NDN and 5G: How two combined network protocols affect security.

Hope Welch
University of Utah
hope.a.welch@utah.edu

Abstract

This paper presents research conducted on the effects that 4G and 5G have on Named Data Networking security. By using a common DDoS attack that targets a weakness of NDN (an Interest Flooding Attack), this paper explores if security works better in 5G conditions. The end goal is to know if combining 5G and NDN makes a more secure network.

1 Introduction

Security is a broad and important topic in the field of networking. It is important to understand how security can be improved. 5G has been heavily advertised to be more secure than 4G. As an article from *Wired* explains, 5G "will . . . enable operators to do what's called 'network slicing'–segmenting the system in numerous virtual networks that can be managed and customized separately. This means that different 'slices' could have different tailored protections for specific types of devices" [6]. But 5G is still vulnerable to a big category of attacks called DDoS (Distributed Denial-of-Service).

Approximately ten years ago, NSF funded projects to create alternative networking protocols that would possibly replace IP in the future. One of those projects was Named Data Networking. Named Data Networking (NDN) security has been tested by many researchers. It is understood that NDN can hold up against several of the most common DDoS attacks because of its design. However, that does not mean it is immune to *all* types of attacks. A malicious attacker can tailor DDoS attacks to target the weaknesses of NDN.

If NDN is resilient against IP tailored DDoS attacks, and if 5G is already marginally more secure than 4G, what would happen to security if these two networks were combined? In this paper, we address this question by conducting a number of experiments to see the effects of security on a 5G network where the sxlices were natively NDN.

To begin, we focus on the most common type of NDN DDoS attack: the Interest Flooding Attack (IFA). By using a simple network setup, we compare the performance of NDN under 4G and under 5G for a regular NDN case, and a IFA case.

The rest of the paper will be ordered as follows: we will talk about the Related Works, then address the necessary background knowledge for understanding the experiment and how we came to choose this particular set up. After that, we will go over the software and programming we used and detail the outline of our experiments. Then we will explain each experiment and provide the resulting data with analysis. After each experiment is done, we will analyze the study as a whole and draw a conclusion. Lastly, we will re-summarize the paper to include the results, and list the References.

2 Related Work

The paper *NDN, CoAP, and MQTT: A Comparative Measurement Study in the IoT* [4] essentially compared IP based protocols with ICN protocols, and within the ICN protocols was Named Data Networking. They found that NDN has the most resource

friendly deployment on nodes, and superior resilience in multi-hop scenarios. [4] The results of this paper is encouraging for our research because they have proven that NDN is a superior choice compared to other protocols. Which means that in an effort to combine protocols for improved security, NDN could be the right choice.

In the paper *Bridging the ICN Deployment Gap with IPoC: An IP-over-ICN protocol for 5G Networks* [8], there is a protocol proposed for using NDN with 5G, and specifically addresses how NDN can simplify mobile handover. Although it is not directly involved with the security aspect of things, it is an interesting approach to solving a problem using NDN.

The paper *Performance Evaluation of Several Interest Flooding Attack (IFA) Countermeasure Method on ISP-like Topology for Named Data Networking* [7] goes over heavy testing of IFA on NDN, and includes countermeasures that they created. Unlike them, however, we are not attempting to come up with a new countermeasure for IFA. This paper also outlined in detail the various types of Interest Flooding Attacks, which we used as a guide to properly set up an IFA situation.

Two years after NDN was created, a paper by the people who created it was published, called *DoS & DDoS in Named-Data Networking* [3]. Their research for this paper set the ground work for future research in security for NDN. They tested NDN against several IP-based DDoS attacks, and explained in detail the different types of NDN-based DDoS attacks. They concluded with their plan for future studies in this area and the different countermeasures that they see are needed. Today, we know that there has been considerable research involving security and NDN, and there have been countermeasures implemented.

3 Background

3.1 How NDN Works in Summary

Consider Figure 1 to be a simple topology of an NDN network. The consumer, a UE for example, wants data under a prefix (or 'name'). For example: 'greetings'.

1. The UE makes a request, or an *interest packet*

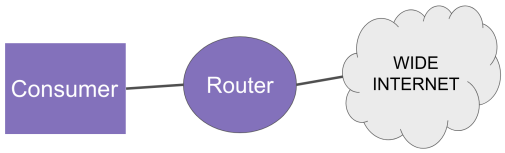

Figure 1: A simple topology

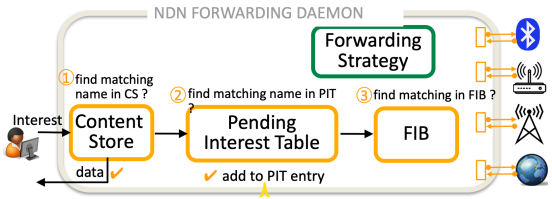

Figure 2: Detailed representation of NDN router [9]

to the router it is connected to. This router is an NDN router that contains three important tables. The Content Store, PIT Table, and FIB Table. Figure 2 shows a nice visual of the steps a router takes when receiving an interest packet.

2. The Router receives this interest packet for data under a prefix (ex: '/ndn/greetings'). It first searches the Content Store (CS), which is a cache on the router, for the data under that name. If it finds the matching *data packet* in the CS, it will send that packet to the UE. If not, the router searches for a similar interest packet in the Pending Interest Table (PIT) and either adds the interface from which the packet came from to a matching entry, or creates a new entry signaling a 'pending interest' for the data.

