Fast Detection and Traceback-based Mitigation of Interest Flooding Attack

Naveen Kumar (nk10121989@gmail.com)
Siksha O Anusandhan University https://orcid.org/0000-0003-0882-3119
Shashank Srivastava
Motilal Nehru National Institute of Technology

Research Article

Keywords: Named Data Networking, NDN, Interest Flooding Attack, ANN, Feature Selection, Traceback

Posted Date: April 27th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-437520/v1

Noname manuscript No.
(will be inserted by the editor)

Fast Detection and Traceback-based Mitigation of Interest Flooding Attack

Naveen Kumar · Shashank Srivastava

Received: date / Accepted: date

Abstract NDN Pending Interest Table (PIT) helps NDN by storing the state of a request within the router. This state information helps the router to redirect the data packet towards the requester. However, an attacker can send malicious requests, which could flood the PIT; this attack is known as Interest Flooding Attack (IFA). In our previous work, we have found the most relevant features needed to detect IFA and applied a few machine learning approaches for the offline detection of IFA. In this article, a trained Artificial Neural Network (ANN) classifier has been deployed on each NDN router for the online detection of IFA. A novel traceback-based mitigation is proposed, which is triggered after the detection. The proposed approach is found better than the previous approach in terms of the satisfaction ratio and throughput of the legitimate consumers.

Keywords Named Data Networking; NDN; Interest Flooding Attack; ANN; Feature Selection; Traceback

1 Introduction

The TCP/IP model, which was earlier developed to overcome the problem of communication among hosts, is now being used for sharing content. Many hacks such as P2P network [5] and Content Delivery Network (CDN) [19] as an overlay are being tried for adopting TCP/IP for content sharing. However, the content has to face delays due to the underlying network.

New types of networks specially designed to support content sharing are being developed to overcome this problem. These networks use the name of the

N. Kumar
Shiksha 'O' Anushandhan University, ITER
E-mail: naveenkumar@soa.ac.in

S. Srivastava
Motilal Nehru National Institute of Technology Allahabad

content rather than the address of the host. These networks come under the umbrella of Information-Centric Networking (ICN) [3]. Few examples of the ICNs are DONA [16], COMET [10], Content-Centric Networking (CCN) [14], and Named Data Networking (NDN) [22].

Recently NDN evolves as the most prominent candidate among all ICNs [**?**]. NDN overcomes the problem of content sharing by in-network caching and fetching the content using its name. NDN is more secure than the TCP/IP as the trust model between the producer and consumer ensures the data packet's provenance and integrity. Confidentiality can be ensured by additionally encrypting the data packet. However, NDN is vulnerable to new types of attacks, such as IFA [11], cache privacy attack [4], cache pollution attack [11], content poisoning attack [12].

The attacks mentioned above either degrade QoS or affects the privacy of the user. However, IFA can cease the flow of traffic through the network. This makes IFA more severe than other NDN attacks. The attacker floods PIT by intentionally requesting non-existing contents. Entries get created in the PITs of the in-between NDN routers due to these requests. Thus PIT becomes unavailable for the legitimate users because these malicious entries persist in PIT till timeout.

Most of the previous approaches [1,8,7,20,21,23] detect IFA using one or two features based on static thresholds. However, the features which are necessary for attack detection have not been analyzed in the previous works. In our previous work [17,18], 12 features have been analyzed that get affected due to IFA, out of which 9 features were chosen using information gain [15] based ranking. Four different machine learning approaches were applied out of which two approaches, i.e., Multi-Layer Perceptron (MLP) with BackPropagation (BP) [9,13] and J48 [13], were found better. This paper deals with the online detection and mitigation of IFA. Few changes have been made to our previous work to adapt it for the online IFA detection. The detection is divided into two phases, i.e., malicious interface detection and malicious prefix detection. For the detection of the interface, we have taken only those features which are computed per interface.

After doing the above changes, the feature selection is re-performed using information gain based ranking. Then ANN classifier is trained using the selected features. The trained ANN classifier is deployed on the router for online detection; the outcome of detection is a malicious interface. After detecting the malicious interface, the malicious prefix is detected using a statistical approach. Traceback-based mitigation is applied after the detection of IFA. The proposed approach is compared with [7] approach.

The major contributions of this paper are:

- Performing IFA on Tree topology and DFN like topology.
- Selecting the most appropriate features for IFA detection.
- Offline detection of IFA using the ANN classifier.
- Deploying trained ANN detector in the NDN router.
- A traceback-based mitigation approach for IFA.

– Comparison of the proposed approach with the previous approach.

The rest of the paper is organized as follows. Section 2 presents basic NDN architecture. Section 3 presents the work done by researchers for the mitigation of IFA. Section 4 presents the proposed IFA mitigation approach. Section 5 describes the experimental setup and results. Section 6 discusses the conclusion and future work.

2 Background Details

NDN uses two types of packets for a communication, i.e., interest packet and data packet. The contents are requested using the interest packet. The data packet contains actual content that acts as a reply to the interest packet.

There are three data structures that are used by NDN, i.e., Pending Interest Table (PIT), Forwarding Information Base (FIB), and Content Store (CS) for forwarding interest and data packet. PIT stores the interest packet's name and the interface on which the interest packet is received until the matching data packet is received. The FIB is like the routing table in TCP/IP. It has a list of named prefixes and the interfaces from which the interest packet should be forwarded. The CS caches the contents received by the router.

NDN forwarding pipeline is shown in Figure 1. Upon receiving an interest packet, the router searches CS for the matching data packet; if it is found, it is replied through the interface from which the interest packet is received. Else, a lookup is performed by the router in the PIT for finding the matching entry. If a matching entry is found, the corresponding interface is added to the matching PIT entry's interface list. Otherwise, a new entry is created in the PIT. Additionally, the interest packet is forwarded through the interface given by FIB. When a router receives a data packet, it searches for the matching PIT entry. If a matching entry is found, the data packet is forwarded through interfaces present in the matching PIT entry, and the data packet is cached in the CS. Else, the router will drop the data packet.

3 Related Work

The DoS attack in NDN was introduced as "interest flooding" by [11]. [11] have given a countermeasure in which the attack is detected using stats such as pending interest packets per outgoing interface, interest packets per incoming interface, and pending interest packets per namespace. The router reduces the PIT quota for the malicious namespace on the malicious interface after the IFA detection. This information is propagated to downstream routers, which applies a countermeasure on the malicious interface. The authors have not provided an implementation or evaluation of their approach.

[1] have proposed three algorithms that apply a limit to interest packets that are forwarded through each interface. These algorithms are token bucket with per-interface fairness, satisfaction-based Interest acceptance, and

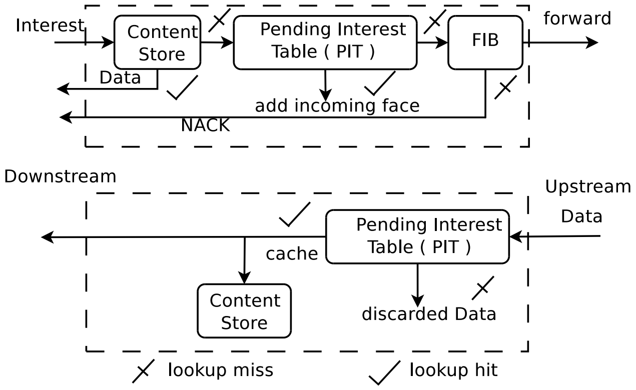


Fig. 1 NDN Forwarding Pipeline

satisfaction-based pushback algorithm. In the first algorithm, each outgoing interface has a fixed share of PIT entries, which is equally distributed among all the incoming interfaces. In the second algorithm, the router allows interest packets based on the satisfaction ratio of interfaces. In the third algorithm, a limit is given to each incoming interface to satisfy the interest packets. The routers announce limits to downstream neighbors, which are used by the neighbors to set their limits. The limitation of these algorithms is that they restrict every packet on the malicious interface; thus, legitimate interest packets may also suffer. Also, this approach does not stop the attacker from attacking.

