

# Secure Network Coding for SDN-based Mobile Small Cells

Vipindev Adat, Ilias Politis, Christos Tselios  
and Stavros Kotsopoulos

Wireless Telecommunications Laboratory \*  
University of Patras, Greece  
{vipindev, ipolitis, tselios, kotsop}@ece.upatras.gr

**Abstract.** The future wireless networks including the fifth generation of mobile networks have to serve a very dense heterogeneous network of devices with high resiliency and reliability. Network coding is also emerging as a potential key enabler for optimizing bandwidth requirements and energy consumption in highly dense mobile network environments. However, network coding deployments still need to consider security vulnerabilities and their countermeasures, before they can be adapted as part of the emerging mobile network deployments. On the other hand the software defined networking can be employed in the mobile small cell environment to achieve highly efficient and easily configurable network architecture. This paper studies the scope of utilizing the SDN based mobile small cells to implement secure network coded mobile small cells minimizing the overheads and delays.

**Keywords:** Random Linear Network Coding · Pollution Attacks · 5G small cells.

## 1 Introduction

The fifth generation (5G) network paradigm has already emerged with stringent throughput and energy requirements [1, 2] for accommodating all recently introduced verticals [3, 4]. As the future wireless environment is conceptualized it is expected to include different types of cells such as macro, pico and small cells. The concept of cooperated small cells as the basis for the new mobile cell architecture is proposed on this front and network coding schemes can be a key enabler in such a network model to achieve high throughput and resilience [5]. The network coded cooperated small cell environment can provide high data rates at a low energy for the dense population of devices in the 5G era. However, implementing network coding in the mobile environment of small cells can lead to security threats including denial of service, intrusion, byzantine fabrication

---

\* This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement H2020-MSCA-ITN-2016 SECRET-722424

and false identity etc. This paper addresses the problem of pollution attacks in network coded mobile small cell environment and performance of security schemes in terms of communication and computational overhead. We consider the homomorphic message authentication codes and signatures to ensure the security of the network. Further, we consider the possibility of the software defined architecture to achieve easily configurable cooperated mobile small cells in an efficient way. The availability of the central controller will also add to ensuring the security of the whole network.

## 2 Network Coding for Mobile Small Cells

The problem of secure network coding was first studied in [6] which proposed a scheme of admissible linear network codes which will protect the message from eavesdropping. As the possibilities of network coding was explored as a strong energy efficient high throughput communication scheme, more specific threats related to network coding also popped up. The mixing of packets which forms the base of network coding schemes increases the effect of a byzantine fabrication attack since a single corrupted packet can widely spread into the network and corrupt the whole message resulting in devastating effects on throughput and network utilization. This, widely known as pollution attack, is addressed as one of the major security threat in network coded environment. As the network coding schemes varies from interflow to intraflow networks, state aware to stateless protocols, the security schemes against pollution attacks also differs [7–9]. However, for the mobile wireless environment, random linear network coding (RLNC) has been considered as the best suited [10] option due to the frequently changing network situation and we focus more into preventing pollution attacks in a RLNC based mobile small cell environment.

### 2.1 Random Linear Network Coding and Pollution Attacks

As per the widely used principles of random linear network coding, a message is considered as a number of generations where each generation consists of various packets. Each native packet  $P_i$  is considered as a vector of  $n$  elements such as  $P_{i1}, P_{i2}, \dots, P_{in}$  over finite field  $F_q^n$  where  $q$  defines the finite field size. A generation consisting of  $m$  such packets will be a  $m \times n$  matrix which can be considered as the native generation. However, to enable proper encoding and decoding, the native packets will be augmented with a unit vector of size  $m$  which will have all zeros but a 1 at the corresponding position of the native packet in the generation. These augmented packets are encoded with locally generated random coefficients and transmitted by the source node to its neighbouring nodes. The intermediate nodes, on the reception of an innovative generation of packets, re encode it with its own locally generated random coefficients before transmission. This procedure is followed till the receiving nodes. However, a malicious intermediate node can pollute the whole system by introducing a polluted packet. Due to the mixing of packets at the intermediate nodes, the pollution attacks in network

