathbf{b}_{i,2} \\ \vdots \\ \mathbf{b}_{i,m+n} \end{bmatrix}_{(m+n)*1} + \begin{bmatrix} \mathcal{C}_{1,m+n+1} & \ldots & \mathcal{C}_{1,m+n+L} \\ \vdots & \vdots & \vdots \\ \mathcal{C}_{L,m+n+1} & \ldots & \mathcal{C}_{L,m+n+L} \end{bmatrix}_{L*L} * \begin{bmatrix} \mathbf{t}_1 \\ \mathbf{t}_2 \\ \vdots \\ \mathbf{t}_L \end{bmatrix}_{L*1} = 0 \quad (4)$$

3) The L tags are swapped based on the shared secret key (SV) between the SN and DNs, according to (5), to avoid tag pollution attacks.

$$\overline{\mathbf{b}}_i = Swap(\mathbf{b}_i)_{SV} \quad (5)$$

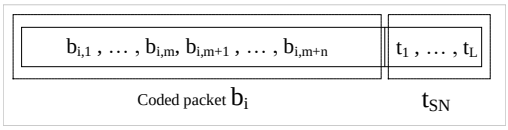

Fig. 2. Generated L tags for each packet in source node.

4) The KDC creates new keys based on the set of keys that were distributed to the SN in step 1 using the swapping vector SV, and the KDC generates them according to (6). Then, the keys are distributed to the intermediate nodes and DNs to verify the received coded packets.

$$\mathcal{C}_i^{'} = Swap(\mathcal{C}_i)_{SV} \quad (6)$$

5) Finally, each intermediate node and DN verifies the received coded packet based on the following equation:

$$\delta = Swap(\mathcal{C}_i)_{SV} * Swap(\mathbf{b}_i)_{SV} = \sum_{j=1}^{m+n+L} \mathcal{C}_{i,j}^{'} * \overline{\mathbf{b}}_{i,j} \quad (7)$$

If $\delta = 0$, then the received coded packet is verified and acceptable to be transmited to the next nodes. Otherwise, it should be dropped.

B. Locating Scheme

The main is concern is when the exact location of the adversaries are identified to prevent nodes from deceiving the SDN Controller. For this reason, each intermediate node is responsible for verifying the received coded packet by taking advantage of the detection scheme. The intermediate node checks the validity of the received coded packets and decides to pursue either one of the two following options: i) if there is no pollution attack, it recodes the received coded packets and sends it to the next nodes, or ii) and a pollution were to be detected, it creates a report based on the received corrupted packet and broadcasts it to the neighbors.

When an adversary in the MSC creates a polluted packet, the polluted packet reaches the hotspot and all neighbors, and hotspot reports it to the SDN controller. In this network, it is assumed that a hotspot is one of the mobile devices; thus, it can be a compromised node. Therefore, each neighbor node (the next upstream and downstream nodes) which received the corrupted packet creates a report and broadcasts it to reach the hotspots in the neighbor MSCs. When the hotspots in the neighborhood receive the reports, they forward it to the SDN Controller, that is responsible for identifying the exact location of adversary mobile devices.

1) Report: Every time an intermediate or destination node detects any polluted packet (which is defined as e), the receiving node generates a report. As shown in Figure 3 the generated report contains four parts: i) $\mathcal{ID}_{i-1}$, ii) $\mathcal{ID}_i$, iii) $\{e||s_i\}$, and iv) C.

i. $\mathcal{ID}_{i-1}$**:** is the media access control address (i.e., MAC address) of an adversary, that pollutes the network.

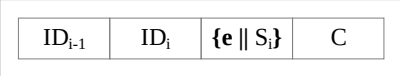

Fig. 3. The structure of the report.

ii. $\mathcal{ID}_i$**:** is the MAC address of the given node which identify the polluted packet and creates the report.

iii. ***Signature*** $\{e||s_i\}$**:** The intermediate node signs the received polluted packet by the shared key between SDN Controller and itself. This signature protects our network from an intelligent adversary deceiving the SDN Controller by sending different reports.

iv. ***Counter*** C**:** A counter is created by the given node that reports the pollution. C is the number of hops to reach the hotspots of neighbor MSCs through the network. Therefore, C (hop counter) is chosen according to the following approach:

- Calculation of pathloss: The Signal-to-Noise Ratio is defined as the the ratio of signal power to the noise power threshold by xdB (e.g., $3dB$). So, if the transmit power of the sender (the mobile device) and the allocated bandwidth are known, it is possible to calculate the Path loss (PL), which is the reduction in power density. Where,

$$PL = 10 * nlog_{10}^{(d+c)} \tag{8}$$

$$log_{10}^{d} = \frac{(PL - c)}{10n} \tag{9}$$

where d is the maximum distance for the receiver to receive the packet with $3dB$ SNR, n)is the path loss exponent, and c is the context.