[8] have used PIT size as a metric for the detection of IFA. When the PIT size increases more than a threshold, the router looks for an unsatisfied interest packet with the longest name. This interest packet is replied with a spoofed data packet, which contains information about malicious namespace. The originating router applies a filter on the malicious interface after receiving the spoofed data packet.

[7] have proposed a framework called Poseidon for the detection and mitigation of IFA. It uses two parameters for IFA detection, i.e., the ratio of incoming & outgoing data packets and PIT space per interface. The attack is detected when both the parameters exceed a predefined threshold. The interest packets received on the malicious interface are dropped after the IFA detection, and an alert message is sent through the malicious interface. The router decreases the threshold value of the above two parameters on receiving the alert message. In this approach, the mitigation is applied to an interface; therefore, incoming legal interest packets may also suffer from IFA.

[20] have proposed an approach called Disabling PIT Exhaustion (DPE) for IFA mitigation. Each router has a malicious list (m-list) which contains the number of expired interest packets for each namespace as a parameter for IFA detection. When this parameter goes beyond a predefined threshold, then the namespace present in the corresponding m-list is considered malicious. The router will not create an entry for the malicious namespace. The malicious namespaces remain in the m-list till decay time.

[21] have proposed a collusive IFA detection approach based on wavelet analysis. This approach uses a namespace frequency distribution called Power Spectral Density (PSD) as a parameter for IFA detection. When the value of PSD low, the collusive IFA is detected. The authors have chosen the detection threshold experimentally. The main drawback of this approach is it is only applicable to collusive IFA.

A detection approach should be accurate, fine-grained, and fast. Most of these approaches rely on the detection or mitigation of IFA using one or two features. The IFA mitigation is done based on a statistical threshold. These approaches are fast, but they have low accuracy, and they are not fine-grained (detect interface as well as a malicious prefix). We have used six different features to detect malicious interfaces. These features are selected from eleven features based on IG-based ranking. These features are used to train ANN, whose accuracy is 98.5%. This approach is faster as time is only consumed in the training phase; once the ANN is trained, the detection takes few milliseconds. This trained ANN is deployed in the NDN router for the online detection of the malicious interface. After the malicious interface detection, the malicious prefix has been detected. After detection, we have applied traceback-based mitigation. Thus, the proposed approach is accurate, fine-grained, and fast.

4 Interest Flooding Attack

IFA makes network services unavailable for legitimate consumers. [11] proposed three types of IFA based on interest packets used for the attack, i.e., Type-1 (existing or static), Type-2 (dynamically-generated), and Type-3 (non-existent). In Type1, the existing set of contents is requested repeatedly. These contents are cached by the nearby routers due to which the requests are satisfied by the CS. Thus, less number of PIT entries are created. In Type2, the attacker generates dynamic contents which are satisfied by the producer on demand. The producer spends some time creating these contents. Thus, this attack affects a producer as well as a router. In Type-3, the attacker requests non-existing contents. These requests create PIT entries that are not satisfied. PIT entries corresponding to the requests remain in the PIT till timeout. Thus, PIT Type-3 is more severe than Type-2 because the PIT entries created due to the Type-3 attack remain in PIT until timeout and timeout duration is large. This article considers only Type-3; in the rest of the paper, IFA means Type-3.

Figure 2 demonstrates IFA in NDN on a simple topology. It has one consumer, one attacker, and one producer. The producer publishes content corresponding to prefix “/prefix.” The attacker sends a large number of synthetic interest packets by concatenating the prefix with a random string. These interest packets are forwarded to the publisher by the NDN routers. This results in the creation of PIT entries on the routers which are present in the path fol-

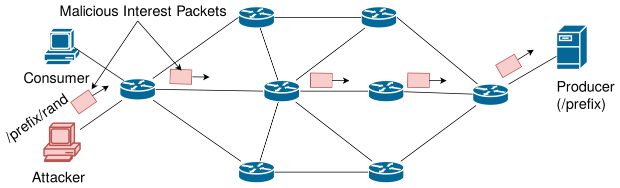


Fig. 2 IFA Demo

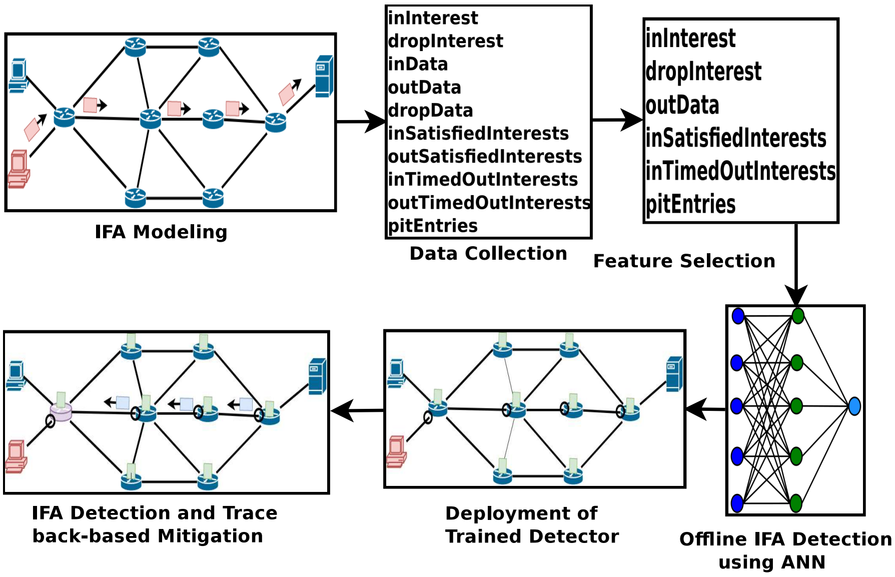
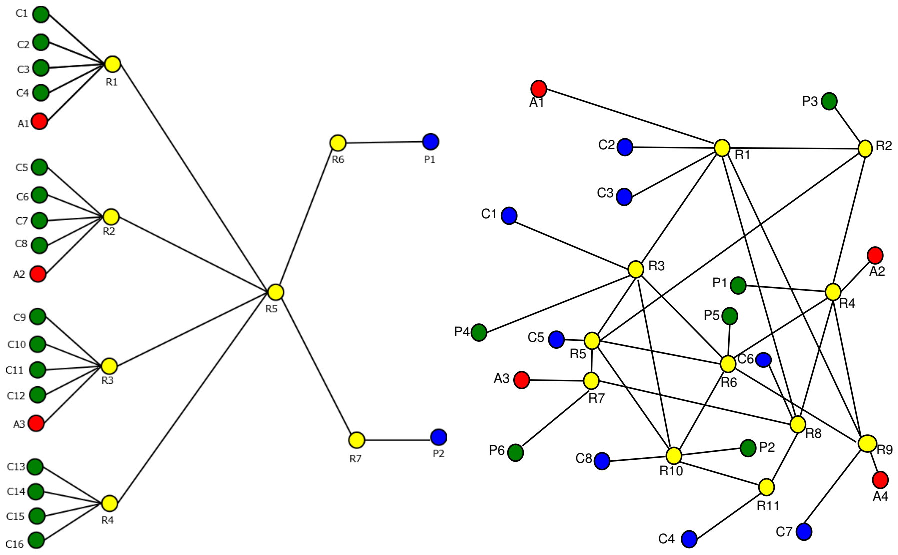


Fig. 3 Series of Processing Done for the Mitigation of IFA

lowed by the malicious interest packets. These entries consume PIT, making it unavailable for legitimate users.