coded environment, if unchecked, can spread over the transmission infecting all the communication involving the initial polluted packet and its parts. The homomorphic MAC scheme proposed by Aggrawal et. al [11] was successful in preventing this pollution attacks with a probability of  $1/q^L$ , where  $q$  is the field size and  $L$  is the number of tags. However it suffers from the tag pollution attacks in which the adversary tries to pollute the tags attached to the packets to verify its integrity. In tag pollution attacks, malicious nodes pollute tags of genuine packets resulting in such packets being discarded when incorrect tags are detected, which leads to poor network performance. MacSig [12] proposes the usage of a homomorphic signature over the MAC scheme to certify that the tags attached to the packets are corresponding to the packet itself. Dual HMAC and HMAC [13,14] try to reduce the computational and communicational overhead of MacSig using a novel key distribution model based on cover free family. This also provide security against a situation in which a number of compromised nodes act together to pollute the network at a lower key storage overhead at intermediate nodes.

Further, in this study, we consider software defined mobile small cell network for highly configurable efficient deployment as shown in Fig. 1. This will help the system to ensure better efficiency in terms of network utilization. Further if network coding is deployed over this SDN based mobile small cells, the throughput and resiliency of the whole environment can be improved to match the requirements in the 5G era. In this paper, we also propose how the availability of a centralized software defined controller connected to the nodes in the network can be better utilized for ensuring the security of the network. In our proposal, along with the control message some secure information needs to be communicated with the central unit and it reduces the overhead in the communication lines between the nodes and prevents pollution attacks with a high probability.

### 3 Secure Network Coding in SDN Based Mobile Small Cells

This security scheme is a modification of some existing approaches like Dual HMAC and Homomac [11,13] by utilizing this central unit to ensure the security. In this approach, the centralized controller is also considered as a trusted party which is connected to all the nodes. We consider the homomorphic hashing schemes discussed in [11,12] for the integrity of messages and a signature for the authenticity of messages. We further utilize the centralized controller to ensure the security of the scheme with higher efficiency and reduce the computational cost at the intermediate nodes.

#### 3.1 Proposed Security Scheme

Our scheme follows similar message authentication schemes, but utilizes the availability of centralized controller to reduce the computational and communication cost over the channels. The proposed scheme can be explained in the following four steps:

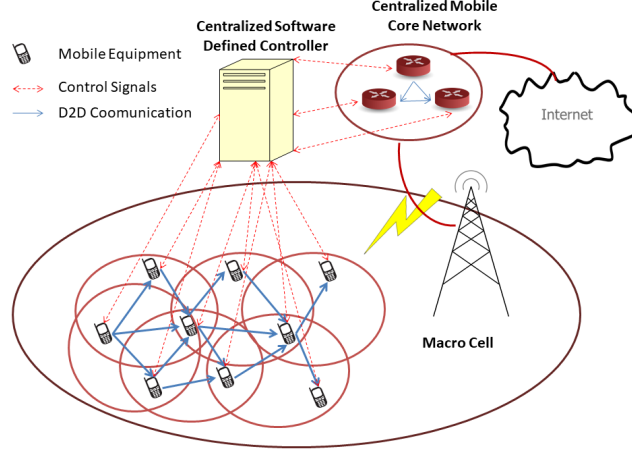


Fig. 1: SDN Based Mobile Small Cell Architecture.

