Security Threats in Network Coding-enabled Mobile Small Cells

Reza Parsamehr[1,2], Georgios Mantas[1,3], Ayman Radwan[1], Jonathan Rodriguez[1], José-Fernán Martínez[2]

[1] Instituto de Telecomunicações, Aveiro, Portugal
[2] Universidad Politécnica de Madrid, Spain
[3] Faculty of Engineering and Science, University of Greenwich, UK
{reza, gimantas, aradwan, jonathan}@av.it.pt
jf.martinez@upm.es

Abstract. The recent explosive growth of mobile data traffic, the continuously growing demand for higher data rates, and the steadily increasing pressure for higher mobility have led to the fifth-generation mobile networks. To this end, network-coding (NC)-enabled mobile small cells are considered as a promising 5G technology to cover the urban landscape by being set up on-demand at any place, and at any time on any device. In particular, this emerging paradigm has the potential to provide significant benefits to mobile networks as it can decrease packet transmission in wireless multicast, provide network capacity improvement, and achieve robustness to packet losses with low energy consumption. However, despite these significant advantages, NC-enabled mobile small cells are vulnerable to various types of attacks due to the inherent vulnerabilities of NC. Therefore, in this paper, we provide a categorization of potential security attacks in NC-enabled mobile small cells. Particularly, our focus is on the identification and categorization of the main potential security attacks on a scenario architecture of the ongoing EU funded H2020-MSCA project "SECRET" being focused on secure network coding-enabled mobile small cells.

Keywords: Mobile Small Cells, 5G Communications, Security, Network Coding, D2D Communications.

1 Introduction

The recent explosive growth of mobile data traffic, the continuously growing demand for higher data rates, and the steadily increasing pressure for higher mobility have led to the fifth-generation (5G) of mobile communications. 5G communications target to achieve big data bandwidth, infinite capability of networking and extensive signal coverage to support a plethora of high-quality personalised services to subscribers, while at the same time the capital and operating expenditures (i.e., CAPEX and OPEX) of mobile operators are being reduced. Towards this direction, 5G communications systems will integrate a wide spectrum of enabling technologies [1-5].

Small cells technology is considered as a major 5G enabling technology, as it can enable effective delivery of ubiquitous 5G services in a cost-effective and energy efficient manner. Indeed, mobile small cells can cover the urban landscape by being set up on-demand at any place, and at any time on any device. The mobile small cell hotspots are the vehicle for experiencing a plethora of 5G broadband services at low cost with reduced impact on mobile battery lifetime [6-8].

In addition, Network Coding (NC) technology can be foreseen as a promising solution for the wireless network of mobile small cells to increase its throughput and improve its performance. In fact, NC technology is an emerging communication paradigm that has the potential to provide significant benefits to networks as it can decrease packet transmission in wireless multicast [9, 10], provide network capacity improvement [11], and achieve robustness to packet losses [12] and low energy consumption [13]. However, despite the significant advantages of NC technology, network coding-enabled wireless networks are vulnerable to various types of attacks [12, 14-18]. Based on that and the fact that the security is critical factor for the success of upcoming 5G networks, such as the network coding-enabled mobile small cells, novel security mechanisms against these types of attacks are required [19-22]. Towards this direction, the first step is the identification of the security threats in such networks.

Therefore, in this paper, we provide a categorization of potential security attacks in network coding-enabled mobile small cells due to the inherent vulnerabilities of NC. In particular, our focus is on the identification and categorization of the main potential security attacks on a scenario architecture of the EU funded H2020-MSCA project “SECRET” [23] focused on secure network coding-enabled mobile small cells.

Following the introduction, this paper is organized as follows. In section 2, we provide an overview of the studied scenario architecture which is focused on secure network coding-enabled mobile small cells. In Section 3, a brief overview of the two types of network coding protocols is given. In Section 4, the main categories of potential security attacks in network coding-enabled mobile small cells due to the inherent vulnerabilities of NC are presented. Finally, Section 5 concludes this paper.