- Defintion of maximum distance: based on the PL, it is possible to estimate the maximum distance d for the receiver to receive the packet with $3dB$ of SNR through the following equations:

$$d = 10^{\frac{(PL - c)}{10n}} \tag{10}$$

- Determination of hop counter: given the distance d, it is possible to calculate the number of hops C based on the distance between the sender and the receiver D.

$$C = \frac{D}{d} \tag{11}$$

C. Identify the Exact Location of Adversaries at the SDN Controller

There are some instruction that each mobile device should follow to identify the eaxact location of adversaries. According to the detection scheme, when each mobile device detects any pollution, it drops the polluted packet and creates a report based on the locating scheme. Then the mobile device who received the polluted packet broadcasts the created report to the neighbor nodes. Afterward, when each neighbor node receives the report, it would check the counter (C) and make the decision to broadcast the received report or drop it; i) if $C > 0$, the neighbor node broadcasts the received report, ii) if $C = 0$, the neighbor node drops the received report.

The hotspot of each neighbor MSCs would receive the report after crossing mobile devices. Then each hotspot would forward the received report to the SDN Controller, who is responsible for identifying the exact location of the adversary mobile device(s).

Based on the number of the MSCs in the neighborhood of the polluted MSC, the SDN Controller should receive some reports from different hotspots against the same mobile device, where this number of received reports is defined as g'. Furthermore, the number of neighbor nodes that received the polluted packet and create the report is defined as h'. The g' and the h' are different for each network based on network topology.

Afterward, when the SDN Controller receives the reports, it first checks $\mathcal{ID}_{i-1}$, $\mathcal{ID}_i$ and their signatures. Then, the SDN Controller checks how many hotspots (g) and how many neighbor nodes (h) of node $\mathcal{ID}_{i-1}$ report this pollution against node $\mathcal{ID}_{i-1}$. If $g \geq g'$ and $h \geq h'$, the SDN Controller considers the reported node as an adversary and makes a decision about the most appropriate preventive action (e.g., block adversary mobile device(s) from accessing the network) that should be taken to protect the network from the adversary.

D. Locating Scheme Scenarios

When an intermediate node receives a packet, it checks the validity of the received packet based on the detection scheme. If there is no pollution attack, the intermediate node recodes the received coded packets and sends them to the next nodes. However, if the received packet is polluted, the intermediate node creates a report and broadcasts it to the neighbors (see Figure 4). When the neighbor nodes receive the report, they check the counter, and if $C > 0$, they broadcast the received report until the reports are received by hotspots in the neighbors MSCs, and they forward the reports to the SDN Controller. Also, the local hotspot detects the polluted packet and reports it to the SDN Controller. The SDN Controller decides about the most appropriate preventive action based on the reports received from different hotspots and neighbor nodes.

The following three scenarios are considered in order to present how the proposed IDLP-BNWC mechanism can identify the adversary's location:

- ***Scenario 1- One or more nodes are adversaries:*** When an adversary creates a polluted packet (see Figure 4), the neighbor nodes detect the pollution attack and drop the polluted packet. Then, each neighbor node creates a report regarding the compromised node that created the polluted packet and broadcasts it to the network. These reports will be created by the different nodes in the range of the compromised node which received the polluted