1. Setup: This first phase of scheme includes the key distribution. A Key distribution centre (KDC) is responsible for this. Since the MAC scheme uses symmetric keys for creating and verifying the tags, KDC distributes a set of  $L$  keys to each node in the network. This procedure can be done prior to the actual communication starts. Thus each node will have a set of keys  $K_i$  where each key have  $n + 1$  symbols in it. The size of a key in our scheme is comparatively less than the other comparable schemes like HMAC and Mac-Sig because we define the tags over the native packets only, excluding the augmented vector part. This is more clearly explained in the tag generation section. Further, each source node will have its own private key to create the signature over the tags. All the intermediate and receiving nodes will need the corresponding public key to verify the signature. KDC take care of this public key private key generation and distribution as well.
2. Tag generation: In our proposed scheme, tags are generated only at the source nodes, reducing the computational cost at the intermediate nodes considerably. Further only the native packets are considered so that the size of a key is also smaller. The integrity of the packets are ensured by tags created using the key set provided by the KDC. A tag will be generated as

$$Tag_l = \frac{\left( \sum_{j=1}^n P_{i,j} \times K_{l,j} \right)}{K_{l,j+1}}, \quad l \in (1, L) \quad (1)$$

Since a generation of  $m$  packets are considered in one transmission, there will be  $L \times m$  number of tags associated with a particular generation, attached to it. Further, our scheme introduces a novel tag communication scheme including the centralized controller to prevent pollution attacks. For this,

each source compute a signature over the tags for a particular generation and communicate this set of tags along with the signature and generation number to the central controller.

---

**Algorithm 1:** Verification Algorithm

---

**Data:** Received packet  $\mathbf{C}_i$ ,  $\mathbf{L}$  tags corresponding to  $\mathbf{C}_i$  retrieved from the central unit, Key set  $\mathbf{K}_s$

**Result:** **1** if verification is successful and **0** if verification is failed.  
In case of a failed verification, the type of the attack is also reported.

- 1 **Step 1:**
  - 2 Retrieve the coefficient matrix from the received packet
  - 3 **Step 2:**
  - 4 Multiply the tags retrieved from the central unit with the corresponding coefficients
  - 5 **Step 3:**
  - 6 Compare the tags with those appear in the received codeword.
  - 7 **if they dont match then**
  - 8 | Report Warning and Proceed
  - 9 **else**
  - 10 | Proceed
  - 11 **Step 4:**
  - 12 Create tags for the received packet using MAC algorithm (without considering the coefficient part)
  - 13 **Step 5:**
  - 14 **if MAC algorithm output matches with the tags retrieved from central unit then**
  - 15 | 1  $\leftarrow$  Return
  - 16 **else**
  - 17 | 0  $\leftarrow$  Return
- 

3. Verification: The verification process happens at each receiving node. It ensures that the tags attached to the received packets are genuine and created at the source. The centralized controller along with the tags attached to the received packets enables this verification. On receiving a coded generation, the receiving node will check for the corresponding entry of tags in the central controller from the source. The authenticity of this entry in the centralized unit can be verified by the public key corresponding to the private key used to sign the entry. Once the right entry is retrieved from the centralized unit, then the integrity of the received message can be verified by comparing the tags in the entry retrieved from the centralized unit and the tags in the received packet. The verification algorithm shown above gives a step by step explanation of the verification procedure. Once a generation of packets completes the verification process successfully, they are re-encoded by the intermediate nodes or decoded to retrieve the original message at the destination nodes.

