

A Location-aware IDPS scheme for Network Coding-enabled Mobile Small Cells

1st Reza Parsamehr
Instituto de Telecomunicações
Aveiro, Portugal.
Universidad Politécnica de Madrid
Madrid, Spain.
parsamehr.r@av.it.pt
r.parsamehr@alumnos.upm.es

2nd Alireza Esfahani
Instituto de Telecomunicações
Aveiro, Portugal.
alireza@av.it.pt

3rd Georgios Mantas
Instituto de Telecomunicações
Aveiro, Portugal.
University of Greenwich
London, UK
gimantas@av.it.pt

4th Jonathan Rodriguez
Instituto de Telecomunicações
Aveiro, Portugal.
University of South Wales
Wales, UK
jonathan@av.it.pt

5th Jose-Fernán Martínez-Ortega
Universidad Politécnica de Madrid
Madrid, Spain.
jf.martinez@upm.es

Abstract—Due to an explosive growing demand for higher data rates that have led to the 5th generation of mobile networks, Network Coding-enabled mobile small cells are observed as a promising technology for 5G networks that can cover the urban landscape by being set up on-demand at any place, and at any time on any device. Despite the benefits of network coding technology on these networks, pollution attacks should be addressed before network coding technology reaches its full potential in 5G mobile small cells. In this paper, we have proposed an intrusion detection and prevention scheme which is able not only to detect and prevent pollution attacks but also to detect the exact location of adversary nodes which are the source of pollution attacks.

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

I. INTRODUCTION

Currently, in 5G mobile networks, the main focus has been on supporting excellent coverage and acceptable throughput for their communication [1]–[5]. In this regard, small cells technology not only tries to extend the coverage of the networks but also increase bandwidth and decrease latency. The small cells technology (see Fig. 1) is one of the significant 5G enablers for effective delivery of ubiquitous 5G services in an energy-efficient and cost-effective manner. Small cell is a new concept which will provide Device to Device (D2D) communication between mobile devices beside communication between small cells and macro-cell to extend the coverage [6], [7].

Due to power consumption, packet loss and low communication bandwidth, NC can be a promising solution for increasing the throughput and improving the performance of the wireless network in mobile small cells [8], [9]. NC was proposed for the first time by Ahlswede et al. [10]. In NC, when the intermediate

node receives packets from its parents, it will combine them and send to its children unlike “store and forward” approach which receives and simply forwards them [11]. However, due to combining packets, network coding-enabled networks are vulnerable to pollution attacks [12], [13].

Although several mechanisms against pollution attacks [12], [14]–[16] have been proposed, few research studies have been proposed in order to detect the attackers location [16]–[18]. In this paper, we propose an intrusion detection and prevention scheme (IDPS) which is able not only to detect and prevent pollution attacks, but also to detect the exact location of the adversary node. The proposed IDPS is based on the Null Space MAC approach, as it was presented in [12], in order to detect pollution attacks and adversary node location. Specifically, the adversary node locating takes place at the Hotspot node of each mobile small cell. To facilitate the adversary node locationing process, we have considered that the Hotspot node keeps a number of shared keys which have also been distributed between the source node and all the intermediate nodes in advance.

This paper is organized as follows: section II introduces the related works. Our IDPS scheme is proposed in section III. Finally, section IV concludes the paper.

II. RELATED WORK

This section has considered three parts: 1) Secure network coding 2) The pollution attack resistance mechanisms and 3) locating schemes for adversary’s location detection;

A. Secure network coding

By using the network coding protocol, several security attacks, including eavesdropping attacks and pollution attacks,

