Journal of Engineering Science and Technology
Vol. 17, No. 2 (2022) 0997 - 1009

CAPTURING COLLUSIVE INTEREST FLOODING ATTACKS SIGNAL: A NOVEL MALAYSIA'S STATE NAMED-DATA NETWORKING TOPOLOGY (MY-NDN)

REN-TING LEE[1], YU-BENG LEAU[2,*],
YONG-JIN PARK[2], MOHAMMED F.R. ANBAR[3]

[1]Knowledge Technology Research Unit (Industry Development),
Faculty of Computing and Informatics, Jalan UMS,
Universiti Malaysia Sabah, 88400 Kota Kinabalu, Sabah, Malaysia
[2]Cybersecurity Research Group, Faculty of Computing and Informatics, Jalan UMS,
Universiti Malaysia Sabah, 88400 Kota Kinabalu, Sabah, Malaysia
[3]National Advanced IPv6 Centre of Excellence (NAv6), School of Computer &
Mathematical Sciences Building, Universiti Sains Malaysia, 11800 USM, Penang, Malaysia
*Corresponding Author: lybeng@ums.edu.my

Abstract

Named-Data Networking (NDN) is a future Internet architecture known as the most innovative Information-centric Networking (ICN) system capable of resolving many traditional IP-based networking issues. To track suspicious and unsatisfied interests, much current research focuses on network threats such as Non-Collusive Interest Flooding Attacks (NCIFA) rather than Collusive Interest Flooding Attacks (CIFA). CIFA is an attack that aims to exhaust the Pending Interest Table (PIT) on a targeted NDN router by returning malicious Interest packets with matching data packets before the PIT entries that are running with a Malicious Data Producer. When the attacks are directed at satisfied interests, the entire process appears to be rational. Because the captured signals are very similar to legitimate requests, identifying CIFA is difficult. CIFA is ineligible for NCIFA's prevention and reduction strategies. We use the CIFA model to capture the CIFA signals, based on MY-NDN topology, through detailed simulation with ndnSIM simulator, because the test dataset and simulated signals for CIFA are unavailable. This paper provides a PIT Capacity, Performance, and Trendline comparison model for the NDN system, as well as an analysis of simulated CIFA signals. The PIT usage is kept below 100 entries, the throughput is kept below 500, and the trendline is not steep before an attack is launched. After the attack is launched, PIT usage remains above 180 entries and close to peak, throughput can be identified as being above 1000, and the trendline shows an exponential difference. This claims that an IFA-based attack will have an impact on the performance of the NDN network.

Keywords: Attack signals, CIFA, Collusive interest flooding attacks, Named-data networking, NDN.

1. Introduction

Industry 4.0 is a shift of manufacturing technologies from conventional output to digitised solution across a whole field. Mesh of a tiny wireless electronic system with a simple contact protocol transmits a static payload operating in a Low Power Wide Area Network (LPWAN). Often computers with wireless networking are also called the Internet of Things (IoT) Beacon. IoT is a mesh network system with a unique identifier and wireless networking for sensing, data storage and environment-based decision making. Such communication helps the sharing of collected data for further study and consequently contributes to increased efficiency and economic benefits [1]. One of the exciting future Internet architectures, Named-Data Networking (NDN), is an Information-centric Networking (ICN). It is a new communication paradigm which had emerged to many new features which promised to allow broad conception than a conventional networking. It does not require a centre to identify what and who is sent or receive any packets and open to public gaze which availability to all. It future names an entity to be retrieved safely by in-network storage and anycast naming-based route that fits the peculiarities of IoT applications [2]. Besides, a modern industry machine will generate huge data running at 1 Petabyte data per day [3]. In order to support huge volume on demand, IoT need to be introduced with a customisation architecture and standardise in data transmission. Because of the NDN design, it allows accessibility easy to identify what the consumer was searching for and did not anticipate the information.

In accordance with a secure end-to-end network, conventional Internet uses IP to share details, whereas NDN is "application safe." Consumers can access protected content or information themselves, mixing it with data integrity and confidence as the property of the content [4]. NDN architecture will ease the effect of today's most common network threats, Distributed Service Denial (DDoS). It anticipates a new form routing attack in NDN architecture named Interest Flooding Attacks (IFA), further classified as Non-Collusive Interest Flooding Attacks (NCIFA) and Collusive Interest Flooding Attacks (CIFA). Both attacks are overwhelming Pending Interest Table (PIT) NDN router. Any incoming interest that is not yet satisfied would generate a PIT entry. The entry will not be discarded before the subsequent Data Packet returns to the user or ends the period for that transaction. Consequently, network traffic would be congested and the legitimate demands to be dropped. The PIT in NDN is useful however, if the intruder abuses it and causes catastrophe as indicated [5]. Many scholars rely on NCIFA, which was thoroughly studied. Moreover, CIFA cannot be traced by using current NCIFA detection or countermeasure system [6].