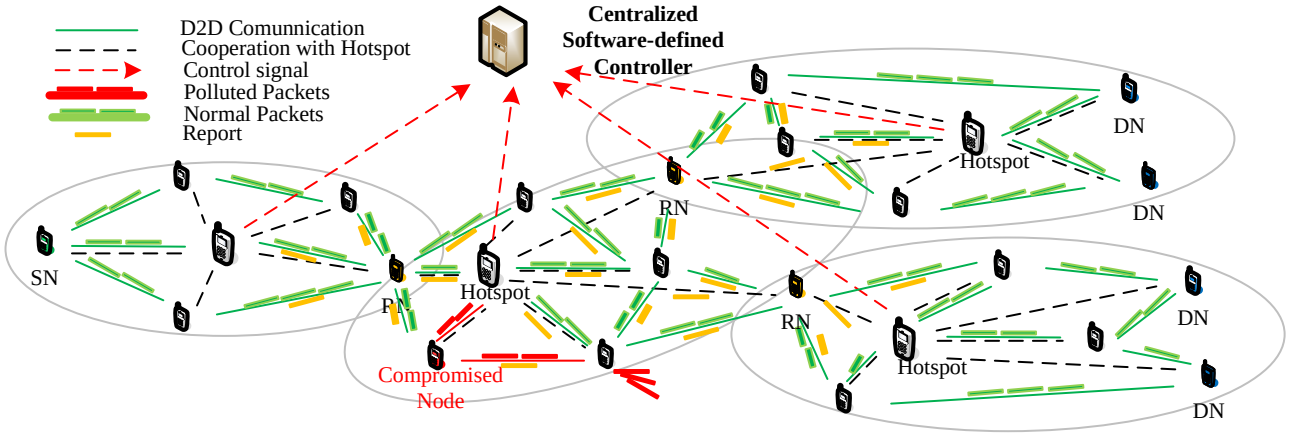

Fig. 4. Scenario 1: One or more normal nodes are an adversaries.

packet. The hotspot in the neighbor MSCs receives various reports from different nodes. The hotspots in each MSC forward the reports to the SDN controller. Then, the SDN Controller makes a decision decides regarding the exact location of the adversaries.

- ***Scenario 2- One or more nodes are adversaries, and the hotspot in the same MSC as the adversary as well:*** In this case, when some nodes create polluted packets, the hotspot does not report pollution to the SDN controller, because it is an adversary. However, when neighbor nodes receive the polluted packet, they create a report regarding the compromised node and broadcasts it to the network. The hotspots in the neighbor MSCs receives these reports. Then, they forward it to the SDN controller. Afterward, the SDN controller makes a decision about the exact location of adversaries and the hotspot within the polluted MSC.
- ***Scenario 3- An adversary creates a fake report:*** When an adversary creates a fake report on the detection of pollution attack and broadcasts it to deceive the hotspots in the neighbor MSCs. In this scenario, when the hotspots forward the reports to the SDN Controller, the SDN Controller finds out that the reports are from one node with the same $\mathcal{ID}_i$, which shows just one mobile device reported the pollution attack, so $h' \geq h$. The SDN Controller expects to receive some different reports from different nodes regarding the same adversary node thanks to the broadcast nature of the wireless medium, and it should be $h \geq h'$. Therefore, the SDN Controller finds out that it is a fake report and makes a decision about the pollution reporter.

III. Performance Evaluation

In this section, the proposed IDLP-BNWC, the IDLP proposed in [2] and the SpaceMac presented in [1] are compared. First of all, three butterfly topologies, including 18 normal nodes and one adversary node are implemented and the assumptions are same as the previous comparisons where adversary node is considered at a fixed position; the probability that the adversary node pollutes a relayed packet is 1 and the pollution scheme is continuous. The implementation is based on the RLNC approach of the Network Coding library of Kodo. The packet generation size is 64 symbols and the symbol size is set between $1,000$ to $10,000$ bytes. For both IDLP mechanisms, the value of L (i.e., number of tags) can be 27, 42, or 54 [19]. However, for SpaceMac the value of L is always 1. The Galois field in use is $GF(2^8)$. During the implementation and performance evaluation, the machine had following characteristics: a $2.7GHz$ Core $i7$ CPU with $8GB$ of physical memory. In this section, the performance evaluation and the comparison of IDLP-BNWC, IDLP and SpaceMac in terms of decoding probability when there is one attacker, are provided.

A. Decoding Probability

The P_r is defined as the probability that a corrupted packet is not detected in the verification phase. According to our implementation results, when there is one attacker the P_r is almost 0 for all three mechanisms. This is because when there is one attacker and one of these three mechanisms is applied, the adversary does not have any chance to distribute the corrupted packet in the network due to the fact that the detected adversaries are blocked from access to the network.

However, when there are two or more adversaries in a row, the P_r of IDLP and IDLP-BNWC are still 0 (see Figure 5), since these two mechanisms block the attackers after detection, but the P_r of SpaceMac is 1 because SpaceMac cannot identify the exact location of the attackers and block them even after detection at the destination nodes [20].

