Network Random Refresh

Aman Chawla

Abstract

In this brief paper, the authors outline an attack against a 5G network in which one or more of the internal nodes of the network go rogue. The attack is highly deleterious since a rogue node can cause much disruption and launch further attacks. The authors propose a network reconstruction to mitigate the possibility of such attacks, if not prevent them altogether. The paper is a preliminary presentation of a novel strategy to defend against these so-called auto-immune attacks. The sequel to this paper will present extensive simulation results implementing this strategy.

1 Introduction

5G networks are the current state-of-the-art in networking technology, for many application domains. Due to their rich capabilities, they are widely deployed and therefore one of the key requirements is to secure them and ensure privacy for the users. Some of the advantages of 5G networks over earlier variants include: high speed, low latency, high capacity and efficient slicing. At the physical layer level, 5G networks use technologies that enable broader coverage areas and reliable transmissions using better error correction and other related techniques.

These advantages make them vulnerable targets for attackers. There are several possible attacks against a cellular network that have been studied. These include the ToRPEDO, the PIERCER and various Denial-of-Service attacks. Inspired by the antibody-antigen system present in biological organisms, in this paper we divide attacks into two categories - exogenous and endogenous, in Section 7. We present a review of the literature from the biological as well as the 5G side in Section 2. In Section 10 we present a possible strategy to mitigate the attack. In Section 11 we conclude.

2 Literature Review

The aim of this section is to present a review of a couple of relevant papers that discuss the attacks we are interested in. We first discuss [1]. In this paper, the authors study 5G and 4G networks, with the goal of identifying vulnerabilities to various types of attacks. In particular, they propose a Torpedo attack and its countermeasure. In this attack, the attacker is able to accurately locate the

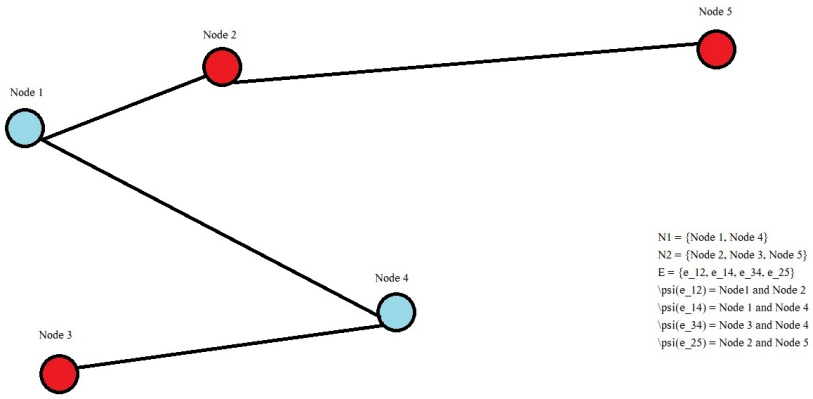

Figure 1: A bimodal graphical network.

victim in a geographical cell and thereafter launch a couple of more attacks which completely recover the victim's identity. Then they propose the Piercer attack which similarly allows location tracking of the victim. Another attack discussed is the IMSI-Cracking attack for 4G/5G networks.

In [2], the authors review the Denial of Service attack and the Torpedo attacks. They also discuss countermeasures to these attacks. [3] is an early survey of security in information operations. Along with defining what defensive information operations do, it also mentions the role of artificial neural networks in acquiring data from the network for analysis and prediction in the security context.

3 Bimodal Graphs and Networks

A bimodal network is defined as a network whose graph is bimodal. A bimodal graph is one where there can be two different types of nodes, for example, "user-equipment (UE)," and "router (R)." In this case, N is replaced by N_1 and N_2. Thus the model becomes $(N1, N2, E, \psi)$. Figure 1 illustrates such a graph.

4 Rogues

A rogue node is defined as a previously normal node of the network, that 'turns' into an adversary for any reason. In what follows we will assume a bimodal graphical network $(N1, N2, E, \psi)$, but we will make the further assumption that nodes in the set N_1 do not start any type of attack. Thus all potential rogue nodes belong to the set N_2.