2 Scenario Architecture

In this section, we provide the scenario architecture of the EU funded H2020-MSCA project “SECRET” (See Figure 1) which is focused on secure network coding-enabled mobile small cells [23] This scenario architecture consists of a macro cell which is splitted into a number of mobile small cells. Each mobile small cell is controlled by a cluster-head (i.e., hotspot), a mobile device (i.e., mobile node) within the identified cluster of mobile devices that is nominated to play the role of the local radio manager in order to control and maintain the cluster. Moreover, the cluster-heads (i.e., hotspots) of the 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 the cluster-heads (i.e., hotspots) of the different clusters are controlled by a centralized software-defined controller. Finally, the data communication between the mobile devices (i.e., mobile nodes) is established through Device-to-Device (D2D) communications and optimized by network coding 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., Random Linear Network Coding) and traverse multiple devices, over a multi-hop D2D network, before arriving to the DNs, locating at another mobile small cell, where they are decoded. The multi-hop D2D network consists of a number of User Equipments (UEs), such as legitimate mobile nodes, and relay mobile nodes (RNs), as depicted in Figure 1.

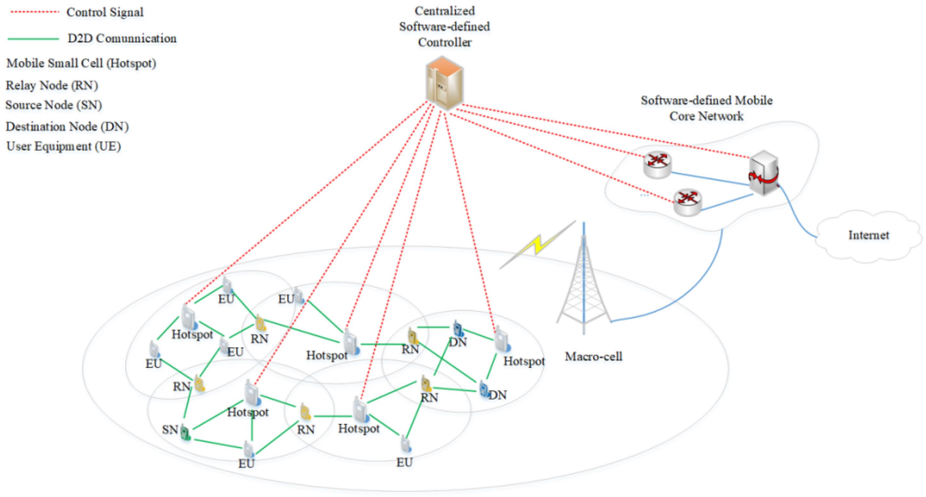

Figure 1. Scenario Architecture

3 Network Coding

Due to low communication bandwidth, packet loss and power consumption constraints, network coding can be a good solution for wireless networks [6, 7]. Network coding methods are generally classified into state-aware network coding protocols and stateless network coding protocols.

In state-aware network coding protocols, each node has partial or full network state information, such as network topology and the packets in the buffer of its neighbours Based on this information, a network code is generated that is decodable by the neighboring nodes. However, the state-aware network coding protocols confront several security issues due to the available knowledge of the network sate information.

On the other hand, the stateless network coding protocols do not rely on the network state information in order to decide when and how to mix the packets at each intermediate node. Thus, the stateless network coding protocols are not affected by dynamically changing topologies. Finally, this kind of network coding protocols are more immune to security threats compared to the state-aware network coding protocols due to their independence of the network state information [11, 12].

4 Security Threats in Network Coding-enabled Mobile Small Cells

In this section, we present the main categories of potential security attacks in network coding-enabled mobile small cells due to the inherent vulnerabilities of NC.

4.1 Eavesdropping

An eavesdropper aims to retrieve sensitive information such as native packets, public keys, private keys, and passwords of other nodes by wiretapping one or several wired links, or overhearing the wireless transmission. In this regard, eavesdroppers neither inject packets nor modify them. They only listen to links to get the essential information that should be kept secret during the communication. Therefore, eavesdropping is known as a passive attack. Eavesdroppers can not only be external nodes but also malicious intermediate nodes. If they are able to access an adequate number of linearly independent combinations of packets, then they can decode the packets and have access to all transmitted information (see Figure 2) [14, 24, 25].