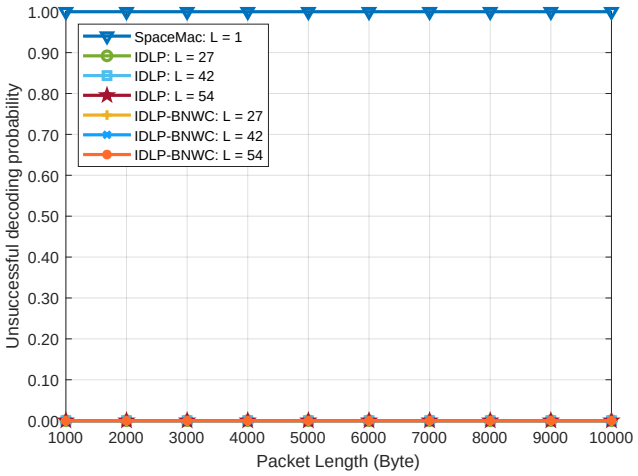

Fig. 5. P_r for different number of tags in IDLP [2], SpaceMac [1] and proposed IDLP-BNWC

IV. CONCLUSION

This chapter presented a new IDLP mechanism for NC-MSCs. The proposed IDLP mechanism consists of detection scheme and locating scheme. We used the null space-based homomorphic MAC scheme [9] for the detection scheme which is adapted to the MSC environment, and we use broadcast nature of wireless medium for locating scheme. The proposed IDLP-BNWC mechanism does not only detect the pollution attacks, but also detects the exact location of the attacker(s) and decides about the preventive actions (e.g., block compromised mobile device from accessing the network) that should be taken to stop the attack and protect the resources of the network. The proposed IDLP-BNWC mechanism, SpaceMac proposed in [1] and the IDLP mechanism proposed in [2] have been implemented in Kodo and their performance show that when there are two or more adversary in a row, the decoding probability for the proposed IDLP-BNWC and IDLP proposed in [2] is 0, but for SpaceMac proposed in [1] is 1.

REFERENCES

[1] A. Le and A. Markopoulou, "Cooperative defense against pollution attacks in network coding using spacemac," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 2, pp. 442–449, 2012.

[2] 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.

[3] C.-X. Wang, F. Haider, X. Gao, X.-H. You, Y. Yang, D. Yuan, H. M. Aggoune, H. Haas, S. Fletcher, and E. Hepsaydir, "Cellular architecture and key technologies for 5g wireless communication networks," *IEEE communications magazine*, vol. 52, no. 2, pp. 122–130, 2014.

[4] A. Gupta and R. K. Jha, "A survey of 5g network: Architecture and emerging technologies," *IEEE access*, vol. 3, pp. 1206–1232, 2015.

[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] 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.

[7] R. Parsamehr, G. Mantas, A. Radwan, J. Rodriguez, and J.-F. Martínez, "Security threats in network coding-enabled mobile small cells," in *International Conference on Broadband Communications, Networks and Systems*. Springer, 2018, pp. 337–346.

[8] 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.

[9] A. Esfahani, G. Mantas, and J. Rodriguez, "An efficient null space-based homomorphic mac scheme against tag pollution attacks in rlnc," *IEEE Communications Letters*, vol. 20, no. 5, pp. 918–921, 2016.

[10] 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.

[11] Y. Li, H. Yao, M. Chen, S. Jaggi, and A. Rosen, "Ripple authentication for network coding," in *2010 Proceedings IEEE INFOCOM*. IEEE, 2010, pp. 1–9.

[12] V. Adat, I. Politis, C. Tselios, and S. Kotsopoulos, "Secure network coding for sdn-based mobile small cells," in *Broadband Communications, Networks, and Systems*, V. Sucasas, G. Mantas, and S. Althunibat, Eds. Cham: Springer International Publishing, 2019, pp. 347–356.

[13] 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)*, Dec 2018, pp. 1–7.

[14] B. Maboudi and P. Pahlevani, "Security overhead of random linear network coding in multicast relay networks," *Transactions on Emerging Telecommunications Technologies*, p. e3963, 2020.

[15] M. J. Siavoshani, C. Fragouli, and S. Diggavi, "On locating byzantine attackers," in *2008 Fourth Workshop on Network Coding, Theory and Applications*. IEEE, 2008, pp. 1–6.

[16] R. Parsamehr, A. Esfahani, G. Mantas, J. Rodriguez, and J.-F. Martínez-Ortega, "A location-aware idps scheme for network coding-enabled mobile small cells," in *2019 IEEE 2nd 5G World Forum (5GWF)*. IEEE, pp. 91–96.

[17] 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.

[18] R. Parsamehr, "Intrusion detection and prevention for nc-enabled mobile small cells," *In J. Rodriguez, N. Passas, and C. Verikoukis, editors, Converged and Virtual Optical-Wireless Communication Platform for Beyond 5G, Springer*, pp. x–x, 2020.

[19] 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.

[20] R. Parsamehr, G. Mantas, J. Rodriguez, and J.-F. Martínez-Ortega, "On the performance analysis of IDLP and spacemac for network coding-enabled mobile small cells," *IEEE Communications Letters*, 2020.