This paper describes a new scheme of CIFA 's destructive roots in NDN. In specific, we consider the malicious source linked to target nodes in the NDN network. We chose to capture NDN Node Topology via comprehensive state-based simulation in Malaysia due to a lack of available data or capturing CIFA signals.

2. Background

2.1. NDN architecture

The NDN is viewed as a Future Internet infrastructure and regarded as the most promising solution to a clean-slate, content-cantered system driver platform.

NDN 's basic operations involve three main components. Figure 1 demonstrates the NDN architecture.

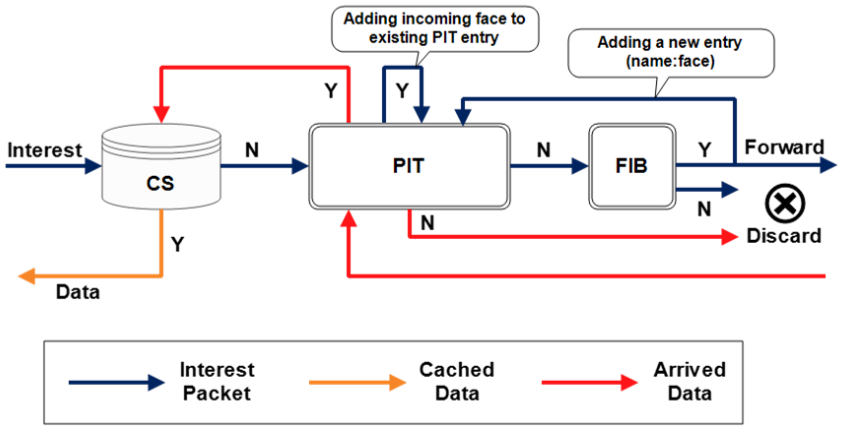

Fig. 1. Operations in NDN architecture.

A request (Interest) packet with data name is sent from a consumer node to the data producer node. Intermediate NDN router checks whether the required data resides in its Content Store (CS), which is the data cache, throughout transmission. If so, a reply packet (data) is sent back to the node. If not, the Pending Interest Table (PIT) will investigate whether the data has an outstanding forwarded request of the same name. If found, the incoming interface (Face) would be inserted, and the request packet discarded. The PIT retains return path information. If not, the request packet is routed to the Forward Information Base (FIB) and sent to the next router. Upon delivery, the request packet returns a response (Data) packet. Using PIT information in intermediate routers eventually reaches the consumer node [7].

2.2. Comparison on content delivery network (CDN) and NDN

A CDN is designed to distribute large amounts of content that are frequently requested over the Internet. Based on network flow, load status, and target response time, a new architecture with some network overlay will be required to be deployed. The CDN, on the other hand, is proprietary, and the points are not linked in a system. The deployment of multiple datacentres and servers required for synchronous updating for real-time applications such as video streaming, video conferences, SNS applications, and so on will be prohibitively expensive. However, it lacks superiority.

The NDN principal will allow users to focus on what content to retrieve or deliver regardless of where they are. At the most basic level, it is a named-based content-oriented architecture with no notion. The NDN protocol includes a stack protocol that can be integrated into today's TCP/IP network. NDN has basic networking functions, routing and forwarding, and network security, which can support the efficiency of content distribution in a secure and faster manner due to in-network caching [8].

Overall, NDN can aid in the avoidance of network conflict and congestion, the elimination of end-to-end connections, and the improvement of reliability, efficiency, and performance in large-scale content distribution over the Internet.

2.3. Non-collusive interest flooding attack (NCIFA)

Traditional Interest Flooding Attacks known as Non-Collusive Interest Flooding Attack (NCIFA). Instead of the entire NDN networks, the attacks target the data producer in the architecture. Figure 2 illustrates the NCIFA model.

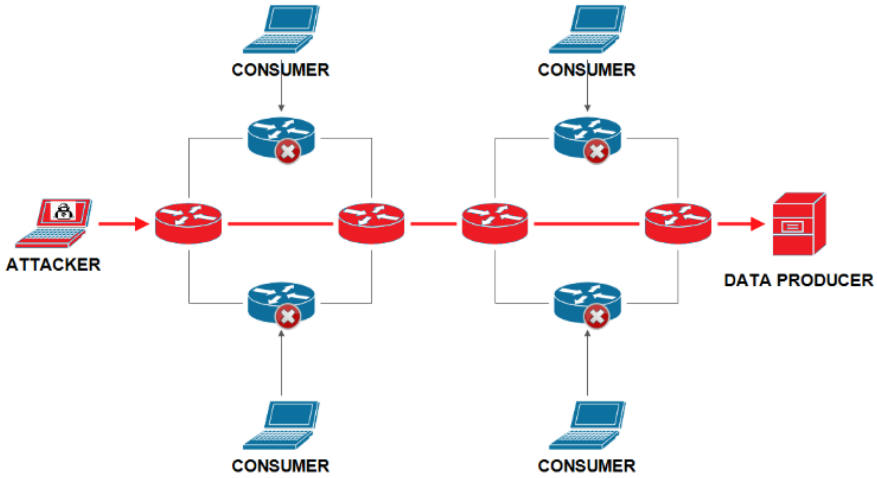

Fig. 2. Non-collusive interest flooding attacks (NCIFA) model.

