IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received January 24, 2020, accepted February 7, 2020, date of publication March 2, 2020, date of current version March 12, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2977428

IDLP: An Efficient Intrusion Detection and Location-Aware Prevention Mechanism for Network Coding-Enabled Mobile Small Cells

REZA PARSAMEHR[1,2], (Member, IEEE), GEORGIOS MANTAS[1,3], (Member, IEEE), JONATHAN RODRIGUEZ[1,4], (Senior Member, IEEE), AND JOSÉ-FERNÁN MARTÍNEZ-ORTEGA[2], (Senior Member, IEEE)

[1]Instituto de Telecomunicações, 3810-193 Aveiro, Portugal
[2]Departamento de Ingeniería Telemática y Electrónica, Escuela Técnica Superior de Ingeniería y Sistemas de Telecomunicación, Universidad Politécnica de Madrid, 28031 Madrid, Spain
[3]Faculty of Engineering and Science, University of Greenwich, London SE10 9LS, U.K.
[4]Faculty of Computing, Engineering and Science, University of South Wales, Pontypridd CF37 1DL, U.K.

Corresponding author: Reza Parsamehr (parsamehr.r@av.it.pt)

This work was partly supported by the European Union's Horizon 2020 Research and Innovation Programme under Grant H2020-MSCA-ITN-2016-SECRET-722424, and by the European Regional Development Fund (FEDER), through COMPETE 2020, POR ALGARVE 2020, Fundação para a Ciência e Tecnologia under i-Five Project (POCI-01-0145-FEDER-030500).

ABSTRACT Mobile small cell technology is considered as a 5G enabling technology for delivering ubiquitous 5G services in a cost-effective and energy efficient manner. Moreover, Network Coding (NC) technology can be foreseen as a promising solution for the wireless network of mobile small cells to increase its throughput and improve its performance. However, NC-enabled mobile small cells are vulnerable to pollution attacks due to the inherent vulnerabilities of NC. Although there are several works on pollution attack detection, the attackers may continue to pollute packets in the next transmission of coded packets of the same generation from the source node to the destination nodes. Therefore, in this paper, we present an intrusion detection and location-aware prevention (IDLP) mechanism which does not only detect the polluted packets and drop them but also identify the attacker's exact location so as to block them and prevent packet pollution in the next transmissions. In the proposed IDLP mechanism, the detection and locating schemes are based on a null space-based homomorphic MAC scheme. However, the proposed IDLP mechanism is efficient because, in its initial phase (i.e., Phase 1), it is not needed to be applied to all mobile devices in order to protect the NC-enabled mobile small cells from the depletion of their resources. The proposed efficient IDLP mechanism has been implemented in Kodo, and its performance has been evaluated and compared with our previous IDPS scheme proposed in [1], in terms of computational complexity, communicational overhead, and successfully decoding probability as well.

INDEX TERMS Network coding, pollution attacks, intrusion detection, location-aware prevention, efficiency, 5G.

I. INTRODUCTION

Fifth generation of mobile networks is being deployed and expected to meet the high quality of service provision, the high data rate, and low end to end latency communications. The concept of small cells enables 5G to improve its quality of experience to remote areas by extending the coverage in a cost effective manner [2]–[6]. Device to device communication further improves the energy efficiency and ensures effective deployment of ubiquitous services that the 5G envisions [7], [8]. However, studies are still going on how to harness the available bandwidth efficiently and tackle the challenges due to packet loss during transmission. Network Coding (NC) appears to be an effective solution to address these challenges [9], [10]. SECRET [11] proposes a NC-enabled mobile small cell environment (see Fig. 2) where network coding is applied to address the challenges of next generation wireless networks. NC [12] improves the

The associate editor coordinating the review of this manuscript and approving it for publication was Marco Martalo.

efficiency of the network by coding the packets and allowing the intermediate nodes to recode the packets instead of simply 'store and forward'. More specifically, random linear network coding [13] proves to be an efficient solution for the wireless environment. Deploying NC techniques also improve the energy efficiency of the network since it reduces the number of transmissions required for communications. Furthermore, NC also provides some inbuilt resistance to wiretapping and eavesdropping [14], [15]. However, network coding suffers from attacks [15], especially pollution attacks.

The NC-enabled environment suffers from pollution attacks where malicious intermediate nodes manipulate packets in transition. These modified packets (i.e., polluted packets) will result in erroneous decoding at the receivers. Furthermore, if the polluted packets are allowed to pass through genuine nodes, they can pollute more packets on the fly. Thus, identifying the polluted packets as well as the exact location of malicious users are equally important tasks. Even though there are many integrity schemes against pollution attacks [14], [16]–[24], only a few focusing on identifying the location of malicious users [24]–[27].

In this work, an efficient intrusion detection, and location-aware prevention (IDLP) mechanism is proposed to detect pollution attacks and locates the attacker's exact location and prevent pollution attacks in NC-enabled mobile small cells. The proposed IDLP mechanism is an extension of our proposed location-aware IDPS scheme for network coding-enabled mobile small cells presented in [27]. We use the null space-based homomorphic MAC scheme [14] for both the detection and locating schemes, which is adapted to the mobile small cell environment. The detection scheme gives us this opportunity 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 of the same generation from the source node to the destination nodes, which leads to a waste of the network's throughput. Therefore, in this work, we focus on the identification of the exact attackers' location and blocking them to protect the network from future pollution attacks. The proposed IDLP mechanism consists of two phases to prevent the network from the depletion of their resources. In the first phase, the proposed mechanism applies to Relay Nodes (RNs) and Destination Nodes (DNs), and it is not needed to be applied to all nodes when there is no attack in the network. Therefore, in this mechanism, we do not take time for verification in all the intermediate nodes when there is no attack. The mechanism is described in section IV precisely. Moreover, the proposed IDLP mechanism is Implemented on Kodo and is compared with the proposed IDPS scheme in [1].

The rest of this paper is organized as follows. Section II introduces the scenario architecture. In Section III, we provide the background and related work of NC technology, secure NC, and security schemes against pollution attacks in NC-enabled networks. In Section IV, the detailed description of the proposed efficient intrusion detection and location-aware prevention (IDLP) mechanism for network coding-enabled mobile small cells are given. In Section V, we provide details of the implementation of the proposed scheme in Kodo. In Section VI, we provide the performance evaluation of the proposed mechanism and compare it with our previous IDPS scheme. Finally, Section VII concludes this paper.

II. RELATED WORK

Defending against pollution attacks in NC-enabled networks mainly depends on ensuring the integrity of the packets in transition. However, basic integrity schemes do not work with network coding due to the recoding of packets at intermediate nodes. Schemes with homomorphic property become essential to ensure the integrity of packets in NC-enabled networks. In this section, we discuss:

1) Pollution attacks
2) Secure network coding
3) Locating schemes
4) IDPS schemes

A. POLLUTION ATTACKS

Pollution attacks or byzantine modification attacks are the most severe attacks in a network coding-enabled environment. An adversary tries to inject polluted packets to the network in order to deplete network resources (e.g., CPU power, memory, and battery level). If any nodes use the polluted packets to combine with other packets and create coded packets, this pollution will publish in the whole network. Thus, the receivers would not be able to decode the native packets. Pollution attacks can be divided into two types, data pollution attacks, and tag pollution attacks. In data pollution attacks, the adversary tries to pollute (e.g., modify) the data packets being transferred. However, in tag pollution attacks, the adversary pollutes the tags attached to the packets to prevent the destination nodes from decoding correctly, which results in reduced efficiency of the network [15], [28], [29].

Furthermore, both types of pollution attacks can be launched by either an external adversary or an internal compromised node (i.e., byzantine modification attacks). The external adversary tries to inject corrupted packets into the network in order to corrupt other coded packets. However, an internal compromised node aims to pollute the transmitted packets by modifying them and thus compromising their integrity [15], [28], [29].