The following series of processing has been done for the mitigation of IFA.

1. IFA Modeling and Implementation– In this phase, the simulation of IFA is done using ns-3 based ndnSIM [6] simulator.
2. Data Collection– In this phase, the relevant features are collected from the simulator and pre-processing is performed to make them suitable for further processing.
3. Feature Selection– In this phase, Information Gain based feature selection is applied to select the most relevant feature set.
4. IFA Detection– In this phase, the selected features are used for the offline detection of IFA using MLP with BP. After the off line detection, the trained detector is deployed in the NDN routers for the online IFA detection.
5. IFA Mitigation– A traceback-based detection is applied for the mitigation of IFA.



(a) (b)

Fig. 4 Topologies Considered for Attack Modeling (a) Tree Topology and (b) DFN like Toplogy

These phases are shown in Figure 3 and are described in detail in the following subsections:

4.1 IFA Modeling

The ndnSIM network simulator is used for modeling the attack scenario on Tree topology and DFN like topology which is shown in Figure 4(a) and Figure 4(b). The routers, consumers, attackers, and publishers are shown in the figure as R*, C*, A*, and P*, respectively, here * represent a number. The size of the PIT and the expiration time for a PIT entry is taken as 1200KB and 4 seconds for both the topologies. CS uses LRU as replacement policy and can has maximum 100 entries. The length of the queue and the delay for the point-to-point link are taken as 1000 and 10ms, respectively.

All the scenarios for the Tree and DFN like topology run for 300 seconds of simulation time, and the consumers are active in the whole duration. The consumers send interest packets with a frequency of 100 packets, and the attackers request the malicious interest packets with a frequency of 400 packets for the Tree topology. Whereas for the DFN like topology, the consumers send interest packets with a frequency of 200 packets, and the attackers request the malicious interest packets with a frequency of 800 packets. The attackers are active in the duration of 100s-200s of simulation time.

4.2 Data Collection

Data corresponding to 11 different features has been collected after every 500ms. These features are InInterest, OutInterest, DropInterest, InData, OutData, DropData, InSatisfiedInterests, OutSatisfiedInterests, InTimedOutInterests, OutTimedOutInterests, and PitEntries. The description of these features is given in Tab. 1.

Table 1 Features used for the Detection of IFA and its IG Values

Parameters	Meaning	Consider	IG value
InInterests	Interest packets received per interface	Yes	0.38165
OutInterests	Interest packets sent per interface	No	0.03374
DropInterests	Interest packets dropped per interface	Yes	0.15831
InData	Data packets received per interface	No	0.03332
OutData	Data packets sent per interface	Yes	0.09666
DropData	Data packets dropped per interface	No	0.01915
InSatisfiedInterests	Satisfied interest packets received per interface	Yes	0.09666
OutSatisfiedInterests	Satisfied interest packets sent per interface	No	0.03332
InTimedOutInterests	Timeout interest packets received per interface	Yes	0.16082
OutTimedOutInterests	Timeout interest packets sent per interface	No	0.00988
PitEntries	A number of PIT entries per interface	Yes	0.32461

This data is used for selecting the most appropriate features from the feature set.

4.3 Feature Selection

Information Gain (IG) based feature ranking is used for selecting the most appropriate features for IFA detection. The process of selecting features is as follows:

1. Calculate the entropy H(x) for the data set using the formula given below:

$$H(x) = -\sum_{i=1}^{n} p_i log_2 p_i \tag{1}$$

   Here, x is a random variable which takes values $V_1, V_2, ..., V_n$ and $p_1, p_2, ..., p_n$ are respective probabilities of occurrence of $V_1, V_2, ..., V_n$.
2. Information gain of a given feature F_i can be calculated uisng equation below:

$$H(x) = -p_1 log_2 p_1 - p_2 log_2 p_2 \tag{2}$$

3. The fetuares are sorted according to their IG values.
4. Features with high IG values are selected for IFA detection.

The data pre-processing, feature selection, and classification are done using the Waikato Environment for Knowledge Analysis (WEKA) [2]. It is an open-source Java-based application licensed under the GNU General Public

Table 2 Description of mList

Parameter	Meaning
interface	malicious interface
prefixList	malicious prefix list
numPITEntries	number of PIT entries per interface

License. It has collection algorithms for data preparation, classification, regression, clustering, association rules mining, and visualization. Tab. 1 shows eleven features which are used for the analysis of IFA with the corresponding IG values. Out of the eleven features, six prominent features are chosen for IFA detection. These features are InInterest, DropInterest, OutData, InSatisfiedInterests, InTimedOutInterests, and PitEntries. After selecting the most appropriate feature-set the next step is to apply machine learning approach for the classification of traffic.

4.4 IFA Detection

In our previous article [18] we have shown that the ANN classifier is more suitable for the detection of IFA as It has higher accuracy, less training time, and it is easy to deploy. Therefore, a ANN classifier is used for the classification of traffic, and the backpropagation algorithm is used for training the ANN. The detection approach is evaluated using four matrices– accuracy, precision, sensitivity (or recall), and specificity. Ten-fold cross-validation is used for the assessment of the classifier.

4.4.1 Artificial Neural Network based Classifier

A single hidden layer ANN classifier is used for the classification of traffic. This ANN classifier has three layers of neurons, i.e., the input, hidden, and output layer. Same number of neurons are taken for the input and the hidden layer. All the weights in the ANN classifier are updated using the backpropagation [13]. The result of detection is given in Tab. 2. This trained detector is deployed on each router for the detection of malicious interface. The proposed detection approach has already been compared with the previous approaches in our previous work [18].

4.5 IFA Mitigation

In the previous section, we have seen that the ANN classifier checks all the interfaces of each router for finding the malicious interfaces. After this detection phase, the mitigation phase is triggered to cease the attackers. The proposed approach follows a traceback mechanism that traces an attacker attached to a gateway router and then applies the filter to the interface through which the attacker is connected.

Algorithm 1 Periodic Stats Collection And Detection

```
procedure PeriodicStatsCollectionAndAttackDetection($k, detectionInterval$)
    for $j = 0$ ; $j < numInt$ ; $j++$ do
        $stats$ = getStats()
        $isM$ = trainedDetector($stats$)
        if $isM = true$ then
            createNewEntryOrUpdate($j$)
            if $isAccessRouter = true$ then
                removePITEntries($j$)
            else
                prefixList = extractTopKPrefixes($j$ , $k$)
                sendAlertMessage($j, prefixList$)
                removePITEntries($j, prefixList$)
        else
            $it$ = findInMList($j$)
            if $getPIT(j) > PITSize/4$ then
                $mList.erase(it)$
    $sleep(detectionInterval)$
function createNewEntryOrUpdate($j$)
    $it$ = findInMList($j$);
    if it == mList.end() then
        $ml$ = CreateObject<MList>();
        $ml.interface = j$;
        $ml.numPIT = getPIT(j)$;
        $mList.push_back(ml)$;
    else
        $it.numPIT = getPIT(j)$;
function sendAlertMessage($j, prefixList$)
    data = Create<Data> ("/alert");
    data.append (prefixList);
    sendData(data, j)
```

A data structure called *mList* is used for storing information about malicious interfaces. The *mList* gets updated periodically after the detection interval. The interest packets which are received from the interfaces present in the *mList* are restricted on the access routers. For the non-access routers, the interest packets are restricted only when their PIT share exceeds a limit. The detail of the *mList* data structure is given in the Tab. 2.

