A Novel Intrusion Detection and Prevention Scheme for Network Coding-Enabled Mobile Small Cells

Article *in* IEEE Transactions on Computational Social Systems · November 2019

DOI: 10.1109/TCSS.2019.2949153

CITATIONS
10

READS
184

7 authors, including:

Reza Parsamehr
Continental AG
11 PUBLICATIONS **25** CITATIONS
SEE PROFILE

Alireza Esfahani
University of Luxembourg
23 PUBLICATIONS **272** CITATIONS
SEE PROFILE

Ayman Radwan
Alexandria shipyard
105 PUBLICATIONS **903** CITATIONS
SEE PROFILE

Shahid Mumtaz
Institute of Telecommunications
234 PUBLICATIONS **4,197** CITATIONS
SEE PROFILE

A Novel Intrusion Detection and Prevention Scheme for Network Coding-Enabled Mobile Small Cells

Reza Parsamehr, *Student Member, IEEE*, Alireza Esfahani, Georgios Mantas, *Member, IEEE*, Ayman Radwan, *Senior Member, IEEE*, Shahid Mumtaz, Jonathan Rodriguez, *Senior Member, IEEE*, and José-Fernán Martínez-Ortega

***Abstract*— Network coding (NC)-enabled mobile small cells are observed as a promising technology for fifth-generation (5G) networks that can cover the urban landscape by being set up on-demand at any place and at any time on any device. Nevertheless, despite the significant benefits that this technology brings to the 5G of mobile networks, major security issues arise due to the fact that NC-enabled mobile small cells are susceptible to pollution attacks; a severe security threat exploiting the inherent vulnerabilities of NC. Therefore, intrusion detection and prevention mechanisms to detect and mitigate pollution attacks are of utmost importance so that NC-enabled mobile small cells can reach their full potential. Thus, in this article, we propose for the first time, to the best of our knowledge, a novel intrusion detection and prevention scheme (IDPS) for NC-enabled mobile small cells. The proposed scheme is based on a null space-based homomorphic message authentication code (MAC) scheme that allows 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 overhead.**

***Index Terms*— Fifth generation (5G), homomorphic message authentication codes (MACs), intrusion detection and prevention, mobile small cells, pollution attacks, random linear network coding (RLNC).**

Manuscript received April 4, 2019; revised July 15, 2019 and September 7, 2019; accepted October 12, 2019. Date of publication November 28, 2019; date of current version December 9, 2019. This work was supported in part by the European Union's Horizon 2020 Research and Innovation Program under Grant H2020-MSCA-ITN-2016-SECRET-722424 and in part by the European Regional Development Fund (FEDER) through the Competitiveness and Internationalization Operational Program (COMPETE 2020), Regional Operational Program of the Algarve (2020), and Fundação para a ciência e Tecnologia; i-Five: Extensão do Acesso de Espectro Dinâmico para Rádio 5G under Grant POCI-01-0145-FEDER-030500. *(Corresponding author: Reza Parsamehr.)*

R. Parsamehr is with the Instituto de Telecomunicações, 3810-193 Aveiro, Portugal, and also with the Departamento de Ingeniería Telemática y Electrónica, Escuela Técnica Superior de Ingeniería y Sistemas de Telecomunicación, Universidad Politécnica de Madrid, 28031 Madrid, Spain (e-mail: parsamehr.r@av.it.pt).

A. Esfahani, A. Radwan, and S. Mumtaz are with the Instituto de Telecomunicações, 3810-193 Aveiro, Portugal (e-mail: alireza@av.it.pt; aradwan@av.it.pt; smumtaz@av.it.pt).

G. Mantas is with the Instituto de Telecomunicações, 3810-193 Aveiro, Portugal, and also with the Faculty of Engineering and Science, University of Greenwich, London SE10 9LS, U.K. (e-mail: gimantas@av.it.pt).

J. Rodriguez is with the Instituto de Telecomunicações, 3810-193 Aveiro, Portugal, and also with the Mobile and Satellite Communications Research Group, School of Engineering, University of South Wales, Pontypridd CF37 1DL, U.K. (e-mail: jonathan@av.it.pt).

J.-F. Martínez-Ortega is with the Departamento de Ingeniería Telemática y Electrónica, Escuela Técnica Superior de Ingeniería y Sistemas de Telecomunicación, Universidad Politécnica de Madrid, 28031 Madrid, Spain (e-mail: jf.martinez@upm.es).

Digital Object Identifier 10.1109/TCSS.2019.2949153

I. Introduction

THE fifth generation (5G) of mobile communications is expected to provide a connected society [1]–[4]. The small cell technology is one of the major 5G enablers for effective provision of 5G services in an energy-efficient and cost-effective way [5], [6]. It is shown that the network coding (NC) technology, due to power consumption, packet loss, and low communication bandwidth, can be a good solution for increasing the throughput and improving the performance of the wireless network in mobile small cells [7]. Unlike the traditional store-and-forward routing in NC-enabled, the information flow can be mixed. In addition, there are two main approaches of NC: XOR NC and random linear NC (RLNC) (see Fig. 1). NC can provide essential benefits to networks such as: 1) reduction packet transmission in wireless multicast [8], [9]; 2) improving the network capacity [10]; and 3) gain robustness to packet losses [11] and low energy consumption [12]. However, despite the outstanding benefits of NC technology, NC-enabled wireless networks are susceptible to pollution attacks, a security threat, where a malicious node injects corrupted packets into the network that makes destination nodes unable to decode the native packets correctly [13], [14]. The impact of this type of attack is devastating as they lead not only to network resource waste but also to energy waste on the nodes. Based on that the security is a significant factor for the success of 5G technology, novel intrusion detection and prevention scheme (IDPS) against these kinds of attacks in the NC-enabled mobile small cells are needed [15]–[19].

Therefore, in this article, we propose for the first time, to the best of our knowledge, a novel IDPS for NC-enabled mobile small cells. The proposed scheme is based on a null space-based homomorphic message authentication code (MAC) 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 overhead.

The rest of this article is organized as follows. In Section II, we provide the background and related work of NC technology, secure NC, and security schemes against pollution attacks in NC-enabled networks. The scenario architecture is presented in Section III. In Section IV, the detailed description of the proposed novel IDPS for NC-enabled mobile small cells