3. From there, the Router goes to the Forwarding Information Base (FIB) and forwards the interest packet to the next interface where the data might be. An interface could be another NDN router, another consumer, or some other object on the Internet.

4. Once the interest packet reaches a node that has the requested data in its CS (which means it is *hosting* the data), a data packet is sent back, which carries both the prefix and the content

of the data, together with a signature by the producer's key for security. For example, it would have the string 'Hello' under the prefix '/ndn/greetings'. The data packet will be forwarded back the way it came, to the first router.

5. When an NDN router receives a data packet, it searches the PIT for a matching interest packet entry. Using the faces listed in that entry (the faces where the interest came from), the Router sends the data packet to those faces, deletes the entry, and stores the data packet in the CS.

6. One of those faces include our UE, and now it has the data (ex: Data under prefix /ndn/greetings is: Hello).

3.2 Interest Flooding Attack

Generally, as explained by an article from *CloudFlare* "a DDoS attack is a malicious attempt to disrupt normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. From a high level, a DDoS attack is like a traffic jam clogging up a highway, preventing regular traffic from arriving at its desired destination" [1]. Figure 3 is a metaphorical visual representation.

An Interest Flooding Attack (IFA) uses the same concept, targeting an NDN router's PIT table. The paper *DoS and DDoS in Named Data Networking* best describes it this way: "The adversary can take advantage of the state in the PIT to mount an effective DoS attack, which we term 'interest flooding'. The adversary (controlling a set of possibly geographically distributed zombies) generates a large number of closely-spaced interests, aiming to a) overwhelm (PIT-s) in routers, in order to prevent them from handling legitimate interests, and/or b) swamp the targeted content producer(s)." Since NDN interests lack source address and are not signed, by design, it is difficult to determine the attack originator and take targeted countermeasures.[3]

In detail, the paper written by Rotinsulu et al [7] outlines some specifications of an IFA. To summarize, the interest flooding speed is very high, so the

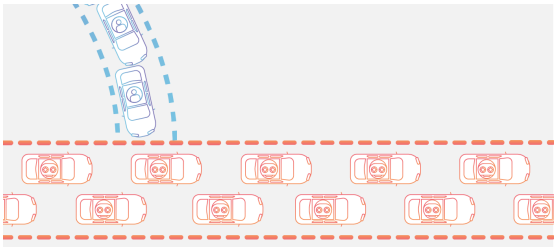

Figure 3: Simple Visualization of a DDoS Attack [1]

router will receive an excessive amount of interests for a certain time. The prefix in a malicious interest packet is identical to the prefix of legitimate interest packets, but the suffix is a random string. For example: '/ndn/greetings/dslziEdfeR'. "An entry can be added to the PIT due to the random suffix. However, these added entries can never be satisfied because the content is missing. As a result, these malicious entries will not be deleted until they expire" [7]. This information is exactly what we use when generating attacks in our IFA cases.

3.3 NDN Native 5G Slicing

As 5G cellular technology is deployed, delivering its promise of massive throughput and minimized latency requires the network architecture to be rethought in many ways. One of these architectural differences is a branching User Plane Function (UPF), a service that can split traffic based on the network protocol being used. This branching UPF enables a separate Information-Centric Network (ICN) to run as part of the 5G core network, before backhauling to the wider internet. Having a separate network closer to the edge enables lower latency for many content requests. Figure 4 gives an abstract visual on how a 5G Core Network would look like.

Originally, we planned on using a free 5G software set up and attach our NDN to it. But due to time constraints of the research internship and the complexity of using the software, we decided to not use a different setup for the 5G cases. Instead, we adjusted the delay to emulate the important part of what makes 5G different, which is the lower latency as explained above. Figure 5 is a simplified topology of Figure 4. If we were to attach NDN to this 5G slice, we would

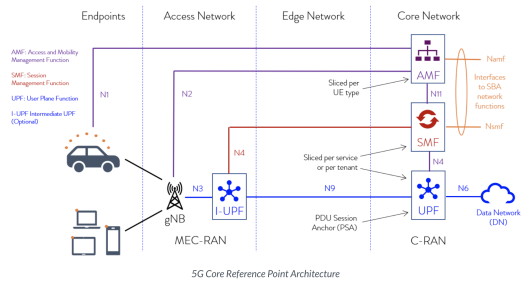

Figure 4: Visual of 5G Core Network [5]

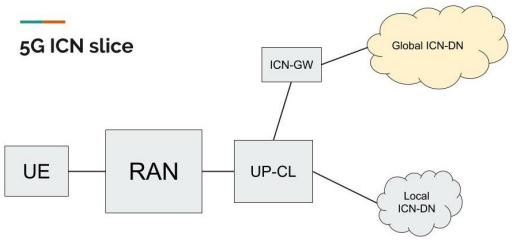

Figure 5: Simplified 5G Topology

replace the Local ICN-DN with the Named Data Network. More details about what we did instead will come in the Experiment section.

3.4 NFD, NLSR and PyNDN Client Library Software

In order to gain more understanding of how NDN works, and to emulate it on our computers, we created a profile on POWDER[2] that contains a physical node (the pnode) and two VM nodes that are linked together by LAN. We adjusted the profile code to pull some scripts from our repository that sets up all of the installation for NFD and NLSR.