The intruder could be on the edge of an NDN router. The attacks usually completed in short intervals with long unsatisfied Interest. It causes the NDN The intruder may be on an NDN router 's side. Attacks typically finished with long unsatisfied interest in quick periods. It fills the PIT entries of the NDN router until the timeout. The NDN router can respond to the attack by forwarding this request to the data source. As a consequence, the targeted NDN router could not accept any other content request from the neighbouring router or legitimate consumers. Many countermeasures have been proposed to detect NCIFA [9-11] such as statistical approach, push back mechanism, safety management, machine learning, etc. All these techniques have improved with a newer contribution, a better approach to identifying malicious Interest through criteria such as patterns, threshold and traceback outlined by Lee et al. [6].

3. Research Focus

This paper addresses CIFA. The attack targets the entire NDN network with a malicious data producer. The attackers send a malicious interest which only satisfied by the malicious data producer in an NDN network. Figure 3 shows CIFA model.

CIFA is an occurrence where attacks mimic a legitimate request. The main difference is that only the Ordinary Data Producer (ODP) can satisfy the satisfied interest of the legitimate user. Simultaneously, Malicious (Fake) Data Producer (MDP) will drop it. This phenomenon has little work, and the proposed countermeasure techniques are still limited to countering this attack. One of them is to change the NDN architecture by eliminating PIT in NDN routers [12], a system to promote identification of NCIFA or CIFA [13], using discreet wavelet analysis [14] and delivery method identified by Lee et al. [6].

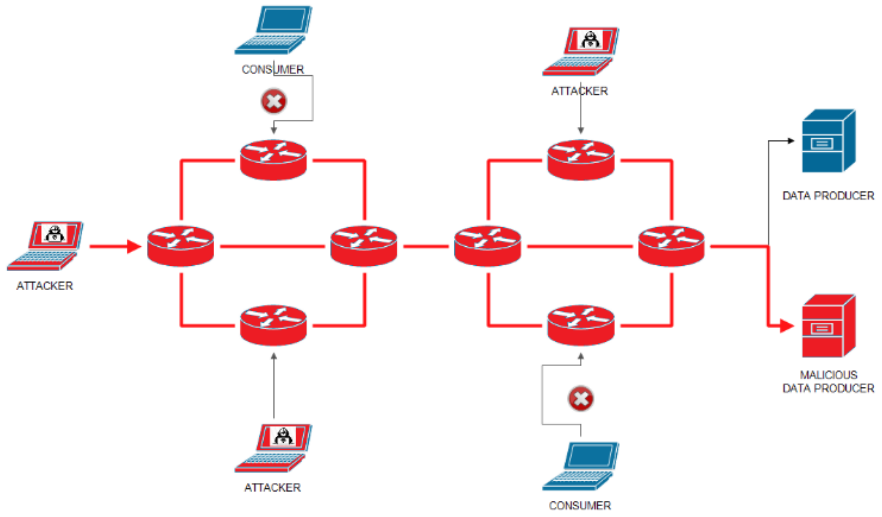

Fig. 3. Collusive interest flooding attacks (CIFA) model.

4. Experiment Design

To our best knowledge, no dataset is available to test the performance of the CIFA model in detecting and identifying CIFA in the NDN environment. All previous investigations used extensive simulation to record the signals generated using ndnSIM (NDN-based simulator) topology. The NDN router PIT entries will have a relatively long-term output value to ensure that the interest packet exists in the CS or NDN content producer. The default PIT entry time is recommended to 4 seconds [15].

4.1. CIFA signaling model

For such an attack, the CIFA signalling model had to be developed. Figure 4 shows the CIFA Signalling Model.

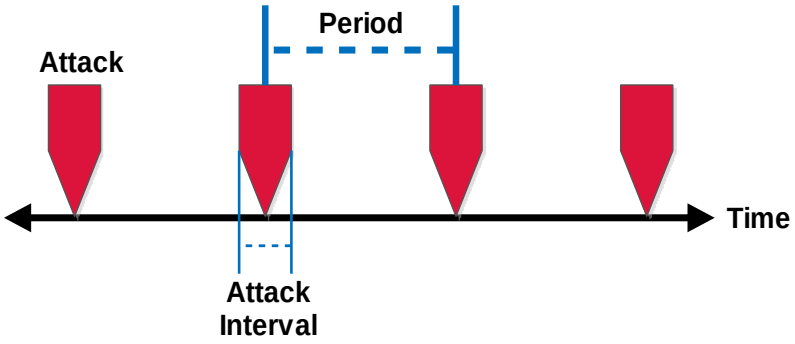

Fig. 4. CIFA signalling model.

