Poisoning Bearer Context Migration in O-RAN 5G Network

Sanaz Soltani *(Student Member, IEEE)*, Mohammad Shojafar *(Senior Member, IEEE)*, Alessandro Brighente *(Member, IEEE)*, Mauro Conti *(Fellow, IEEE)* and Rahim Tafazolli *(Senior Member, IEEE)*

***Abstract*—Open Radio Access Network (O-RAN) improves the flexibility and programmability of the 5G network by applying the Software-Defined Network (SDN) principles. O-RAN defines a near-real time Radio Intelligent Controller (RIC) to decouple the RAN functionalities into the control and user planes. Although the O-RAN security group offers several countermeasures against threats, RIC is still prone to attacks. In this letter, we introduce a novel attack, named *Bearer Migration Poisoning (BMP)*, that misleads the RIC into triggering a malicious bearer migration procedure. The adversary aims to change the user plane traffic path and causes significant network anomalies such as routing blackholes. BMP has a remarkable feature that even a weak adversary with only two compromised hosts could launch the attack without compromising the RIC, RAN components, or applications. Based on our numerical results, the attack imposes a dramatic increase in signalling cost by approximately 10 times. Our experiment results show that the attack significantly degrades the downlink and uplink throughput to nearly 0 *Mbps*, seriously impacting the service quality and end-user experience.**

***Index Terms*—5G, Software-Defined Network (SDN), Open RAN (O-RAN), O-RAN Security, Bearer Context Migration.**

I. Introduction

SOFTWARE-Defined Radio Access Network (SD-RAN) applies the Software-Defined Network (SDN) principles to the cellular network. SD-RAN provides programmability for radio networks by decoupling the User Plane (UP) and Control Plane (CP). 5G RAN, called *5G New Radio* (NR) [1], requires the control capability and programmability of the SD-RAN to achieve maximum flexibility. An industry consortium has adapted SD-RAN principles to 5G NR and created an open, intelligent architecture known as *Open RAN (O-RAN)* [2], [3]. The O-RAN architecture consists of a Radio Unit (RU) located near the antenna, the Distributed Unit (DU) and the Control Unit (CU) as part of the 5G base station. The CU is separated into the Control Plane (CU-CP), and the User Plane (CU-UP). A Near-Real Time RAN Intelligent Controller (Near-RT RIC) is a software-based platform, similar to a SDN controller, that provides programmability and allows network applications to communicate with RAN components. Near-RT RIC runs applications that provide RAN functionalities, known as *xApps*. Open Networking Foundation (ONF) builds an open source project [2] on the microservices-based ONOS (μONOS) controller to develop an SD-RAN that complies with the 3rd Generation Partnership Project (3GPP) [4] standard and follows the O-RAN specification [5].

S. Soltani, M. Shojafar and R. Tafazolli are with 5GIC & 6GIC, University of Surrey, Guildford, UK email: {s.soltani, m.shojafar, r.tafazolli}@surrey.ac.uk. A. Brighente and M. Conti are with University of Padua, Italy email: {alessandro.brighente, mauro.conti}@unipd.it

Excellent academic researches worked on O-RAN in terms of conceptual architecture such as SoftRAN [6], FlexRAN [7], and RIC [3]. They have achieved good results in radio resource optimisation and resource allocation problems in the 5G network [8]. However, the advantages of softwarization in O-RAN would become challenging without appropriate countermeasures against attacks. The O-RAN Alliance has formed a Security Focus Group (SFG) to analyse and address security concerns specific to the O-RAN [9], [10]. They conducted a high level risk assessment on vulnerabilities which could be exploited through attacks against the O-RAN components [11], RIC, and *xApps* [12], [13]. However, several security concerns are still not fully addressed in their studies. As far as we know, besides the specifications published by the SFG, there is no literature contribution on the security of O-RAN.