NFD and NLSR are software made by the Named Data Networking team. NFD (Named Data Networking Forwarding Daemon) provides a simple set up of NDN. It is a little different than a real NDN setup, where the UE, Router, and Faces are separate. In NFD, those three are compounded into the same node, so everything is local. In order to request/host data, there must be a route established between the two nodes, and there must be one for each direction.

NLSR (Named Data Link State Routing Protocol)

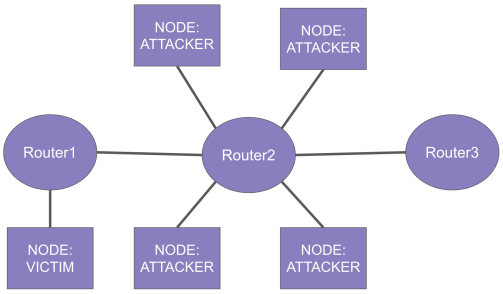

Figure 6: Topology of NDN

is a routing protocol in NDN that populates NDN's Routing Information Base. When a face is created between the two nodes, (and there has to be two faces in order for two-way communication), that allows these nodes to advertise names to each other. Thus, a node can host a data packet, and the other node can send an interest for it and receive it.

The PyNDN Client Library software is a python-based client library that allows a developer to write python scripts to interact with the NFD software.

4 Experiment

4.1 Settings

We conducted 4 experiments:

1. 4G Regular Case
2. 4G IFA Case
3. 5G Regular Case
4. 5G IFA Case

Figure 6 is a simple visual of how the network was set up for each of the 4 experiments. The flow of each case is as follows:

During each regular case, the Victim node sends 100 interests to Router1 for 7 repetitions, pausing for one second in between each repetition. Router3 hosts the 100 pieces of data that the Victim wants, so the interest packets from the Victim node get forwarded through Router1, Router2, and stop at Router3. Router3 will send data packets in return

all the way back to the Victim. The Content Stores (aka the caching) for Routers1 and 2 are turned off. This is because if all three routers had caching on, the interest packets would only go all the way through to Router3 once, then Router1 would cache all the data packets, and the rest of the interests would only reach Router1.

During each IFA case, the Victim will behave the exact same by sending 100 interests 7 times. Router3 also behaves the exact same, by hosting those 100 pieces of data. Caching is still off for Router1 and 2. This time, as soon as the Victim node begins sending interests, the other four Attacker nodes will start sending malicious interests to Router2. The goal is to overload Router2's PIT, and prevent the legitimate interests from the Victim node to be forwarded to Router3, hence 'denial-of-service'. Each Attacker sends interests rapidly with no pausing, and the prefixes are the same as the legitimate ones, but with a 15-character random string attached at the end. None of these malicious interests are satisfiable.

For each 4G case, we set the latency to 23ms, and for each 5G case, the latency was set to 1ms. These latencies are for round-trips from each node. Each Router ran the NFD and NLSR software to enable communication. Each Node ran the PyNDN Client Library.

4.2 Important Notes

There are a few notes to point out about what we discovered while creating this set up. We noticed that when the Victim ran more than 10 repetitions of the same 50 or more requests (no matter how many were satisfiable), the router would consistently begin sending time outs at the 11th repetition. Time outs are sent back after 4 seconds of the router not responding. The NFD software would become unresponsive, making it difficult to determine what made it break: the PIT or some unrelated factor?

We also note that each NDN router generates its own natural traffic with itself. After multiple testing and collecting, we know that the FIB, PIT, and Content Store entries remain at 2 always. Everything else steadily increased over time by various amounts. This makes our graphs that we collect less accurate, but not enough to obscure what is really happening.

Another issue we ran into was the built in countermeasures against IFA. NDN has several general DDoS countermeasures already in place, as was discussed in the Background section. As far as an IFA, it has a push-back scheme implemented that uses the information collected by the PIT. This, with the constrained PIT size that we were unable to adjust, made it difficult to actually create an IFA.

4.3 4G Regular Case

Fig 7 shows the router response time during a regular use of NDN. As is labelled on the graph, Victim node sent 100 interests through Router1, Router2, and Router3, 7 times. Router3 hosted the matching data packets, so the whole run is 100% satisfied. We will point out here that with the 4G latency, the average router response time was 0.041445 seconds. The whole run took 43.5 seconds, and there were only 4 major outliers. It appears that Rep1, Rep3, Rep5, and Rep6 are what gave those outliers.

Fig 8 is a graph of the router status over time. This graph collected the router status every 5 seconds for 1 minute. This graph tells us that there were no unsatisfied interests, a steady increase of satisfied interests, and a steep, initial climb in Content Store entries, before remaining the same. Although the Pit line is not visible, the second point goes from 2 to 8 and then back to 2.

4.4 4G IFA Case

Fig 9 is set up just like Fig 7. This run lasted 36.7 seconds, and there are several more outliers than the regular usage case. As mentioned earlier, an interest has 4 seconds before it times out. As the graph shows, none of the interests timed out. And after looking through the log that records when an interest is sent and what is returned, there were no Nacks either.

Already, we know that this IFA was not successful. If it was, there would be Nacks and time outs. Something puzzling here is that the regular run took 7 seconds longer than this run under attack.