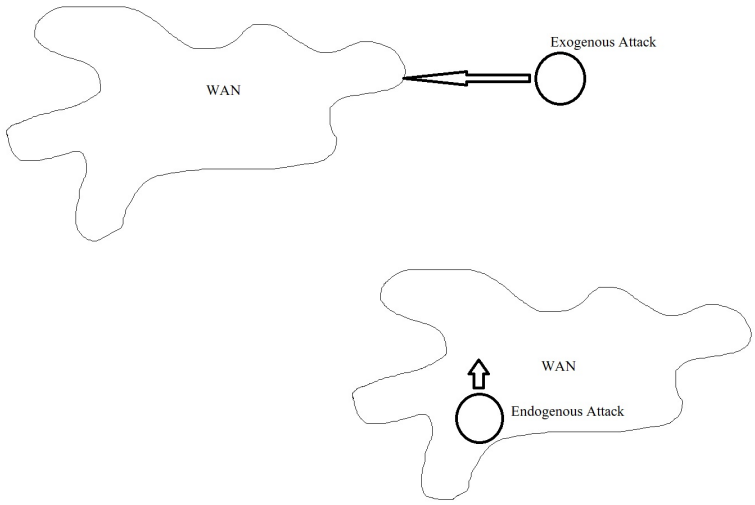

Figure 2: Exogenous and Endogenous Attacks.

5 The Immunological Model

The human immune system is known to defend the body against pathogens. The immune cells gather around and annihilate the intruders. Sometimes, in autoimmune diseases, the immune cell attacks its own system. Whereas there have been studies involving the immune system in more detail and using it to design wireless sensor networks and intrusion detection systems [4], in the present work we will only take broad inspiration from the immune system. The auto-antigen will be called a rogue in our 5G context. This is a bona-fide node in the network.

6 Cases of Interest

Networks can be grouped by the number of rogues present in them at any time. Based on this, we can identify a few cases of interest for modeling purposes:

1. One rogue in the network ($n = 1$)
2. Two rogues in the network ($n = 2$)
3. General case: n rogues in the network with N2 modality-2 nodes.

7 The Endogenous Attack and its Detection: Overview

In a normal large network, not every node will be present in the repertoire of a given node. We are interested in endogenous attacks against distant nodes, not

present in the working repertoire of the given node. Since the auto-antigen node is part of the network, it can correctly correlate a placed call with the resulting paging message, in order to unleash further disruption.

The detection of the endogenous attack is straightforward, since after the node goes rogue and obtains the location of the victim, it can launch one of the known, standard attacks of the three types considered in this paper. The regular detection strategy for the detection of those attacks (for the exogenous case) can be applied to the endogenous case with slight modification.

8 Specifics of Disruption Caused

A rogue can compromise network security and privacy in several possible ways. For example, by flooding a particular node's incoming stream, the rogue can induce denial-of-service. The rogue can also perform Torpedos and, possibly, Piercers [1]. In a Torpedo the attacker can learn the victim's geographical location in a cell with less than ten calls and can cause further damage as well. In a Piercer attack the attacker, with a fake base station, can associate the victim's phone number with its subscriber identity. However, since a fake base station is required in a Piercer attack, it may not be feasible for a rogue to fully implement it.

9 Detection of Disruption

The disruption caused can be detected by its "effects." This is a high-latency mechanism of detection and a more effective detection mechanism would be needed. Some of the ideas of an "adaptive" immune system in [5] can be utilized. An adaptive immune system is present in the human body over and beyond the innate immune system. By aggregating danger signals from the innate immune system, it acts as a second layer of defense.

10 Network Random Refresh (NRR)

In this section we describe how an endogenous attack of a specific type, the theme of this paper, can be prevented. We introduce a novel approach called Network Random Refresh to secure 5G networks.