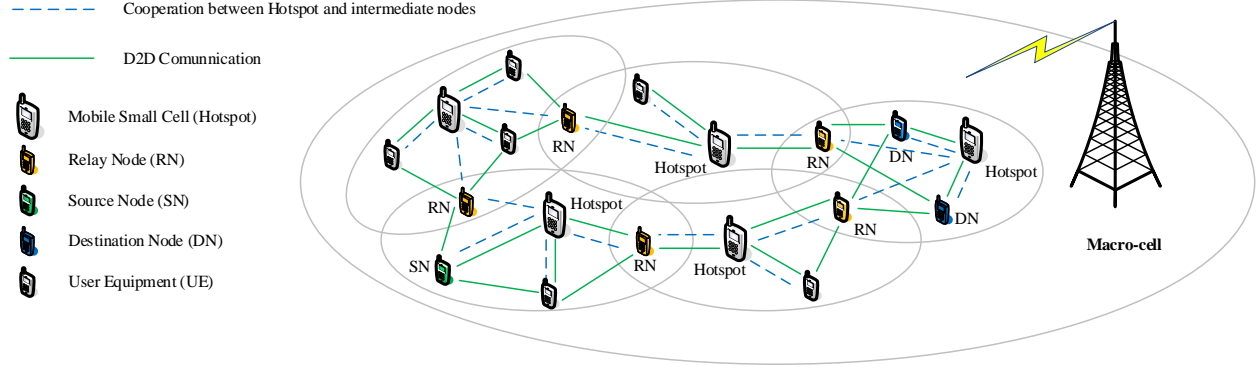


Fig. 1. Small cells technology.

in network coding (NC)-enabled wireless networks have appeared recently. In this context, a lot of effort has been placed on secure NC schemes against these types of attacks.

Several schemes against eavesdropping attacks have been proposed in [19] and [20]. For instance, Cai et al. proposed a scheme that makes a combination of linear codes of original message in a form that an eavesdropper cannot obtain any information about the transmitted messages. In addition, Zhang et al. have defined the external and internal eavesdroppers. Their proposed scheme provides security against these both two external and internal eavesdroppers in RLNC-enabled networks [20].

Furthermore, there are many secure NC schemes against pollution attacks. A security hashing scheme, based on homomorphic functions, proposed by Krohn et al. in [21], where the generated hashes are responsible to validate blocks of rate-less codes. Moreover, a cooperative scheme where legitimate nodes cooperate to protect themselves against adversary nodes is presented in [22]. In this scheme, the cooperation between the nodes enable them to detect and verify malicious nodes. Finally, Ho et al. proposed an approach for detecting Byzantine attacks in multicast RLNC-enabled networks in [23]. More precisely, the proposed approach, first tries to calculate a polynomial function of the data symbols (hash). Then, it augments each source packet with a flexible number of hash symbols calculated earlier.

B. 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, the adversary injects corrupted packets into the network in order to corrupt other coded packets and disrupts the routing operation. However, the adversary in byzantine modification attack aims to make some changes (i.e., invalid coding operations) to data in transit and threat the integrity of the packets in the networks [13], [24], [25]. Both these types can be considered as data pollution attacks and tag pollution attacks. The main target of

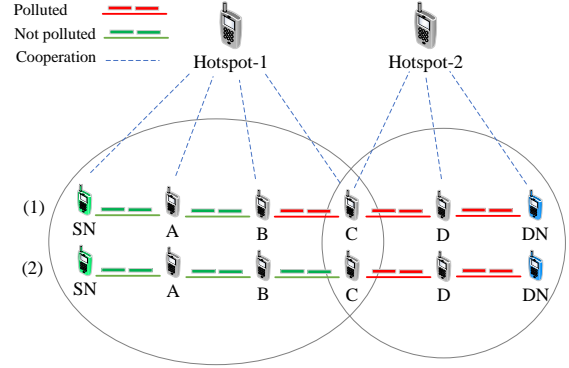


Fig. 2. An example of concluding an attacker's location by the Hotspots, using information about polluted packets through the edges. The attacker is node C. Scenario 1, shows sets of edges when the attacker lies about its incoming packets. However, scenario 2, shows sets of edges when the attacker cannot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

an adversary in data pollution attacks is to modify (i.e., corrupt) the transmitted data packet. On the other hand, in tag pollution attack, the adversary aims to modify the tags appended to the end of data packets.

C. Locating Attackers

The main problem for detecting the exact location of an attacker is that the attacker can deceive about the received data flow. As shown in Fig. 2, 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.

A few research works have been presented in order to detect the adversary location. In the scheme presented by Jafarisiavoshani et al. in [17], each intermediate node should report the packets which have been received from their parents to the controller. Afterward, the controller checks the received packet with source's subspace; if it does not belong to the source packets space, it might be a polluted packet. In this case, controller considers the parent node as an adversary. Le et al.