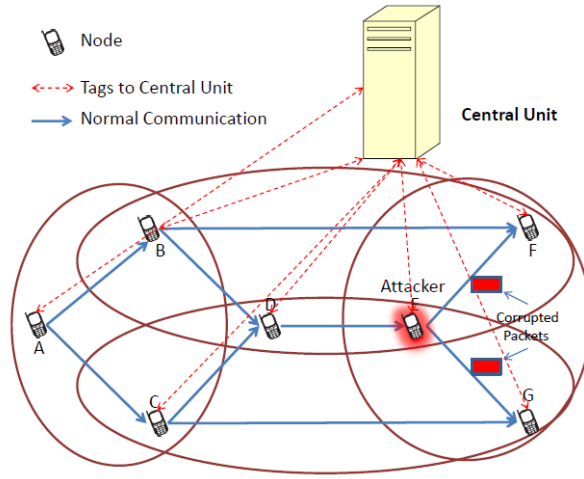


Fig. 2: Architecture for Security Scheme

4. Re-encoding: The intermediate nodes will re-encode the verified messages before forwarding them further. However, in our scheme no more tag generation is performed at the intermediate nodes. The tags are generated only at the source nodes and after the tag generation all the elements in the packet are considered as the same. This reduces the computational requirements at the intermediate nodes considerably. Thus re-encoding process is very much similar to normal RLNC scheme. The verified generations are multiplied by the locally generated random coefficients.

### 3.2 Security Analysis

This section analyses how the proposed scheme ensures protection against pollution attacks using the central controller. The security scheme is analyzed over a butterfly network in the SDN based small cell environment as shown in Fig. 2. Before proceeding to the security analysis, it is necessary to define the capabilities of the adversary node. In the scenario described in this paper, only the intermediate nodes are considered susceptible to attacks. The source nodes are considered as trusted and secure. Also the key distribution scheme is considered as secure, especially the asymmetric keys used for signing the entries to the central unit is kept secure and not shared by the source nodes. However, when an attacker compromises an intermediate node, it can have full control over the resources available to the compromised node. Thus if the attacker compromises an intermediate node, it can access the whole key set available to the node as well as decode and analyze the original packets and tags attached to them. Thus the adversary has strong knowledge over the messaging scheme. Further, we consider a situation in which the attacker could compromise more than one node in a neighbourhood and perform a coordinated attack. However, the direct

connection from central unit to each node in the network nullify any additional advantages achieved by such mass compromising of nodes since the security systems at the immediate benign node will be able to detect and discard polluted packets.

**Data Pollution Attacks:** The adversary try to modify the content of the packet and forward the message to the neighbouring nodes. This pollutes the corrupted packet instantly and with further alterations pollutes more and more genuine packets. This points to the necessity of finding out the corrupted packet at the earliest possible instant and prevent it from mixing with other benign packets. In our scheme, a two level verification of tags ensures that the data pollution attacks are detected efficiently at the immediate genuine node receiving a polluted packet. Since the receiving node already have the key set used to create the tags, it can check whether the tags are genuine to the corresponding message part in the received code word. However, since the adversary also have the keyset available from the compromised node, it may have forged the tag for the corrupted message and attach it to the packet. Thus a strong adversary can pass the first verification. However the second level of verification is matching the tags received in the code word with the corresponding tags retrieved from the central controller. If the adversary has to pass this verification, it needs to forge a corrupted packet which will give exactly the same tag as the original packet. That is same as finding another symbol in the symbol space of the original packet such that the MAC generation will result in the same tag for both the corrupted and original packets. This can be considered as a probability of  $1/q$ , where  $q$  is the field size. Further, if there are  $L$  tags that will be checked, then it needs to satisfy all these tags and then the probability of creating a corrupted packet that will pass the verification test is  $1/q^L$ . In practical cases  $q = 28$  and  $L = 8$  gives a very satisfactory level of protection against the data pollution attacks.

**Tag Pollution Attacks:** Tag Pollution attacks are a serious problem faced by the homomorphic MAC based security schemes in network coded environment. In such cases, the tags created and attached to the original benign packets are altered by the adversary intermediate nodes. Then these packets will travel till it will detect an altered tag and discarded. Such attacks create two serious issues; network resource under utilization and dropping of genuine packets. Thus it is necessary to detect the tag pollution attack at the immediate neighbouring benign node and further process the transaction of genuine packets. This is ensured in our scheme using the secure communication of tags to the central unit and its comparison. The authenticity of the entries in the central unit is verified using the signature attached to it. Comparing the corresponding tags in the received packet with those retrieved from the central unit results in the detection of tag pollution attack. In case of the detection of a tag pollution attack, that node can check whether the content is still the same by creating tags for the packet and comparing with the tags retrieved from the central unit and proceed with the communication after marking a warning against the malicious