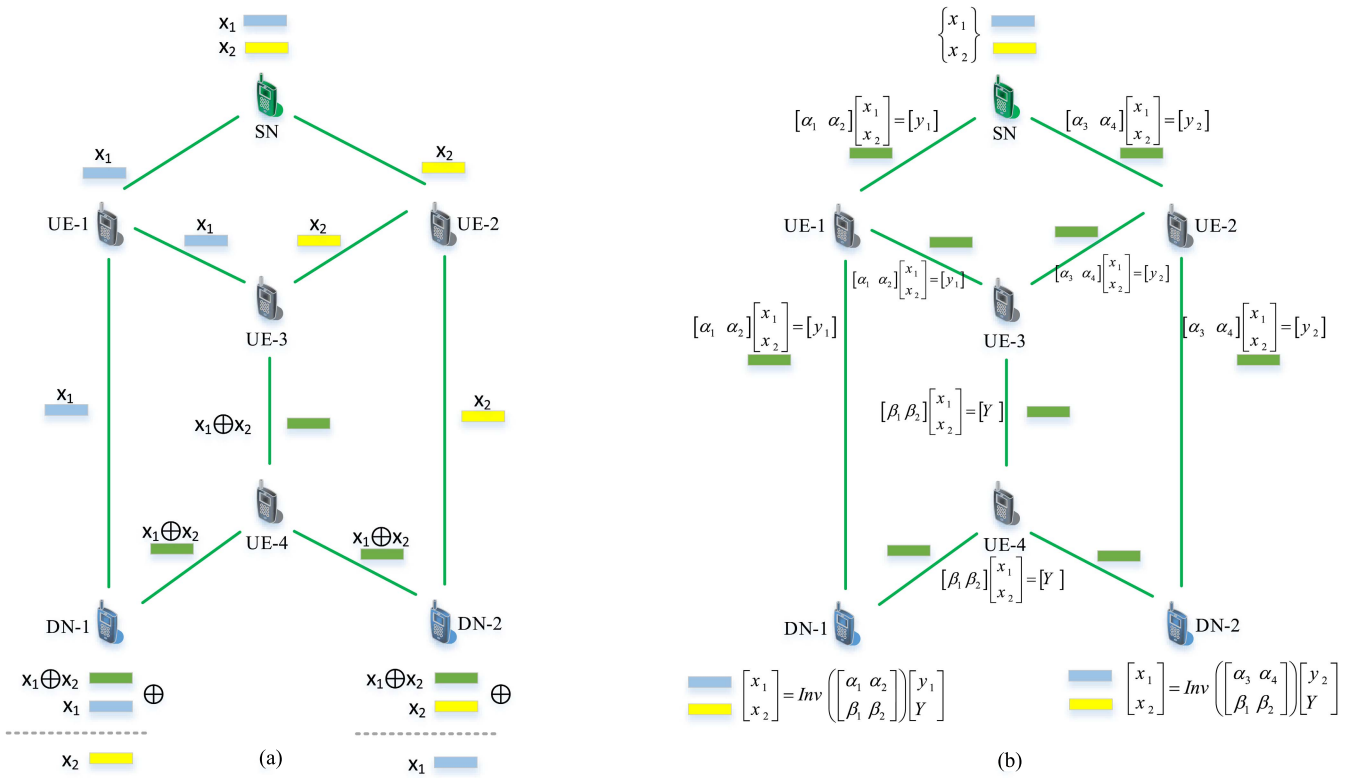

Fig. 1. (a) XOR NC based on the butterfly topology. b) RLNC based on the butterfly topology.

is 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 scheme. Finally, Section VII concludes this article.

II. Related Work

A. Mobile Small Cell in 5G Mobile Networks

New IT technologies, such as the Internet of Things, network resource sharing, network functions virtualization (NFV), software-defined networking (SDN), and NC can reach their high potential by evolving 5G wireless communications. Furthermore, recent research studies have shown that these technologies have the potential to make 5G networks more efficient and less costly [20]. However, recent research studies have identified a few limitations of 5G technology as well. The main limitations include data speed, latency, and reliability. In order to address these limitations of 5G communications, the small cell technology is one of the good solutions. The use of small cell concept provides benefits, including higher capacity, less transmission power, local interference only, and robustness [21]. Nevertheless, the small cell technology introduces new challenges such as complex infrastructure and high handover. In other words, the 5G small cells can play an essential role in order to provide 5G networks with densely deployed heterogeneous networks with increasing demand for capacity. In particular, 5G small cells will be enhanced by incorporating techniques related to massive aggregation, intercell interference mitigation, multicell coordination, new coding, and modulation [22], [23]. In this regard, given the fact that we employ NC to form new energy-efficient and high-speed networking for mobile small cells, a bunch of security challenges have appeared and they are needed to be addressed. As an example, Ferrag *et al.* [24] provide a survey on privacy-preserving and authentication schemes for 5G networks derived from 50 articles. The authors also provide a classification for the attacks in 5G environment. In addition, a classification of countermeasures to mitigate the classified attacks is summarized. This classification is based on cryptographic methods, intrusion detection methods, and human factors [24].

B. Secure NC

By using the NC protocol, several security attacks, including eavesdropping attacks and pollution attacks, in NC-enabled mobile small cells have appeared recently.

Many secure NC schemes against pollution attacks have been proposed. Based on homomorphic functions, a security hashing scheme was proposed by Krohn *et al.* [25], where the generated hashes are responsible to validate blocks of rate-less codes. Moreover, a cooperative scheme where legal nodes collaborate to preserve themselves against adversary nodes is presented in [26]. In this scheme, the cooperation between the nodes enables them to detect and verify malicious nodes. Finally, in multicast RLNC-enabled networks, Ho *et al.* [27] proposed an approach for detecting byzantine attacks. More precisely, the proposed approach first tries to calculate a polynomial function of the data symbols (hash).

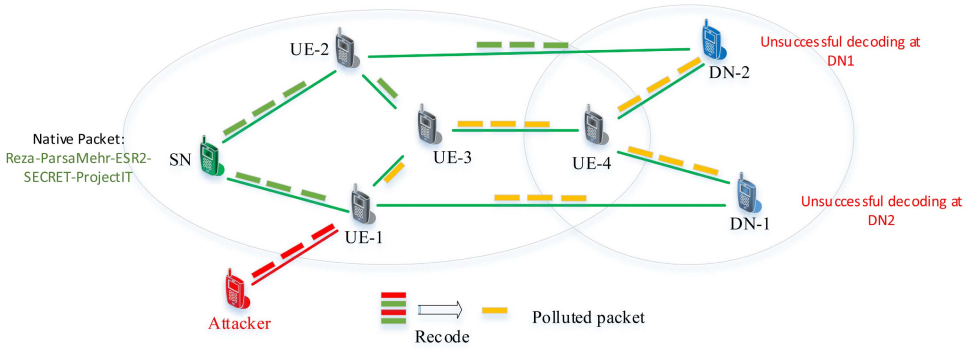

Fig. 2. External attack scenario in the butterfly topology.

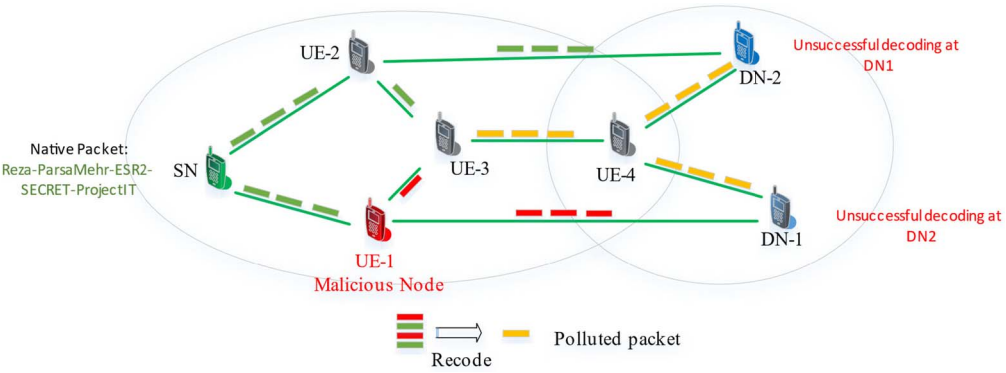

Fig. 3. Byzantine modification attack scenario in the butterfly topology.

Then, it augments each source packet with a flexible number of hash symbols calculated earlier.

C. Pollution Attacks

Pollution attacks can be launched by either an external adversary or an internal adversary (i.e., byzantine modification attacks). In the case of an external adversary, as shown in Fig. 2, the adversary injects corrupted packets into the network in order to corrupt other coded packets and disrupts the routing operation. However, the main effort of an adversary in byzantine modification attack is to execute some changes (i.e., wrong coding operations) to data in transition and threat the integrity of the packets in the networks [14], [23], [24] (see Fig. 3). Both these types of attackers can also be considered as data pollution attacks and tag pollution attacks, as shown in Figs. 2 and 3. In particular, the main target of an adversary in data pollution attacks is to modify (i.e., corrupt) the transmitted data packet, and in tag pollution attacks, the adversary aims to modify the tags appended to the end of data packets.

D. Intrusion Detection and Prevention Systems

IDPSs are mainly focused on identifying potential security incidents and on blocking or preventing detected the malicious activity. Regarding malicious activity detection, IDPSs use signature detection to identify the known malicious behavior or anomaly detection to identify behavior that is not related to legitimate users [30]–[33].

Signature detection is based on a set of known malicious data patterns that are also referred to as signatures. These signatures are compared with current behavior to decide whether the current behavior is a malicious one or not. This method of detection is suitable for detecting only known attacks.