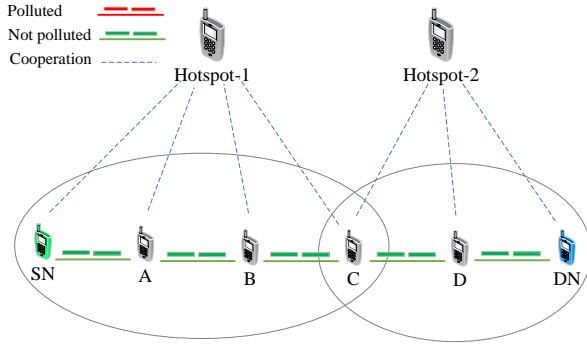


Fig. 3. The network topology.

proposed the SpaceMac mechanism [16] which can compare received packet with space belonging to the intermediate's parent space. The proposed SpaceMac scheme has a significant overhead for the controller which is similar to the overhead of Jafarisiavoshani's scheme.

III. IDPS SCHEME

In this section, we first describe our detection and prevention scheme in order to protect our network model (shown in Fig. 3) against pollution attack in Network Coding-enabled mobile small cells. In addition, we propose a locating scheme which can detect the exact location of adversary nodes which are the source of pollution attacks. The detection and locating schemes of the proposed IDPS scheme are based on Null Space homomorphic MAC scheme [12].

A. Detection Scheme

Following our assumption in our previous work in [12], the source node divides message packets into generations and each generation consist of m messages packets denoted as $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_m$. We assume that each packet \mathbf{v}_i is represented as a vector of n symbols (e.g., $\underline{v}_{i,1}, \underline{v}_{i,2}, \dots, \underline{v}_{i,n}$) which each symbol stands in the finite field \mathbb{F}_p^n . Therefore, the source node generates an expanded packet \mathbf{v}_i represented as follows:

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

Then, the source node sends \mathbf{v}_i to the next intermediate nodes. Each intermediate node receive the coded packets and create a new coded packet \mathbf{v}_i and send it to its neighbour nodes. Our proposed IDPS scheme assumed that the source node generates L tags based on null space properties [26]. We define the following four steps:

1) *Key Distribution to Source Node:* A Key Distribution Center (KDC) distributes L key vectors $\mathcal{D}_1, \mathcal{D}_2, \dots, \mathcal{D}_L$ to the source node. Each of them is represented in the finite field \mathbb{F}_p^{m+n+L} .

2) *Tag generation:* The source node S uses the L key vectors $\mathcal{D}_1, \mathcal{D}_2, \dots, \mathcal{D}_L$ to produce L tags for each coded packet including of $m + n$ symbols. In next figures, we show these

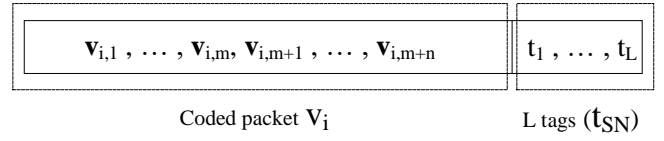


Fig. 4. Generated L tags for each packet in source node.

tags as \mathbf{t}_{SN} , (see Fig. 4). These L tags (t_1, t_2, \dots, t_L , where $t_i \in \mathbb{F}_p$) are calculated according to the following formula:

$$\begin{bmatrix} \mathcal{D}_{1,1} & \dots & \mathcal{D}_{1,m+n} \\ \vdots & \vdots & \vdots \\ \mathcal{D}_{L,1} & \dots & \mathcal{D}_{L,m+n} \end{bmatrix}_{L \times (m+n)} * \begin{bmatrix} \mathbf{v}_{i,1} \\ \mathbf{v}_{i,2} \\ \vdots \\ \mathbf{v}_{i,m+n} \end{bmatrix}_{(m+n) \times 1} + \begin{bmatrix} \mathcal{D}_{1,m+n+1} & \dots & \mathcal{D}_{1,m+n+L} \\ \vdots & \vdots & \vdots \\ \mathcal{D}_{L,m+n+1} & \dots & \mathcal{D}_{L,m+n+L} \end{bmatrix}_{L \times L} * \begin{bmatrix} t_1 \\ t_2 \\ \vdots \\ t_L \end{bmatrix}_{L \times 1} = 0 \quad (2)$$

Afterwards, the source node adds the L tags which calculated by equation 2 to the end of the coded packet \mathbf{v}_i , which is created by prefixing the native packet \underline{v}_i with m coefficients. For simplicity, we show t_1, t_2, \dots, t_L with \mathbf{t}_{SN} in the rest of the paper.