B. SECURE NETWORK CODING

There are plenty of different detection schemes against pollution attacks in network coding, such as information-theoretic schemes, cryptographic schemes, homomorphic signature schemes, and homomorphic MAC-based schemes. We focus on the homomorphic MAC-based schemes whose scope is to ensure integrity in network coded packets, as initiated by Agrawal *et al.* [16]. However, the schemes based on homomorphic MACs are vulnerable to tag pollution attacks. In [30], Zhang *et al.* studied the use of orthogonality

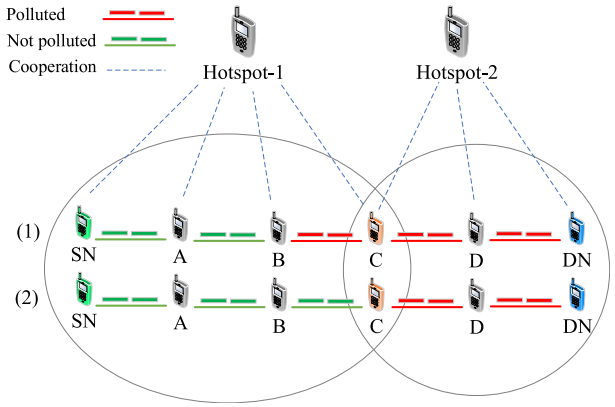

FIGURE 1. An example of identifying an attacker's location by the Hotspots, using information about polluted packets through the edges. The attacker is node C. Scenario 1, shows sets of edges when the attacker lies about its incoming packets. However, scenario 2, shows sets of edges when the attacker cannot lie.

property generating tags. Further, they addressed the issue of tag pollution attack by combining a homomorphic signature to the MAC scheme and thus proposing MacSig. Esfahani *et al.* improved the efficiency of these schemes through a series of works [14], [31], [32]. The works in [32] and [14] are focused on different key sharing approaches and dual MAC schemes for efficient integrity schemes. The work in [14] is focused on a null space-based scheme where the tags are mixed to the original packets based on a randomly generated swapping vector. This also reduces the probability of a successful tag pollution attack without extra overheads. In another set of work, Adat *et al.* [33], [34] address the pollution attacks using different approaches of tag sharing. Authors proposed a detection scheme based on homomorphic mac, and also they have used a central controller and blockchain for preventing the network form tag pollution attack.

C. LOCATING SCHEMES

Identifying the location of a malicious user is equally important as detecting a security attack so that other participating nodes can be informed about the presence of an adversary. Depending only on a single node's detection report and declare any other node as an adversary is not completely acceptable since, in such cases, a malicious node can deceive the network by accusing the previous node of being an adversary. As shown in Fig. 1, node C is an adversary. In scenario 1, we consider that the attacker deceives about its incoming packet. However, in scenario 2, the attacker does not deceive. In this scenario, a malicious node deceives the network and reports a genuine parent node as an adversary, which can lead to an unstable network situation. Thus, additional location schemes or verification of adversaries become essential to maintain a fair network environment. Siavoshni *et al.* proposed an integrity scheme that also locates the adversary using a central controller [25]. In this scheme, the intermediate node reports a pollution attack along with the polluted packets to a central controller, and this trusted controller verifies the pollution. The central controller verifies the packet with the subspace of source packets. If it detects a pollution attack, the parent node, which generated the polluted packet, will be considered as a malicious node. Another integrity scheme discussing locating the adversary is SpaceMac [24]. SpaceMac considers a cooperative environment between parent and child nodes. It enforces the child nodes to create packets only from the signed subspace provided by the parent nodes. The central controller, who knows the complete topology of the graph, verifies whether the packets generated by the child node belongs to the subspace of its parent nodes and locates the adversaries efficiently, if any. However, these schemes have significant overhead and dependency on a central trusted controller.

Finally, Parsamehr *et al.* [27] proposed a location-aware IDPS which does not only detect and drop pollution attacks but also identify the attacker's exact location. The proposed IDPS consists of detection and locating schemes based on null space homomorphic MAC. The detection scheme considers some tags added by the source node to each coded packet to detect pollution attacks by intermediate nodes and destination nodes. In the locating scheme, each intermediate node adds an extra tag to the coded packets to verify itself to the Hotspot, which plays the role of the central controller for each mobile small cell. In addition, when each node detects any pollution, the node reports the pollution to the Hotspot that is responsible for detecting the exact location of the attacker(s) based on received reports.

D. IDPS SCHEMES

Intrusion detection and prevention schemes (IDPSs) are mainly focused on identifying potential security incidents and blocking or preventing malicious activity. Regarding adversaries detection, IDPSs use signature-based detection to identify known adversaries in the networks that are not related to legitimate users [35]–[38]. In our previous IDPS scheme [1], we proposed for the first time, to the best of our knowledge, a novel intrusion detection, and prevention scheme (IDPS) for network coding-enabled mobile small cells. The proposed scheme is based on homomorphic MAC-based scheme to identify known malicious behavior (pollution attacks). It is based on a null space-based homomorphic message authentication code scheme that allows the detection of pollution attacks and takes proper risk mitigation actions when an intrusive incident is detected. The proposed scheme has been implemented in Kodo, and its performance has been evaluated in terms of computational and communicational overhead. Its performance evaluation has shown that it does not add significant computational and communicational overhead.

III. SCENARIO ARCHITECTURE

In this section, we provide the scenario architecture of the EU funded H2020-MSCA project "SECRET" (See Fig. 2), which is focused on secure network coding-enabled mobile small cells [11]. Harnessing ongoing trends on 5G technology

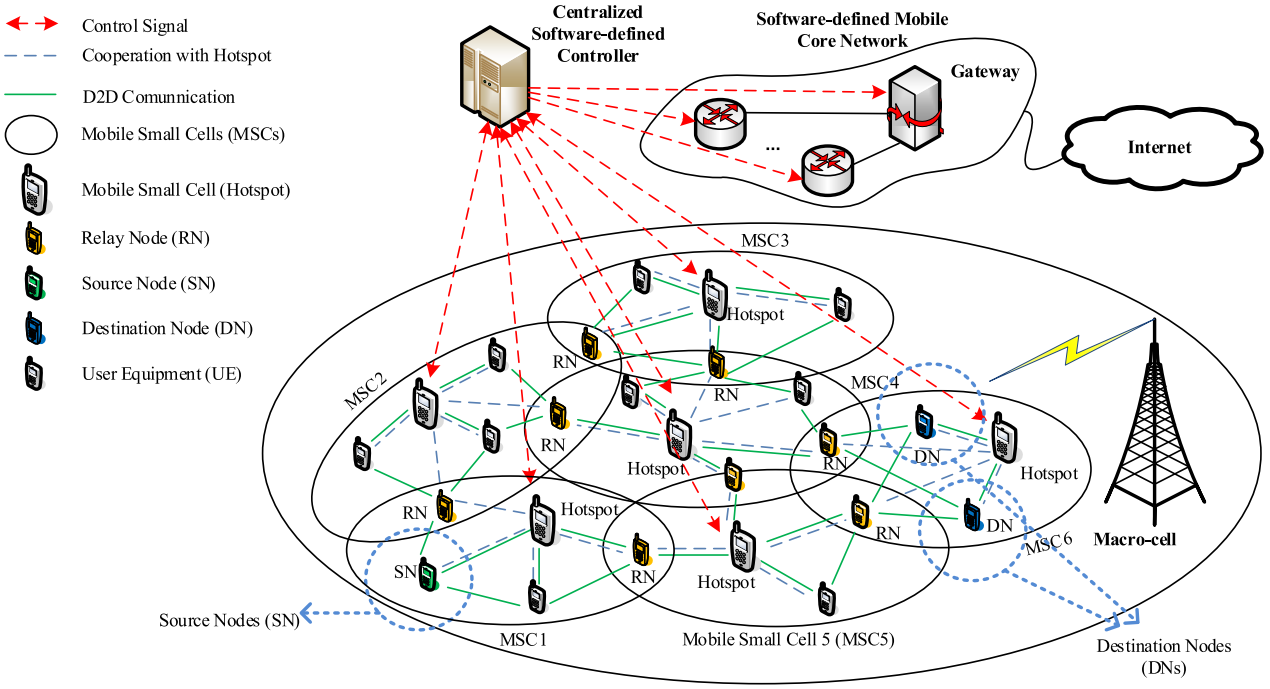

FIGURE 2. Scenario Architecture.

standardization and mobile small cells, a beyond 5G scenario architecture was proposed as shown in Fig. 2. This scenario architecture consists of a Macro Cell, including a number of Mobile Small Cells (MSCs) (i.e., a cluster of mobile devices) that are controlled by a cluster-head (i.e., Hotspot). The Hotspot is a mobile device (i.e., mobile node) within the identified cluster of mobile devices that are nominated to play the role of the local radio manager to control and maintain the cluster. Moreover, the Hotspots of different clusters cooperate to form a wireless network of MSCs that have several gateways/entry points to the mobile network using intelligent high-speed connections. It is worthwhile to mention that a centralized software-defined controller controls the Hotspots of the different clusters. Finally, the data communication between the mobile nodes is established through Device-to-Device (D2D) communications and optimized by network coding technology. In this scenario, it is assumed, as shown in Fig. 2, that a mobile source node (SN) in MSC1 multicasts packets to two mobile destination nodes (DNs) in MSC6. The assumption is that SN and DNs are not in the same MSC and the SN applies Random Linear Network Coding (RLNC) to code and transmit packets, through the multi-hop D2D network, to the DNs where they are decoded. In this scenario, it is assumed that the D2D network consists of legitimate mobile nodes and relay mobile nodes (RNs) that are User Equipments (UEs) and connect the MSCs to each other.

IV. PROPOSED EFFICIENT INTRUSION DETECTION AND LOCATION-AWARE PREVENTION (IDLP) MECHANISM FOR NC-ENABLED MSCS

In this section, we present the proposed intrusion detection and location-aware prevention (IDLP) mechanism consisting of a) a detection scheme that is used to detect pollution attacks; and b) a locating scheme which is a part of the prevention mechanism and supported by the detection scheme that allows the identification of the exact location of the adversary nodes (i.e., the source of pollution attacks). The detection and the locating schemes of the proposed IDLP mechanism are based on the Null Space homomorphic MAC scheme [14].