Fig 10 is set up just like Fig 8. Based on the number of points each line has, we know that this timer only

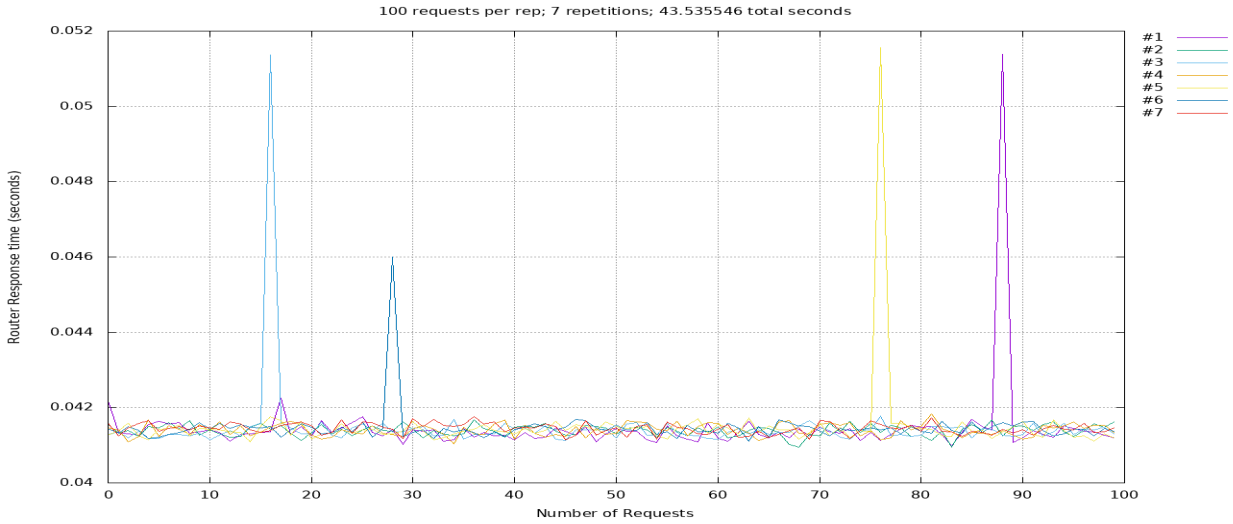

Figure 7: 4G Regular Case Router Response Time

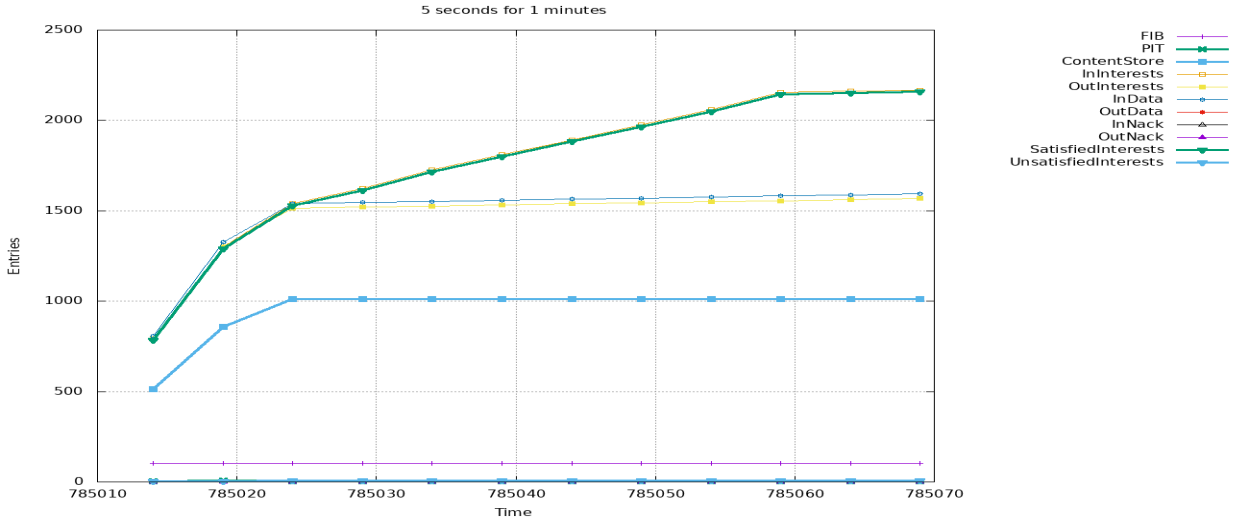

Figure 8: 4G Regular Case Router Status Over Time for Router 3

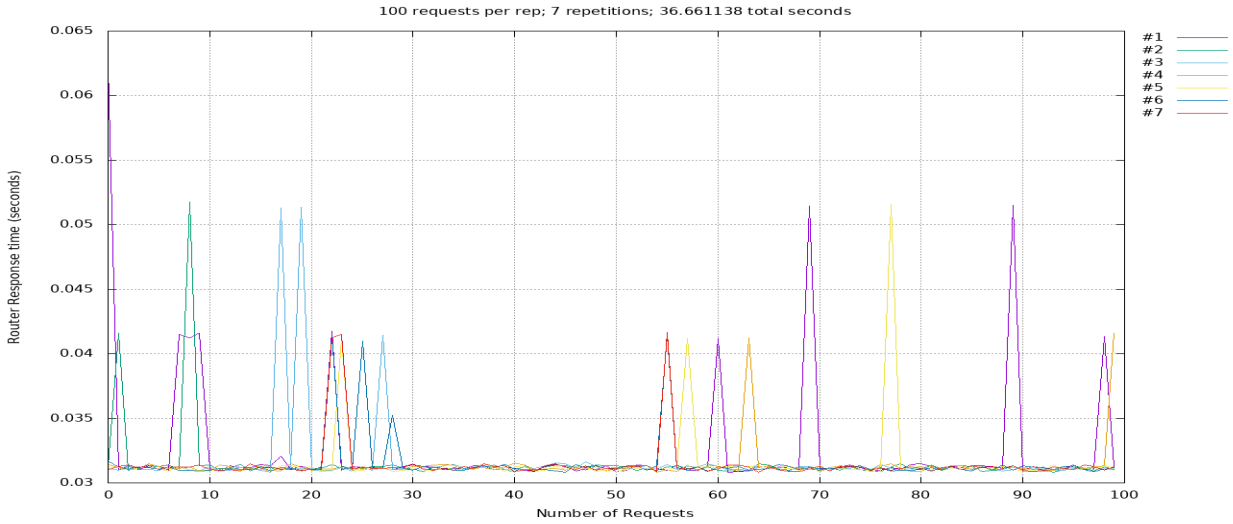