3) *Swapping:* To avoid tag pollution attacks, the L tag symbols of the coded packet \mathbf{v}_i are swapped with only L out of the n symbols of the coded packet \mathbf{v}_i . We should mention that destination nodes can decode correctly due to that the coefficients of the coded packet do not participate in the swapping process. Particularly, the swapping process is based on a secret value SV (i.e., positive integer) that plays the role of the swapping vector. The KDC generate the secret value through a pseudorandom function randomly. The source node and all destination nodes know the secret value. However, it is unknown to the intermediate nodes. The result of this swapping process is a swapped coded packet $\bar{\mathbf{v}}_i$, where the L tags symbols are mixed with the n symbols of the coded packet \mathbf{v}_i . Each swapped coded packet is represented as follows:

$$\bar{\mathbf{v}}_i = \text{Swap}(\mathbf{v}_i)_{SV} \quad (3)$$

It is clear that, an inverse swapping is required before RLNC-decoding at the destination nodes to obtain the native packet.

4) *Key Distribution to Intermediate and Destination Nodes:* The KDC, based on the swapping vector SV mentioned in the swapping step, generates new key vectors $\mathcal{D}'_1, \mathcal{D}'_2, \dots, \mathcal{D}'_L$. More precisely, each key vectors is represented as follows:

$$\mathcal{D}'_i = \text{Swap}(\mathcal{D}_i)_{SV} \quad (4)$$

Our proposed IDPS mechanism follows the key distribution model proposed in [27] which is based on the cover free set systems. Due to the orthogonality of the swapped coded packet and each swapped key vector, we have also assumed only one

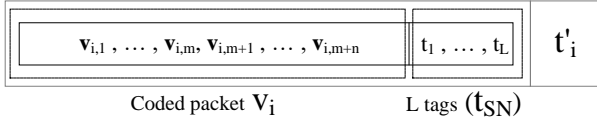


Fig. 5. Generated tags for each packet in each intermediate node which we named t_{SN} .

key vector is required to be assigned by the KDC to each intermediate and destination node.

5) *Verification*: The following formula verifies if a key vector, \mathcal{D}_i , is orthogonal to a swapped coded packet $\bar{\mathbf{v}}_i$:

$$\delta = \text{Swap}(\mathcal{D}_i)_{SV} * \text{Swap}(\mathbf{v}_i)_{SV} = \sum_{j=1}^{m+n+L} \mathcal{D}'_{i,j} * \bar{\mathbf{v}}_{i,j} \quad (5)$$

If $\delta = 0$, then our proposed IDPS accepts the swapped coded packet $\bar{\mathbf{v}}_i$ and sends it to the next nodes. Otherwise, we discard it.

6) *Correctness*: The correctness of our IDPS mechanism is proved by contradiction theorem. In this regards, we assume that the proposed scheme is not correct. If this is true, through the verification step, we should have that $\delta \neq 0$. We consider a coded packet $y^i = (y_1^i, \dots, y_{m+n}^i)$ and L key vectors $D = (\mathcal{D}_1, \dots, \mathcal{D}_L)$, to generate L tags $t^i = (t_1^i, \dots, t_L^i)$ based on Equation 2. According to Equation 5 and by considering $SV = 1$, we have the following:

$$\begin{aligned} & \text{Swap}(D)_{SV} * \text{Swap}(\bar{y}^i)_{SV} = \\ & \begin{bmatrix} \mathcal{D}_{1,1} \dots \mathcal{D}_{1,m+n+1} \dots \mathcal{D}_{1,m+n+L} & \mathcal{D}_{1,m+1} \dots \mathcal{D}_{1,m+L} \\ \vdots & \vdots \\ \mathcal{D}_{L,1} \dots \mathcal{D}_{L,m+n+1} \dots \mathcal{D}_{L,m+n+L} & \mathcal{D}_{L,m+1} \dots \mathcal{D}_{L,m+L} \end{bmatrix} * \\ & \begin{bmatrix} y_1^i & \dots & t_1^i & \dots & t_L^i & \dots & y_{m+n}^i & y_{m+1}^i & \dots & y_{m+L}^i \end{bmatrix}^T \\ & = \begin{bmatrix} \mathcal{D}_{1,1} * y_1^i + \dots \mathcal{D}_{1,m+n+L} * t_L^i \\ \vdots \\ \mathcal{D}_{L,1} * y_1^i + \dots \mathcal{D}_{L,m+n+L} * t_L^i \end{bmatrix}_{L \times 1} \end{aligned} \quad (6)$$

However, the vector $\bar{y}^i = [y_1^i, \dots, y_{m+n}^i, t_1^i, \dots, t_L^i]$ is orthogonal to each of the L key vectors according to Equation 8. Thus, we have the following:

$$\begin{aligned} D * \bar{y}^i &= \begin{bmatrix} \mathcal{D}_{1,1} & \dots & \mathcal{D}_{1,m+n+L} \\ \vdots & \vdots & \vdots \\ \mathcal{D}_{L,1} & \dots & \mathcal{D}_{L,m+n+L} \end{bmatrix} * \begin{bmatrix} y_1^i \\ y_2^i \\ \vdots \\ t_L^i \end{bmatrix} \\ &= \begin{bmatrix} \mathcal{D}_{1,1} * y_1^i + \dots \mathcal{D}_{1,m+n+L} * t_L^i \\ \vdots \\ \mathcal{D}_{L,1} * y_1^i + \dots \mathcal{D}_{L,m+n+L} * t_L^i \end{bmatrix}_{L \times 1} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}_{L \times 1} \end{aligned} \quad (7)$$

By comparison Equations 6 and 7, it is obvious that $\delta = 0$. However, this contradicts the original assumption that $\delta \neq 0$. Therefore, the proposed construction is correct.

B. Locating Scheme

The main requirement for detecting the exact location of adversaries is to prevent nodes from deceiving Hotspot [16]. We have considered an extra tag to each packet for verifying each intermediate node by Hotspot. In order to calculate the proper tag, we use the following equation:

$$\begin{bmatrix} \mathcal{D}'_{1,1} & \dots & \mathcal{D}'_{1,m+n} & \dots & \mathcal{D}'_{1,m+n+L} \end{bmatrix}_{1 \times (m+n+L)} * \begin{bmatrix} \mathbf{v}_{i,1} \\ \mathbf{v}_{i,2} \\ \vdots \\ \mathbf{v}_{i,m+n} \\ t_1 \\ \vdots \\ t_L \end{bmatrix}_{(m+n+L) \times 1} + \mathcal{D}'_{1,m+n+L+1} * t'_i = 0 \quad (8)$$

where $\begin{bmatrix} \mathcal{D}'_{1,1} & \dots & \mathcal{D}'_{1,m+n} & \dots & \mathcal{D}'_{1,m+n+L+1} \end{bmatrix}_{1 \times (m+n+L+1)}$ is the pre-shared key distributed by the KDC to the intermediate nodes and Hotspot, and t'_i is the proper calculated tag. This tag has been added to each packet in order to allow Hotspot to detect the source of the pollution (see Fig. 5).

Our scheme includes two parts (see Fig. 6): i) when an intermediate node receives a packet, it should check the validity of the received packet based on the detection scheme presented in the previous section. If any pollution is detected, then the intermediate nodes reports the result to Hotspot. ii) when an intermediate node is going to send a coded packet to the next node, it should firstly create a tag t'_i signed by the shared secret key (D') between the intermediate node and Hotspot. Then, the signed tag is appended to the coded packet, and the new packet is sent to the next node and Hotspot.

We have considered the following two scenarios to present how the proposed IDPS is able to detect the adversary.