For the first time in the literature, we focus on the attack against bearer context management functions in O-RAN, hoping to raise academic and industry attention to the security of O-RAN. A bearer context refers to a set of signalling information communicated over the E1 interface, i.e. the interface between CU-CP and CU-UP [14]. The purpose of establishing a bearer context is to prepare required resources and information for forwarding user plane services between the CU-UP, the associated DU, and the User Equipment (UE) [4]. To this end, the CU-CP uses bearer context management functions. For example, CU-CP initiates the bearer context setup procedure when a UE initiates an access request, and the bearer context release procedure when a UE detaches or disconnects [15]. Another example is an inter-gNodeB (gNB) handover where CU-CP triggers the bearer context migration procedure to change the user plane traffic from a source CU-UP to the target CU-UP [4]. The Near-RT RIC platform is capable of triggering bearer context management functions [16]. However, this capability makes the O-RAN prone to more security threats. By imposing our proposed attack, an adversary can mislead the Near-RT RIC to trigger a malicious bearer migration procedure, which changes the user plane traffic path and causes signalling overhead.

Motivated by mentioned challenges, we introduce a novel attack, named *Bearer Migration Poisoning (BMP)*, that poisons the Near-RT RIC perception to release a valid context bearer between DU and CU-UP and then establish a new bearer context toward the target CU-UP. The attack could cause network anomalies such as routing blackholes, impacting the overall performance of O-RAN. The attack also dramatically increases signalling costs, thereby growing network latency and wasting radio resources. Consequently, the BMP attack highly impacts the user experience, leading to customer churn and revenue loss for the mobile network operators. The following are our

key contributions to this letter:

- We introduce Bearer Migration Poisoning (BMP) attack in the emulated software defined-RAN. It can be imposed even by the adversary with limited resources like monitoring platforms or computers connected to DU or CU-UP. We are the first to identify the attack in O-RAN to our knowledge.
- We analyse the bearer migration procedures and calculate the signalling cost for both normal and attack scenarios using our designed signalling flow diagram.
- We investigate the effect of the BMP attack on network performance. Our results show that downlink and uplink throughput dramatically decrease to $\approx 0Mbps$, impacting service delivery to users in the area served by RU.

The rest of the letter is as follows. In Section II, we present the threat model and explain how the BMP attack works. In Section III, the signalling cost is carefully calculated, and the impact of the attack on network performance is measured. Section IV presents the conclusion and future works.

II. Poisoning Bearer Context Migration

This section describes the softwarisation principles applied to O-RAN architecture (see Section II-A). Then, we define our threat model and explain the attack methodology in Sections II-B and II-C, respectively.

A. Softwarisation in O-RAN architecture

Fig. 1 presents the architecture of O-RAN which complies with 3GPP and SD-RAN definitions [3]. RAN components, including DU, CU-UP and CU-CP, can be deployed as Virtual Network Function (VNF) or Physical Network Function (PNF). Fronthaul and midhaul are packet-based networks which use shared links [17] and are managed by the routing *xApps*. The *xApp* can subscribe to one or more RAN functions and specify triggering events. For example, the routing management *xApp* can subscribe to receive notifications for any updates on RAN topology. A Non-Real Time RIC (Non-RT RIC) is embedded in the Service and Management Orchestration (SMO) platform and hosts network applications, i.e., *rApp* to provide higher layer optimisation and policy management in O-RAN. For the sake of simplicity, in the rest of the letter, we use RIC to refer to the Near-RT RIC.