On the other hand, anomaly detection is based on data related to normal behavior (i.e., profiles) and derived from monitoring the characteristics of legitimate activity on the system or in the network over a period. Then, the anomaly detection is carried out by analyzing definitions of what action is supposed normal (i.e., created normal behavior profiles) against recognized events in order to identify meaningful deviations, which imply malicious activity. In the anomaly detection process, the profiles can either be static or dynamic. Next, a static profile does not change until the IDPS is forced to create a new profile. On the contrary, a dynamic profile is adjusted continuously as extra events are observed. In fact, based on the fact that systems and networks change over time, the corresponding measures of normal behavior also change. Therefore, static profiles become inaccurate over time, and thus, they should be periodically regenerated. However, although dynamic profiles do not have this issue, they are vulnerable to evasion attempts from attackers. Furthermore, it is worthwhile to mention that in contrast to signature detection, anomaly detection is very strong at identifying unknown attacks. Nevertheless, anomaly-based techniques are characterized by a high false alarm rate due to the fact that

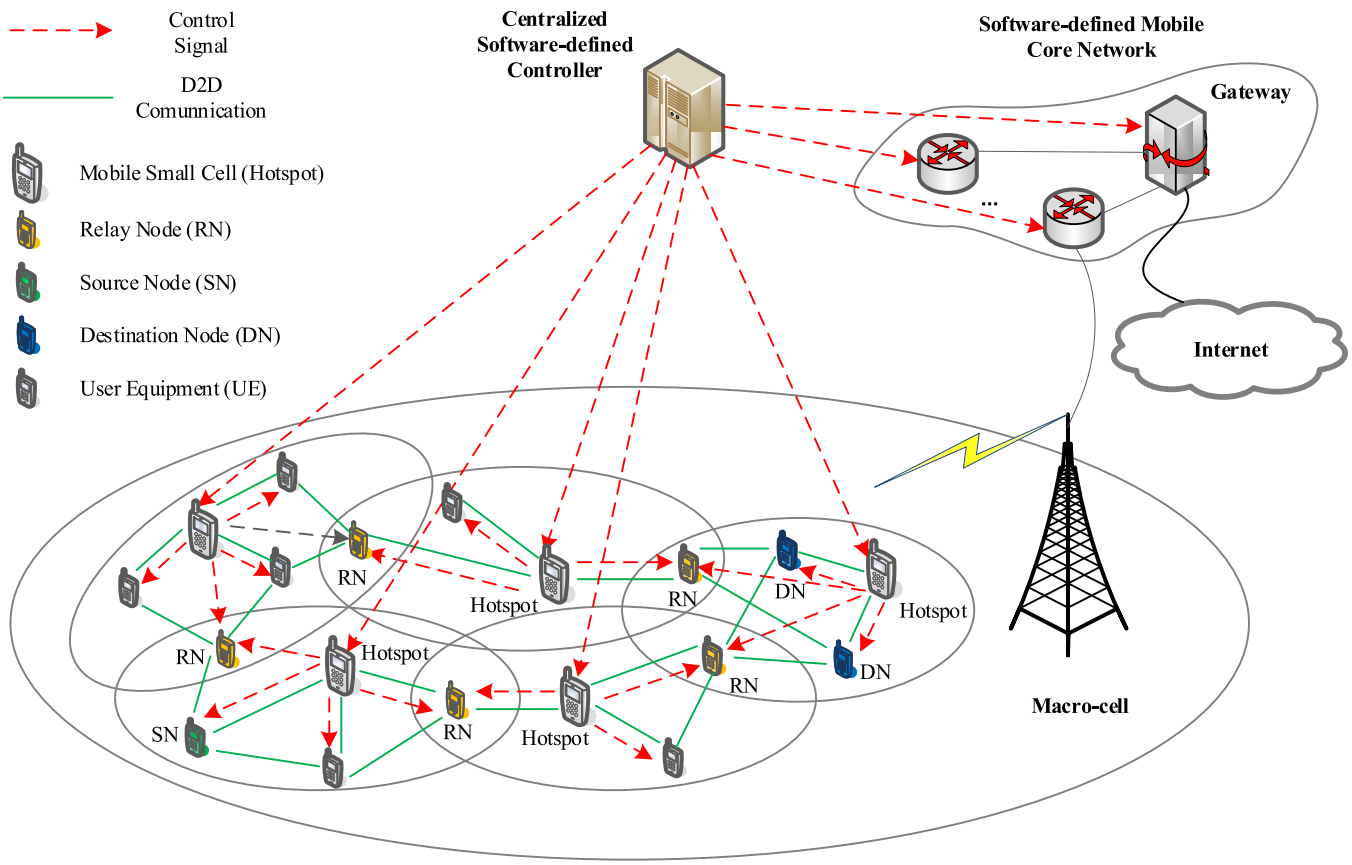

Fig. 4. Scenario architecture of SECRET.

previously unseen normal system/network behaviors may be categorized as anomalies.

III. Scenario Architecture

In this section, we provide the scenario architecture of the EU-funded H2020-MSCA project "SECRET" (see Fig. 4), which is focused on secure NC-enabled mobile small cells [34]. This scenario architecture consists of a macrocell including a number of small cells 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, which is 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 mobile small cells 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 NC technology. In particular, in the studied scenario, it is assumed that a source mobile node (SN), locating at a mobile small cell, wants to multicast packets to two destination mobile nodes (DNs), locating at another mobile small cell. Thus, packets from the SN are coded (i.e., RLNC) and traverse multiple devices, over a multihop D2D network, before arriving at the DNs, where they are decoded. The multihop D2D network consists of several user equipments (UEs), such as legitimate mobile nodes and relay mobile nodes (RNs), as depicted in Fig. 4.

IV. Novel IDPS for NC-Enabled Mobile Small Cells

In this section, we present our proposed IDPS for NC-enabled mobile small cells. Our IDPS is based on a null space-based homomorphic message authentication code (MAC) scheme proposed in [15] and allows the detection of pollution attacks and takes proper risk mitigation actions when an intrusive incident is detected. The focus of our IDPS is on the detection and mitigation of pollution attacks that comprise a severe threat in NC-enabled networks as their impact is similar to the impact of denial-of-service (DoS) attacks and network resource waste and energy waste at the nodes. In fact, the attacker targets the availability of the NC-enabled network and its nodes [16], [28]. The adopted scheme from our previous work in [15] enables the proposed IDPS to detect pollution attacks by checking (i.e., verifying) the orthogonality of the packets with tags and keys as described in the following. In case that the verification result is not equal to zero (i.e., detection of polluted packet), the packet will be dropped (i.e., prevention from pollution).

A. Outline of the IDPS Scheme

First, the source node divides each message into a sequence of native packets and partitions them into generations.

Following our assumption in [15], each generation consists of p messages packets denoted as $\underline{c}_1, \underline{c}_2, L, \underline{c}_p$. We assume that each packet $\underline{c}_i$ is represented as a vector of q symbols [e.g., $(\underline{c}_{i,1}, \underline{c}_{i,2}, \ldots, \underline{c}_{i,q})$] in which each symbol stands in the finite field F_S^q, where S is the finite field size. Consequently, the source node generates an augmented packet c_i

$$c_i = (\overbrace{\underbrace{0, \ldots, 0}_{i-1}, 1, 0, \ldots, 0}^{p}, \underline{c}_{i,1}, \ldots, \underline{c}_{i,q}) \in F_S^{p+q}. \quad (1)$$

Then, the source node sends c_i to its neighbor nodes. During transmission, an intermediate node creates a new coded packet c_i. In our proposed IDPS scheme, we have considered that the source node generates w tags that are based on null space properties [35]. We define the following four steps.