- Scenario 1- An adversary node between 2 normal nodes. A is a normal node and B is an adversary who has two options to report to Hotspot:

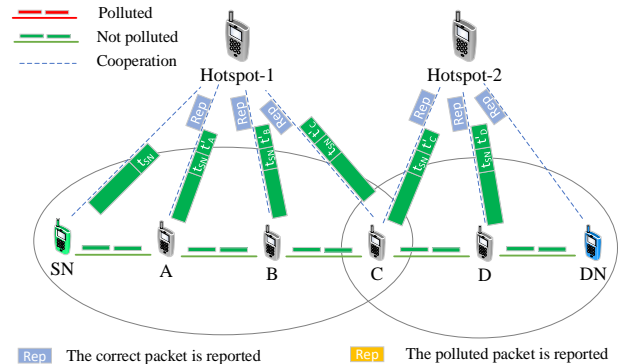


Fig. 6. The information which intermediate node should sends to the controller.

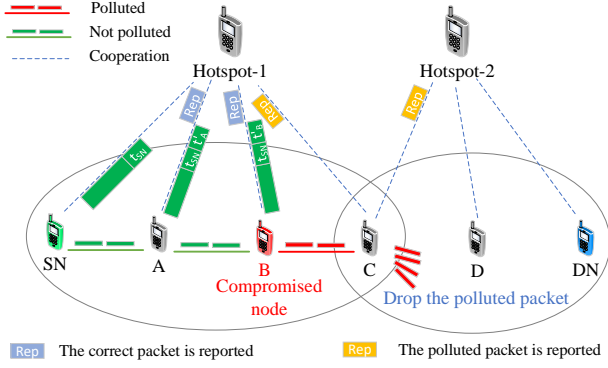


Fig. 7. Scenario 1: A is a normal node and B is an adversary. Node D will not report any pollution and Hotspot will detect B as an adversary because C has dropped the polluted packet and behaved like a normal node.

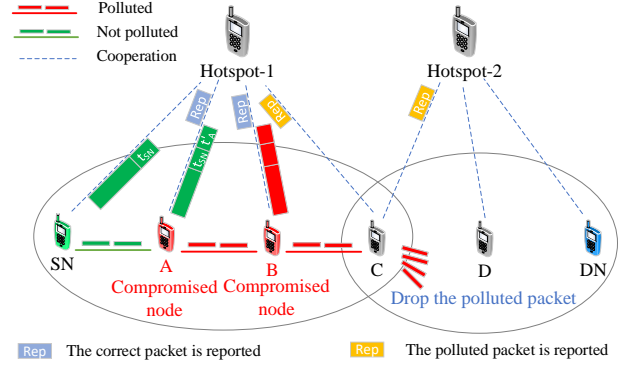


Fig. 8. Scenario 3: both node A and node B are adversary. Node B as an adversary cannot send a valid packet to Hotspot to verify itself, because it has no access to the packet with a valid tag (t_{SN}).

- "Received a polluted packet from node A": B can either send a polluted packet to the next node (node C) or drop the received packet from A. If node B sends the polluted packet to node C, node C will drop it and reports pollution to the Hotspot. Consequently, Hotspot will detect B as an adversary because it did not drop the polluted packet. If node B drops the received packet from A, it will make another kind of attacks which is beyond the scope of this paper (e.g., DoS attack).
- "Received a normal packet from node A": like the previous case, B can either send a polluted packet to node C or drop the received packet from A. If node B sends the polluted packet to node C, then node C will drop it and report pollution to Hotspot. Thus, node D (next node) will not report any pollution and Hotspot will detect B as an adversary because C has dropped the polluted packet and behaved like a normal node (see Fig. 7). Otherwise, If node B drops the received packet from A, it will make another kind of attack which is not our target in this paper (e.g., DoS attack).
- Scenario 2- Two or more adversaries in a row. Node A and node B are both adversary nodes. As shown in Fig. 8, node B as an adversary cannot send a valid packet to Hotspot to verify itself, because it has no access to the packet with a valid tag (t_{SN}). Therefore, Hotspot detects it as an adversary and blocks it from the network (see Fig. 9). As a result, the current network has one adversary (node A) between two normal nodes, which is similar to the first scenario. Moreover, this scenario is valid for more than two attackers in a row when the attackers (who are in a row) could not verify themselves to the Hotspot. In this case, they will be blocked from access to the network.