Figure 9: 4G IFA Router Response Time

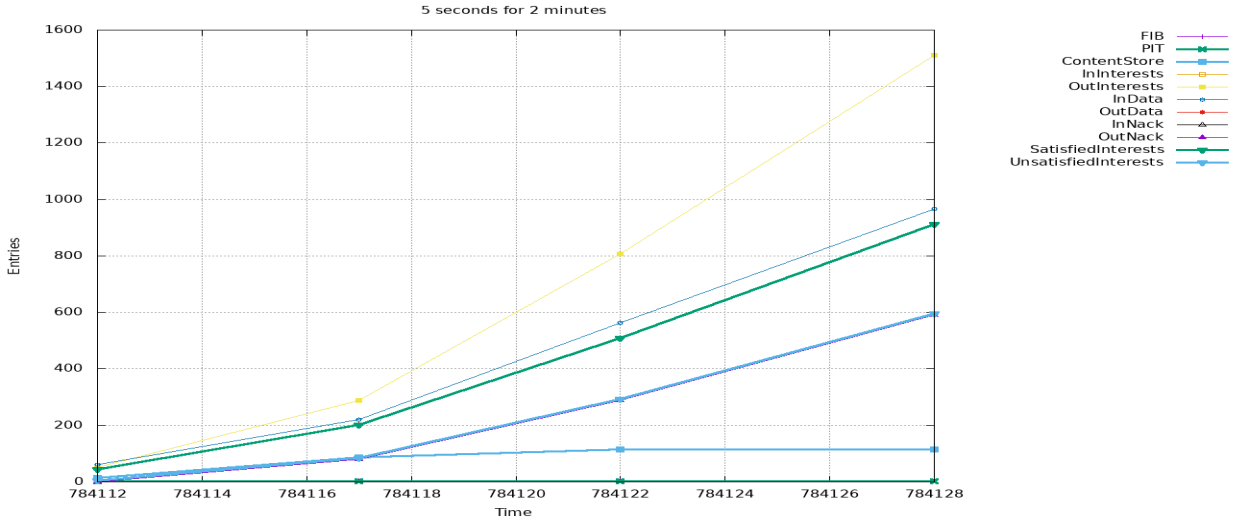

Figure 10: 4G IFA Router Status Over Time for Router 2

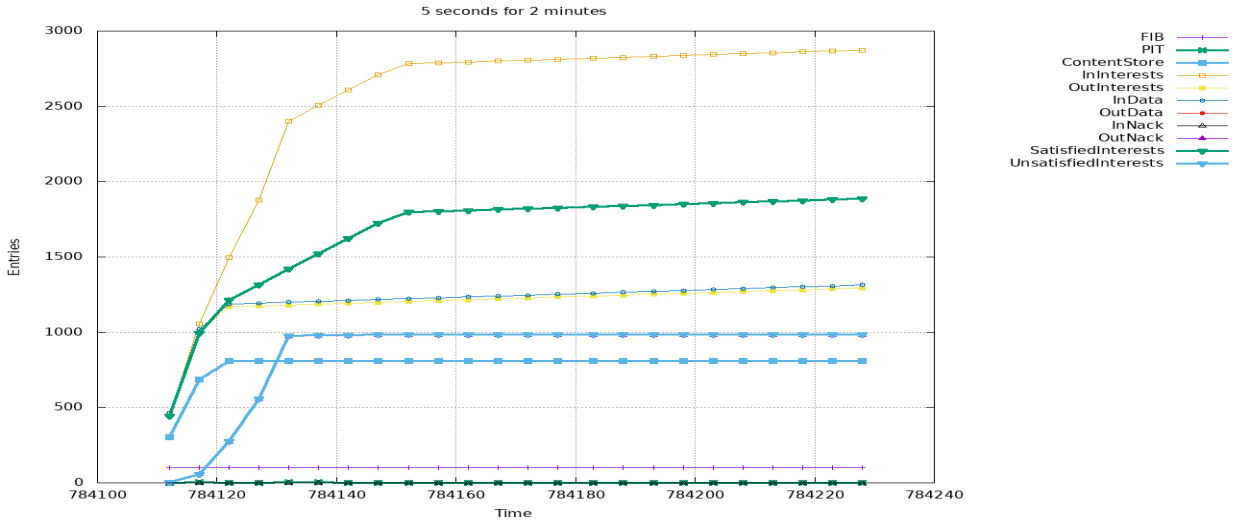

Figure 11: 4G IFA Router Status Over Time for Router 3

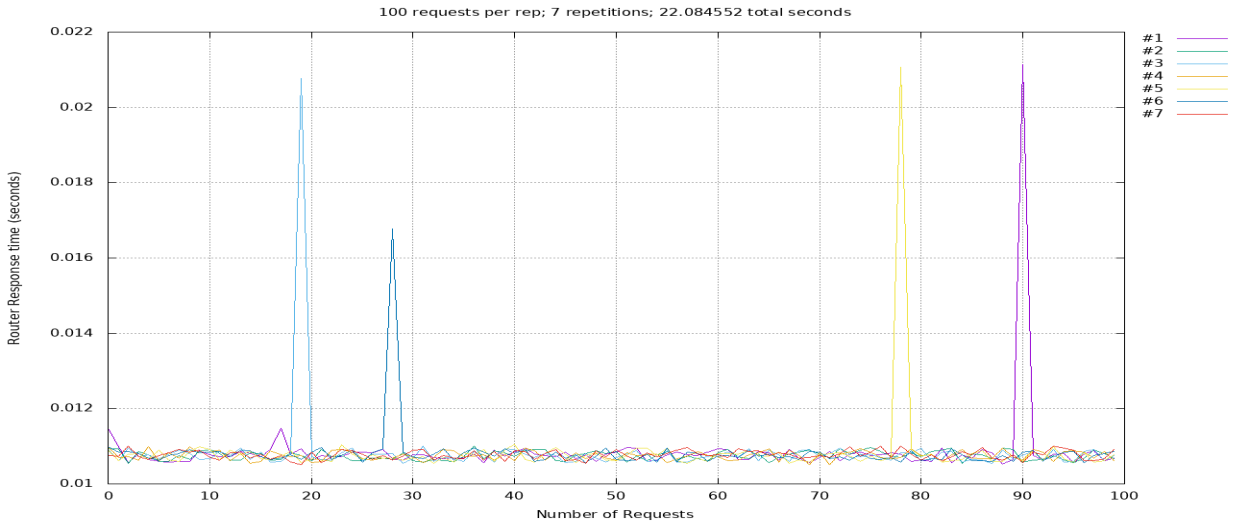

Figure 12: 5G Regular Case Router Response Time