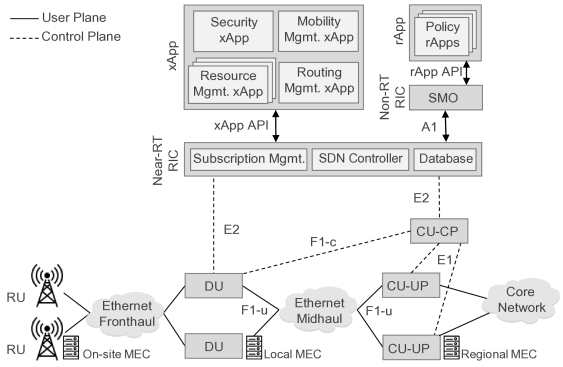


Fig. 1: O-RAN architecture

CU-CP and RIC can follow an event-driven approach for the control plane procedure. For example, when RIC detects that an event occurs, it sends a `RIC CONTROL REQUEST` message toward the CU-CP to initiate the associated procedure [16]. Also, Mobile Edge Computing (MEC) servers can be located near RU, DU, and CU-UP to provide computing capabilities close to the end-user and reduce service latency. CU-CP uses several bearer context management functions to set up, release, or modify the bearer context between DU and CU-UP over the F1 interface. For example, Fig. 2 demonstrates the procedure of changing CU-UP, triggered by CU-CP defined in 3GPP [4]. First, CU-CP initiates `BEARER CONTEXT SETUP` message to establish a new bearer context between target CU-UP and DU. The CU-CP then notifies the DU by `F1 BEARER MODIFICATION` message to change the F1 interface configuration. Finally, CU-CP sends `BEARER CONTEXT RELEASE` message to release the old bearer context. As a result, CU-CP changes the bearer context from the source CU-UP to the target CU-UP for a single DU.

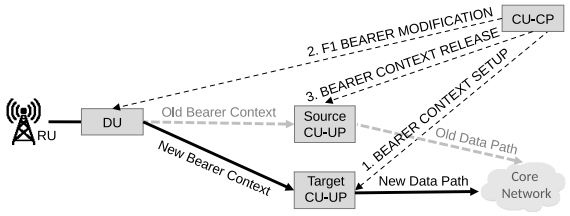


Fig. 2: Bearer context migration procedure

RIC uses a database containing configurations and information relating to RAN components, such as bearer configuration, UE related identities, and network topology information. Based on SD-RAN principles, RIC acts like an SDN controller and RAN components such as DU, CU-UP, and routing devices in the midhaul serve as SDN-based switches. RIC can provide network topology maintenance for RAN components in the data plane over the E2 interface. Fig. 3 illustrates an example of the link discovery process, including one DU, one CU-UP and several routers in the midhaul. In this way, first, the controller creates and sends the Link Layer Discovery Protocol (LLDP) messages to all mentioned entities. In the second step, once each entity has received the LLDP packets, it will broadcast the packets from each of its ports. In the third step, the destination entity forwards the received LLDP to the RIC. Finally, the controller discovers the existing links between different entities. The procedure is repeated at regular periodic intervals.

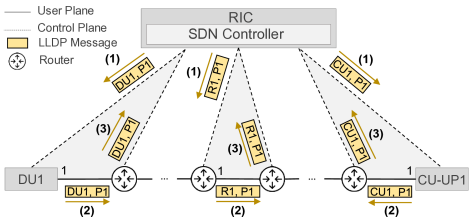


Fig. 3: Link discovery process between DUs, CU-UPs, and routers

B. Threat model

In line with existing security studies [18], [19], we assume that the adversary can use viruses, trojans and malware infection tools to compromise a host, or even in a worse case, the adversary can be an insider. In our proposed attack, we suppose that the adversary can manipulate two hosts, such as

MEC servers, monitoring platforms, or other systems that are directly connected to the DU and CU-UP. The adversary may also provide an out-of-band channel, for example, via a wired or wireless connection, between two hosts. With the help of two malicious hosts that communicate through an out-of-band channel, the adversary can relay the packets between DU and CU-UP, which are a great distance apart. A dual-homed single host, which is directly connected to DU and CU-UP, could be used alternatively.

We call our attack Bearer Migration Poisoning (BMP). The adversary aims to poison the RIC perception into believing that a bearer context migration procedure needs to be triggered. This misjudgement releases the valid bearer context, and a new one is set up towards the incorrect CU-UP using malicious hosts. BMP causes network anomalies such as routing blackholes by misleading data plane traffic paths. As a result, the cell performance is significantly decreased, impacting the delivery of services to UEs in the area served by the RU.