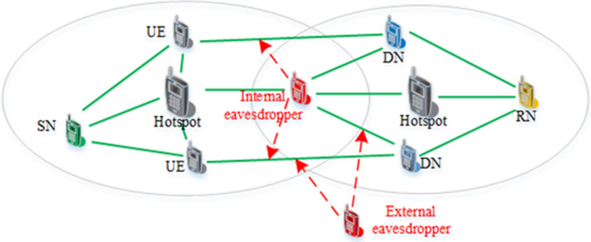

Figure 2. Internal and External Eavesdropping attacker

Eavesdropping attacks are generally classified based on two different views. The first view is based on the level that a node has access to the packets crossing the network and classifies the eavesdropper nodes into three types: i) nice but curious, ii) wiretapping, and iii) worst-case eavesdroppers [25, 26]. Nice but curious nodes are also called non-malicious nodes because they are well behaved in the sense of communication protocols, but they want to obtain some information from the data flows that pass through them. The curious nodes cannot get significant information, because in random linear network coding (RLNC), packets are coded and none of them has access to sufficient number of coded packets. On the other hand, the wiretapping nodes (usually external eavesdroppers) are more capable of accessing the secret information due to their access to subset of communication links (i.e., they have access to more coded packets). Finally, the eavesdropper nodes of the third type are classified as the worst-case node since they have access to all of the transmitted packets. Therefore, in this case, ensuring information confidentiality is not only harder, but also more critical.

The second view is based on the type of the NC protocols (i.e., stateless NC protocols or state-aware NC protocols) [24, 25]. In the case of stateless NC protocols, due to the RLNC properties, eavesdropping attack is less crucial. This is because the eavesdropper is not able to decode the coded packets and obtain native packets until he/she has access to a sufficient number of coded packets. In contrast, in the case of state-aware NC protocols, eavesdropping attack is crucial since the coding is local and each intermediate node decodes packets before recoding them. Thus, the eavesdropper can access native packets.

4.2 Traffic Analysis

Traffic analysis is one of the most common attacks in wireless networks. In traffic analysis attack, the attackers monitor the transmissions in the network in order to extract information about the source and destination of the packets as well as the network topology. In other words, adversaries threat the confidentially of the networks with traffic analysis and monitoring [25, 27]. This threat is crucial in both the state-aware and stateless network coding protocols [24].

4.3 Impersonation

An impersonation attacker sends queries to the victim nodes by using other legitimate node's identity (e.g., MAC or IP address [28]) in order to gain information. State-aware network coding protocols can be affected by this type of attacks due to the fact that these protocols rely on network nodes [14]. In other words, the goal of impersonation attack is to degrade the authenticity property in NC-enabled networks. This attack is a kind of active eavesdropping and sometimes it is the basis for launching further more sophisticated attacks [24].

4.4 Man-in-the-middle

In the Man-in-the-middle attack, the attacker (i.e., a malicious node) lies on a communication link between the sender and the receiver in order to impersonate other nodes and relays received messages by exploiting link spoofing techniques, such as advertising fake links and sending routing control packets, including wrong information (see Figure 3) [24, 29, 30].

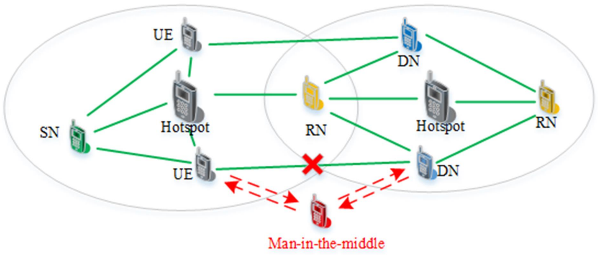

Figure 3. Man-in-the-middle attack.

4.5 Byzantine Fabrication

Byzantine fabrication attack is a severe security threat where an adversary node injects corrupted packets into the network to corrupt other packets based on the nature of packet mixing in network coding schemes [25]. Additionally, this attack can disrupt the routing operation of network in different ways such as forwarding data packets through non-optimal or even invalid routes and generating routing loops (see Figure 4) [14, 24]. This attack is a threat to both stateless and state-aware network coding protocols. In state-aware network coding protocols, packet headers normally include topology states and routing information, and thus the attackers can send wrong information to nodes about the state and neighbors' information. Besides, in stateless network coding protocols, headers normally include needed decoding vectors that attackers can change [25].