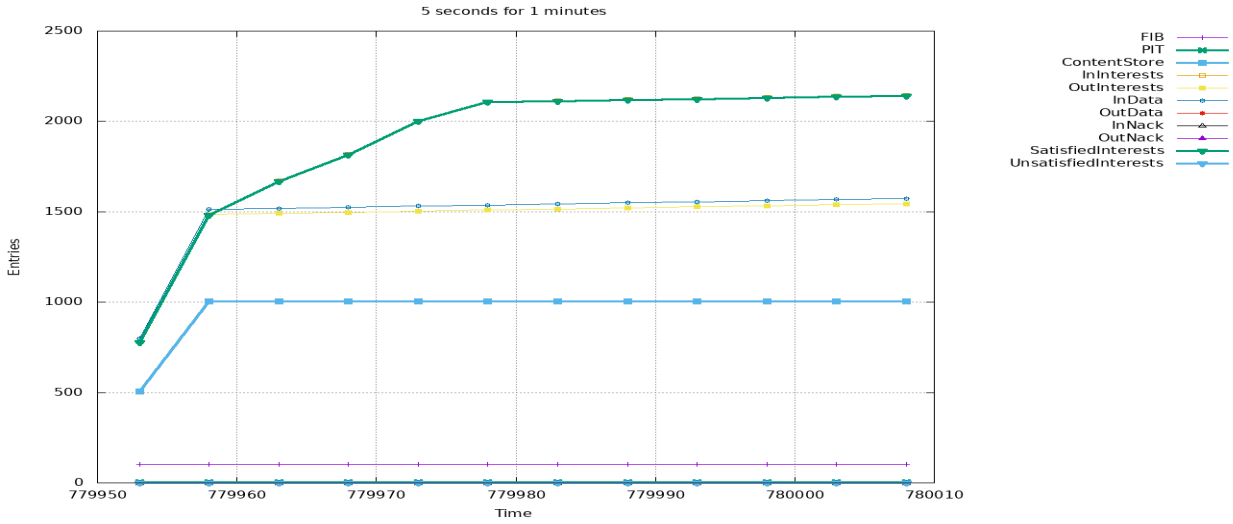

Figure 13: 5G Regular Case Router Status Over Time for Router 3

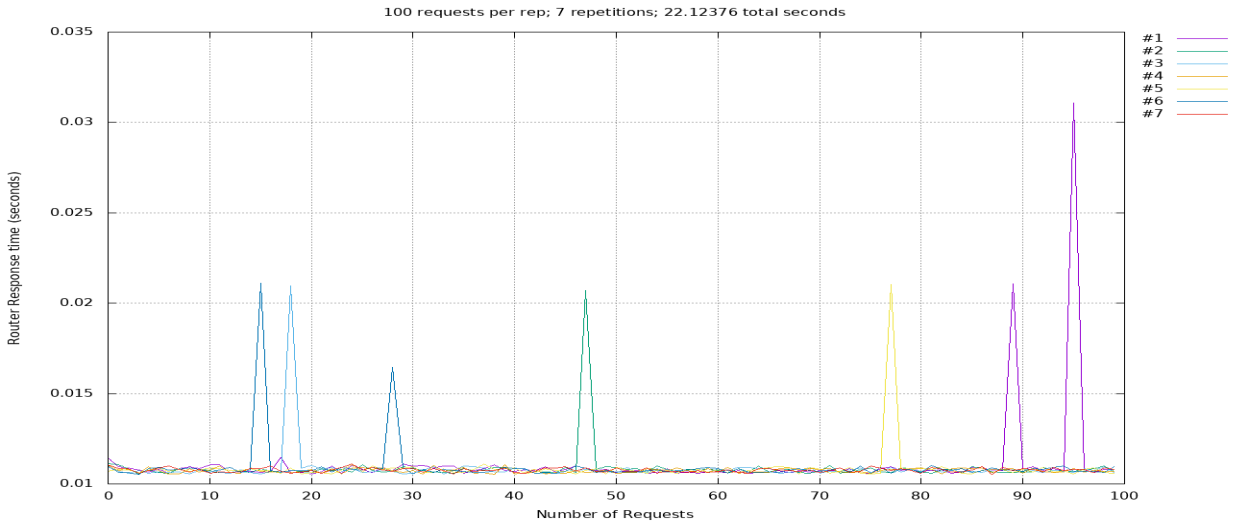

Figure 14: 5G IFA Router Response Time

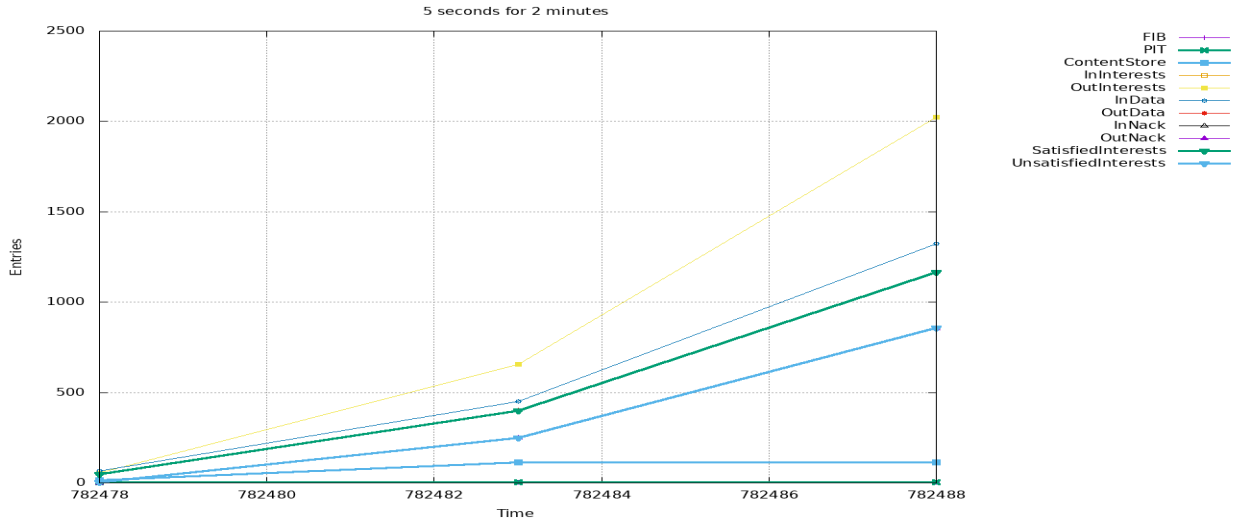

Figure 15: 5G IFA Router Status Over Time for Router 2