C. Attack scenario

We describe our attack scenario using a simplified O-RAN topology with one DU, two CU-UPs, two MEC servers as hosts, and a few routers in the midhaul network, as shown in Fig. 4. DU, CU-UPs, and CU-CP can be VNF and/or PNF. An example of deployment of entities in the attack can be the CU-CP and CU-UPs deployed as VNFs in edge cloud and DUs as PNF in regional sites. We assume the adversary has compromised two MEC hosts, i.e., h_1 and h_2, connected to DU_1 and $CU\text{-}UP_2$, respectively. The adversary on h_1 continuously monitors the port connected to the DU_1, i.e., port 1 in this scenario. Fig. 5 presents the signalling flow diagram of the proposed BMP attack scenario. In this diagram:

- First, RIC sends LLDP packet towards DU_1. As soon as DU receives the LLDP packet, it broadcasts the message from its ports. The adversary on h_1 receives the LLDP packet and then transfers it toward h_2 over the out-of-band channel. The compromised h_2 forwards the relayed LLDP packet to the $CU\text{-}UP_2$, which returns the packet to the RIC (see red malicious messages in Fig. 5). Receiving the LLDP packet from $CU\text{-}UP_2$ tricks the RIC into adding the fabricated link between DU_1 and $CU\text{-}UP_2$ as shown by the dashed red line in Fig. 4. This step is motivated by [18], [19] which is a link fabrication attack (see signalling messages 1-5 in Fig. 5).
- Second, since the routing *xApp* is subscribed to obtain new updates on radio topology, it receives a notification from RIC, i.e., `Topology Update Report`, containing information about the newly added link. The shortest path algorithm, which is widely used in routing, selects the fabricated link because it is shorter than other links between DU_1 and $CU\text{-}UP_2$. Then, the *xApp* sends `Path Update Request` message along with new path information towards RIC (see signalling messages 6-9 in Fig. 5).
- Third, upon detecting the path update event, RIC sends a `RIC Control Request` message towards the CU-CP to initiate the associated bearer context procedure (see signalling message 10 in Fig. 5).
- Finally, CU-CP triggers the change of CU-UP procedure upon receiving the control request from the RIC (see signalling message 11-20 in Fig. 5). Specifically, CU-CP released the bearer context between DU_1 and $CU\text{-}UP_1$ and established a new bearer context between DU_1 and $CU\text{-}UP_2$ as discussed in Section II-A and shown in Fig. 2.