The proposed approach is described using three algorithms, i.e., Algorithm 1 (Periodic Stats Collection And Detection), Algorithm 2 (OnInterest), and Algorithm 3 (OnData). Algorithm 1 runs on each router periodically after a fixed period called *detectionInterval*. Algorithm 2 and Algorithm 3 are called when a router receives an interest packet and data packet, respectively. The detailed description of these algorithms is given below.

The Algorithm 1 extracts stats which are discussed in Section 4.2 and passes it to the trained detector to detect whether an interface is malicious or not. On the detection of a malicious interface, the router checks entry corresponding to the interface in the m-List. Else, the router calls a function *createNewEntryOrUpdate*, which creates a new entry if the entry does not exist. Otherwise, the router sets *numPIT* field to number entries that exist in the PIT for the interface. In the newly created entry $interface$ field is set to the interface on which the attack is detected, $numPIT$ field is set to the number of entries exist in the PIT for the interface.

Algorithm 2 On Interest

```
procedure OnInterest($interest, inFace$)
    $it$ =findInMList($inFace$);
    if $isAccessRouter = 1$ && $it! = mList.end()$ then
        $return$
    else
        if $it! = mList.end()$ then
            if $it.numPIT \geq PITSize/numInt$ then
                return
    Normal interest packet processing
```

Algorithm 3 OnData

```
INPUT: $inFace, data$
  procedure OnData($data$, $inFace$)
      if $data$.GetName() == "/alert" then
          onAlert($data$, $inFace$)
          return
      Normal data packet processing
  function onAlert($data, face$)
      $pl$ = $data$.getPrefixList()
      maxPrefixInt = searchInterfaceMaxPrefix($pl$)
      if $isAccessRouter = true$ then
          removePITEntries($maxPrefixInt$);
          createNewEntryOrUpdate($maxPrefixInt$);
      else
          sendAlertMessage($maxPrefixInt$, $pl$);
```

Next, if the router is an access router, then it removes all the PIT entries corresponding to the interface. Else, the router creates a $prefixList$ by extracting top k prefixes from the PIT corresponding to the interface and $prefixList$. The interface and $prefixList$ are passed to the $sendAlertMessage$ function, which creates a data packet having name field set to "/alert." The $prefixList$ is concatenated to the name field of the data packet then the data packet is sent through the interface. After sending the alert message, the router removes all the PIT entries corresponding to the $prefixList$ and interface.

The $OnInterest$ and $OnData$ functions are called when the interest packet and data packet respectively are received on the router. When an interest packet is received on an interface, then the router first checks the $mList$ for the matching entry. If the entry is found and the router is an access router, then the packet is dropped. Otherwise, if number of PIT entries occupied by the interface is greater than the allowed PIT quota for the interface, then the packet is dropped. If the interest packet is not dropped, then it is processed according to the normal NDN forwarding pipeline.

When the router receives a data packet, it first checks the whether the message is an alert message or not. If it is an alert message, then a function *onAlert* is called which searches interface ($maxPrefixInt$) on which the maximum number of malicious traffic is received. If the router is an access router, then PIT entries corresponding to $maxPrefixInt$ is removed, and *createNewEntryOrUpdate* function is called, which updates the corresponding *mList* or creates new *mList*. Else the alert message is forwarded through the $maxPrefixInt$.

5 Experimental Result

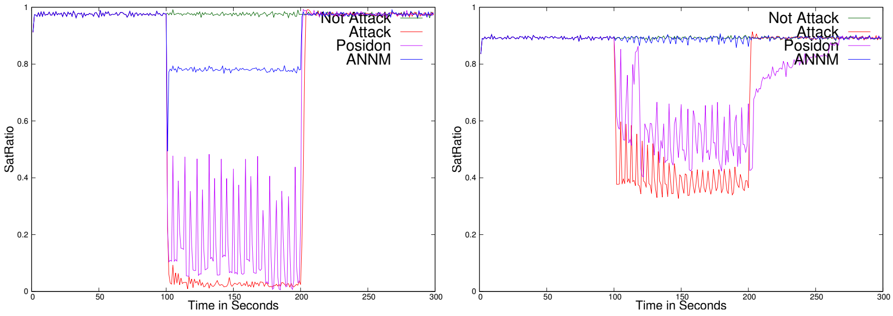
Experimental setup has already been described in Section 4.1. The proposed approach has been compared with [7] approach. Following are the different scenarios considered for the evaluation of the proposed approach.

1. Not Attack: In this scenario, only the consumers are active. Thus no attack traffic flow through the network.
2. Attack: In this scenario, the consumers and the attackers both are active simultaneously.
3. Poseidon: In this scenario, the consumer & the attackers both are active, and the Poseidon approach is applied to each router for the mitigation of IFA.
4. ANN based Mitigation (ANNM): In this scenario, the consumers and the attackers both are active, and our NN based countermeasure is applied to each router for the mitigation of IFA.

Three matrices are used for the comparison, i.e., Satisfaction Ratio (SR), Average PIT Size (APS), and Throughput. The details of these matrices are given below:

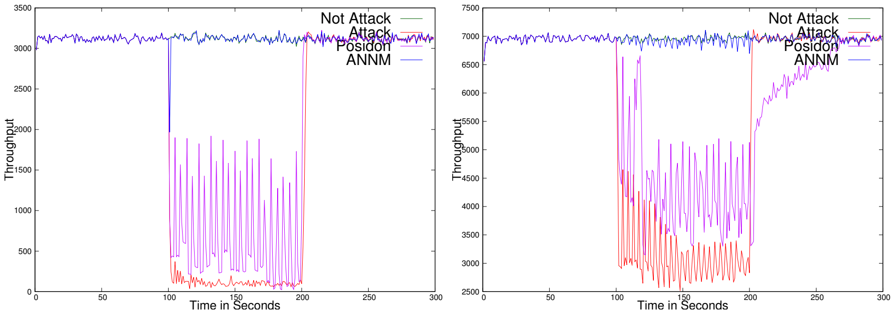
1. Satisfaction Ratio: It is the ratio of the number of data packets received to the number of interest packets sent with respect to time. This is the most commonly used metric for the evaluation of the IFA mitigation approach.
2. Average PIT Size: It is the average of PIT size of all the routers with respect to time.
3. Throughput: It is the number of data packets received by the consumers after sending the interest packets with respect to time.