1) Tag Generation: In this step, first, a key distribution center (KDC) delivers w key vectors $X_1, X_2, \ldots, X_w$ to the source node. The size of each key vector is given by the finite field F_S^{p+q+w}. Then, the source node uses these w key vectors $X_1, X_2, \ldots, X_w$ to calculate w tags for each coded packet. Furthermore, the source node appends the w tags to the end of the coded packet c_i. The following formula is used in order to calculate the w tags:

$$\begin{bmatrix} X_{1,1} & \ldots & X_{1,p+q} \\ \vdots & \vdots & \vdots \\ X_{w,1} & \ldots & X_{w,p+q} \end{bmatrix}_{w*(p+q)} * \begin{bmatrix} c_{i,1} \\ c_{i,2} \\ \vdots \\ c_{i,p+q} \end{bmatrix}_{(p+q)*1} + \begin{bmatrix} X_{1,p+q+1} & \ldots & X_{1,p+q+w} \\ \vdots & \vdots & \vdots \\ X_{w,p+q+1} & \ldots & X_{w,p+q+w} \end{bmatrix}_{w*w} * \begin{bmatrix} t_1 \\ t_2 \\ \vdots \\ t_w \end{bmatrix}_{w*1} = 0. \quad (2)$$

2) Swapping Process: In this step, we use the swapping technique in order to avoid tag pollution attacks. In this regard, the KDC generates a secret positive integer value SV that is the swapping vector. In addition, the secret value SV is sent to the source node and destination nodes. Then, the w tag symbols of the coded packet c_i are swapped with w out of the q symbols of the coded packet c_i. Finally, a swapped coded packet $\overline{c}_i$ is made by the source node with the swapping process and is represented by the following equation:

$$\overline{c}_i = \text{Swap}(c_i)_{\text{SV}}. \quad (3)$$

At the destination side, the nodes have to proceed an inverse swapping in order to obtain the native packet before the RLNC decoding takes place.

3) Key Distribution Process: The KDC, based on SV mentioned in the swapping step, generates new key vectors $X'_1, X'_2, \ldots, X'_w$. More precisely, each key vector is given by

$$X'_i = \text{Swap}(X_i)_{\text{SV}}. \quad (4)$$

Our proposed IDPS mechanism follows the key distribution model proposed in [36], which is based on the cover free set systems. The KDC of our scheme adopts a key distribution model, based on the cover free set systems [37], in order to provide resistance against c compromised nodes. In this model, the maximum number of key vectors that should be assigned to each intermediate and destination node cannot be more than $R = e * \ln(1/q)$, where q is a security parameter (usually $q = 10-3$). In our proposed scheme, this assumption is satisfied since only one key vector is required to be assigned by the KDC to each intermediate and destination node. This is why each key vector is orthogonal to the swapped coded packet, and thus, the intermediate and destination nodes require only one key vector to verify the swapped coded packet.

4) Verification Process: The following formula verifies if a key vector X'_i is orthogonal to a swapped coded packet $\overline{\mathbf{c}}_i$

$$\eta = \text{Swap}(X_i)_{\text{SV}} * \text{Swap}(c_i)_{\text{SV}} = \sum_{j=1}^{p+q+w} X'_{i,j} * \overline{c}_{i,j}. \quad (5)$$

If $\eta = 0$, then our proposed IDPS accepts the swapped coded packet $\overline{c}_i$ and transmits it to the next non-source nodes. If $\eta \neq 0$, our IDPS discards the coded packet $\overline{c}_i$.

B. Correctness

The correctness of our IDPS mechanism is proved by contradiction. In this regard, we consider that our IDPS is not correct. In the case that this is true, through the verification step, we should get $\eta \neq 0$ [from (5)]. Then, we assume that a source node has a coded packet $R^i = (R^i_1, \ldots, R^i_{p+q})$ and w key vectors $(X = X_1, X_2, \ldots, X_L)$. Afterward, it starts generating the w tags $t^i = (t^i_1, \ldots, t^i_w)$ according to (2). For simplicity, we assume SV = 1, and thus,

$$\begin{aligned} &\text{Swap}(X)_{\text{SV}} * \text{Swap}(\bar{R}^{i^T})_{\text{SV}} \\ &= \begin{bmatrix} X_{1,1} \ldots X_{1,p+q+1} \ldots X_{1,p+q+w} \ldots X_{1,p+1} \ldots K_{1,p+w} \\ \vdots \\ X_{w,1} \ldots X_{w,p+q+1} \ldots X_{w,p+q+w} \ldots X_{w,p+1} \ldots X_{w,p+w} \end{bmatrix} \\ &\quad * \begin{bmatrix} R^i_1 \ \ldots \ t^i_1 \ \ldots \ t^i_w \ \ldots \ R^i_{p+q} \ R^i_{p+1} \ \ldots \ R^i_{p+w} \end{bmatrix}^T \\ &= \begin{bmatrix} X_{1,1} * R^i_1 + \ldots X_{1,p+q+w} * t^i_w \\ \vdots \\ X_{w,1} * R^i_1 + \ldots X_{w,p+q+w} * t^i_w \end{bmatrix}_{w*1}. \end{aligned} \quad (6)$$

Nevertheless, $\bar{R}^i = [R^i_1, \ldots, R^i_{p+q}, t^i_1, \ldots, t^i_w]$ is orthogonal to each of the w key vectors based on (2). Therefore, $X * \bar{R}^{i^T}$ is calculated as

$$\begin{aligned} &X * \bar{R}^{i^T} \\ &= \begin{bmatrix} X_{1,1} & \ldots & X_{1,p+q+w} \\ \vdots & \vdots & \vdots \\ X_{w,1} & \ldots & X_{w,p+q+w} \end{bmatrix} * \begin{bmatrix} R^i_1 \\ R^i_2 \\ \vdots \\ t^i_w \end{bmatrix} \\ &= \begin{bmatrix} X_{1,1} * R^i_1 + \ldots X_{1,p+q+w} * t^i_w \\ \vdots \\ X_{w,1} * R^i_1 + \ldots X_{w,p+q+w} * t^i_w \end{bmatrix}_{w*1} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}_{w*1}. \end{aligned} \quad (7)$$

By comparing (6) with (7), we can see that $\eta = 0$. However, it is a contradiction to our original assumption where we had assumed that $\eta \neq 0$. Therefore, our IDPS is correct.

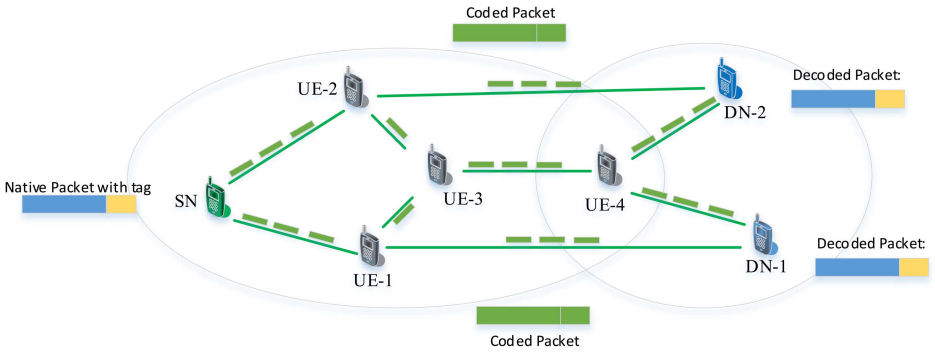

Fig. 5. Scenario 1: our IDPS mechanism implementation when pollution attack does not exist.

V. Implementation

To evaluate the performance of the proposed IDPS, we first implement the butterfly topology where the RLNC approach is applied. Then, we implement the external attack scenario (Fig. 2) and the byzantine modification attack scenario (Fig. 3). Our 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 [38]. Kodo is an open-source NC library, which is used as a practical open-source library in order to allow researchers and students to implement NC algorithms. Although Kodo is based on C++, it allows users familiar with other programming languages other than C++ (e.g., C and Python) to use the library functionality [38]–[41]. Kodo supports various NC algorithms, e.g., standard RLNC, systematic RLNC, and sparse RLNC. The Kodo libraries are described in detail in [19] and [38]. However, due to the limitations of Kodo to allow customized generation of packets and keys as well as tag generation, we used MATLAB. Specifically, we used MATLAB to generate the packets and the required keys of the source node and to generate the proper tags at the source node and the intermediate nodes. Then, we included the generated packets, keys, and tags manually in Kodo.