IV. CONCLUSION

This paper proposed location-aware IDPS scheme for Network Coding-enabled Mobile Small Cells. The proposed

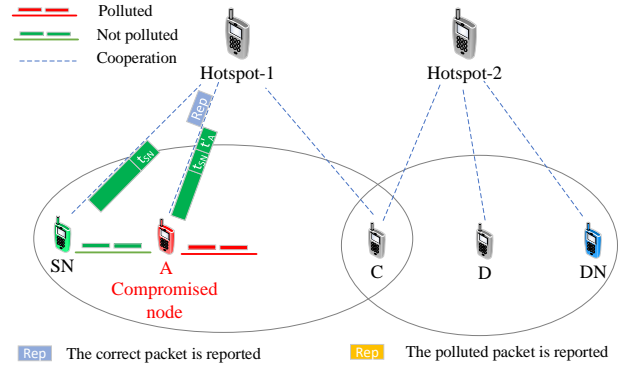


Fig. 9. Scenario 3. Node B has been detected as an adversary by Hotspot and blocked from the network. So, the scenario will change to one adversary (node A) between two normal nodes, which is similar to scenario 1.

scheme is able not only to detect and prevent pollution attacks, but also to detect the exact location of adversary source. This gives us the opportunity to block attackers from having access to the network and making pollution. As a future work, we plan to extend the proposed IDPS into a collaborative IDPS that will not only allow the detection of the source(s) of the pollution attacks but also, protect network-coding enabled mobile small cells from depletion of their resources (e.g. CPU power, memory and battery level), when exposed to these attacks.

ACKNOWLEDGMENT

This research work leading to this publication has received funding from the European Union's Horizon 2020 Research and Innovation program under grant agreement H2020-MSCA-ITN-2016-SECRET-722424 [28].