Due to a large number of mobile devices, the execution of the proposed IDLP mechanism on all nodes in each MSC will lead to the waste of a huge amount of devices' resources (e.g., CPU power, memory, and battery level) per verification time. Thus, we consider the application of the proposed IDLP into two phases in order to improve its efficiency in terms of resources consumption (see Fig. 4);

- ***Phase 1: Identification of the MSC where pollution attack occurred.*** Initially, the detection scheme of the proposed IDLP mechanism is applied to all RNs and DNs, which are the final receivers of the packets. We consider that each RN connects two MSCs, and all transferred data between the two MSCs pass through this RN, as shown in Fig. 3. Therefore, RNs are located in the best position to detect attacks and protect the whole network from pollution. However, in the case that the SN and DNs are in the same MSC, then the DNs are responsible for attack detection. When an RN detects a pollution attack, it drops the polluted packet and reports the attack to the Hotspots of the MSCs in which it belongs to. On the other hand, when a DN detects a pollution attack, it drops the polluted packet and reports the attack to the Hotspot of the MSC where it belongs to. Then, each Hotspot forwards the received report to the SDN Controller, which is responsible for identifying

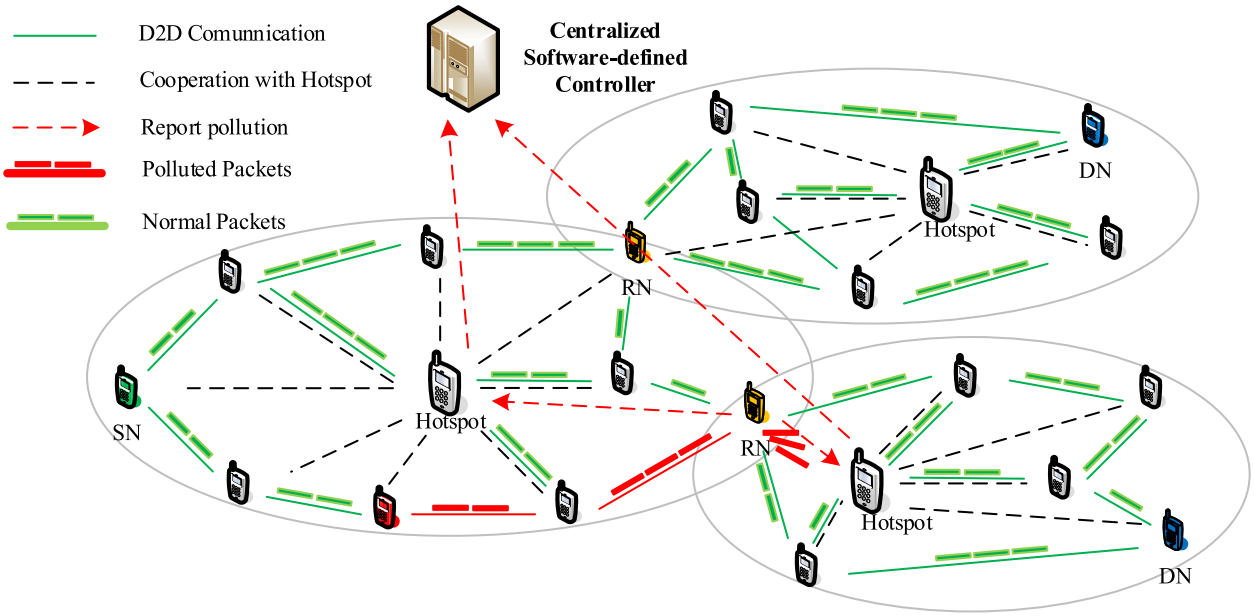

FIGURE 3. Three butterfly topologies.

the MSC where a pollution attack occurred based on the received reports.

- ***Phase 2: Identification of the adversary node's location within the polluted MSC.*** The detection scheme and the locating scheme are applied to all mobile devices of the polluted MSC, which was identified in Phase 1. When a mobile device, within the polluted MSC, detects a polluted packet and drops it, then the mobile device creates a new report, based on the locating scheme, which is sent to the Hotspot of the identified MSC. In addition, according to the locating scheme, each mobile device, within the polluted MSC, creates an expanded coded packet that is sent to the next node and the Hotspot as well. Afterward, the Hotspot forwards: a) the received report from the device that detected the polluted packet, and b) the expanded coded packet to the SDN controller that is responsible for identifying the exact location of the adversary mobile device(s). In particular, the SDN controller makes use of the information included in the received report and expanded packet in order to identify the adversary's location. As a next step, after the identification of the adversary's location, the SDN controller will decide 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.

A. DETECTION SCHEME

The detection scheme of the proposed IDLP mechanism is based on the null space-based homomorphic MAC scheme that was presented in our previous works [1] and [14] and makes use of orthogonality to verify the tags appended to the end of each packet. According to [1], the SN divides the message into a generation of native packets denoted as $\underline{b}_1, \underline{b}_2, \ldots, \underline{b}_m$, where m is generation size and each packet $\underline{b}_i$ consists of n symbols (i.e., $\underline{b}_{i,1}, \underline{b}_{i,2}, \ldots, \underline{b}_{i,n}$) in the finite field $\mathbb{F}_p^n$. Therefore, the source node will generate a coded packet $\mathbf{b}_i$ according to (1) and send 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:

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

After that 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 linear combination of all the received coded packet belonging to the same generation, where β is randomly selected from $\mathbb{F}_p$ and all arithmetic operation 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 [1], when an SN creates the coded packet, it generates L tags, based on null space properties [30], that are used to detect pollution attacks. There are five steps to create the tags and also 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 $(\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_L)$ in the finite field $\mathbb{F}_p^{m+n+L}$ and distributes them to the source node.

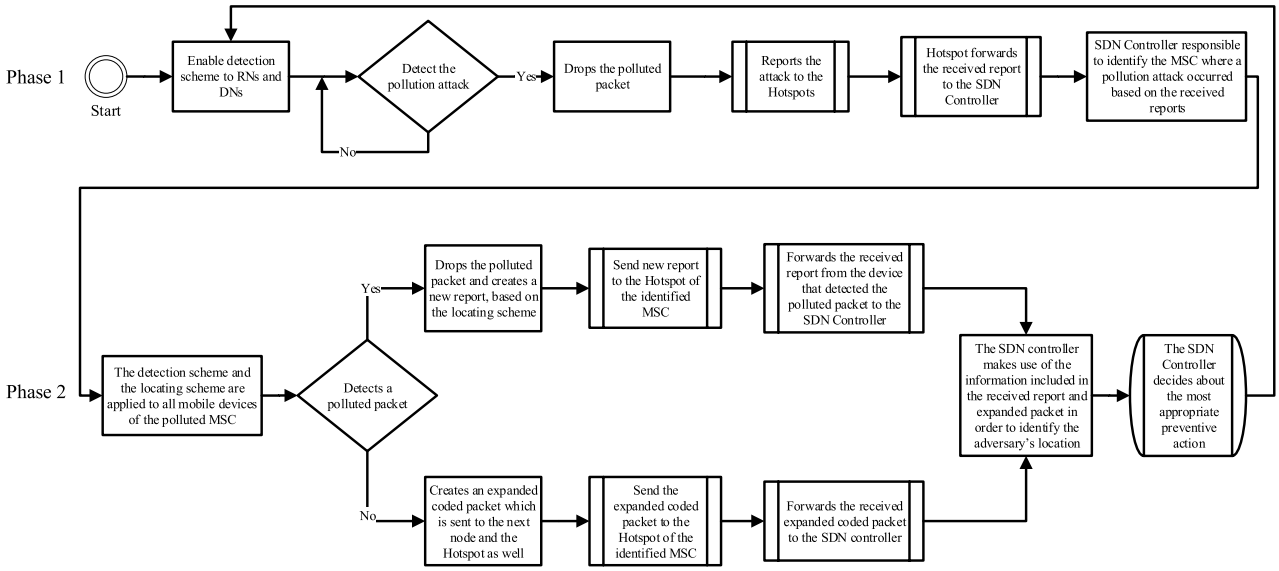

FIGURE 4. Proposed Efficient Intrusion Detection and Location-aware Prevention (IDLP) Mechanism for NC-enabled MSCs.

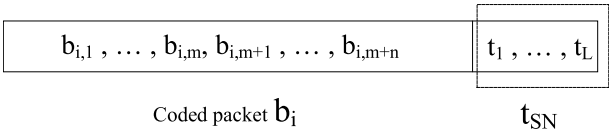

FIGURE 5. L tags appended to the end of coded packet b_i.

2) The source node creates L tags (i.e., $t_1, t_2, \ldots, t_L$) by 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 Fig. 5.

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

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.