Throughout the performance measurements, we used a generation size of 16 symbols. The symbol size is set between 1000 and 10 000 bytes, as shown in Figs. 11–19. As we mentioned, these packets and the required keys are generated randomly in MATLAB. The Galois field in use is GF(2^8) and we take into consideration that the number of the tags appended to the end of each coded packet is L, where L is equal to $L = 27, 42$, and 54 [41]. We run the whole implementation process on a 2.7-GHz Core i7 machine with 8 GB of physical memory.

A. Scenarios

Since no attack has not been considered and defined in the Kodo library yet, we have generated the external attack and byzantine modification attack in the butterfly topology in order to evaluate the performance of the proposed IDPS mechanism. In this regard, we first implemented on Kodo the butterfly topology without any attacks as shown in Fig. 5. In particular, Fig. 6 shows the successful decoding of the received coded packets at the destination nodes.

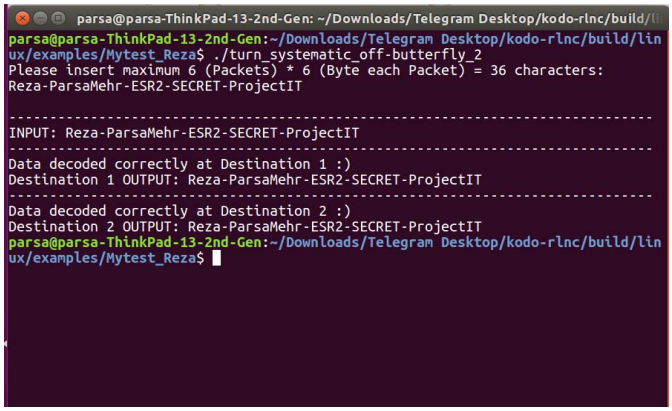

Fig. 6. Implementation results in the butterfly topology.

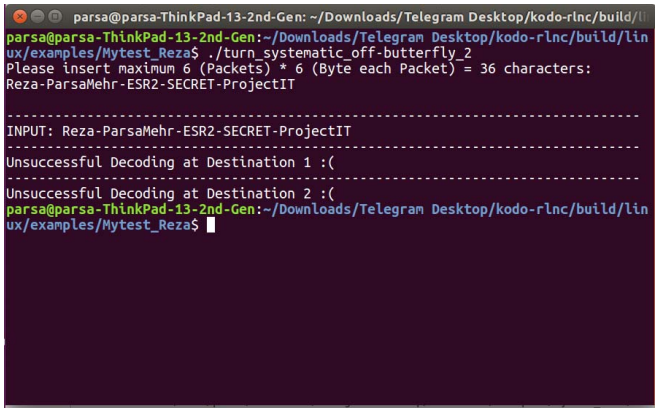

Fig. 7. Implementation result when pollution attack occurs.

Then, we considered pollution attacks in the butterfly topology, which make the destination nodes unable to decode the packets successfully (see Fig. 7).

Afterward, we implemented our IDPS mechanism on Kodo over the butterfly topology and we show that the proposed scheme can detect and drop the corrupted packets inserted in the network due to pollution attacks (i.e., external attack and byzantine modification attack). In addition, our proposed IDPS mechanism does not bring high computational complexity.

1) Scenario 1: Well-Behaved Network (No Pollution Attack): We have implemented the proposed IDPS mechanism

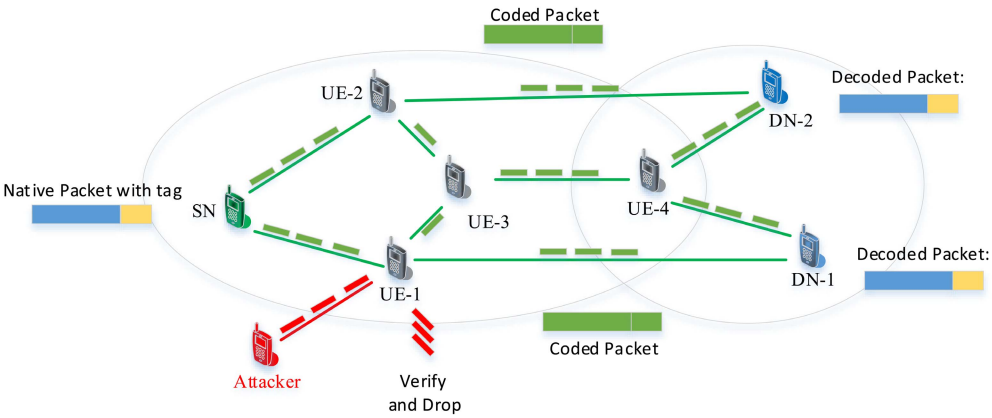

Fig. 8. Scenario 2: our IDPS mechanism implementation when an external attack exists.

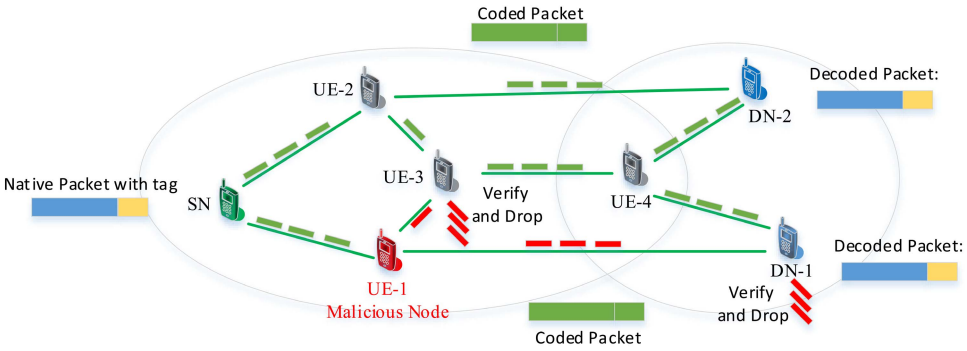

Fig. 9. Scenario 3: our IDPS mechanism implementation when the byzantine modification exists.

over the butterfly topology as shown in Fig. 5. Since there is not any adversary, the destination nodes decode the packets successfully (see Fig. 6) and the proposed IDPS mechanism does not detect any corrupted packet.

2) Scenario 2: External Attack: In this scenario, we consider that an external attack is carried out as an attacker pollutes a coded packet at node UE-1 (see Fig. 8). However, our proposed IDPS scheme detects and drops the corrupted packet.

3) Scenario 3: Byzantine Modification Attack: The byzantine modification attack is shown in Fig. 9, where an attacker inserts a corrupted packet in the network. It is worthwhile to mention that our proposed IDPS scheme detects and drops the corrupted packet (Fig. 10).

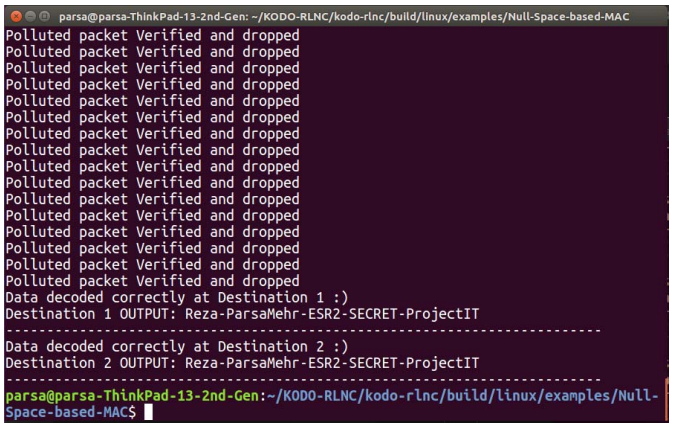

Fig. 10. Implementation result in scenarios 2 and 3.

VI. Performance Evaluation

In this section, we have provided the proposed IDPS mechanism performance evaluation in terms of computational and communication overheads as well as successfully decoding probability.

A. Computational Overhead

Following [42], we take into consideration that the number of the tags appended to the end of each coded packet is L (i.e., $L = 27, 42$, and 54), and the selected Galois fields is GF(2^8). In addition, we consider that the symbol size is set between 1000 and 10 000 bytes.