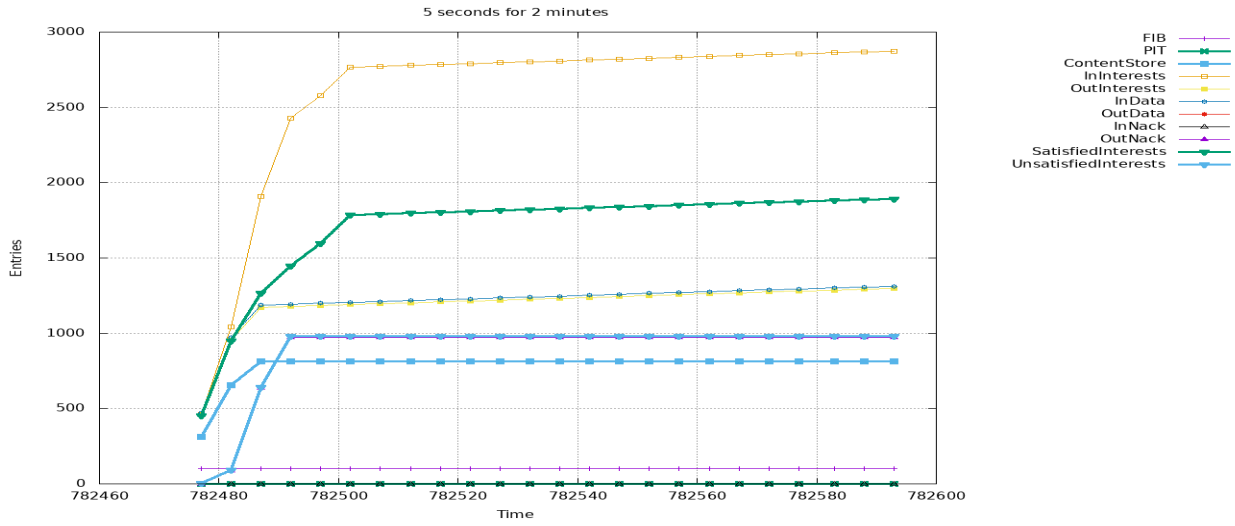

Figure 16: 5G IFA Router Status Over Time for Router 3

lasted 15 seconds before the NFD software stopped responding. The Pit entries stayed at 2 until the very end when it rose to 3. The Content Store remained at 114 after rising rapidly. The rate of satisfied and unsatisfied interests are parallel.