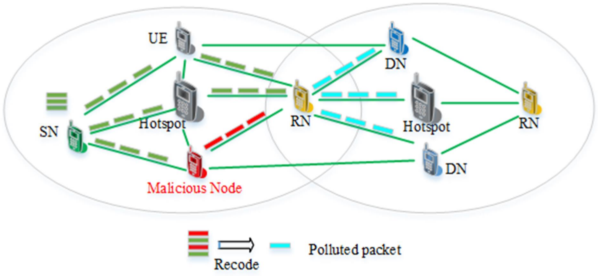

Figure 4. Byzantine Fabrication attack.

4.6 Byzantine Modification (Pollution)

In a byzantine modification attack, adversary aims to make some changes (i.e., invalid coding operations) to data in transit and threat the integrity of the packets in the networks [29]. They inject corrupted packets or modify them. There are a lot of attacks which use this technique to threat the networks, such as wormhole, black hole, selective forwarding and dropping attack, man-in-the-middle, link spoofing, routing attacks and repudiation [24]. These attacks can be considered as special types of Byzantine modification attacks. In stateless network coding, the adversary injects or modifies packets in transit, whereas in state-aware network coding the adversary injects or modifies not only packets in transit but also state information such as topology information and buffer state [14, 26].

4.7 Byzantine Replay

In Byzantine replay attack the malicious nodes or SN can reuse coded packets with the same logical identifier that were authenticated previously (e.g., old coded packets that were previously stored on compromised nodes and had successfully passed the integrity verification. Due to sending these old messages, the network resources are wasted and eventually throughput rate is degraded [31, 32]. If a malicious or compromise node is able to find and reuse old coded packets, the data decoding condition could be broken, because they are linearly dependent with other coded blocks that are currently stored (see Figure 5). Replay attack can reduce network coding throughput, wasting resources and processing time in both stateless and state-aware network coding protocols by injection packets which are repeated into the information flow [14].

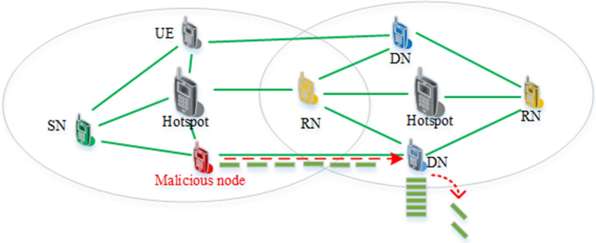

Figure 5. Byzantine Reply attack.

4.8 Wormhole

In this attack two or more malicious nodes collaborate and create a tunnel between two nodes (see Figure 6). Then, they persuade the neighbor nodes that two side of tunnel are in the same range. Afterwards, these wormhole attackers can record packets and retransmit them through the tunnel. Wormhole attack can have more severe impact on state-aware NC protocols (e.g., disruption of the route discovery process) compared to its impact on stateless protocols [14, 33].

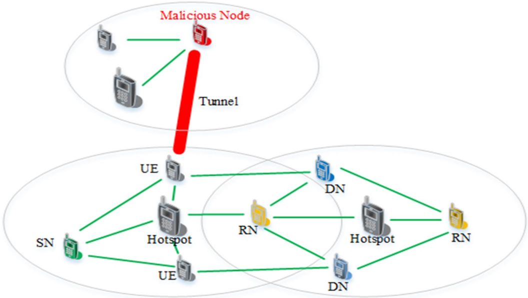

Figure 6. Wormhole attack.

4.9 Black hole

The attacker exploits routing protocols to advertise itself as a valid and the shortest path to a destination. In this regard, the nodes are convinced to use this path to send data packets towards that destination. Hence, data packets can be intercepted/eavesdropped or the routing operations simply can be denied (i.e., black-hole attack) that decrease the network performance. This attack can reduce performance of the network in both state-aware and stateless protocols [24, 34].