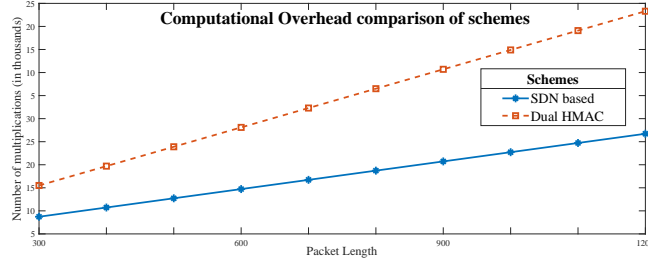


Fig. 3: Computational Overhead for different schemes

node. By this way, the network resource wastage and unnecessary dropping of genuine packets can be tackled. It is ensured that this detection of pollution attacks happen at the immediate benign node in the system after adversary.

## 4 Performance Evaluation

### 4.1 Computational Overhead

This secure RLNC scheme for SDN based mobile small cell environment requires some extra computations to be performed at each node. A source node has to create the tags and a signature over the tags and all other nodes need to verify the tags and signature. For each tag creation as per the scheme  $n + 1$  multiplications are required and for creating a signature over  $L$  number of tags,  $L + 1$  multiplications will be performed. Thus, a scheme having  $L$  tags will have an extra overhead of  $L \times (n + 2) + 1$  multiplications over each packet generated at the source node. For the receiving nodes, the verification of MAC requires the same  $L \times (n + 1)$  multiplications to verify the  $L$  tags. However, the verification of signature over the tags retrieved from the central unit requires  $L + 1$  exponentiation. Each exponentiation corresponds to  $\frac{3}{2}|q|$  multiplications [12]. This shows a significant advantage over the computational cost caused by the security scheme compared to other similar schemes. For example, HMAC scheme proposed by Alireza et.al [13], which is proved to be secure against both data and tag pollution attack suffers from a computational overhead in the second order of  $L$ . Fig. 3 shows a comparison of computational cost of both the schemes when the same number of tags are used ( $L=8$ ).

### 4.2 Communication overhead

The communication overhead results from the extra bits associated to each packet for security purpose. In our scheme, similar to any other MAC based scheme, this corresponding to the tags associated to each packet. Each tag created as per eq. (1) provide a security level of  $1/q$  probability to be broken by the adversary. In the general case of  $L$  number of tags attached to each packet, where each tag is a symbol, an  $L/(m + n)$  communication overhead is suffered

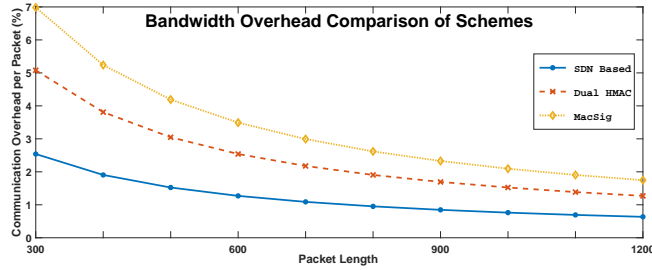


Fig. 4: Communication Overhead for different schemes

per packet, same as the overhead in [11]. Additionally, the tags will be sent to the central unit via control channel which is independent from the communication channel between the devices. Comparing this scheme with other schemes secure against tag pollution attacks, we understand that for the same number of tags, our scheme produces a much lesser communication overhead compared to Dual HMAC [14] and MacSig [12]. Fig. 4 shows the comparison of communication overhead induced by each security scheme (for  $L=8$ ).