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

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

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

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

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

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

B. LOCATING SCHEME

The locating scheme is carried out in Phase 2 of the proposed IDLP mechanism in order to identify the exact location of the adversary mobile node within the polluted MSC. Particularly, the locating scheme is applied to all mobile devices of the polluted MSC that was identified in Phase 1. According to the locating scheme, each mobile node is responsible to: a) generate an expanded coded packet, based on the received coded packet, and transmit it to the next node and the Hotspot as well, and b) send a report to the Hotspot when a polluted packet is detected through the detection scheme. Both the expanded coded packet and the report are forwarded to the SDN Controller which leverages them in order to identify the exact location of the adversary.

1) EXPANDED CODED PACKET

The most critical problem for detecting the exact location of an adversary mobile node is derived from the fact that nodes may deceive Hotspots (see Fig. 1). For example, a node can report that the received packet from the previous legal node is polluted [24]. Therefore, an extra tag is added to each coded packet for verifying each intermediate node to the SDN Controller. This tag is created based on the pre-distributed share key between each node and the SDN Controller. To calculate

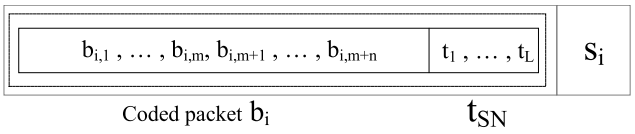

FIGURE 6. Expanded Coded Packet $\{\mathbf{b}_i||t_{SN}||s_i\}$.

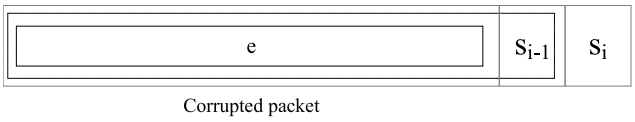

FIGURE 7. The generated report $\{e||s_{i-1}||s_i\}$.

the proper tag, the following Equation is used:

$$\left[\mathcal{C}''_{1,1}\ \dots\ \mathcal{C}''_{1,m+n}\ \dots\ \mathcal{C}''_{1,m+n+L}\right]_{1*(m+n+L)} * \begin{bmatrix} b_{i,1} \\ b_{i,2} \\ \vdots \\ b_{i,m+n} \\ t_1 \\ \vdots \\ t_L \end{bmatrix}_{(m+n+L)*1} + \mathcal{C}''_{1,m+n+L+1} * \mathbf{s}_i = 0 \quad (8)$$

where $\left[\mathcal{C}''_{1,1}\ \dots\ \mathcal{C}''_{1,m+n}\ \dots\ \mathcal{C}''_{1,m+n+L+1}\right]_{1*(m+n+L+1)}$ is the pre-shared key distributed by the KDC, and s_i is the properly calculated tag.

As we can see in Fig. 6, each intermediate node attaches a tag s_i to each coded packet in order to create an expanded coded packet. Then, each intermediate node sends the expanded coded packet $\{\mathbf{b}_i||t_{SN}||s_i\}$ to the next node and Hotspot. Where bi is the coded packet, t_{SN} represents the set of appended tags by SN, and s_i is the appended tag by the given intermediate node. The Hotspot forwards the expanded coded packet received from each intermediate node to the SDN Controller so that the SDN Controller can verify legal nodes.

The SDN controller verifies the received expanded coded packet $\{\mathbf{b}_i||t_{SN}||s_{i-1}\}$ based on the following formula which if $\delta = 0$, then the received expanded coded packet is verified.

$$\delta = \sum_{j=1}^{m+n+L+1} \mathcal{C}''_{i,j} * \overline{\{b_{i,j} \parallel t_{SN} \parallel s_i\}} \quad (9)$$

2) REPORT

Every time that an intermediate node or a DN detects any polluted packet (e) signed by the previous mobile device's key ($\{e||s_{i-1}\}$), a report is generated by the given node. As shown in Fig. 7 the generated report is the received polluted packet ($\{e||s_{i-1}\}$) signed by the given node and is represented as $\{e||s_{i-1}||s_i\}$. Then, the node sends the report to the Hotspot, and the Hotspot forwards it to the SDN Controller. This report allows the SDN Controller to identify the attacker's location.

The SDN controller verifies the sender of the received report $\{e||s_{i-1}||s_i\}$ based on the following Equation which if $\delta = 0$, then the sender is verified.

$$\delta = \sum_{j=1}^{m+n+L+2} \mathcal{C}''_{i,j} * \overline{\{e \parallel s_{i-1} \parallel s_i\}} \quad (10)$$

Afterward, the SDN controller verifies the signature of the adversary node (s_{i-1}) based on the following Equation which if $\delta = 0$, then the signature is verified.

$$\delta = \sum_{j=1}^{m+n+L+1} \mathcal{C}''_{i,j} * \overline{\{e \parallel s_{i-1}\}} \quad (11)$$

3) SCENARIOS FOR LOCATING SCHEME

Each intermediate node should check the validity of the received packets $\{\mathbf{b}_i||t_{SN}||s_{i-1}\}$ based on the detection scheme (see Fig. 8). The intermediate node checks the tags t_{SN} appended to the end of the received packet by the SN. If there is no pollution attack, the intermediate node deletes tag s_{i-1}, attached by the previous node, and creates the coded packet by combining received genuine packets and also creates s_i, and attaches it to the end of the coded packet. Then, the intermediate sends $\{\mathbf{b}_i||t_{SN}||s_i\}$ to the next node and the Hotspot as well. Otherwise, if the intermediate node detects any polluted packet, it should drops it and creates a report $\{e||s_{i-1}||s_i\}$ and sends it to the Hotspot. Hotspot forwards it to the SDN controller who is responsible to identify the exact location of adversary mobile devices.

As we discussed in the pollution attacks section, there are two different adversaries; external and internal adversaries. External adversaries attempt to inject some corrupted packets to make pollution, and internal adversaries are the compromised nodes which make pollution by modifying transmitted packets or injecting polluted packets. After applying our locating scheme, the external adversaries cannot verify themselves to the Hotspot (see Fig. 9), because they do not have access to the shared key between the SDN Controller and each valid node to create a valid signature s_i. So, when the SDN Controller receives polluted packets $\{e||s'_i\}$ (i.e., s'_i is an invalid created tag by an external adversary), then it is able to detect the adversary and decide about the preventive actions (e.g., block compromised mobile device from accessing the network) that should take. However, the most serious challenge is the internal pollution attacks which are created by compromised nodes because, as assumed, they have access to the shared secret key between each intermediate node and the SDN Controller. We have considered the following two scenarios to present how the proposed locating scheme can identify the internal adversary's location.

- ***Scenario-1 An internal adversary node, B, between two normal nodes, A and C:*** B is an adversary who has four options to report to Hotspot in order to deceive the SDN Controller according to the following two cases:
  - "***When B receives a normal packet from node*** A": Node B has two options to launch an attack.
    i. ***To send a polluted packet*** $\{e||s_B\}$ ***to the next node*** C ***(pollution attack):*** If node B sends a

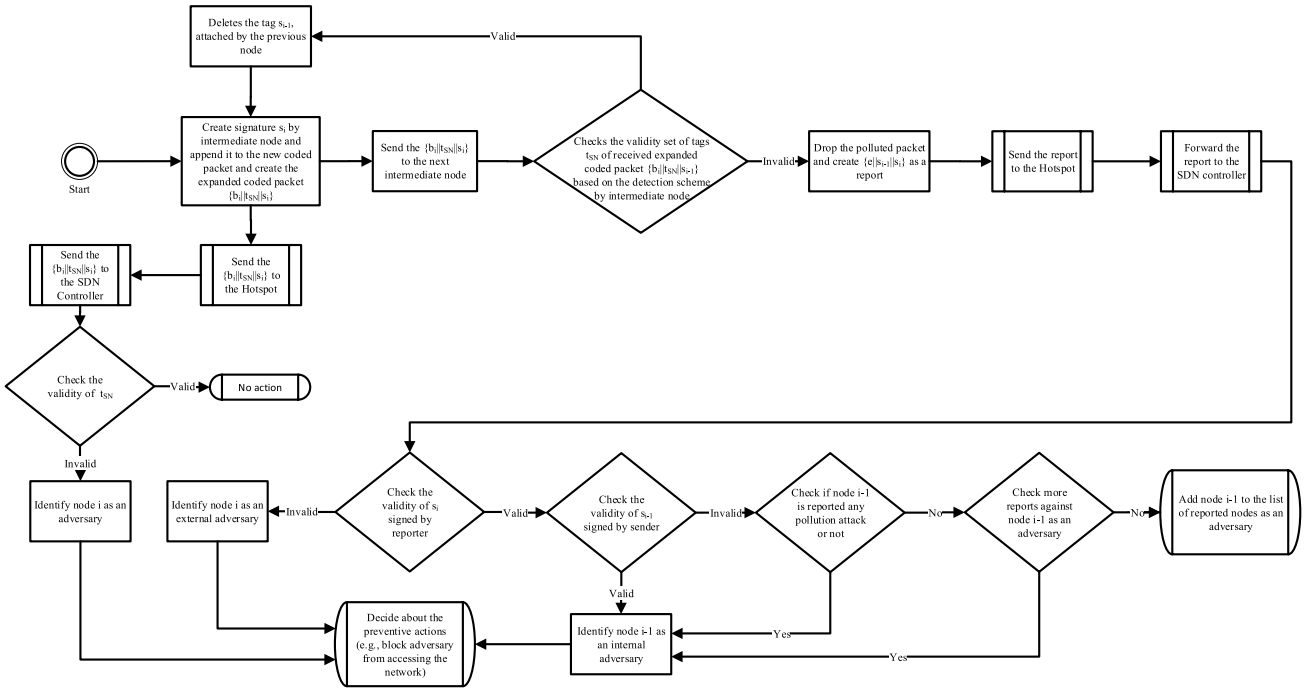

FIGURE 8. Locating scheme of the Proposed IDLP Mechanism for NC-enabled MSCs.