In this signal, adversaries should halt until the next collusive Interest is sent. Once the MDP satisfies the last interest, sporadic and periodic attack traffic characteristics will be identified. As this process continues, collusive interest is transmitted to fill the PIT in a short time, the router responds to the attack and

forwards it to both data producers in the network. ODP will drop the request while MDP reverses the data packet. After receiving the data packet, the next collusive Interest is re-sent. This attack plan ensures maximum damage and extends to all namespaces. All NDN routers start with empty PIT entries. Where attackers start attacks, NDN routers receive an incoming interest and collectively generate PIT entries. Once at a specific time, PIT entries are fully occupied, it cannot accept any incoming interest. Since the PIT entries have an expiry period, the interest is released at another point so that the incoming interest can be received again. The attack will cause severe damage to the entire NDN network if the NDN router's attack time is not measured correctly at stopping status [16].

4.2. Malaysia's state named-data networking topology (MY-NDN)

Malaysia currently lacks NDN topology. This paper therefore proposes an NDN node topology based on Malaysia 's State, MY-NDN. In Malaysia, the federation consists of 16 nodes with 13 states and three federal territories, as shown in Fig. 5. All topology nodes are the primary nodes for IoT applications using NDN routers at the national level. We assume nodes are at the highest level or known as master nodes before adding and expanding the default MY-NDN topology.

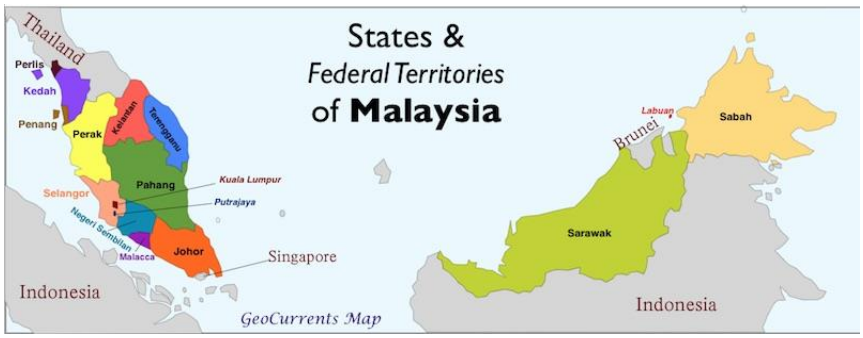

Fig. 5. States and federal territories of Malaysia.

As shown in Fig. 6, My-NDN has a total of 16 nodes, including ODP and MDP and a monitoring Node.

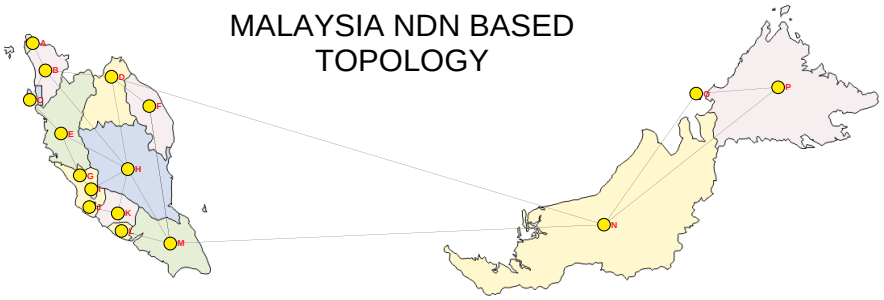

Fig. 6. MY-NDN topology.

Based on MY-NDN topology, the legitimate or ODP will be placed in Peninsular Malaysia. MDP will be in East Malaysia, while the monitoring node

will be in Johor State. Placing nodes is geographically located. A node is indicating each state.

4.3. Signal extraction procedure

The attacks primarily targeted malicious NDN nodes, which had a significant impact on PIT size, $\boldsymbol{PIT_{size}}(\boldsymbol{node}_{\{A,B,\dots P\}}) = (\boldsymbol{n})$ and satisfaction rates. The attacks are difficult to distinguish because the ODP serves legitimate interests while the MDP serves malicious interests. As a result, a MY-NDN topology-based monitoring router for the Internet of Things is deployed across the NDN network. Through a certificate route from ODP to Monitoring Router, the monitoring router distinguishes between legitimate and malicious interests. The signal extraction procedure is illustrated in Table 1.