Figure 5(a) and Figure 5(b) show the SR of the legitimate consumers with respect to time for Tree and DFN like topology respectively. In the case of the Tree topology, the satisfaction ratio is approximately one when no attack is going on. For the Tree topology, the SR drops to 0.0092, which is 99% drop as compared to the normal traffic in the attack scenario. The Poseidon approach shows a fluctuation of SR between 0.5 to 0.01 during the attack. ANNM shows a sudden drop in SR, which reaches 0.5 at the starting of the



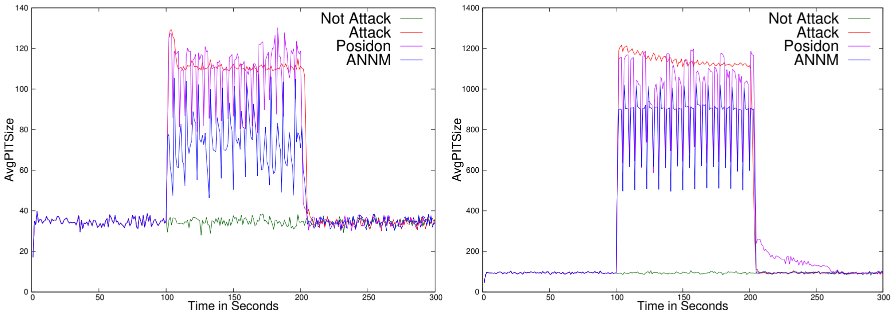
(a) (b)

Fig. 5 Satisfaction Ratio (SR) of Normal Consumers w.r.t. Time for (a) Tree Topology and (b) DFN like Toplogy



(a) (b)

Fig. 6 Throughput of Normal Consumers w.r.t. Time for (a) Tree Topology and (b) DFN like Toplogy



(a) (b)

Fig. 7 Average PIT Size of Routers w.r.t. Time for (a) Tree Topology and (b) DFN like Toplogy

attack. A second later, the SR increases to 0.78 after this the SR shows a little fluctuation between 0.76 to 0.79. This shows the effectiveness of the proposed ANNM approach.

A simillar behaviour can be seen in case of DFN like topology. In the case of DFN like topology, the satisfaction ratio is approximately 0.9 when no attack is going on. For the DFN like topology, the SR drops to 0.327 in the attack duration. The Poseidon approach shows a fluctuation of SR between 0.403 to 0.67 during the attack. The proposed ANNM approach shows a minor fluctuation in SR between 0.86 to 0.9. A similar trend can be seen in the Figure 6(a) and Figure 6(b) in the Throughput metric for Tree and DFN like topology, respectively.

Figure 7(a) and Figure 7(b) show the average PIT size with respect to time for the Tree and DFN like topology respectively. For the Tree topology, the PIT size for the normal scenario fluctuates between 28 to 40. In the attack scenario, the size of the PIT fluctuates between 76 to 130 during the attack (100s-200s). The Poseidon approach shows a wide range of fluctuation in the PIT size between 76 to 130. The proposed ANNM approach shows a minor fluctuation in the PIT size between 46 to 108 in the attack duration. For the DFN topology, the PIT size for the normal scenario fluctuates between 46 to 105. In the attack scenario, the size of the PIT fluctuates between 611 to 1215 during the attack (100s-200s). The Poseidon approach shows a wide range of fluctuation in the PIT size between 576 to 1196. The proposed ANNM approach shows a minor fluctuation in the PIT size between 495 to 1027 in the attack duration.

6 Conclusion

Most of the previous approaches use one or two features for the detection and mitigation of IFA. These approaches were based on a hard threshold. In our previous work, we have shown that these approaches have less accuracy than machine learning-based approaches. This paper presents a traceback-based mitigation approach for IFA. Firstly, six features are selected out of eleven using IG-based ranking. These selected features are used for building a trained ANN-based classifier. This classifier is deployed in the NDN routers for online IFA detection. On IFA detection, the router stores malicious interface and prefix-list in the m-list. The router sends an alert message to the gateway router to inform it about the attack. The gateway router adds them to its m-list. The gateway router restricts the interest packets which match with the m-list. The proposed approach performs better than the previous approach in terms of the satisfaction ratio and throughput of normal consumers. In the future, we try to adapt our approach to the mitigation of different types of IFAs.

Declarations

Funding: Not Applicable.
Conflicts of interest: None.
Availability of data and material: Not Applicable.
Code availability: Not Applicable.
Authors' contributions : All the authors have immensely contributed for the research work

References

1. Afanasyev, A., Mahadevan, P., Moiseenko, I., Uzun, E., Zhang, L.: Interest flooding attack and countermeasures in named data networking. In: 2013 IFIP Networking Conference, pp. 1–9. IEEE (2013)
2. Afanasyev, A., Moiseenko, I., Zhang, L., et al.: ndnsim: Ndn simulator for ns-3. University of California, Los Angeles, Tech. Rep **4**, 1–7 (2012)
3. Ahlgren, B., Dannewitz, C., Imbrenda, C., Kutscher, D., Ohlman, B.: A survey of information-centric networking. IEEE Communications Magazine pp. 26–36 (2012)
4. Arianfar, S., Koponen, T., Raghavan, B., Shenker, S.: On preserving privacy in content-oriented networks. In: Proceedings of the ACM SIGCOMM workshop on Information-centric networking, pp. 19–24 (2011)
5. Barkai, D.: Peer-to-peer computing: technologies for sharing and collaborating on the net. Intel Press (2001)
6. Bhargava, N., Sharma, G., Bhargava, R., Mathuria, M.: Decision tree analysis on j48 algorithm for data mining. Proceedings of international journal of advanced research in computer science and software engineering **3**(6) (2013)
7. Compagno, A., Conti, M., Gasti, P., Tsudik, G.: Poseidon: Mitigating interest flooding ddos attacks in named data networking. In: 38th annual IEEE conference on local computer networks, pp. 630–638. IEEE (2013)
8. Dai, H., Wang, Y., Fan, J., Liu, B.: Mitigate ddos attacks in ndn by interest traceback. In: 2013 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 381–386. IEEE (2013)
9. Demuth, H.B., Beale, M.H., De Jess, O., Hagan, M.T.: Neural network design. Martin Hagan (2014)
10. García, G., Beben, A., Ramón, F.J., Maeso, A., Psaras, I., Pavlou, G., Wang, N., Śliwiński, J., Spirou, S., Soursos, S., et al.: Comet: Content mediator architecture for content-aware networks. In: 2011 Future Network & Mobile Summit, pp. 1–8. IEEE (2011)
11. Gasti, P., Tsudik, G., Uzun, E., Zhang, L.: Dos and ddos in named data networking. In: 2013 22nd International Conference on Computer Communication and Networks (ICCCN), pp. 1–7. IEEE (2013)
12. Ghali, C., Tsudik, G., Uzun, E., et al.: Needle in a haystack: Mitigating content poisoning in named-data networking. In: Proceedings of NDSS Workshop on Security of Emerging Networking Technologies (SENT) (2014)
13. Hecht-Nielsen, R.: Theory of the backpropagation neural network. In: Neural networks for perception, pp. 65–93. Elsevier (1992)
14. Jacobson, V., Mosko, M., Smetters, D., Garcia-Luna-Aceves, J.: Content-centric networking. Whitepaper, Palo Alto Research Center pp. 2–4 (2007)
15. Kent, J.T.: Information gain and a general measure of correlation. Biometrika **70**(1), 163–173 (1983)
16. Koponen, T., Chawla, M., Chun, B.G., Ermolinskiy, A., Kim, K.H., Shenker, S., Stoica, I.: A data-oriented (and beyond) network architecture. In: Proceedings of the 2007 conference on Applications, technologies, architectures, and protocols for computer communications, pp. 181–192 (2007)