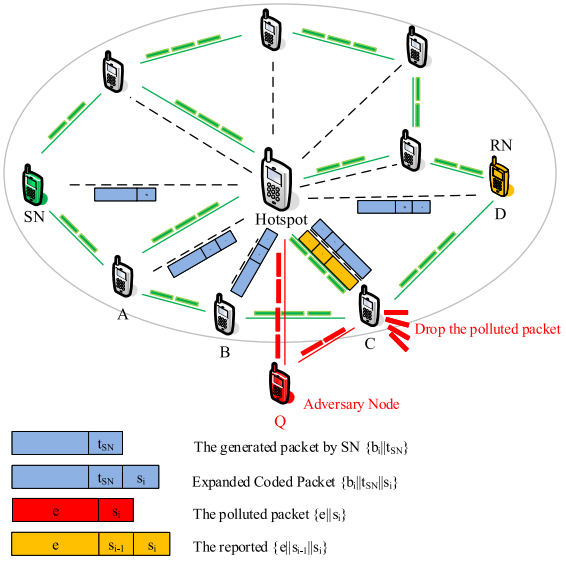

FIGURE 9. An external pollution attack.

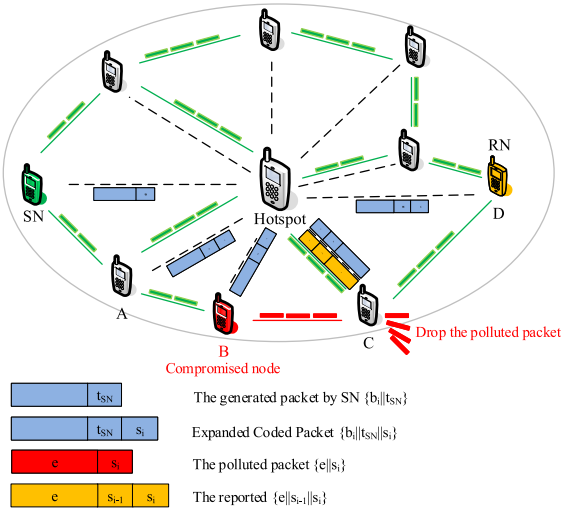

FIGURE 10. An Internal pollution attack; A is a normal node and B is an adversary.

polluted packet $\{e||s_B\}$ to node C, then node C will drop it and reports a pollution $\{e||s_B||s_C\}$ to the Hotspot and Hotspot forwards the report to the SDN Controller. When SDN Controller verifies s_C and s_B, it detects that node B is an adversary (see Fig. 10). However, if the polluted packet $\{e||s'_B\}$, which is sent to node C, has an invalid tag s'_B, it means that node B acted as an intelligent adversary and generated an invalid signature for the expanded coded packet. In this case, the SDN Controller is not sure that node B is an adversary and thus, the SDN Controller should wait to receive more reports against node B until to decide whether node B is an adversary or not and take a prevention action against node B.

ii. ***To drop the received packet from node A:*** If node B drops the received packet from node A, it will achieve another kind of attack (i.e., DoS attack), which is, however, out of the scope of this paper.

– "***When B receives a polluted packet from node A***": Similar to previous case, node B has two options to launch an attack:

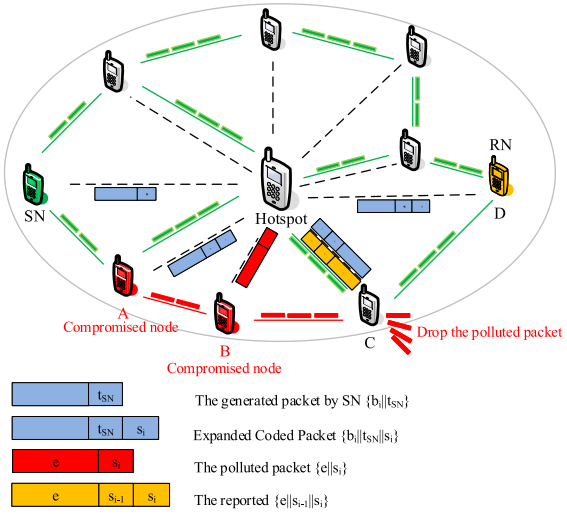

FIGURE 11. An Internal pollution attack; both node A and node B are adversaries.

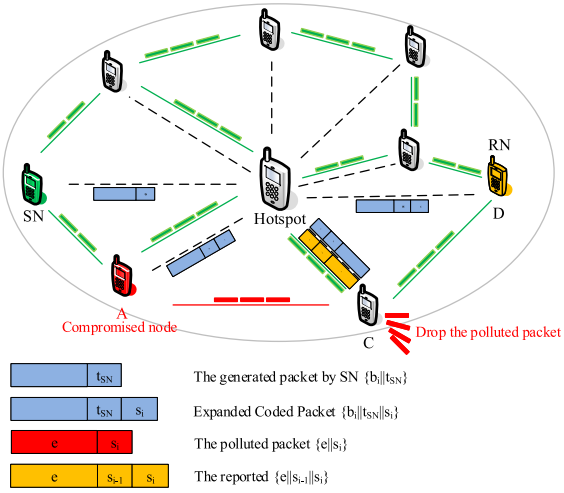

FIGURE 12. An Internal pollution attack; node B has been detected as an adversary by Hotspot and blocked from the network.

i. ***To send a polluted packet $\{e||s_B\}$ to the next node C:*** If node B sends a polluted packet $\{e||s_B\}$ to node C, then node C will drop it and reports a pollution $\{e||s_B||s_C\}$ to the Hotspot and Hotspot forwards the report to the SDN Controller. When SDN Controller verifies s_C and s_B, it detects that node B is an adversary. However, if the polluted packet $\{e||s'_B\}$, which is sent to node C, has an invalid tag s'_B, it means that node B acted as an intelligent adversary and generated an invalid signature for the expanded coded packet. In this case, the SDN Controller is sure that node B is an adversary because node B has already reported the pollution but it did not drop the polluted packet. Then, the SDN Controller takes the appropriate prevention actions against node B.

ii. ***To drop the received packet from node A:*** If node B reports that A is an adversary ($\{e||s'_A||s_B\}$) and drops the received packet from node A, then the SDN Controller, despite the invalid tag s'_A, will not consider node A as an adversary until it receives more reports against node A. However, more reports against node A will not be received by the SDN Controller because node A is a normal node.

- ***Scenario-2 Two or more adversaries in a row:*** In this scenario, node A and node B are considered as adversary nodes. As shown in Fig. 11, node B, as an adversary, cannot send a valid expanded coded packet $\{\mathbf{b}_i||t_{SN}||s_i\}$ to Hotspot because it will receive a polluted packet from the previous node, A, which is an adversary and does not have access to the valid tag (t_{SN}) to get verified successfully by the SDN Controller. Therefore, the SDN Controller detects and blocks the adversary node, B, from the network. After blocking node B from the network, the network has now one adversary node (i.e., node A) between two normal nodes (see Fig. 12), which is similar to the first scenario. Moreover, it is worthwhile to mention that Scenario 2 is valid for more than two adversaries in a row when the adversaries cannot verify themselves to the SDN Controller. In this case, they will be blocked from accessing the network.

V. IMPLEMENTATION

In this section, the implementation process is discussed regarding the proposed IDLP mechanism and is compared with our previous IDPS scheme [1], which was the first time that a novel intrusion detection and prevention scheme for NC-enabled mobile small cells was proposed. First of all, we implemented three butterfly topologies, including 18 normal nodes and 1 adversary node (see Fig. 13), and applied the RLNC approach to it. In addition, we programmed the adversary node to modify its received packets so as to demonstrate a pollution attack.