Please note that the attacks are triggered on a $\boldsymbol{t_{alarm}}$, that first runs the attacking model with typical high-rate traffic attack, followed by CIFA in different execution. Each attack is executed once an attacking model is done and the system resource returns to idle mode. Results have many raw unclassified parameters which are ODP's Valid Interest Path, $\boldsymbol{I_{path}}(node_{x=\{A,B,\dots P\},x\neq\{D,G,M,P\}}) = \boldsymbol{is.exist}(\boldsymbol{x.path} \in \{\boldsymbol{path}:/\boldsymbol{MY/UMS/FCI}\})$.Valid Interest Satisfaction Rate, $\boldsymbol{I_{status}}(node_{x=\{A,B,\dots P\},x\neq\{D,G,M,P\}}) = \{\boldsymbol{satisfied}, \boldsymbol{unstatisfied}\}$.

MDP 's Malicious Interest Path $\boldsymbol{I_{path}}(node_{x=\{D,G,M,P\}}) = \boldsymbol{is.exist}(\boldsymbol{x.path} \in \{\boldsymbol{path}:/\boldsymbol{MY/UMS/FKI}\})$ and Malicious Interest Satisfaction Rate $\boldsymbol{I_{status}}(node_{x=\{D,G,M,P\}}) = \{\boldsymbol{satisfied}, \boldsymbol{unstatisfied}\}$.

These metrics will be pushed to the monitoring router because Interest (dummy certificate) has a similar digital signature in this simulation experiment.

Table 1. The procedure of signal extraction.

Initialise:
Simulate traffics with forwarded interests captured in monitoring router. Characteristics of signals include interest path, satisfaction rate, PIT Usage across NDN node and valid certification information at real-time.

Running:
Monitoring of NDN nodes from beginning till attack initiated. PIT Size overwhelm trigger at $\boldsymbol{t_{alarm}}$ triggered.

1. Load in MY-NDN Topology
2. Load in Attacking Model (CIFA | Normal High Rate Traffic Attack)
3. Initialise Attack Time, $\boldsymbol{Th} = \boldsymbol{Duration}(\boldsymbol{t_{attack}})$, assign to $\boldsymbol{t_{alarm}}$
4. Log PIT Size, $\boldsymbol{PIT_{size}}(\boldsymbol{node_x})$
5. Log Interest Path, $\boldsymbol{I_{path}}(node_x)$
6. Log Interest Satisfaction Status, $\boldsymbol{I_{status}}(node_x)$
7. Export the results in CSV

Table 1 shows the procedure of Signal Extraction from simulator. MY-NDN Topology is applied to deploy NDN nodes in Malaysia, this are high level nodes, using state as top level NDN router. Once the network is up, attack scheme is introduced to the network. For both attack, data to be capture such as

$\boldsymbol{PIT_{size}(node_x)}$, $\boldsymbol{I_{path}}(node_x)$ and $\boldsymbol{I_{status}}(node_x)$. After capture successfully, the data is exported and save as csv.

4.4. Network model and settings

The experiment captures the CIFA signal. We assume that all consumers send interest to the randomised idle time between two consecutive interests at constant average rates. This technique ensures that the user produces equal regular traffic without excessive buffering. Distributing content to legitimate consumers and attackers is done using Zipf-Mandelbrot, which guarantees uniform distribution and is available in the latest ndnSIM module [17]. Table 2 summarises simulation parameters and values.

Table 2. Main simulation parameters.

Parameters	Values
Link bandwidth (Mbps)	100
Link delay (ms)	10
Content Store Size	0
PIT Size	200
PIT Entry Life Time (s)	4
Zipf-Mandelbrot distribution (q, s)	0, 1
ODP Serving Name	/MY/UMS/FCI
MDP Serving Name	/MY/UMS/FKI
Legitimate Request Rate	50
Malicious Request Rate (δ, τ, T) δ = Attack Power τ = Attack Interval T = Period	10, 0.5, 5
Simulation Time (s)	0 - 300
Legitimate Request Time (s)	0 - 300
Malicious Request Time (s)	230 - 300

The extensive simulation loads MY-NDN topology as shown in Fig. 6. We assign Kuala Lumpur to the ODP node, Sabah to the MDP node, and Johor to the monitor node. Nine nodes are connected to legitimate consumer devices and four nodes to attackers. Moreover, the colluding interest generated by the attackers will be distributed globally, while legitimate requests follow Mandelbrot 's distribution.