17. Kumar, N., Singh, A.K., Srivastava, S.: Evaluating machine learning algorithms for detection of interest flooding attack in named data networking. In: Proceedings of the 10th International Conference on Security of Information and Networks, pp. 299–302 (2017)
18. Kumar, N., Singh, A.K., Srivastava, S.: Feature selection for interest flooding attack in named data networking. International Journal of Computers and Applications pp. 1–10 (2019)
19. Pathan, M., Buyya, R., Vakali, A.: Content delivery networks: State of the art, insights, and imperatives. Content Delivery Networks pp. 3–32 (2008)
20. Wang, K., Zhou, H., Qin, Y., Chen, J., Zhang, H.: Decoupling malicious interests from pending interest table to mitigate interest flooding attacks. In: 2013 IEEE Globecom Workshops (GC Wkshps), pp. 963–968. IEEE (2013)
21. Xin, Y., Li, Y., Wang, W., Li, W., Chen, X.: Detection of collusive interest flooding attacks in named data networking using wavelet analysis. In: MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM), pp. 557–562. IEEE (2017)
22. Zhang, L., Afanasyev, A., Burke, J., Jacobson, V., Claffy, K., Crowley, P., Papadopoulos, C., Wang, L., Zhang, B.: Named data networking. ACM SIGCOMM Computer Communication Review **44**(3), 66–73 (2014)
23. Zhi, T., Luo, H., Liu, Y.: A gini impurity-based interest flooding attack defence mechanism in ndn. IEEE Communications Letters **22**(3), 538–541 (2018)

Naveen Kumar has done his Bachelors of Technology (Computer Science and Engineering) from U.P. Technical University, Lucknow, in 2012. He has done his Masters of Technology (Software Engineering) in the Computer Science and Engineering Department at MNNIT Allahabad, Prayagraj, India in 2014. He is currently pursuing **Ph.D.** in the Department of Computer Science and Engineering at MNNIT Allahabad. His research interest includes peer to peer systems, future internet technologies, network security, and Named Data Networking.

Dr. Shashank Srivastava has done his Bachelors of Technology (Computer Science and Engineering) from U.P. Technical University, Lucknow. He has done **M.S.** in Information Security from Indian Institute of Information Technology Allahabad, India. He obtained his **Ph.D.** degree in Information Technology from Indian Institute of Information Technology Allahabad, India in 2014. He is currently working as Assistant Professor in the Department of CSE, MNNIT Allahabad, 211004, India. He possesses an experience of more than six years in the field of teaching and research. He is having the Membership of IEEE, ACM, CSI and CRSI (Cryptographic Research Society of India). He has supervised one doctoral thesis and currently guiding four research scholars at MNNIT Allahabad. His areas of expertise are Software Defined Networking (SDN), Named Data Networking (NDN), Network flow optimization and security, information security, and future internet technologies. He has published various research papers in reputed journals and conferences.