We have added the status over time for Router3 as well, in Fig 11. This truly ran for 2 full minutes. The timing for these two graphs was not perfectly simultaneous, so it is hard to perfectly line up when Router2 broke, but it is obvious that after 784130, the lines start leveling out and record its own naturally generated traffic. This is further proof that the attack interests from the attacker nodes did not get past Router2 when it stopped responding.

4.5 5G Regular Case

Fig 12 shows once again the router response time from Victim node, this time on 5G latency. At first glance, there seems to be no difference between this graph and Fig 7. We thought that the graphs would be similar to an extent, but not practically the same. The major difference though is the time. This run took 22.1 seconds, almost half the time it took for the 4G run. The router response time was also faster, the outliers do not make it to 0.022, which is about half of the average response time for 4G.

Unsurprisingly, the router status for this 5G regular usage case Fig 13 is extremely similar to the 4G counterpart.

4.6 5G IFA Case

Just like 4G, we recorded Victim node, Router2, and Router3 for this attack run. From Fig 14 we know that this run took 22.124 seconds, and the 5G run took 22.083 seconds. That is a 0.019208 difference. Different from the 4G graph, there are not as many outliers, but there are more outliers than the regular usage case.

Again, there is a lack of Nacks and timeouts for Victim node, which means this IFA failed again.

Fig 15 is the status over time for Router2. This only lasted 10 seconds, which makes sense because the latency is not as long as the 4G latency. There is a slight difference in the Pit line; the second point goes to a 3.

Results for Router3 shown in Fig 16 are very similar to Fig 11, the 4G counterpart.

	Mean	**Max**	**Min**
4G Regular	0.041445	0.051565	0.040950
4G IFA	0.031587	0.051742	0.030800
5G Regular	0.010807	0.021146	0.010508
5G IFA	0.010862	0.031088	0.010514

Table 1: Statistics from each Router Response

5 Evaluation

Above in Table 1, we have listed the mean, maximum, and minimum of each router response case. The average response time changed between 4G Regular and 4G IFA, whereas the average for the two 5G cases remain practically the same. This is understandable because the 4G IFA had several outliers, whereas 5G IFA only had a few. It would seem that the faster latency of 5G enables the countermeasures in the NDN to work better; there was less interference by the attacks.

Although we were not able to truly create an IFA, the work done for this paper still gives important information for future research. As was said earlier, there are already countermeasures built into NDN for protection against IFA. In order to overwhelm the router for the right reasons, there would need to be further study on why the software stopped responding the way it did. There would also need to be a more complex network system like the related papers use, with more routers and more attackers. After that, the next step forward could be to actually connect an NDN network to the ICN of a 5G network, and test how neighboring slices are affected by IFA.

6 Conclusion

This research study was about experimenting with NDN and applying 4G and 5G to it to see the effects of security. By using NDN software and building a

simple topology to emulate an Interest Flooding Attack, then applying 4G and 5G latency, we were able to measure how an IFA and the difference in latency affected the router response time, a key measurement in knowing if the IFA succeeded or not.

We were able to produce a baseline of tests and results for this research, even if we could not get a successful denial-of-service. From here, further research can be conducted using the information we have gathered. We did find that NDN and its security measures work better in a 5G environment than in a 4G one. We think that this could indicate that 5G and NDN combined would make a more secure network than 5G alone.

Acknowledgments

It should be noted that Isaak Getz from the same research internship contributed to the Background section, as well as the creation of the testbed profiles and some communication scripts that we modified and expanded on to fit our needs. He also created Fig 5 and was kind enough to let us use it in our paper.

We performed our experiments in the POWDER advanced wireless testbed [2]. This material is based upon work supported by the National Science Foundation under Grant Number 1827940.

References

[1] CloudFlare. What Is A DDoS Attack?

[2] Flux Research Group. POWDER: Platform for open wireless data-driven experimental research. `https://powderwireless.net/`, 2020.

[3] P. Gasti, G. Tsudik, E. Uzun, and L. Zhang. DoS and DDoS in Named Data Networking. In *2013 22nd Int'l Conf on ICCCN*, pages 1–7, 2013.

[4] Cenk Gündoğran, Peter Kietzmann, Martine Lenders, Hauke Petersen, Thomas C. Schmidt, and Matthias Wählisch. NDN, CoAP, and MQTT: A Comparative Measurement Study in the IoT. ICN '18, page 159–171. Association for Computing Machinery, 2018.

[5] Metaswitch Networks. What is the 5G User Plane Function (UPF)?

[6] Lily Hay Newman. 5G Is More Secure Than 4G and 3G-Except When It's Not, Dec 2019.

[7] M. R. Rotinsulu and R. Fitri Sari. Performance Evaluation of Several Interest Flooding Attack (IFA) Countermeasure Method on ISP-like Topology for Named Data Networking. pages 0826–0831, 2018.

[8] Susmit Shannigrahi, Chengyu Fan, and Greg White. Bridging the ICN Deployment Gap with IPoC: An IP-over-ICN Protocol for 5G Networks. NEAT '18, page 1–7. Association for Computing Machinery, 2018.

[9] L. Zhang. An Overview of Named Data Networking, 2017.