REFERENCES

- [1] B. Bangerter, S. Talwar, R. Arefi, and K. Stewart, "Networks and devices for the 5g era," *IEEE Communications Magazine*, vol. 52, no. 2, pp. 90–96, 2014.
- [2] I. Chih-Lin, C. Rowell, S. Han, Z. Xu, G. Li, and Z. Pan, "Toward green and soft: A 5g perspective," *IEEE Communications Magazine*, vol. 52, no. 2, pp. 66–73, 2014.
- [3] G. Mantas, N. Komninos, J. Rodriguez, E. Logota, and H. Marques, "Security for 5g communications," 2015.
- [4] V. Sucasas, G. Mantas, and J. Rodriguez, "Security challenges for cloud radio access networks," *Backhauling/Fronthauling for Future Wireless Systems*, pp. 195–211, 2016.
- [5] C.-X. Wang, F. Haider, X. Gao, X.-H. You, Y. Yang, D. Yuan, H. M. Aggoune, H. Haas, S. Fletcher, and E. Hepsaydir, "Cellular architecture and key technologies for 5g wireless communication networks," *IEEE communications magazine*, vol. 52, no. 2, pp. 122–130, 2014.
- [6] A. Gupta and R. K. Jha, "A survey of 5g network: Architecture and emerging technologies," *IEEE access*, vol. 3, pp. 1206–1232, 2015.
- [7] S.-F. Chou, T.-C. Chiu, Y.-J. Yu, and A.-C. Pang, "Mobile small cell deployment for next generation cellular networks," in *2014 IEEE Global Communications Conference*. IEEE, 2014, pp. 4852–4857.
- [8] Y.-J. Chen, L.-C. Wang, K. Wang, and W.-L. Ho, "Topology-aware network coding for wireless multicast," *IEEE Systems Journal*, no. 99, pp. 1–10, 2018.
- [9] S. Katti, H. Rahul, W. Hu, D. Katabi, M. Médard, and J. Crowcroft, "Xors in the air: Practical wireless network coding," in *ACM SIGCOMM computer communication review*, vol. 36, no. 4. ACM, 2006, pp. 243–254.
- [10] R. Ahlswede, N. Cai, S.-Y. Li, and R. W. Yeung, "Network information flow," *IEEE Transactions on information theory*, vol. 46, no. 4, pp. 1204–1216, 2000.
- [11] T. Ho and D. Lun, *Network coding: an introduction*. Cambridge University Press, 2008.
- [12] A. Esfahani, G. Mantas, and J. Rodriguez, "An efficient null space-based homomorphic mac scheme against tag pollution attacks in rlnc," *IEEE Communications Letters*, vol. 20, no. 5, pp. 918–921, 2016.
- [13] R. Parsamehr, G. Mantas, A. Radwan, J. Rodriguez, and J.-F. Martínez, "Security threats in network coding-enabled mobile small cells," in *International Conference on Broadband Communications, Networks and Systems*. Springer, 2018, pp. 337–346.
- [14] S. Agrawal and D. Boneh, "Homomorphic macs: Mac-based integrity for network coding," in *International Conference on Applied Cryptography and Network Security*. Springer, 2009, pp. 292–305.
- [15] Y. Li, H. Yao, M. Chen, S. Jaggi, and A. Rosen, "Ripple authentication for network coding," in *2010 Proceedings IEEE INFOCOM*. IEEE, 2010, pp. 1–9.
- [16] A. Le and A. Markopoulou, "Cooperative defense against pollution attacks in network coding using spacemac," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 2, pp. 442–449, 2012.
- [17] M. J. Siovoshani, C. Fragouli, and S. Diggavi, "On locating byzantine attackers," in *2008 Fourth Workshop on Network Coding, Theory and Applications*. IEEE, 2008, pp. 1–6.
- [18] Q. Wang, L. Vu, K. Nahrstedt, and H. Khurana, "Identifying malicious nodes in network-coding-based peer-to-peer streaming networks," Tech. Rep., 2009.
- [19] N. Cai and R. W. Yeung, "Secure network coding," in *Proceedings IEEE International Symposium on Information Theory*. IEEE, 2002, p. 323.
- [20] P. Zhang, Y. Jiang, C. Lin, Y. Fan, and X. Shen, "P-coding: secure network coding against eavesdropping attacks," in *2010 Proceedings IEEE INFOCOM*. IEEE, 2010, pp. 1–9.
- [21] M. N. Krohn, M. J. Freedman, and D. Mazieres, "On-the-fly verification of rateless erasure codes for efficient content distribution," in *IEEE Symposium on Security and Privacy, 2004. Proceedings. 2004*. IEEE, 2004, pp. 226–240.
- [22] C. Gkantsidis, P. Rodriguez *et al.*, "Cooperative security for network coding file distribution," in *INFOCOM*, vol. 3, no. 2006, 2006, p. 5.
- [23] T. Ho, M. Médard, R. Koetter, D. R. Karger, M. Effros, J. Shi, and B. Leong, "A random linear network coding approach to multicast," *IEEE Transactions on Information Theory*, vol. 52, no. 10, pp. 4413–4430, 2006.
- [24] 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," *Cyber Physical Systems: From Theory to Practice*, pp. 395–414, 2015.
- [25] L. Lima, J. P. Vilela, P. F. Oliveira, and J. Barros, "Network coding security: Attacks and countermeasures," *arXiv preprint arXiv:0809.1366*, 2008.
- [26] E. Kehdi and B. Li, "Null keys: Limiting malicious attacks via null space properties of network coding," in *IEEE INFOCOM 2009*. IEEE, 2009, pp. 1224–1232.
- [27] T. Ho, D. R. Karger, M. Médard, and R. Koetter, "Network coding from a network flow perspective," in *IEEE International Symposium on Information Theory, 2003. Proceedings*. IEEE, 2003, p. 441.
- [28] J. Rodriguez, A. Radwan, C. Barbosa, F. H. Fitzek, R. A. Abd-Alhameed, J. Noras, S. M. Jones, I. Politis, P. Galitos, G. Schulte *et al.*, "Secret—secure network coding for reduced energy next generation mobile small cells: A european training network in wireless communications and networking for 5g," in *2017 Internet Technologies and Applications (ITA)*. IEEE, 2017, pp. 329–333.