5. Results Analysis

Each complete cycle is performed with the ndnSIM simulator for 300 seconds. Experiments are repeated iteratively until results almost consistent. Therefore, data are evaluated based on the best fit exponential rate.

$$y = e^{kx} \tag{1}$$

In Eq. (1), k is a constant that represents an exponential line's steepness. After the experiment, several comparisons are made between Normal High Rate Traffic Attack and CIFA. The experiments will be initialised using the proposed topology, as in Fig. 6, based on the suggested parameters in Table 1. The simulation begins with the Normal High Rate Traffic attack based on the set of parameters starting in

the 230s. There will be two types of attacks, high-rate legitimate requests (satisfied by ODP itself) for natural and CIFA attacks based on the model in Fig. 4 (satisfied by MDP). 200 entries will exhaust the limit of PIT entries. For further review, the current directory will collect and export all signals. This is important to understand the corresponding router and the attacks occur in that node or network.

5.1. Average PIT Size in attacking NDN node

In a similar timeframe, attack signals are collected and finalised with the typical PIT node. The experiments are assembled as indicated in the previous section. Figure 7 compares the PIT size between CIFA and Normal High Rate Attack. Before being targeted, the PIT frequency holds dynamically below 110 entries (< 230s) and ends with 200 entries (> 230s) when attacks occur. The graph clearly shows that for both scenarios, the PIT entries peaked. Based on the captured results, the PIT Usage is remaining 110 entries per second and below and when attack is initialised, PIT Usage are hitting the peak, close to 200 entries per second. But CIFA's reduced as a fluctuation due to timeout entries. The process continues until the simulation is finished. Note that the Normal High Rate Attack is not an attack by attackers, but a large volume of legitimate requests deployed in the NDN setting. However, as shown in Fig. 4, CIFA is a signal model showing a risky attack wave, and attacks include wave changes as they have components consisting of a constant attack interval and a halt time throughout the pattern of attack.

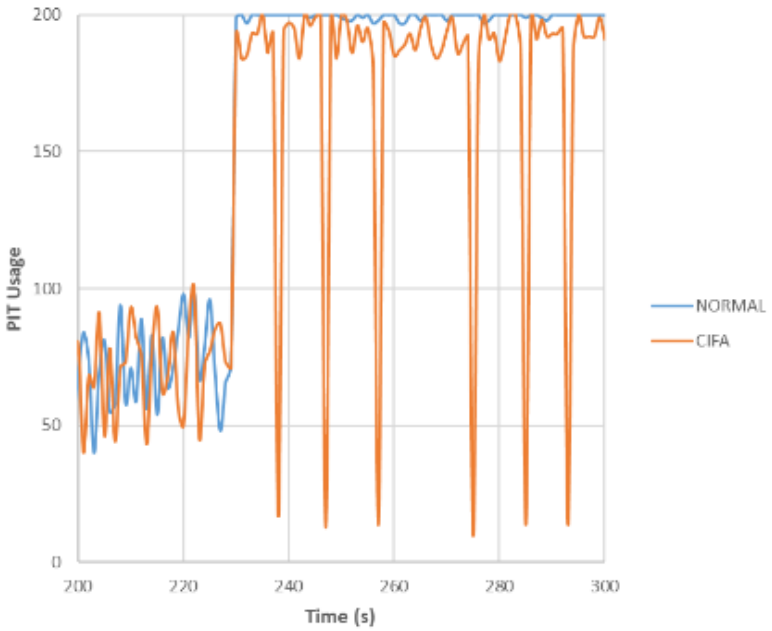

Fig. 7. Comparison of PIT size between normal high rate traffic attack and CIFA.

5.2. Throughput comparison

Throughput is a common way of measuring how effectively packets reach the destination. Figure 8 shows a comparison of CIFA and typical traffic throughput.

The attacker sends collusive Interests packets of $\tau = 0.5s$ and remains idle of $T = 5s$ in CIFA. Both scenarios are measured against simulation time. Based on the captured results, the throughput is caping at below 500 packets per second and hitting above 1000 packets per second when attack is initialised. The throughput clearly shows the impact of the PIT size hitting the peak and depleting network resources as soon as the attacks start. From the findings, we conclude that CIFA is deceptive, and discriminating against raw signals is challenging. However, CIFA can be distinguished from traditional attack models by following the processing pattern. The sudden increase and decrease in throughput can be used to distinguish CIFA and conventional attacks.