10.1 Random Configuration

Suppose the network configuration, that is, a graphical representation of the network, including the list of inter-nodal distances is randomly and periodically reconfigured. By this we mean the following. Suppose there is a 'file' which contains details of how the network is systematically arranged, information about which node is connected to which other node, and what are the protocols in place for communication between those nodes. We'll call this the configuration file. It

applies to the entire network, to the remotest node. By a re-configuration, we mean that we will take this file and modify some of the details. For example, we may alter the fact that node 2 is connected to (can talk to) node 20 easily via protocol B and insert instead the commandment that node 2 cannot talk to node 20 at all, it can only communicate with any node within 3 hops of it, and that too only via protocol A. Once we are finished with making all these and sundry changes, we say the new file specifies a network re-configuration.

10.2 Random Timing

Further, by allowing the timing of when the re-configuration is made, to be 'random', we mean that there isn't a fixed formula for determining if the network needs to be presently re-configured. Instead, a coin is tossed at each discrete time step, so to say, and if it lands on Heads, one reconfigures the network using the new file, and if on Tails, one leaves the present configuration in place.

10.3 Implications for Rogues

This random, period re-configuration implies that no single node could ever be sure of correlating a call it places with the resulting paging message. In turn, this guarantees that a node gone rogue can be contained. This can be easily seen as follows. Suppose I'm a rogue node and I wish to attack the network. For this I need to know the configuration file. I have one on hand. I start to use it to determine which node to attack and how to reach it, using which protocol. As I begin to implement my strategy, the coin is tossed and the network is refreshed, voila, a new configuration file is in place. So my efforts have been in vain.

10.4 Addressing the non-Rogue Setting

On the flip-side, when such rare rogue events are not occurring, the rule for obtaining the list of inter-nodal distances (essential for successfully matching a call with the resulting paging message) should be modified in such a way that two nodes would share the table of inter-nodal distances between them, each normally possessing only half of it. When a node needs to make a call, it would be required to first establish nearest-neighbor communication and obtain the other half of the table from the neighbor. This implies that two nodes would be required to go rogue together, at minimum in order for an endogenous attack to be executed.

10.5 Summary of the NRR Mitigation/Counter-measure

We proposed "Network Random Refresh" (NRR) as a counter-measure to a probable rogue attack. In NRR an unbiased coin is tossed at every discrete time instant and if the coin lands on 'Heads,' then the network is refreshed into a new random state. By a random state we mean that whereas (N_1, N_2, E) remain unchanged, a random assignment function ψ_r is used. Furthermore, in a future

work, we can also allow random re-allocation of communication protocols along various edges. The NRR is performed subject to constraints. These constraints specify that more 'changes' need to be put in place in areas where there are suspected rogues than in areas where there are mostly trusted nodes.

10.6 Ensuring good service on non-rogue-event days

On most days, there won't be rogue activity in the network. If NRR is in place, how do we ensure that the network doesn't get too bogged down in all these refreshes and remains functional? Assume that after each refresh the network tells each node the new ψ_r function, however concealing part of it. The information is provided in such a way that by one "conversation" with a nearest neighbor, a node can acquire the complete picture of the ψ_r function; this allows good activity to go on. At the same time, it deters 'lone-wolf' rogues who would be reluctant to establish a conversation with anyone as it might reveal their malicious intent.

As a note, overall connectivity is maintained while choosing a new ψ_r, even though specific edges may no longer exist or be added; only this can guarantee that the network is still useful and functional.

10.7 Allocation and Detection of Rogues

One can 'throw' rogues randomly onto the network's nodes, thereby converting them into rogues. It may be possible to analytically show in this setting, that the probability is low for two nearest neighbor nodes to both be allocated as rogues, thereby avoiding the case where two rogues together get access to the entire ψ_r.

As mentioned, a rogue is detected by its deleterious "effects." The question arises as to who observes and decides that such and such an effect is deleterious. There are at least two possibilities:

a. Local Observer: Under this setting, there is a central observer which decides whether nodes are behaving odd or not.

b. Global/non-local/Distributed observer: Under this setting, a distributed ML algorithm acting over time detects and predicts the presence of nodes.