The implementation is based on the recoding library of Kodo which allows encoding at the source node, recoding at the intermediate nodes, and decoding at the destination nodes [39]. This is the most famous network coding library that academic community uses in order to implement network coding algorithms on Kodo which is an open-source library based on C++, but allows the use of the library functionality with different programming languages, like C, C++, Python, etc. [39]–[43]. Various network coding algorithms such as Systematic RLNC, Sparse RLNC, and Standard RLNC, are supported by Kodo [40], [44]. However, Kodo has some limitations regarding the creation of a customized generation of packets and keys and also regarding tag generation. Therefore, in our implementation, the packets, their proper tags, and the required keys at the source node and intermediate nodes were generated by Matlab. Then, the generated packets, keys, and tags were included manually in Kodo so as to achieve the desired functionality of the implemented scenario on Kodo.

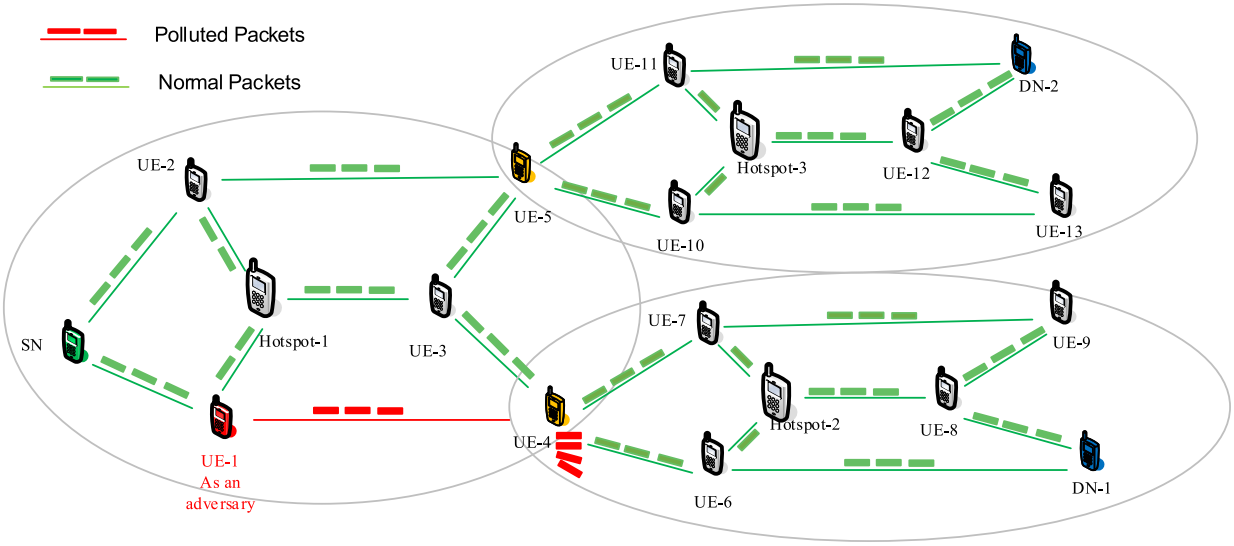

FIGURE 13. Implemented three butterfly topologies.

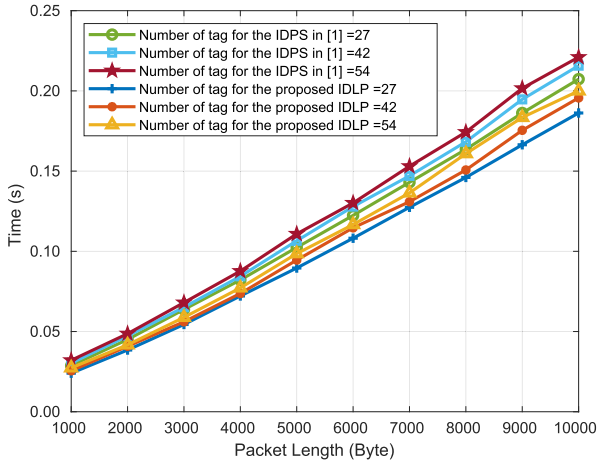

FIGURE 14. The T_{total} for different number of tags in [1] and the proposed IDLP mechanism.

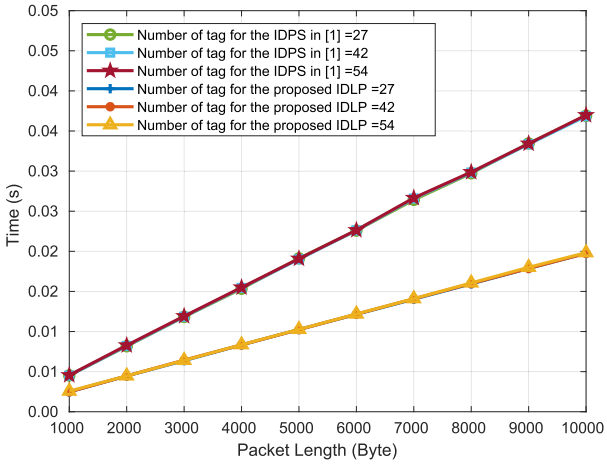

FIGURE 15. The T_{ver} for different number of tags in [1] and the proposed IDLP mechanism.

The packet generation size is selected to be 64 symbols and the symbol size is set between 1, 000 to 10, 000 bytes, as shown in Fig. 14 to Fig. 17. In addition, the number of tags appended to the end of each packet is L, which can be 27, 42, or 54 [30], and the Galois field in use is $GF2^8$. Finally, it is worthwhile to mention that the machine used for running the whole implementation has the following characteristics: a 2.7 *GHz* Core *i*7 CPU with 8*GB* of physical memory.

VI. PERFORMANCE EVALUATION

In this section, the performance evaluation of the proposed IDLP mechanism, in terms of computational and communication overheads, as well as the successfully decoding probability are provided and compared with the IDPS scheme proposed in [1]. It should be noted that the proposed IDLP 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 protects the resources of the network. While the IDPS scheme proposed in [1] only detects and drops the polluted packets, which, however, allows attackers to continue making pollution attacks that lead to waste of network resources. Also, the implementation of the previous IDPS scheme showed that it does not bring high overhead computational complexity. On the other hand, the proposed IDLP mechanism has better performance not only in the decoding probability but also in computational and communication overheads. In particular, the proposed IDLP mechanism has less unsuccessful decoding probability because when the attacker's location is detected, the attacker is blocked by the SDN Controller, and the attacker cannot continue polluting. Thus, the probability that the attackers can overpass the proposed IDLP mechanism is close to zero. The comparisons are described in the following sections. Regarding the implementation, it is noteworthy to highlight that the proposed IDLP mechanism was implemented on Kodo over 3 butterfly topologies, as shown in Fig. 13, similar

to the implementation of the IDPS scheme proposed in [1], and this allows us to compare their performance evaluation results in terms of computational complexity, computational overhead, and unsuccessful decoding probability.

A. COMPUTATIONAL OVERHEAD

As it was mentioned before, based on [30], the number of the tags appended to the end of each coded packet is assumed to be L, where L can be 27, 42, or 54, and the Galois field in use is GF(2^8). Also, the selected generation size is 64 symbols, and the symbol size is set between 1, 000 bytes and 10, 000 bytes.

It should be mentioned that the total time elapsed from when the packet is generated to when the packet is verified and decoded at the destination nodes is given by the following Equation:

$$T_{total} = T_{enc} + T_{rec} + T_{dec} + T_{ver} \tag{12}$$

In this Equation, T_{enc} is the time for encoding at the source node, T_{rec} is the time for recoding at each intermediate node, T_{dec} is the time for decoding at the destination node, and T_{ver} is the time for verifying at the intermediate and destination nodes.

The T_{total}, for the IDPS scheme presented in [1] and the proposed IDLP mechanism are illustrated in Fig. 14. This figure include three curves based on the number of tags (i.e., $L = 27, 42, 54$) for each approach. As shown, by increasing the number of tags, the T_{total} increases as well. However, the T_{total} for a different number of tags in the proposed IDLP mechanism (e.g., $T_{total,L=54} = 0.20$ when the packet length is 10, 000 bytes) is less than the T_{total} in the IDPS scheme (e.g., $T_{total,L=54} = 0.22$ when the packet length is 10, 000 bytes) presented in [1].

It is worthwhile to mention that the reason why the T_{total} in the proposed IDLP mechanism decreases compared to the T_{total} in IDPS scheme presented in [1], despite the fact that the IDLP mechanism provides not only detection but also locating functionality, is that in the IDLP mechanism the detection scheme does not need to apply to all the intermediate nodes, unlike the IDPS scheme presented in [1].

Additionally, the time required to verify and detect any corrupted packet in the network for both the previous IDPS scheme and the proposed IDLP mechanism is presented in Fig. 15, respectively. As shown in this figure, the required time for verification in the proposed IDLP mechanism is less than the IDPS scheme presented in [1]. However, it should be pointed out that the IDLP mechanism, during the verification and detection time, does not only detect and drop the polluted packet but also detects the exact location of the attacker(s) and block them from the network.