## 5 Conclusion

Since the 5G paradigm is yet to be finalized [15], network coding is being considered for harnessing the bandwidth available for wireless communication. Further, the network coded architecture can be considered to meet the high throughput requirements of heterogeneous mobile small cells with low energy requirements. Since the security challenges needs to be addressed beforehand, an SDN based mobile small cell environment supported by network coding is studied in this work, with specific focus on the security issues. More specifically, the paper discusses a message authentication code based security scheme against pollution attacks in the SDN based small cell environment. The performance analysis and it's comparison with other well known security schemes points out that the computational and communication overheads of security scheme can be considerably reduced at the expense of a secure communication channel between the central controller and other nodes.

## References

1. C. Tselios and G. Tsolis, "On QoE-awareness through virtualized probes in 5G networks," in *2016 IEEE 21st International Workshop on Computer Aided Modelling and Design of Communication Links and Networks (CAMAD)*, Oct 2016, pp. 159–164.
2. C. Tselios, I. Politis, M. Tsagkaropoulos, and T. Dagiuklas, "Valuing quality of experience: A brave new era of user satisfaction and revenue possibilities," in *2011 50th FITCE Congress - "ICT: Bridging an Ever Shifting Digital Divide"*, Aug 2011, pp. 1–6.

3. C. Tselios and G. Tsolis, "A Survey on Software Tools and Architectures for Deploying Multimedia-Aware Cloud Applications," in *Lecture Notes in Computer Science: Algorithmic Aspects of Cloud Computing*. Springer International Publishing, 2016, vol. 9511, pp. 168–180.
4. C. Tselios, I. Politis, and S. Kotsopoulos, "Enhancing SDN security for IoT-related deployments through blockchain," in *2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*, Nov 2017, pp. 303–308.
5. J. Rodriguez, A. Radwan, C. Barbosa, F. H. P. Fitzek, R. A. Abd-Alhameed, J. M. Noras, S. M. R. Jones, I. Politis, P. Galotos, 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 *2017 Internet Technologies and Applications (ITA)*, Sept 2017, pp. 329–333.
6. N. Cai and R. W. Yeung, "Secure network coding," in *Proceedings IEEE International Symposium on Information Theory*, 2002, pp. 323–.
7. J. Dong, R. Curtmola, and C. Nita-Rotaru, "Practical defenses against pollution attacks in wireless network coding," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, p. 7, 2011.
8. J. Dong, R. Curtmola, C. Nita-Rotaru, and D. K. Y. Yau, "Pollution attacks and defenses in wireless interflow network coding systems," *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 5, pp. 741–755, Sept 2012.
9. S. Jaggi, M. Langberg, S. Katti, T. Ho, D. Katabi, M. Medard, and M. Effros, "Resilient Network Coding in the Presence of Byzantine Adversaries," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2596–2603, June 2008.
10. T. Ho, M. Medard, 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, Oct 2006.
11. S. Agrawal and D. Boneh, "Homomorphic MACs: MAC-Based Integrity for Network Coding," in *Applied Cryptography and Network Security*, M. Abdalla, D. Pointcheval, P.-A. Fouque, and D. Vergnaud, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 292–305.
12. P. Zhang, Y. Jiang, C. Lin, H. Yao, A. Wasef, and X. Shen, "Padding for orthogonality: Efficient subspace authentication for network coding," in *2011 Proceedings IEEE INFOCOM*, April 2011, pp. 1026–1034.
13. A. Esfahani, G. Mantas, J. Rodriguez, and J. C. Neves, "An efficient homomorphic mac-based scheme against data and tag pollution attacks in network coding-enabled wireless networks," *International Journal of Information Security*, vol. 16, no. 6, pp. 627–639, 2017.
14. A. Esfahani, D. Yang, G. Mantas, A. Nascimento, and J. Rodriguez, "Dual-homomorphic message authentication code scheme for network coding-enabled wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 11, no. 7, p. 510251, 2015.
15. L. T. Bolivar, C. Tselios, D. M. Area, and G. Tsolis, "On the deployment of an open-source, 5g-aware evaluation testbed," in *2018 6th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)*, March 2018, pp. 51–58.