4.10 Entropy Attack

In entropy attacks, the attacker creates packets containing information already known by the systems (i.e., non-innovative packets). In particular, the adversary node creates a non-innovative coded packet that is a non-random linear combination of coded packets so that the coded packet is linearly dependent with the coded packets stored at downstream node. The valid but linearly dependent coded packet wastes resources as it does not provide any useful information to the receivers so that they can decode the original packets [31]. Furthermore, the authors in [31] have classified the entropy attacks into two main categories which require deferent capabilities from an attacker: a) Local entropy attack: the attacker generates non-innovative coded packets to the local neighboring nodes; b) Global entropy attack: the attacker generates coded packets that are seemingly innovative to local neighboring nodes but are non-innovative to at least one distant downstream node.

4.11 Denial of Service (DOS):

In Denial of Service (DoS) attack, the attacker attempts to make the resources of a system unavailable to the legitimate users, Actually, the attacker targets the availability of the system [14]. For example, in a network coding-enabled network, the adversary can send a lot of requests, such as packet processing and forwarding, to the victim in order to deplete its resources [24]. Moreover, it is worthwhile to mention that there are different types of DoS attacks at different layers that affect differently the network. Thus, DoS attacks include the following main types of attacks: jamming and tempering at the physical layer, collision and exhaustion at the link layer, black holes and routing table overflow at the network layer, SYN flooding and de-synchronization at the transport layer, and finally failure in the web services at the application layer [34]. Finally, in NC state-aware schemes, a malicious node can easily perform a DoS attack by flooding its neighbours with a high volume of corrupted packets or even legitimate packets but old and repetitive packets [14].

5 Conclusion

In this paper, we provided a categorization of potential security attacks in network coding-enabled mobile small cells due to the inherent vulnerabilities of NC. More precisely, we focused on the identification and categorization of the main potential security attacks on a scenario architecture of the EU funded H2020-MSCA project “SECRET” which is based on secure network coding-enabled mobile small cells.

Acknowledgments

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

References

1. Wang, C.-X., et al., *Cellular architecture and key technologies for 5G wireless communication networks.* IEEE Communications Magazine, 2014. **52**(2): p. 122-130.

2. Chih-Lin, I., et al., *Toward green and soft: a 5G perspective.* IEEE Communications Magazine, 2014. **52**(2): p. 66-73.

3. Bangerter, B., et al., *Networks and devices for the 5G era.* IEEE Communications Magazine, 2014. **52**(2): p. 90-96.

4. Sucasas, V., G. Mantas, and J. Rodriguez, *Security Challenges for Cloud Radio Access Networks.* Backhauling/Fronthauling for Future Wireless Systems, 2016: p. 195-211.

5. Mantas, G., et al., *Security for 5G communications.* Fundamentals of 5G Mobile Networks, John Wiley & Sons- 2015: p. 207-220.

6. Gupta, A. and R.K. Jha, *A survey of 5G network: Architecture and emerging technologies.* IEEE Access, 2015. **3**: p. 1206-1232.

7. Chou, S.-F., et al. *Mobile small cell deployment for next generation cellular networks*. in *Global Communications Conference (GLOBECOM), 2014 IEEE*. 2014. IEEE.

8. Saghezchi, F., et al., *Drivers for 5G.* Fundamentals of 5G Mobile Networks, 2015: p. 1-27.

9. Katti, S., et al. *XORs in the air: Practical wireless network coding*. in *ACM SIGCOMM computer communication review*. 2006. ACM.

10.Chen, Y.-J., et al., *Topology-Aware Network Coding for Wireless Multicast.* IEEE Systems Journal, 2018.

11.Ahlswede, R., et al., *Network information flow.* IEEE Transactions on information theory, 2000. **46**(4): p. 1204-1216.

12.Ho, T. and D. Lun, *Network coding: an introduction*2008: Cambridge University Press.

13.Wu, Y., P.A. Chou, and S.-Y. Kung, *Minimum-energy multicast in mobile ad hoc networks using network coding.* IEEE Transactions on communications, 2005. **53**(11): p. 1906-1918.

14.Esfahani[1], A., et al., *Towards Secure Network Coding-Enabled Wireless Sensor Networks in Cyber-Physical Systems.*Cyber Physical Systems: From Theory to Practice. CRC Press. 2015: p. 395-414.