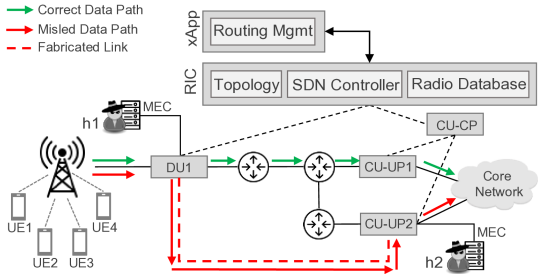


Fig. 4: An example topology for BMP attack scenario

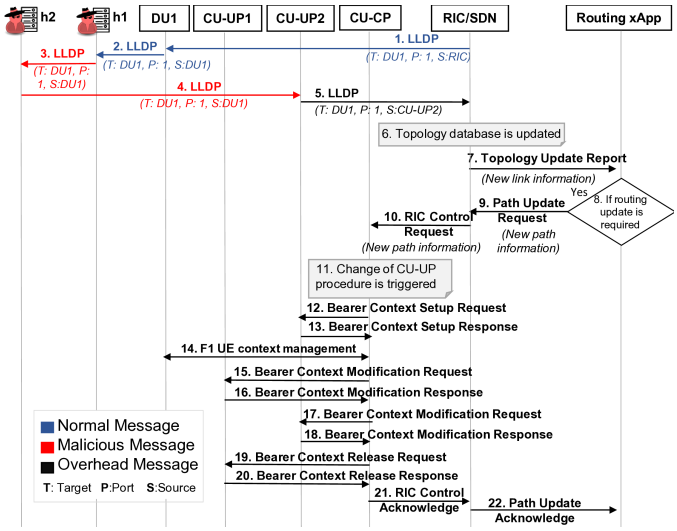


Fig. 5: The impact of BMP attack on 3GPP signalling flow

Migrating bearer context from $CU\text{-}UP_1$ to $CU\text{-}UP_2$ leads to forwarding the user traffic over the fabricated link (see the solid red arrows in Fig. 4), impacting the performance on cells served by the RU. The BMP attack may trigger an alert by a network monitoring system that several degradations in the O-RAN Key Performance Indicators (KPIs) have occurred. However, determination of the root cause is left to the operators and may require a follow-up investigation. In addition, this notification does not interrupt the ongoing attack. It is important to note that the message authentication mechanism is also ineffective when facing this sort of relay attack. A deep inspection and analysis of network behaviour and system logs are required to detect the attack. It might even require either a fundamental redesign of the bearer context migration procedure or patching the RIC for this vulnerability to provide a comprehensive defence.

III. Performance Evaluation

In this section, we analyse the overall signalling cost for attack-free and under our attack environments. In addition, we report the impact of the BMP attack on network performance.

A. Signalling cost analysis

In this letter, the signalling cost is the signalling overhead caused in attack-free and under-attack networks. The cost is

derived from exchanged messages between involved components, including DU, CU-UP, CU-CP, RIC and *xApp*, as shown in Fig. 5. Table I lists the parameters used to calculate the cost. Eq. (1) calculates the signalling cost as follows:

$$\mathbf{c} = \mathbf{N} \times \mathbf{s}, \tag{1}$$

where $\mathbf{c}$ is a vector with size 2×1 elements, presenting the average signalling cost for normal and attack scenarios. $\mathbf{N}$ is a matrix with size 2×5 elements, where each row presents the number of times each signalling cost listed in Table I will be involved in normal or attack scenarios. In addition, $\mathbf{s}$ is a vector with size 5×1, presenting the actual value of each signalling cost as defined using Eq. (2).

$$\mathbf{s^T} = \left[c_1, c_2, c_3, c_4, c_5\right]. \tag{2}$$

TABLE I: Signalling cost parameters

Message type	**Message number in Fig. 5**	**Message cost**
LLDP	1, 2, 5	c_1
Topology Update Request	7	c_2
Path Update Request/ Response	9, 22	c_3
RIC Control Request/ Response	10, 21	c_4
Bearer Context Setup/ Modification/ Release Request/ Response	12, 13, 14, 15, 16, 17, 18, 19, 20	c_5

Let n be the number of fabricated links created by the adversary in the network (see Section II-C). We compute the matrix $\mathbf{N}$ based on Fig. 5 and using Eq. (3). So, we have

$$\mathbf{N} = \begin{bmatrix} 2 & 0 & 0 & 0 & 0 \\ 2+n & 1 & 2 & 2 & 9n \end{bmatrix}. \tag{3}$$

A LLDP message is sent from RIC to DU_1 and then from DU_1 to h_1. In the attack-free network, upon receiving the LLDP message, h_1 drops it. Only two LLDP messages are exchanged (see normal blue messages in Fig. 5). However, under the attack, several 3GPP and O-RAN defined procedures are triggered, as we discussed in Section II-C. Specifically, the LLDP message and all bearer context messages, labelled with numbers 5 and 12-20 in Fig. 5, are sent n times. Hence, the cost is calculated as:

$$\mathbf{c} = \begin{bmatrix} 2c_1 \\ (2+n)c_1 + c_2 + 2c_3 + 2c_4 + 9nc_5 \end{bmatrix}. \tag{4}$$