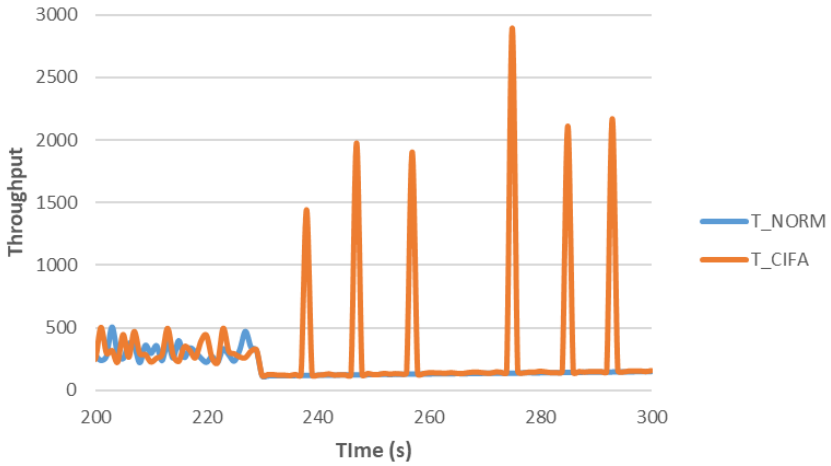

Fig. 8. Throughput comparison between normal high rate traffic attack and CIFA.

5.3. Trendline comparison

Trendline lets researchers determine general graph trends. Figure 9 shows a comparison of the pattern of attack, suggesting that CIFA misleads the trend of results in which the overall trend is exponential. The CIFA and regular traffic signals act similarly, having an intersection when no attacks occur. Contrary, both signals differ on the basis of an exponential trend graph, where typical high-rate traffic growth rates are higher than the CIFA attack.

Based on the captured results, the trendline shows a significant difference before and after the attack. Prior to the attack, the trendlines of both signals were trending in the same direction. When such attacks occur in the network, the steeper the exponential plots indicate a high level of attack and risk. Normal high-rate attacks are more dangerous than CIFA because they completely disrupt the service, causing the entire network to fail. On the other hand, CIFA interferes with the service for a specified period, leading to temporary network inaccessibility but restoring normal performance and remaining for a short time. It had a lot of existing research on it for the normal high-rate attack, but much less approach in distinguishing and countermeasure CIFA.

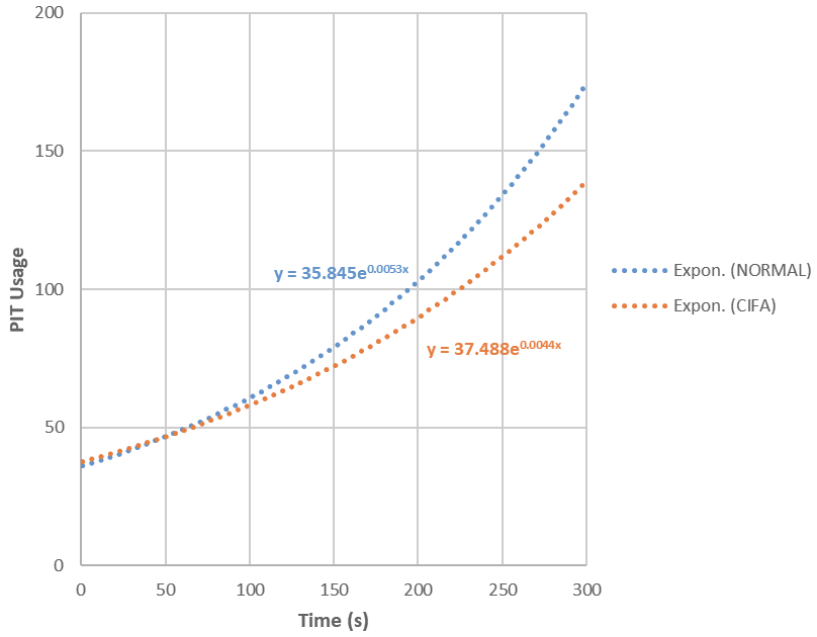

Fig. 9. Trendline between normal high rate traffic attack and CIFA.

6. Conclusion and Future Work

Our primary contribution is a definitive CIFA signalling model that we feed into the MY-NDN topology via extensive NDN simulations. The purpose is to generate a hypothesis for the proposed topology, which is illustrated at the highest level of backbone nodes and is ready for connection to gateway and user nodes. Although the scale is small, it contains sufficient nodes for us to study and its effect can also be accurately simulated to demonstrate the effect of CIFA on the NDN network.

The Collusive Interest Flooding Attacks described in this paper involve adversaries transmitting interest to an MDP collecting PIT resources on a targeted NDN router. The distribution of requested consumer content is guaranteed to adhere to the zipfmandelbort distribution. The impact of CIFA on the NDN network is examined through three lenses: PIT utilisation, throughput comparison, and trendline comparison. The PIT usage should be kept below 100 entries, the throughput should be kept below 500, and the trendline should not be steep before an attack is initiated.

After the attack is initiated, PIT usage remains above 180 entries and close to the peak level, throughput is greater than 1000, and the trendline exhibits an exponential difference. This type of attack is referred to as a PIT-oriented routing attack because it results in relatively minor changes in average network traffic, making it difficult to distinguish between legitimate and malicious requests. In comparison to conventional IFA or even normal high-rate traffic attacks, CIFA manipulates the attack pattern to meet legitimate demands. Long-term attacks can degrade performance and exhaust the resources of NDN routers.