Figures

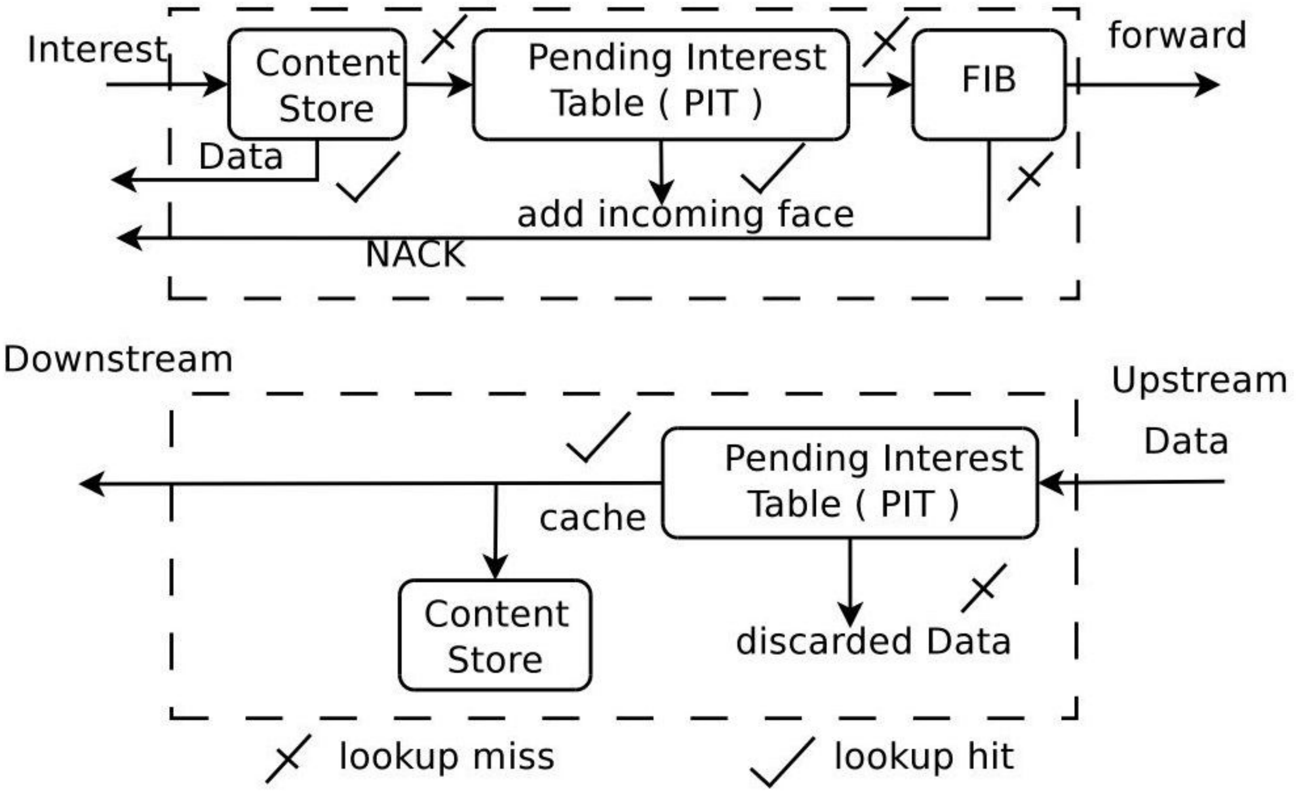


Figure 1

NDN Forwarding Pipeline

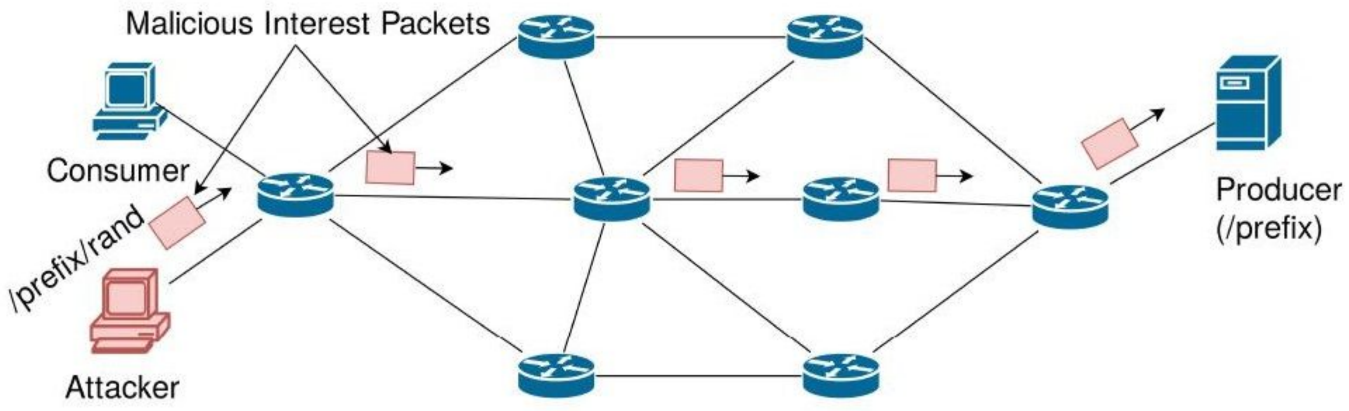


Figure 2

IFA Demo

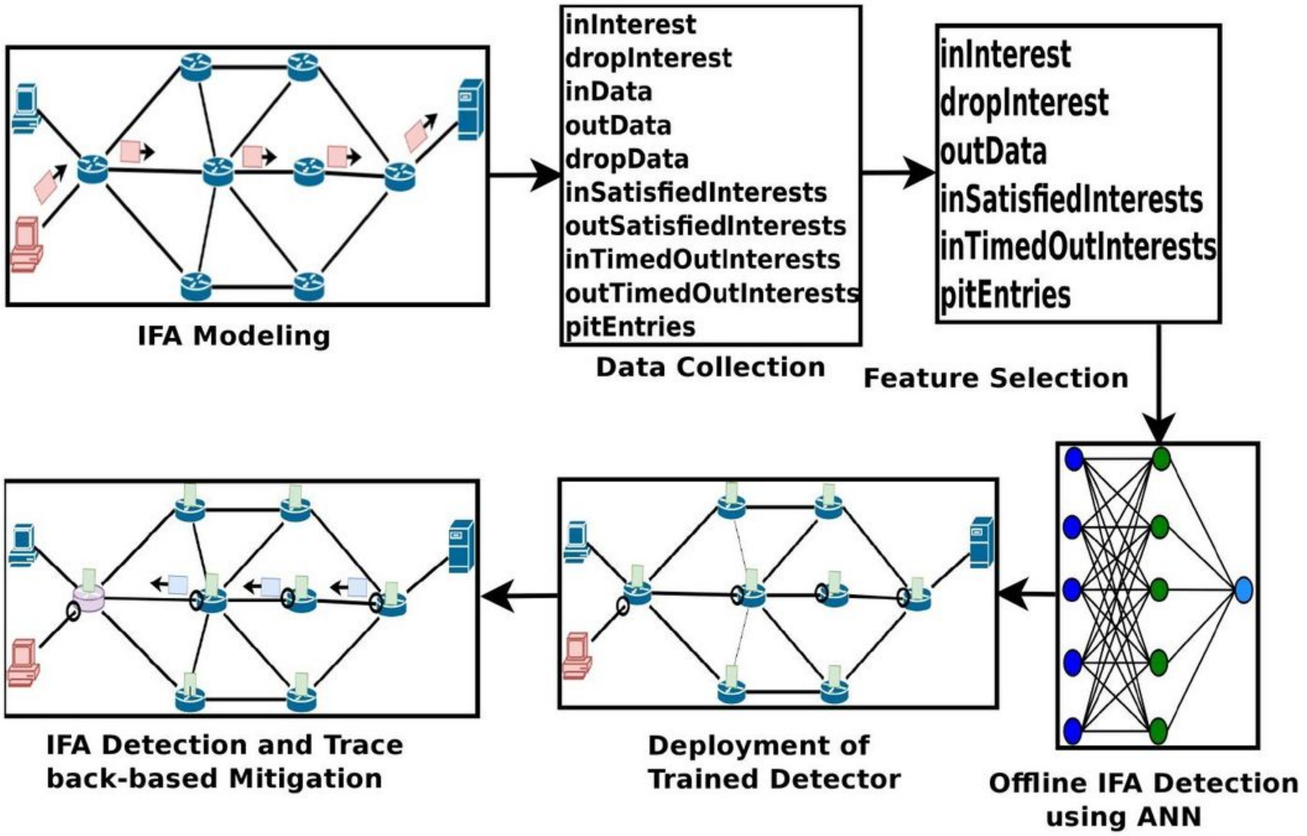
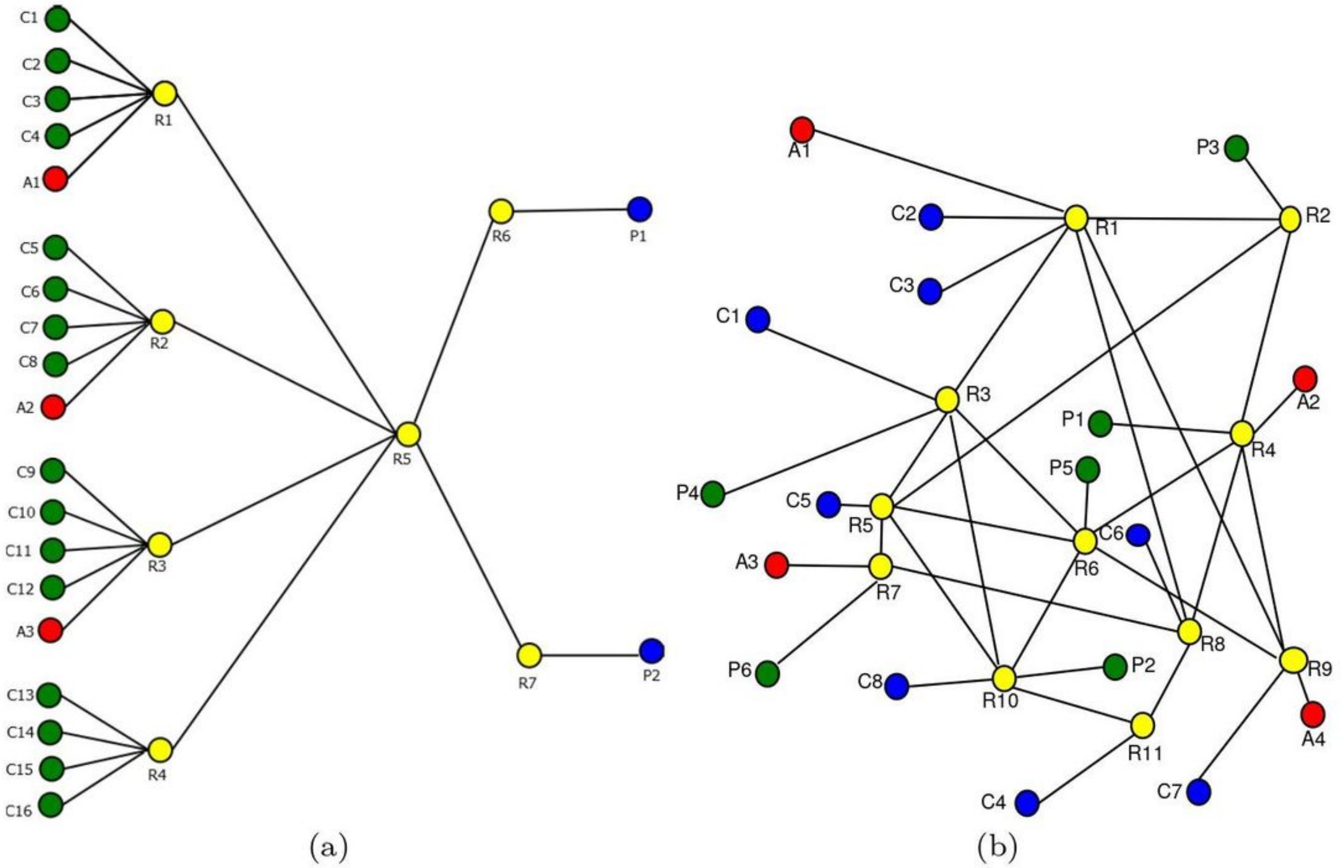