The key point is that the result of the conditional statement in step 8 of signalling flow (see Fig. 5) could change the number of exchanged messages and, consequently, the signalling cost. The conditional statement checks whether the new link could change the current traffic path based on routing policy. We assume that the conditional statement is true with the average rate λ, $0 \leq \lambda \leq 1$. We call λ the bearer migration rate because for n added fabricated links, λ links meet the requirement of the conditional statement and then trigger the bearer migration procedure. However, the remained links, i.e., $1-\lambda$ links, can not satisfy the requirement. Then, the signalling cost for n fabricated links with bearer migration rate λ is calculated as:

$$\tilde{\mathcal{C}}\left(n, \lambda\right) = \begin{cases} 2c_1, & n = 0, \\ \lambda\tilde{\mathcal{C}}(n,1) + (1-\lambda)\tilde{\mathcal{C}}(n,0), & n \neq 0, 0 \leq \lambda \leq 1, \end{cases} \tag{5}$$

where

$$\tilde{\mathcal{C}}(n,1) = (2+n)c_1 + c_2 + 2c_3 + 2c_4 + 9nc_5, \tag{6a}$$

$$\tilde{\mathcal{C}}(n,0) = (2+n)c_1 + c_2. \tag{6b}$$

According to [20], we consider the signalling cost based on the latency required to send or process the signalling messages, such as the coding and decoding process. For simplicity, we assume that different signalling messages have the same length of m bits on average. Let t_e be the time it takes for every bit of information to be exchanged between two entities. Additionally, the processing time for each message on a single entity is equal to t_p. Then, the signalling cost is calculated as:

$$\tilde{\mathcal{C}}\left(n, \lambda\right) = \begin{cases} 2(mt_e + t_p), & n = 0, \\ \lambda(7+10n)(mt_e + t_p) & \\ +(1-\lambda)(3+n)(mt_e + t_p), & n \neq 0, 0 \leq \lambda \leq 1. \end{cases} \tag{7}$$

We consider a constant delay of $1ms$ for t_e and t_p and the length of 64 bytes for each signalling message. Fig. 6 illustrates the average signalling cost versus average bearer migration rate λ. The results show that, as expected, the signalling cost increases with λ where it reaches $\approx 55s$ for $\lambda = 1$ and $n = 10$. Similarly, as the number n increases, the signalling cost also increases. It can be seen when comparing the cost for the attack-free network, i.e., $n = 0$, with the under-attack network, i.e., $n > 0$. For example, for $n = 1$ and $n = 10$, the signalling cost grows ≈ 10 and ≈ 50 times compared with attack-free network. The cost significantly wastes radio resources and increases network latency in gNBs.

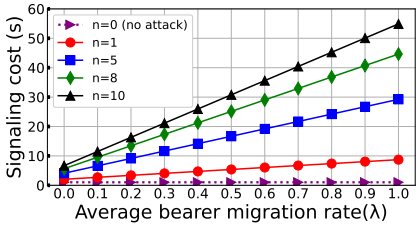


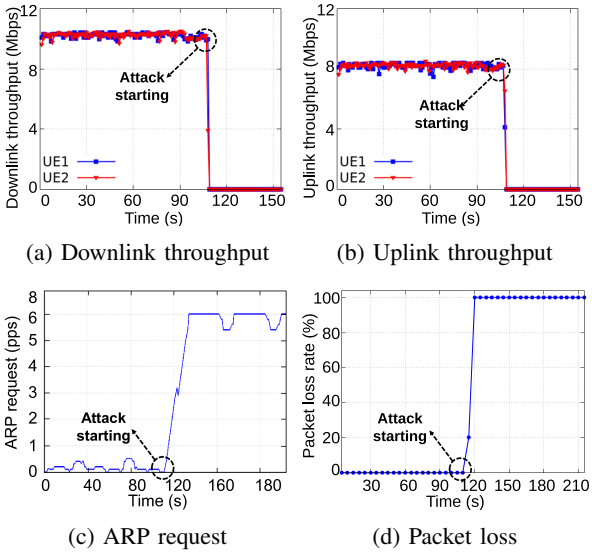
Fig. 6: Impact of BMP attack on signalling cost, for $t_e = 1ms$, $t_p = 1ms$, $m = 64$ bytes and different number of fabricated link, n.