The total time T_{total} elapsed from when the packet is generated to when the packet is verified and decoded at the destination nodes is given by the following formula:

$$T_{\text{total}} = T_{\text{enc}} + T_{\text{rec}} + T_{\text{dec}} + T_{\text{ver}} \tag{8}$$

where T_{enc}, T_{dec}, T_{rec}, and T_{ver} are the time for encoding at the source node, decoding at the destination node, recoding at each intermediate nodes, and verifying at the intermediate and destination nodes, respectively. T_{total}, in the first scenario is illustrated in Fig. 11. Based on the number of tags, this

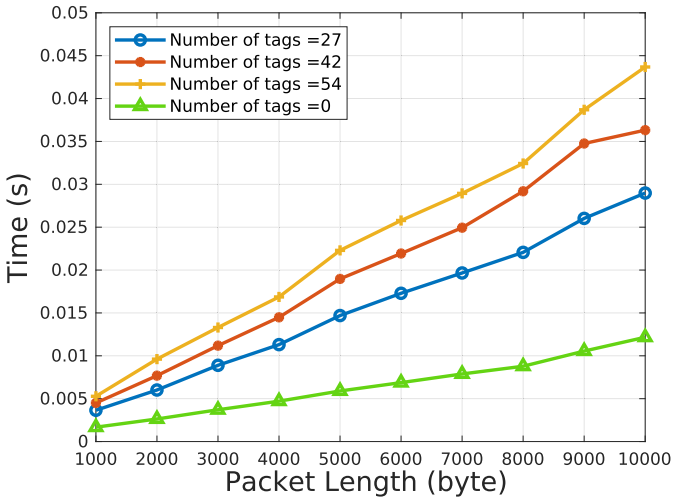

Fig. 11. T_{total} for different numbers of tags when pollution attack has not occurred.

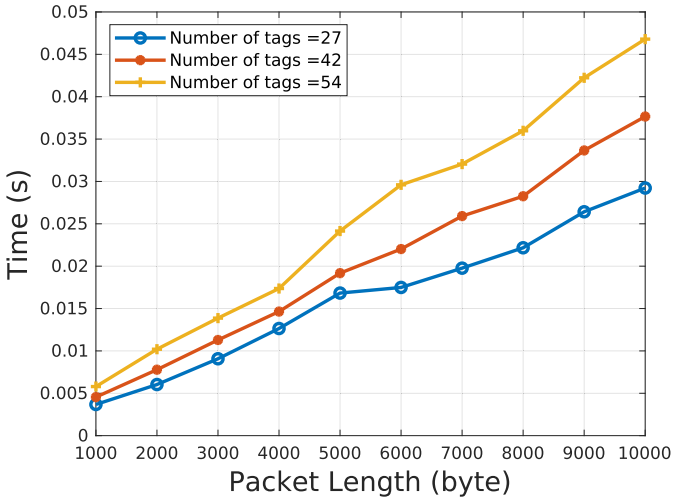

Fig. 12. T_{total} for different numbers of tags when the byzantine fabrication attack is carried out.

figure includes four curves. As shown, by increasing the number of tags, T_{total} increases as well.

On the other hand, in scenario 2, T_{total} for different numbers of tags (e.g., 27, 42, and 54) is shown in Fig. 12. Furthermore, T_{total} for different numbers of tags (e.g., 27, 42, and 54), in scenario 3, is shown in Fig. 13. It is worthwhile to mention that T_{total} in scenario 2 and scenario 3 increases compared to T_{total} in scenario 1. The reason is that the proposed IDPS mechanism needs additional time which is required to drop the corrupted packet.

In addition, the time required by our IDPS scheme to verify and detect any corrupted packet in the network, for both scenarios 2 and 3, is presented in Figs. 14 and 15, respectively. As we can see from these figures, the required time for different numbers of tags is almost the same and does not add significant computational overhead to T_{total}.

B. Communication Overhead

To determine the communication overhead of the proposed IDPS scheme, we consider that the communication time T_{comm}

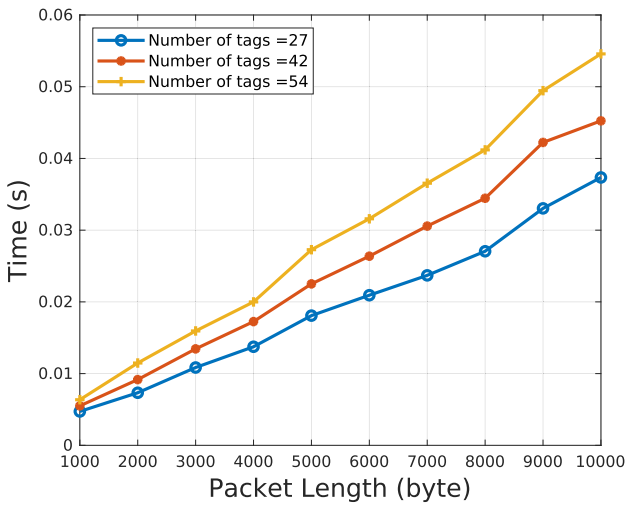

Fig. 13. T_{total} for different numbers of tags when the byzantine modification attack is carried out.

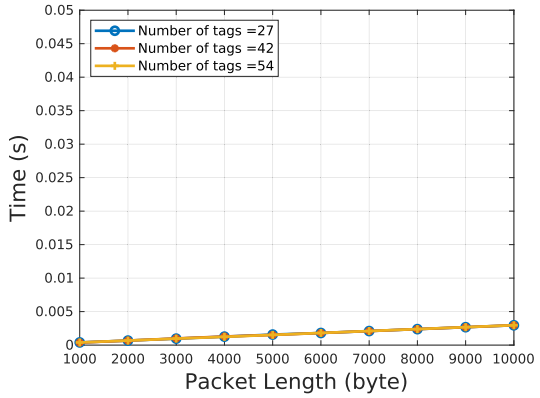

Fig. 14. Verification time for different numbers of tags when the byzantine fabrication attack is carried out.

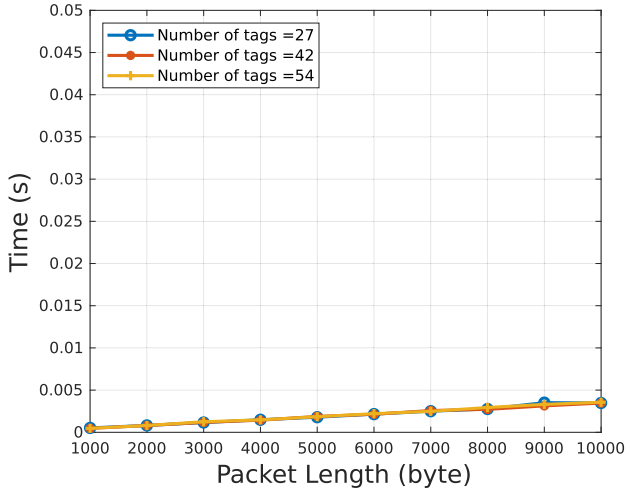

Fig. 15. Verification time for different numbers of tags when the byzantine modification attack is carried out.

is defined as follows:

$$T_{\text{comm}} = T_{\text{total}} - T_{\text{ver}}. \tag{9}$$

Figs. 16 and 17 show T_{comm} based on different numbers of tags used in scenario 2 and scenario 3, respectively. Our results show that T_{total} is almost the same as T_{comm} because

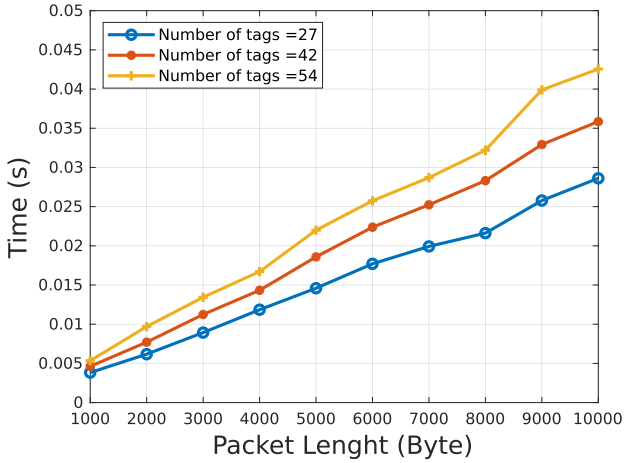

Fig. 16. Communication time for different numbers of tags when the byzantine fabrication attack is carried out.