B. COMMUNICATIONAL OVERHEAD

To determine the communication overhead of the proposed IDLP mechanism, the communication time T_{comm} is defined as follows:

$$T_{comm} = T_{total} - T_{ver} \tag{13}$$

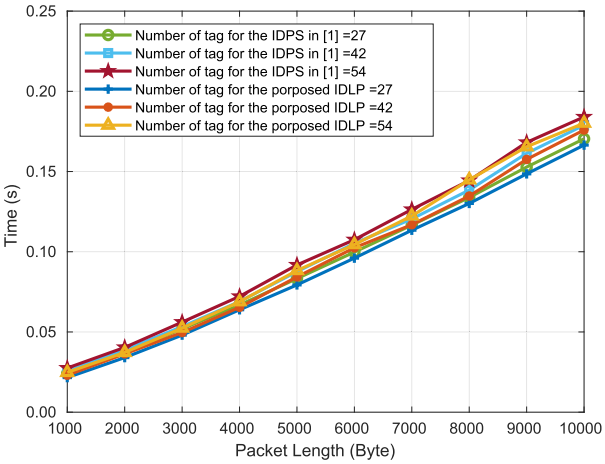

FIGURE 16. The T_{comm} for different number of tags in [1] and the proposed IDLP mechanism.

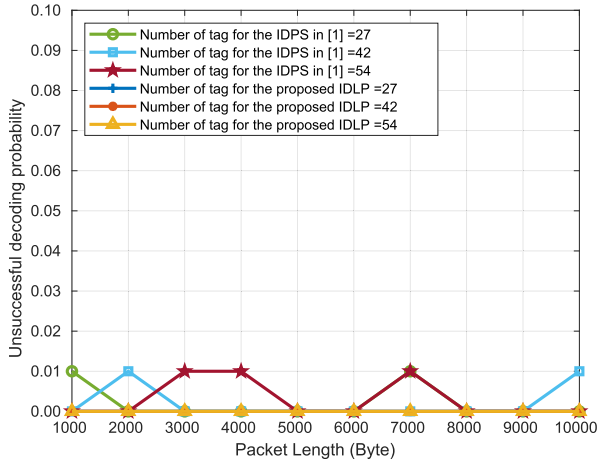

FIGURE 17. The P_r for different number of tags in [1] and the proposed IDLP mechanism.

Fig. 16 shows the T_{comm} based on the different numbers of tags used in the IDPS scheme presented in [1] and the proposed IDLP mechanism, respectively. The results show that the T_{comm} for the proposed IDLP is less than the T_{comm} for the IDPS in [1]. The difference is due to the fact that the proposed IDLP mechanism blocks the adversaries and thus, they are not able anymore to modify the packets in transit. Therefore, the SN does not need to resend packets.

C. DECODING PROBABILITY

The P_r is defined as the probability that a corrupted packet is not detected in the verification phase. Fig. 17 shows the P_r for the proposed IDLP mechanism and the IDPS scheme presented in [1] based on three different number of tags ($L = 27, 42$, and 54). As shown in this figure, the P_r is almost 0 for the proposed IDLP mechanism. However, the IDPS proposed in [1] is near to 0. In other words, in the IDPS scheme, the adversary does not have any chance to distribute the corrupted packet in the network. However, they can make pollution in the next transmission for coded packet from SN to DNs in the network. Nevertheless, in the proposed IDLP

mechanism, the detected adversaries are blocked from access to the network in the future.

VII. CONCLUSION

This paper proposed an efficient IDLP mechanism for Network Coding-enabled Mobile Small Cells. The proposed IDLP mechanism is an extension of our previously proposed location-aware IDPS scheme for network coding-enabled mobile small cells presented in [27] and consists of detection schemes and locating scheme. We use the null space-based homomorphic MAC scheme [14] for both the detection and locating schemes, which is adapted to the mobile small cell environment. The proposed IDLP 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. It is worthwhile to mention that the proposed IDLP mechanism is more efficient than the previous IDPS scheme proposed in [1], which is the first proposed IDPS for NC-enabled mobile small cells, because it is not needed to be applied to all mobile devices in order to protect the NC-enabled mobile small cells from the depletion of their resources. Both the IDLP mechanism and the IDPS scheme proposed in [1] have been implemented in Kodo and their performance has been evaluated in terms of computational complexity, communicational overhead, and successfully decoding probability as well. The performance evaluation results verified that the proposed IDLP mechanism is more efficient than the IDPS scheme proposed in [1] since it demonstrates reduced computational complexity, communicational overhead, and unsuccessfully decoding probability.

ACKNOWLEDGMENT

This work was partly supported by the European Union's Horizon 2020 Research and Innovation Programme under Grant H2020-MSCA-ITN-2016-SECRET-722424, and by the European Regional Development Fund (FEDER), through COMPETE 2020, POR ALGARVE 2020, Fundaçẽo para a Ciência e Tecnologia under i-Five Project (POCI-01-0145-FEDER-030500).

REFERENCES

[1] R. Parsamehr, A. Esfahani, G. Mantas, A. Radwan, S. Mumtaz, J. Rodriguez, and J.-F. Martinez-Ortega, "A novel intrusion detection and prevention scheme for network coding-enabled mobile small cells," *IEEE Trans. Comput. Social Syst.*, vol. 6, no. 6, pp. 1467–1477, Dec. 2019.

[2] B. Bangerter, S. Talwar, R. Arefi, and K. Stewart, "Networks and devices for the 5G era," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 90–96, Feb. 2014.

[3] I. Chih-Lin, C. Rowell, S. Han, Z. Xu, G. Li, and Z. Pan, "Toward green and soft: A 5G perspective," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 66–73, Feb. 2014.

[4] G. Mantas, N. Komninos, J. Rodriuez, E. Logota, and H. Marques, "Security for 5G communications," in *Fundamentals of 5G Mobile Networks*, J. Rodriguez, Ed. Hoboken, NJ, USA: Wiley, 2015, pp. 207–220.

[5] V. Sucasas, G. Mantas, and J. Rodriguez, "Security challenges for cloud radio access networks," *Backhauling/Fronthauling Future Wireless Syst.*, pp. 195–211, Sep. 2016.

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

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

[8] S.-F. Chou, T.-C. Chiu, Y.-J. Yu, and A.-C. Pang, "Mobile small cell deployment for next generation cellular networks," in *Proc. IEEE Global Commun. Conf.*, Dec. 2014, pp. 4852–4857.

[9] Y.-J. Chen, L.-C. Wang, K. Wang, and W.-L. Ho, "Topology-aware network coding for wireless multicast," *IEEE Syst. J.*, vol. 12, no. 4, pp. 3683–3692, Dec. 2018.

[10] S. Katti, H. Rahul, W. Hu, D. Katabi, M. Médard, and J. Crowcroft, "XORs in the air: Practical wireless network coding," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 36, no. 4, pp. 243–254, 2006.

[11] J. Rodriguez, A. Radwan, C. Barbosa, F. H. P. Fitzek, R. A. Abd-Alhameed, J. M. Noras, S. M. R. Jones, I. Politis, P. Galiotos, G. Schulte, A. Rayit, M. Sousa, R. Alheiro, X. Gelabert, and G. P. Koudouridis, "SECRET—Secure network coding for reduced energy next generation mobile small cells: A European training network in wireless communications and networking for 5G," in *Proc. Internet Technol. Appl. (ITA)*, Sep. 2017, pp. 329–333.

[12] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network information flow," *IEEE Trans. Inf. Theory*, vol. 46, no. 4, pp. 1204–1216, Jul. 2000.

[13] T. Ho and D. Lun, *Network Coding: An Introduction*. Cambridge, U.K.: Cambridge Univ. Press, 2008.

[14] A. Esfahani, G. Mantas, and J. Rodriguez, "An efficient null space-based homomorphic MAC scheme against tag pollution attacks in RLNC," *IEEE Commun. Lett.*, vol. 20, no. 5, pp. 918–921, May 2016.

[15] R. Parsamehr, G. Mantas, A. Radwan, J. Rodriguez, and J.-F. Martínez, "Security threats in network coding-enabled mobile small cells," in *Proc. Int. Conf. Broadband Commun., Netw. Syst.* Cham, Switzerland: Springer, Sep. 2018, pp. 337–346.

[16] S. Agrawal and D. Boneh, "Homomorphic MACs: MAC-based integrity for network coding," in *Proc. Int. Conf. Appl. Cryptography Netw. Secur.* Berlin, Germany: Springer, 2009, pp. 292–305.

[17] A. Fiandrotti, R. Gaeta, and M. Grangetto, "Securing network coding architectures against pollution attacks with band codes," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 3, pp. 730–742, Mar. 2019.

[18] S. Jaggi, M. Langberg, S. Katti, T. Ho, D. Katabi, and M. Médard, "Resilient network coding in the presence of byzantine adversaries," in *Proc. 26th IEEE Int. Conf. Comput. Commun. (INFOCOM)*, May 2007, pp. 616–624.

[19] T. Ho, B. Leong, R. Koetter, M. Medard, M. Effros, and D. R. Karger, "Byzantine modification detection in multicast networks with random network coding," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2798–2803, Jun. 2008.