B. Effectiveness of the attack

We have carried out our simulation of the network topology in Fig. 4 with the help of Mininet and Floodlight controller [21]. The reason is that the available tools, including SD-RAN [2] and srsRAN [22], can not simulate DU and CU as two separate modules at present. As far as we know, the srsRAN project is in progress to implement all O-RAN components. We suppose that all links have 5 milliseconds (ms) of latency, and the bandwidth of our experimental network is equal to $10Mbps$ and $8Mbps$ for downlink and uplink, respectively. We also install the shortest path routing *xApp* on RIC to minimise the latency of user traffic. Two compromised hosts connected to DU_1 and CU-UP_2 are considered as MEC servers. Hosts communicate over an out-of-band channel with a $10ms$ latency.

Fig. 7 shows the impact of the BMP attack on network performance. The downlink and uplink throughput of UE_1 and

UE_2 under the attack are monitored and presented in Fig. 7(a) and 7(b), respectively, where the adversary started the attack at time 110 second (s). We generate the UDP packets via the `iperf` command to simulate the user traffic for measuring the network throughput before and after the attack. During the normal execution of the network, i.e., the time interval between $0s$ and $110s$, we forward the traffic toward CU-UP_1 based on the shortest path routing policy. The maximum throughput for UE_1 and UE_2 achieved are $\approx 10Mbps$ and $\approx 8Mbps$ for downlink and uplink, respectively.



(a) Downlink throughput (b) Uplink throughput

(c) ARP request (d) Packet loss

Fig. 7: BMP attack impacts on network performance

Upon imposing the BMP attack at time $110s$, the throughput graphs drop to $0Mbps$. The reason is that our attack misleads the RIC to migrate the bearer from CU-UP_1 toward CU-UP_2 and then reroute the user traffic toward the fabricated link, which does not genuinely exist. In this case, no packets could be sent from DU toward the network as there is no real link between DU and CU-UP_2. As a result, a blackhole is created in the network, which causes a growth in the number of ARP requests, as shown in Fig. 7(c). In addition, Fig. 7(d) demonstrates the packet loss rate where the `ping` command is used to generate a high volume of traffic toward the network. The packet loss rate is calculated every $5s$ on user traffic, where it upsurges to 20% and then 100% upon imposing the attack. The reason for the high packet loss is that the BMP attack misguided the traffic toward the malicious path where there is a fake connection between DU and CU-UP_2. Thus, all user traffic will be dropped in DU.

The results above show that the user experience for call and data service is highly impacted due to our BMP attack.

IV. Conclusions and Future Remarks

In this letter, we introduced a novel attack, named *Bearer Migration Poisoning (BMP)*, to raise researcher awareness of O-RAN security issues. In this attack, the adversary seeks to poison the RIC perception by making it believe that a bearer context migration procedure needs to be initiated. Then, we calculate the average signalling cost using our designed signalling message flow diagram for attack-free and under-attack networks. Our signalling analysis demonstrates that the BMP attack causes a dramatic increase in the signalling cost. The cost can grow by increasing the number of fabricated links and the bearer migration rate. Our network performance evaluation shows that the BMP attack leads to catastrophic drops in throughput and a sharp increase in packet loss rate due to creating the blackhole in the network. In future work, we plan to find a countermeasure to detect the attack and mitigate the risk of user service drop. A possible solution could leverage the packet inspection technique to gain insight into exchanged messages between the RIC, CU-CP and *xApp*. We also plan to deploy it in a real O-RAN environment.

References

[1] E. Dahlman, S. Parkvall, and J. Skold, *5G NR: The next generation wireless access technology*. Academic Press, 2020.

[2] O. Sunay *et al.*, "ONF's software-defined RAN platform consistent with the O-RAN architecture," Open Networking Foundation, 2020. [Online]. Available: https://opennetworking.org/wp-content/uploads/2020/08/SD-RAN-v2.0.pdf

[3] B. Balasubramanian *et al.*, "RIC: A RAN intelligent controller platform for AI-enabled cellular networks," *IEEE Internet Computing*, vol. 25, no. 2, pp. 7–17, 2021.