11 Discussion and Conclusion

In the context of the impact of technology on society [6], networks play an important role. Scalable and secure networks that can be easily deployed in diverse environmental conditions are a boon. Consider, for example, a disaster area 100 sq-kilometer wide, where there is much flooding due to a dam-burst. Villages have been submerged but some survivors exist, having improvised boats and rafts, some on roof-tops of *pucca* houses. In such a setting, when first responders come, they need to be able to rapidly deploy a basic communication

infrastructure which is secure. Since crooks are always present to take advantage of others even in a disaster, this security must be of the highest order. 5G rapidly deployable user equipment (UEs) can be distributed to the survivors in order to facilitate communication among themselves and with the relief providers. Later on, post-disaster, the network can be disbanded. This use case has many more technological details that need to be worked out before it can become practicable to execute on the field. Our present work represents only a small step in this direction.

The insights obtained here are relevant in many respects to cortical communication networks. It has been observed by MacNaughton et. al. [7] that packet communication takes place in the cortex as well. At some level, there might also be an 'application layer' in the cortex, though this is only a hypothesis at this stage. It would be interesting to investigate whether concepts such as network slicing mimic what happens in biology or not. It is also relevant to point out that deep sleep might be an analog of the NRR strategy proposed herein. These overlaps and cross-insights are quite interesting to explore in future work.

Consciousness in particular and biology in general generate systems which mimic in many ways the very generative structure itself. It also motivates us to ask if the man-made world is not just an extension of the brain(s) that developed it. If this is the case, then fundamental principles govern it, operating in a hierarchical or nested manner. These are ultimately the principles of biophysics. Simple laws such as charge conservation, which govern brain-wide phenomena such as ephaptic coupling or synchronization [8] may therefore ramify at every scale, including the meso- and macro-scale. And these are the laws of the universe since the Big Bang. Thus we see how, in the spirit of David Bohm [9, 10] and the Vedic *rsis*, wholeness is implicit in every part of the subjects which science studies, which are aspects of Nature in general.

Acknowledgment

The author acknowledges the contribution of Mr. Priyansh Singh in formulating the intrusion detection aspects and Prof. Vireshwar Kumar, CSE Department, IIT Delhi, in assigning the overall task of developing a new attack and defense for 5G networks.

References

[1] Syed Rafiul Hussain, Mitziu Echeverria, Omar Chowdhury, Ninghui Li, and Elisa Bertino. Privacy attacks to the 4g and 5g cellular paging protocols using side channel information. *Network and distributed systems security (NDSS) symposium2019*, 2019.

[2] John A Khan and Md Minhaz Chowdhury. Security analysis of 5g network. In *2021 IEEE International Conference on Electro Information Technology (EIT)*, pages 001–006. IEEE, 2021.

[3] Tim Bass. Intrusion detection systems and multisensor data fusion. *Communications of the ACM*, 43(4):99–105, 2000.

[4] Peter Parham. *The immune system*. Garland Science, 2014.

[5] Vishwa Teja Alaparthy and Salvatore Domenic Morgera. A multi-level intrusion detection system for wireless sensor networks based on immune theory. *IEEE Access*, 6:47364–47373, 2018.

[6] Aaditeshwar Seth. *Technology and (dis) empowerment: A Call to Technologists*. Emerald Group Publishing, 2022.

[7] Artur Luczak, Bruce L McNaughton, and Kenneth D Harris. Packet-based communication in the cortex. *Nature Reviews Neuroscience*, 16(12):745–755, 2015.

[8] Aman Chawla and Salvatore D Morgera. Ephaptic synchronization as a mechanism for selective amplification of stimuli. *BMC Neuroscience*, 15(1):1–1, 2014.

[9] David Bohm. *Wholeness and the implicate order*. Routledge, 2005.

[10] David Bohm and Henry P Stapp. The undivided universe: An ontological interpretation of quantum theory, 1994.