[20] M. Kim, L. Lima, F. Zhao, J. Barros, M. Medard, R. Koetter, T. Kalker, and K. J. Han, "On counteracting byzantine attacks in network coded peer-to-peer networks," *IEEE J. Sel. Areas Commun.*, vol. 28, no. 5, pp. 692–702, Jun. 2010.

[21] M. Kim, M. Medard, and J. Barros, "Algebraic watchdog: Mitigating misbehavior in wireless network coding," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 10, pp. 1916–1925, Dec. 2011.

[22] F. Zhao, T. Kalker, M. Medard, and K. J. Han, "Signatures for content distribution with network coding," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2007, pp. 556–560.

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

[24] A. Le and A. Markopoulou, "Cooperative defense against pollution attacks in network coding using SpaceMac," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 2, pp. 442–449, Feb. 2012.

[25] M. J. Siavoshani, C. Fragouli, and S. Diggavi, "On locating Byzantine attackers," in *Proc. 4th Workshop Netw. Coding, Theory Appl.*, Jan. 2008, pp. 1–6.

[26] Q. Wang, L. Vu, K. Nahrstedt, and H. Khurana, "Identifying malicious nodes in network-coding-based peer-to-peer streaming networks," Tech. Rep., 2009.

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

[28] A. Esfahani, G. Mantas, D. Yang, A. Nascimento, J. Rodriguez, and J. Neves, "Towards secure network coding-enabled wireless sensor networks in cyber-physical systems," in *Cyber-Physical Systems: From Theory to Practice*. Boca Raton, FL, USA: CRC Press, 2015, pp. 395–414.

[29] L. Lima, J. P. Vilela, P. F. Oliveira, and J. Barros, "Network coding security: Attacks and countermeasures," 2008, *arXiv:0809.1366*. [Online]. Available: http://arxiv.org/abs/0809.1366
[30] P. Zhang, Y. Jiang, C. Lin, H. Yao, A. Wasef, and X. Shenz, "Padding for orthogonality: Efficient subspace authentication for network coding," in *Proc. IEEE INFOCOM*, Apr. 2011, pp. 1026–1034.
[31] 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," *Int. J. Inf. Secur.*, vol. 16, no. 6, pp. 627–639, 2017.
[32] A. Esfahani, D. Yang, G. Mantas, A. Nascimento, and J. Rodriguez, "Dual-homomorphic message authentication code scheme for network coding-enabled wireless sensor networks," *Int. J. Distrib. Sensor Netw.*, vol. 11, no. 7, Jan. 2015, Art. no. 510251.
[33] 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, Switzerland: Springer, 2019, pp. 347–356.
[34] V. Adat, I. Politis, C. Tselios, P. Galiotos, and S. Kotsopoulos, "On blockchain enhanced secure network coding for 5G deployments," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2018, pp. 1–7.
[35] K. Scarfone and P. Mell, "Guide to intrusion detection and prevention systems (IDPS)," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, NIST Special Pub. (SP) 800-94 Rev. 1 (Draft), 2012.
[36] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to integrating forensic techniques into incident response," *NIST Special Publication*, vol. 10, no. 14, pp. 800–886, 2006.
[37] K. Kent and M. Souppaya, "Guide to computer security log management," *NIST Special Publication*, vol. 92, pp. 1–72, Sep. 2006.
[38] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, "Computer security incident handling guide," *NIST Special Publication*, vol. 800, no. 61, pp. 1–147, 2012.
[39] M. V. Pedersen, J. Heide, and F. H. Fitzek, "Kodo: An open and research oriented network coding library," in *Proc. Int. Conf. Res. Netw.* Berlin, Germany: Springer, 2011, pp. 145–152.
[40] P. Pahlevani, H. Khamfroush, D. E. Lucani, M. V. Pedersen, and F. H. P. Fitzek, "Network coding for hop-by-hop communication enhancement in multi-hop networks," *Comput. Netw.*, vol. 105, pp. 138–149, Aug. 2016.
[41] J. Hansen, J. Krigslund, D. E. Lucani, P. Pahlevani, and F. H. P. Fitzek, "Bridging inter-flow and intra-flow network coding in wireless mesh networks: From theory to implementation," *Comput. Netw.*, vol. 145, pp. 1–12, Nov. 2018.
[42] J. Krigslund, J. Hansen, D. E. Lucani, F. H. Fitzek, and M. Médard, "Network coded software defined networking: Design and implementation," in *Proc. Eur. Wireless, 21th Eur. Wireless Conf. (VDE)*, May 2015, pp. 1–6.
[43] Y. Fan, Y. Jiang, H. Zhu, and X. Shen, "An efficient privacy-preserving scheme against traffic analysis attacks in network coding," in *Proc. IEEE 28th Conf. Comput. Commun. (INFOCOM)*, Apr. 2009, pp. 2213–2221.
[44] A. Esfahani, G. Mantas, H. Silva, J. Rodriguez, and J. C. Neves, "An efficient MAC-based scheme against pollution attacks in XOR network coding-enabled WBANs for remote patient monitoring systems," *EURASIP J. Wireless Commun. Netw.*, vol. 2016, no. 1, p. 113, Apr. 2016.

REZA PARSAMEHR (Member, IEEE) received the M.Sc. degree in information technology from the Graduate University of Advanced Technology (GUAT), Kerman, Iran, in 2012. He is currently pursuing the Ph.D. degree in system and services engineering for the Information Society with the Universidad Politécnica de Madrid, Spain. From 2012 to 2017, he was working at the Institute for Advanced Studies in Basic Sciences, Zanjan, Iran, where he worked as a Faculty Member with the Department of Computer Science and Information Technology. He joined the Instituto de Telecomunicações, Aveiro, in 2017 as a Researcher, who is a member of SECRET Project which is a collaborative European Training Network (ETN) research projects that received funding from the European Union's Horizon 2020 Research and Innovation programme. He is currently a Researcher with the Instituto de Telecomunicações, Aveiro, Portugal. His main research interests include network coding, network and system security, intrusion detection and prevention systems in 5G, and authentication mechanisms.

GEORGIOS MANTAS (Member, IEEE) received the Diploma degree in electrical and computer engineering from the University of Patras, Greece, in 2005, the M.Sc. degree in information networking from Carnegie Mellon University, Pittsburgh, PA, USA, in 2008, and the Ph.D. degree in electrical and computer engineering from the University of Patras, Greece, in 2012. In 2014, he became a Postdoctoral Researcher at the Instituto de Telecomunicações, Aveiro, Portugal, where he has been involved in research projects such as ECSEL–SemI40, CATRENE–MobiTrust, CATRENE–NewP@ss, ARTEMIS–ACCUS, FP7–CODELANCE, and FP7–SEC-SALUS. Since 2018, he has been a Lecturer with the University of Greenwich, U.K. His research interests include network and system security, authentication mechanisms, privacy-preserving mechanisms, intrusion detection systems, and secure network coding.

JONATHAN RODRIGUEZ (Senior Member, IEEE) received the master's degree in electronic and electrical engineering and the Ph.D. degree from the University of Surrey, U.K., in 1998 and 2004, respectively. In 2005, he became a Researcher at the Instituto de Telecomunicações, Portugal, where he was a member of the Wireless Communications Scientific Area. In 2008, he became a Senior Researcher, where he established the 4TELL Research Group targeting next generation mobile systems. He has served as a Project Coordinator for major international research projects, including Eureka LOOP and FP7 C2POWER whilst serving as a Technical Manager for FP7 COGEU and FP7 SALUS. He is currently the Coordinator of the H2020-SECRET Innovative Training Network. Since 2009, he has been serving as an Invited Assistant Professor with the University of Aveiro, Portugal, and attained Associate Level in 2015. In 2017, he was appointed as a Professor of mobile communications with the University of South Wales, U.K. He has authored more than 450 scientific works, including ten book editorials. His professional affiliations include Chartered Engineer (C.Eng.) since 2013 and Fellow of the IET, in 2015.

JOSÉ-FERNÁN MARTÍNEZ-ORTEGA (Senior Member, IEEE) received the B.S. degree in electronic and telecommunications engineering and the Ph.D. degree in telecommunications engineering from the Universidad Politécnica de Madrid (UPM), Spain, in 1993 and 2001, respectively. From 1993 to 1996, he was a Technical Responsible in research projects at national telecommunications company TELECOM, Colombia. He was the Technical Manager in his own company S and H Ltda. He is currently an Associate Professor with the Department of Engineering and Telematic Architectures, UPM. He has participated on several international and European projects. His main interest areas and expertise are ubiquitous computing and the Internet of Things, smart cities, wireless sensor and actuators networks, next-generation telematic network and services, software engineering and architectures, distributed applications and intermediation platforms (middleware), and high performance and fault-tolerant systems. He has authored several national and international publications included in the Science Citation Index in his interest areas. He is a member of different international and scientific committees, and a Technical Reviser and the Chair of technical national and international events on telematics.