15.Esfahani, A., et al. *A null space-based MAC scheme against pollution attacks to Random linear Network Coding*. in *Comm Workshop (ICCW), 2015 IEEE Int. Conf. on*. 2015. IEEE.

16.Esfahani, A., et al. *An improved homomorphic message authentication code scheme for RLNC-enabled wireless networks*. in *Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), 2014 IEEE 19th International Workshop on*. 2014. IEEE.

17.Esfahani, A., et al. *Analysis of a Homomorphic MAC-based scheme against tag pollution in RLNC-enabled wireless networks*. in *Computer Aided Modelling and Design of Communication Links and Networks (CAMAD), 2015 IEEE 20th International Workshop on*. 2015. IEEE.

18.Yang, D., et al. *Jointly padding for subspace orthogonality against tag pollution*. in *Comp. Aided Mod. and Des. of Comm. Links and Netw. (CAMAD), 2014 IEEE 19th Int Workshop on*. 2014. IEEE.

19.Esfahani, A., et al., *Dual-homomorphic message authentication code scheme for network coding-enabled wireless sensor networks.* Int. J. of Distributed Sensor Networks, 2015. **11**(7).

20.Esfahani, A., et al., *An efficient homomorphic MAC-based scheme against data and tag pollution attacks in network coding-enabled wireless networks.* International Journal of Information Security, 2017. **16**(6): p. 627-639.

21.Esfahani, A., G. Mantas, and J. Rodriguez, *An efficient null space-based homomorphic MAC scheme against tag pollution attacks in RLNC.* IEEE Comm. Letters, 2016. **20**(5): p. 918-921.

22.Esfahani, A., et al., *An efficient MAC-based scheme against pollution attacks in XOR network coding-enabled WBANs for remote patient monitoring systems.* EURASIP Journal on Wireless Communications and Networking, 2016. **2016**(1): p. 113.

23.*SEcure Network Coding for Reduced Energy nexT generation Mobile Small cells*. H2020-MSCA-ITN-2016-722424 01 January 2017 - 31 December 2020; Available from: http://h2020-secret.eu/index.html

24.Talooki, V.N., et al., *Security concerns and countermeasures in network coding based communication systems: A survey.* Computer Networks, 2015. **83**: p. 422-445.

25.Ostovari, P. and J. Wu, *Towards network coding for cyber-physical systems: Security challenges and applications*2017: Wiley.

26.Lima, L., et al., *Network coding security: Attacks and countermeasures.* arXiv preprint arXiv:0809.1366, 2008.

27.Fan, Y., et al. *An efficient privacy-preserving scheme against traffic analysis attacks in network coding*. in *INFOCOM 2009, IEEE*. 2009. IEEE.

28.Wu, B., et al., *A survey of attacks and countermeasures in mobile ad hoc networks*, in *Wireless network security*2007, Springer. p. 103-135.

29.Jawandhiya, P.M., et al., *A survey of mobile ad hoc network attacks.* International Journal of Engineering Science and Technology, 2010. **2**(9): p. 4063-4071.

30.Dong, J., et al., *Pollution attacks and defenses in wireless interflow network coding systems.* IEEE Transactions on Dependable and Secure Computing, 2012. **9**(5): p. 741-755.

31.Newell, A.J., R. Curtmola, and C. Nita-Rotaru. *Entropy attacks and countermeasures in wireless network coding*. in *Proc of the 5th ACM conf on Sec.& Priv in Wireless and Mobile Networks*. 2012. ACM.

32.Chen, B., et al. *Remote data checking for network coding-based distributed storage systems*. in *Proc. of the 2010 ACM workshop on Cloud computing security workshop*. 2010. ACM.

33.Chiu, H.S. and K.-S. Lui. *DelPHI: wormhole detection mechanism for ad hoc wireless networks*. in *Wireless pervasive computing, 2006 1st international symposium on*. 2006. IEEE.

34.Mishra, A. and K.M. Nadkarni. *Security in wireless ad hoc networks*. in *The handbook of ad hoc wireless networks*. 2003. CRC Press, Inc.