[4] 3GPP, "NG-RAN: Architecture description," 3rd Generation Partnership Project (3GPP), Tech. Spec. (TS) 38.401,version 17.1.1, 2022.

[5] O.-R. SFG, "O-RAN-Architecture-Description," O-RAN Alliance, Tech. Spec. (TS) ,version 06.00, 2022.

[6] A. Gudipati, D. Perry, L. E. Li, and S. Katti, "SoftRAN: Software defined radio access network," in *2nd ACM HotSDN workshop*, 2013, pp. 25–30.

[7] X. Foukas, N. Nikaein, M. M. Kassem, M. K. Marina, and K. Kontovasilis, "FlexRAN: A flexible and programmable platform for software-defined radio access networks," in *12th ACM CoNEXT*, 2016, pp. 427–441.

[8] E. Amiri, N. Wang, M. Shojafar, and R. Tafazolli, "Optimizing Virtual Network Function Splitting in Open-RAN Environments," in *IEEE 47th LCN*. IEEE, 2022, pp. 422–429.

[9] O.-R. SFG, "O-RAN Security Requirements Specifications," O-RAN Alliance, Tech. Spec. (TS) ,version 03.00, 2022.

[10] S. Soltani, M. Shojafar, R. Taheri, and R. Tafazolli, "Can Open and AI-enabled 6G RAN Be Secured?" *IEEE Consumer Electronics Magazine*, 2022.

[11] O.-R. SFG, "O-RAN Security Threat Modeling and Remediation Analysis," O-RAN Alliance, Tech. Spec. (TS) ,version 03.00, 2022.

[12] ——, "Study on Security for Near Real Time RIC and xApps," O-RAN Alliance, Tech. Spec. (TS) ,version 01.00, 2022.

[13] ORAN-SFG, "Study on Security for Non-RT-RIC," O-RAN Alliance, Tech. Spec. (TS) ,version 01.00, 2022.

[14] O-RAN, "O-RAN Open F1/W1/E1/X2/Xn Interfaces Working Group, NR C-plane profile," O-RAN Alliance, Tech. Spec. (TS) ,version 08.00, 2022.

[15] G. Masini, "A guide to NG-RAN architecture," in *5G and Beyond*. Springer, 2021, pp. 233–258.

[16] O.-R. SFG, "Near-Real-time RAN Intelligent Controller Architecture and E2 General Aspects and Principles," O-RAN Alliance, Tech. Spec. (TS) ,version 01.00, 2022.

[17] F. W. Murti, J. A. Ayala-Romero, A. Garcia-Saavedra, X. Costa-Pérez, and G. Iosifidis, "An Optimal Deployment Framework for Multi-Cloud Virtualized Radio Access Networks," *IEEE Transactions on Wireless Communications*, vol. 20, no. 4, pp. 2251–2265, 2020.

[18] S. Soltani, M. Shojafar, H. Mostafaei, Z. Pooranian, and R. Tafazolli, "Link Latency Attack in Software-Defined Networks," in *17th CNSM*, 2021, pp. 187–193.

[19] R. Skowyra *et al.*, "Effective topology tampering attacks and defenses in software-defined networks," in *48th IEEE DSN*, 2018, pp. 374–385.

[20] J. S. Ho and I. F. Akyildiz, "Local anchor scheme for reducing signaling costs in personal communications networks," *IEEE/ACM Transactions on Networking*, vol. 4, no. 5, pp. 709–725, 1996.

[21] Floodlight. Open SDN controller. [Online]. Available: https://floodlight.atlassian.net/wiki/spaces/floodlightcontroller

[22] Software Radio Systems. Open source SDR 4G/5G software suite from Software Radio Systems (SRS). [Online]. Available: https://github.com/srsran/srsran