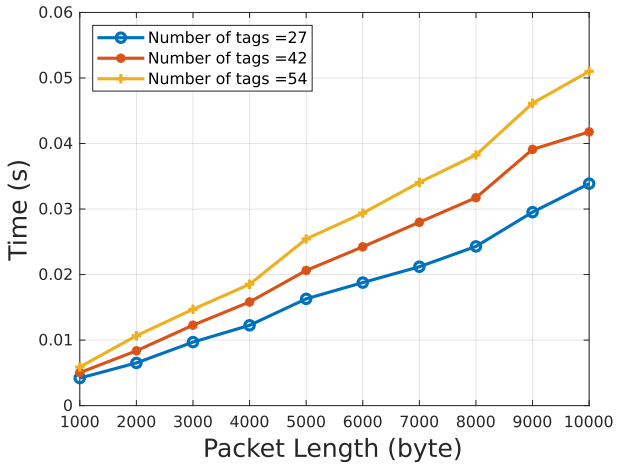

Fig. 17. Communication time for different numbers of tags when the byzantine modification attack is carried out.

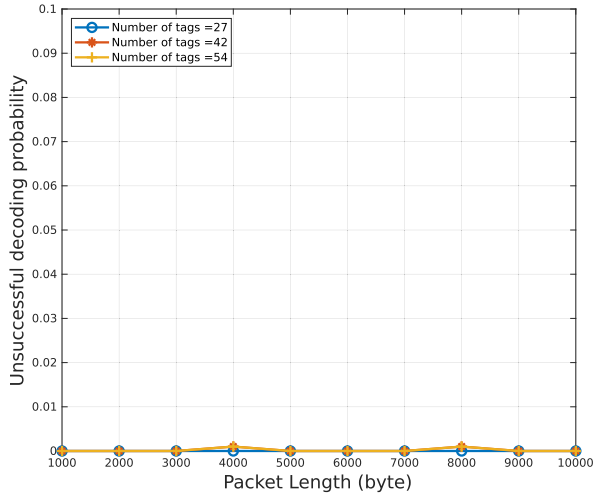

Fig. 18. P_r for different numbers of tags when the byzantine fabrication attack is carried out.

the verification time T_{ver} required by the proposed IDPS mechanism is negligible.

C. Decoding Probability

We define P_r the probability that a corrupted packet is not detected in the verification phase. Figs. 18 and 19 show P_r

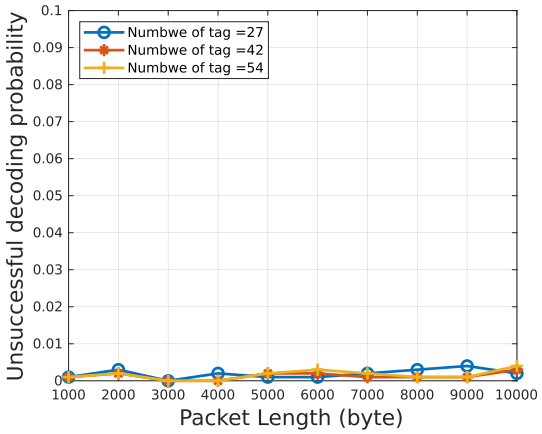

Fig. 19. P_r for different numbers of tags when the byzantine modification attack is carried out.

based on three different numbers of tags (27, 42, and 54). As shown in these figures, P_r is almost 0%. In other words, in our proposed IDPS mechanism, the adversary does not have any chance to distribute the corrupted packet in the network without being detected.

VII. Conclusion

In this article, we proposed for the first time, to the best of our knowledge, a novel IDPS for NC-enabled mobile small cells. The proposed scheme has been implemented in Kodo and its performance evaluation has shown that it does not add significant computational overhead. The proposed scheme is based on a null space-based homomorphic MAC scheme that allows the detection of pollution attacks that comprise a severe security threat in NC-enabled networks. Moreover, the proposed scheme drops the corrupted packets that are detected and the adversary does not have any chance to distribute the corrupted packet in the network without being detected in order to protect the NC-enabled mobile small cells from network resource waste and energy waste. However, it is not enough because the attackers may continue to make pollution in the next rounds, which can lead to waste of the network's throughput. As a future work, we plan to extend the proposed IDPS into a collaborative IDPS that will also allow the detection of the source(s) of the pollution attacks and the localization of the attackers in order to block them from having access to the network. Also, we plan to enhance the proposed IDPS in order to support correction of detected corrupted packets as well.

References

[1] 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.

[2] 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.

[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] V. Sucasas, G. Mantas, and J. Rodriguez, "Security challenges for cloud radio access networks," in *Backhauling/Fronthauling for Future Wireless Systems*, 2016, pp. 195–211.
[5] F. B. Saghezchi *et al.*, "Drivers for 5G: The 'pervasive connected world,'" in *Fundamentals of 5G Mobile Networks*. 2015, pp. 1–27.
[6] 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. (GLOCOM)*, Dec. 2014, pp. 4852–4857.
[7] J. Sen, "A survey on wireless sensor network security," Nov. 2010, *arXiv:1011.1529*. [Online]. Available: https://arxiv.org/abs/1011.1529
[8] 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.
[9] Y.-J. Chen, L.-C. Wang, K. Wang, and W.-L. Ho, "Topology-aware network coding for wireless multicast," *IEEE Systems J.*, vol. 12, no. 4, pp. 3683–3692, Dec. 2018.
[10] 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.
[11] T. Ho and D. Lun, *Network Coding: An Introduction*. Cambridge, U.K.: Cambridge Univ. Press, 2008.
[12] Y. Wu, P. Chou, and S.-Y. Kung, "Minimum-energy multicast in mobile ad hoc networks using network coding," *IEEE Trans. Commun.*, vol. 53, no. 11, pp. 1906–1918, Nov. 2005.
[13] A. Esfahani, G. Mantas, J. Rodriguez, A. Nascimento, and J. C. Neves, "A null space-based MAC scheme against pollution attacks to random linear network coding," in *Proc. IEEE Int. Conf. Commun. Workshop (ICCW)*, Jun. 2015, pp. 1521–1526.
[14] A. Esfahani, D. Yang, G. Mantas, A. Nascimento, and J. Rodriguez, "An improved homomorphic message authentication code scheme for RLNC-enabled wireless networks," in *Proc. IEEE 19th Int. Workshop Comput. Aided Modeling Design Commun. Links Netw. (CAMAD)*, Dec. 2014, pp. 80–84.
[15] 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.
[16] 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.
[17] A. Esfahani, G. Mantas, V. Monteiro, K. Ramantasy, E. Datsikay, and J. Rodriguez, "Analysis of a homomorphic MAC-based scheme against tag pollution in RLNC-enabled wireless networks," in *Proc. IEEE 20th Int. Workshop Comput. Aided Modelling Design Commun. Links Netw. (CAMAD)*, Sep. 2015, pp. 156–160.
[18] 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.
[19] 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, 2016.
[20] M. Olsson, C. Cavdar, P. Frenger, S. Tombaz, D. Sabella, and R. Jantti, "5GrEEn: Towards Green 5G mobile networks," in *Proc. IEEE 9th Int. Conf. Wireless Mobile Comput., Netw. Commun. (WiMob)*, Oct. 2013, pp. 212–216.
[21] M. H. Qutqut, "Mobile small cells in cellular heterogeneous networks," Ph.D. dissertation, Queens Univ., Kingston, ON, Canada, 2014.
[22] V. Jungnickel *et al.*, "The role of small cells, coordinated multipoint, and massive MIMO in 5G," *IEEE Commun. Mag.*, vol. 52, no. 5, pp. 44–51, May 2014.
[23] C.-N. Liu, "Trend, technology and architecture of small cell in 5G era," in *Proc. Int. Symp. VLSI Design, Automat. Test (VLSI-DAT)*, Apr. 2016, pp. 1–2.
[24] M. A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos, and H. Janicke, "Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes," *J. Netw. Comput. Appl.*, vol. 101, pp. 55–82, Jan. 2017.
[25] M. N. Krohn, M. J. Freedman, and D. Mazieres, "On-the-fly verification of rateless erasure codes for efficient content distribution," in *Proc. IEEE Symp. Secur. Privacy*, May 2004, pp. 226–240.
[26] C. Gkantsidis and P. Rodriguez, "Cooperative security for network coding file distribution," in *Proc. INFOCOM*, vol. 3, 2006, p. 5.
[27] T. Ho *et al.*, "A random linear network coding approach to multicast," *IEEE Trans. Inf. Theory*, vol. 52, no. 10, pp. 4413–4430, Oct. 2006.
[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," Sep. 2008, *arXiv:0809.1366*. [Online]. Available: https://arxiv.org/abs/0809.1366
[30] 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.
[31] T. Grance, S. Chevalier, K. K. Scarfone, and H. Dang, "Guide to integrating forensic techniques into incident response," Special Pub. (NIST SP)-800-86, 2006.
[32] K. Kent and M. Souppaya, "Guide to computer security log management," NIST Special Pub., Sep. 2006.
[33] 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.
[34] E. Kehdi and B. Li, "Null keys: Limiting malicious attacks via null space properties of network coding," in *Proc. IEEE INFOCOM*, Apr. 2009, pp. 1224–1232.
[35] T. Ho, D. R. Karger, M. Médard, and R. Koetter, "Network coding from a network flow perspective," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun./Jul. 2003, p. 441.
[36] 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, 2015, Art. no. 510251.
[37] M. V. Pedersen, J. Heide, and F. H. P. Fitzek, "Kodo: An open and research oriented network coding library," in *Proc. Int. Conf. Res. Netw.* Springer, 2011, pp. 145–152.
[38] 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.
[39] 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.
[40] J. Krigslund, J. Hansen, D. E. Lucani, F. H. P. Fitzek, and M. Médard, "Network coded software defined networking: Design and implementation," in *Proc. Eur. Wireless 21st Eur. Wireless Conf.*, 2015, pp. 1–6.
[41] 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.