Figure 3

Series of Processing Done for the Mitigation of IFA

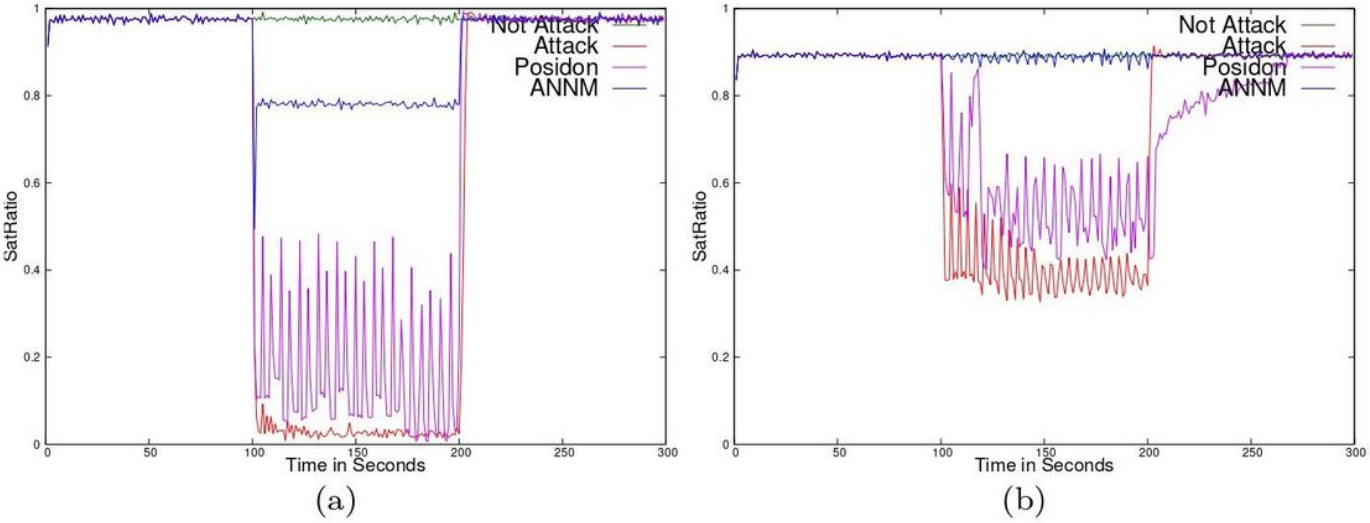


(a)

(b)

Figure 4

Topologies Considered for Attack Modeling (a) Tree Topology and (b) DFN like Toplogy

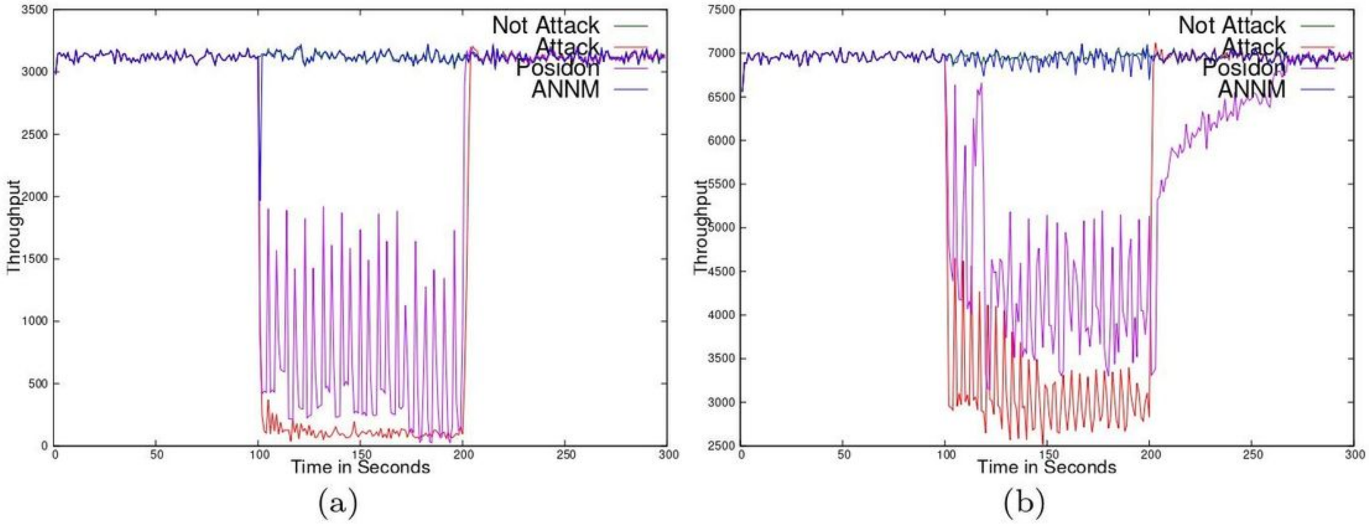


(a)

(b)

Figure 5

Satisfaction Ratio (SR) of Normal Consumers w.r.t. Time for (a) Tree Topology and (b) DFN like Toplogy

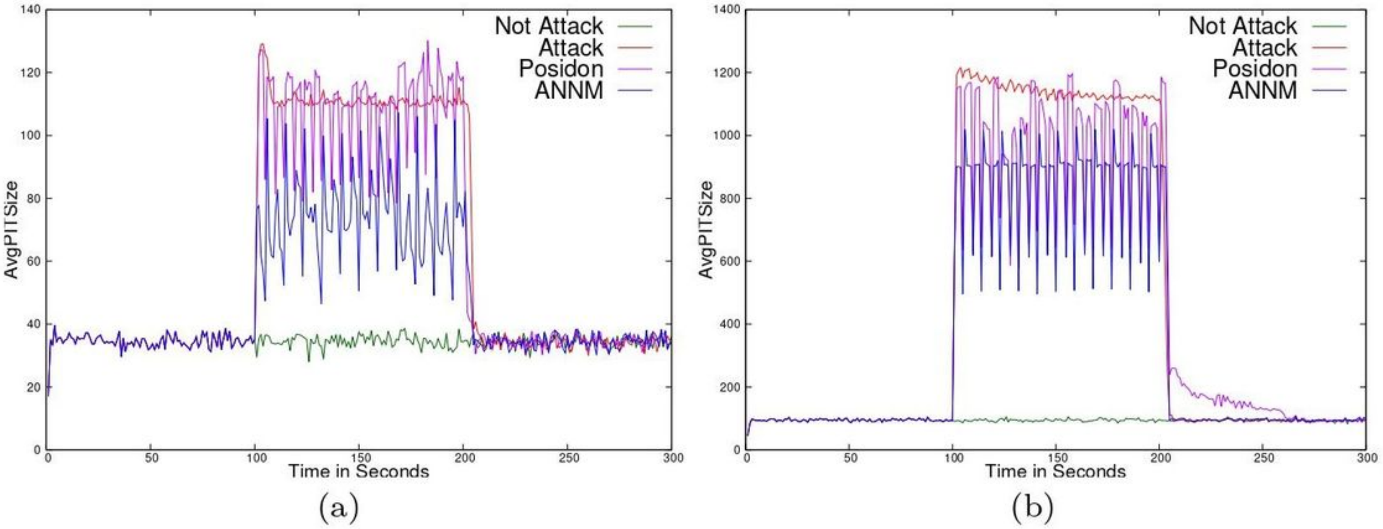


(a)

(b)

Figure 6

Throughput of Normal Consumers w.r.t. Time for (a) Tree Topology and (b) DFN like Toplogy



(a)

(b)

Figure 7

Average PIT Size of Routers w.r.t. Time for (a) Tree Topology and (b) DFN like Toplogy