This paper will aid in the future development of a CIFA defence system capable of identifying and isolating MDP and suspicious requestors from the NDN network.

Acknowledgement

This work was funded by Acculturation Grant Scheme (SGA), Universiti Malaysia Sabah (Grant No: SGA0087-2019). The authors would like to thank Faculty of Computing and Informatics, Universiti Malaysia Sabah.

References

1. Boyes, H.; Hallaq, B.; Cunningham , J.; and Watson ,T. (2014). The industrial internet of things (IIoT): An analysis framework. *Computers in Industry*, 101, 1-12.
2. Amadeo, M.; Campolo, C.; Iera, A.; and Molinaro, A. (2014). Named data networking for IoT: An architectural perspective. 2014 *European Conference on Networks and Communications* (*EuCNC*), Bologna, Ital, 1-5.
3. Cisco. (2016). *Cisco global cloud index: Forecast and methodology*. Cisco White Paper, 2015-2020.
4. Ting, L.R; Leau, Y.-B; Park, Y.J; and Obit, J.H. (2018). Enhancing the performance of elliptic curve digital signature algorithm (ECDSA) in named data networking (NDN). 2018 8th *IEEE International Conference on Control System, Computing and Engineering* (*ICCSCE*), Penang, Malaysia, 65-69.
5. Yi, C.; Afanasyev, A.; Moiseenko, I.; Wang, L.; Zhang, B; and Zhang, L. (2013). A case for stateful forwarding plane. *Computer Communications*, 36(7), 779-791.
6. Lee, R.T; Leau, Y.B; Park, Y.J; and Obit, J.H; (2020). *A perspective towards NCIFA and CIFA in named-data networking architecture*. Springer Lecture Notes in Electrical Engineering, 481-490.
7. Alex, A.; Jeff, B.; Tamer, R.; Lan, W.; Beichuan, Z.; and Lixia, Z. (2018). A brief introduction to named data networking. *IEEE Military Communications Conference* (*MILCOM*), Los Angeles, United States, 1-6.
8. Afanasyev, A.; Moiseenko, I.; and Zhang, L. (2012). ndnSIM: NDN simulator for NS-3 (Technical Report NDN-0005). Retrieved January 1, 2021, from https://named-data.net/publications/techreports/trndnsim/.
9. Ahlgren, B.; Damnewitz, C.; Imbrenda, C.; Kutscher, D.; and Ohlman, B. (2012). A survey of information-centric networking. *Communications Magazine*, 50(7), 26-36.
10. Compagno, A.; Conti, M.; Gasti, P.; and Tsudik, G. (2013). Poseidon: Mitigating interest flooding DDos attacks in named data networking. 38th *Annual IEEE Conference on Local Computer Networks* (*LCN*), Sydney, NSW, Australia, 630-638.
11. Dai, H.; Wang, Y.; Fan, J.; and Liu, B. (2013). Mitigate DDoS attacks in NDN by interest traceback. 2013 *IEEE Conference on Computer Communications Workshops* (*INFOCOM*) *Workshops*, Turin, Italy, 381-386.
12. Ghali, C.; Tsudik, G.; Uzun, E.; and Wood, C.A. (2015). Living in a PIT-less world: A case against stateful forwarding in content-centric networking. *Computer Science - Networking and Internet Architecture*, Cornell University, New York.
13. Hani, S.; Julian, W.; and Thorsten, S. (2015). Coordination supports security: A new defence mechanism against interest flooding in NDN. *Proceedings of*

the 40*th Annual IEEE Conference on Local Computer Networks*. Florida, United States, 73-81.

14. Xin, Y.; Li, Y.; Wang, W.; Li, W.; and Chen, X. (2017). Detection of collusive interest flooding attacks in named data networking using wavelet analysis. *MILCOM* 2017 - 2017 *IEEE Military Communications Conference* (*MILCOM*), Baltimore, MD, USA, 557-562.
15. Kuzmanovic, A.; and Knightly, E.W. (2003). Low-rate tcp-targeted denial of service attacks: the shrew vs. the mice and elephants. *SIGCOMM '*03*: Proceedings of the* 2003 *conference on Applications, technologies, architectures, and protocols for computer communications*. New York, United States, 75-86.
16. Mastorakis, S.; Afanasyev, A.; and Zhang, L. (2017). On the evolution of ndnSIM: an open-source simulator for NDN experimentation. *ACM SIGCOMM Computer Communication Review*, 47(3), 19-33.
17. Ding, K.; Liu, Y.; Cho, H.; Chao, H.; and Shih, T.K. (2016). Cooperative detection and protection for interest flooding attacks in named data networking. *International Journal of Communication Systems*, 29(13), 1968-1980.