Reza Parsamehr (S'18) 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, Madrid, Spain.

From 2012 to 2017, he was a Faculty Member with the Department of Computer Science and Information Technology, Institute for Advanced Studies in Basic Sciences, Zanjan, Iran. In 2017, he joined the Instituto de Telecomunicações, Aveiro, Portugal, as a Researcher and a member of SECRET project that is a collaborative European Training Network (ETN) research project that received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant agreement H2020-MSCA-ITN-2016-SECRET-722424. He is currently a Researcher with the Instituto de Telecomunicações. His current research interests include network coding, network and system security, intrusion detection and prevention systems in 5G, and authentication mechanisms.

Alireza Esfahani received the joint Ph.D. degree in telecommunications from the Universities of Minho, Aveiro and Braga, Braga, Portugal, in 2017, under the joint MAP-Tele Doctoral Program.

He was a Post-Doctoral Researcher with the Instituto de Telecomunicações (IT), Universidade de Aveiro, Aveiro, and he has been involved in several research projects such as FP7-CODELANCE, SMARTVISION, and ECSEL-SemI40. He is currently a Research Associate with the CritiX Laboratory (Critical and Extreme Security and Dependability), SnT—the Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg, Luxembourg City, Luxembourg. He is involved in two of four EU pilot cybersecurity projects (SPARTA and CyberSec4Eu projects). He has authored more than 20 scientific works. His current research interests include security and cryptography over wireless communications, end-to-end secure communications, software-defined networking (SDN), IDPS, BFT, and secure network coding.

Georgios Mantas (M'07) received the Diploma degree in electrical and computer engineering from the University of Patras, 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 in 2012.

In 2014, he became a Post-Doctoral Researcher with 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, London, U.K. His current research interests include network and system security, authentication mechanisms, privacy-preserving mechanisms, intrusion detection systems, and secure network coding.

Ayman Radwan (SM'17) received the master's degree in applied science from Carleton University, Ottawa, ON, Canada, in 2003, and the Ph.D. degree from Queen's University, Kingston, ON, Canada, in January 2009.

In January 2010, he joined the Instituto de Telecomunicações (IT), Aveiro, Portugal, as a Senior Researcher and the EU Project Co-ordinator and the Technical Manager. He was the Technical Manager of FP7 ICT-C2POWER and the Co-ordinator of CELTIC-PLUS Green-T. He is currently the Co-ordinator of CELTIC-PLUS MUSCLES, as well as participating in the managing team of H2020 ITN-SECRET. He has an extended experience in participating in EU-funded projects, in different tools, including FP7, H2020, and CELTIC. He has authored more than 100 scientific works in the field of wireless networks, with emphasis on future generations of mobile communications, virtualization, and the Internet of Things.

Shahid Mumtaz received the M.Sc. degree from the Blekinge Institute of Technology (BTH), Karlskrona, Sweden, in 2006, and the Ph.D. degree from the University of Aveiro, Aveiro, Portugal, in 2011, both in electrical and electronic engineering.

In 2005, he was a Research Intern with the Ericsson and Huawei Research Labs, Karlskrona. He has more than ten years of wireless industry experience and is currently a Senior Research Scientist and the Technical Manager with the Instituto de Telecomunicações (IT), Aveiro. His M.Sc. and Ph.D. degrees were funded by the Swedish Government and FCT Portugal. He has been involved in several EC Research and Development Projects in the field of green communication and next-generation wireless systems. He has several years of experience in 3GPP radio systems research with experience in HSPA/LTE/LTE-A and strong track record in relevant technology field, especially physical-layer technologies, LTE cell planning and optimization, protocol stack, and system architecture.

Jonathan Rodriguez (SM'13) received the master's degree in electronic and electrical engineering and the Ph.D. degree from the University of Surrey, Guildford, U.K., in 1998 and 2004, respectively, and was granted C.Eng. (Chartered Engineer) status by IET in 2013.

In 2005, he was a Researcher with the Instituto de Telecomunicações, Aveiro, Portugal, where he was a member of the Wireless Communications Scientific Area. In 2008, he was promoted to Senior Researcher status, establishing the 4TELL Research Group targeting next-generation mobile systems. He has served as a Project Co-ordinator for major international research projects, including Eureka LOOP and FP7 C2POWER while serving as the Technical Manager for FP7 COGEU and FP7 SALUS. He is currently the Co-ordinator of the H2020-SECRET Innovative Training Network. Since 2009, he has been serving as an Invited Assistant Professor with the University of Aveiro, Aveiro, and attained an Associate Level in 2015. In 2017, he was appointed as a Professor of Mobile Communications at the University of South Wales, Pontypridd, U.K. He has authored more than 450 scientific works, including ten book editorials.

Dr. Rodriguez was elected Fellow of the IET in 2015.

José-Fernán Martínez-Ortega received the B.S. degree in electronics and telecommunications engineering and the Ph.D. degree in telecommunications engineering from the Technical University of Madrid (UPM), Madrid, Spain, in 1993 and 2001, respectively.

From 1993 to 1996, he was technically responsible for research projects at national telecommunications company TELECOM, Colombia. He was the Technical Manager in his own company S&H Ltda. He is currently an Associate Professor with the Department of Engineering and Telematics Architectures, UPM. He has participated in several international and European projects. His current research interests include ubiquitous computing and the Internet of Things, smart cities, wireless sensor and actuators networks, next-generation telematics 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.

Dr. Martínez-Ortega is a member of different international and scientific committees. He is a Technical Reviser and the Chair of technical national and international events on telematics.