# Forwarding Loop Attacks and Counter Measures in Content Centric Networks

Sarat Chandra Velijala, Yong Guan
Dept. of Electrical and Computer Engineering
Iowa State University
Ames, IA, USA

***Abstract*— Content Centric Networking(CCN) is a novel networking approach that aims at overcoming some of the limitations of the current Internet. In particular, CCN aims at providing better security and privacy by focusing on the data rather than on the location of data. However, this new networking concept opens up avenues for launching several new types of attacks including the "Forwarding Loop attacks". This paper describes how malicious customers can attack the availability of Content Centric Networks (CCNs) by creating forwarding loops. These loops cause one request to be processed repeatedly or even indefinitely, resulting in unwanted resource consumption and potential Denial-of-Service attacks. Next, we propose detection and mitigation techniques that will allow routers to identify and prevent the formation of such loops. To evaluate the practicality of such forwarding-loop attacks, we use the popular CCN simulation software, ndnSIM to simulate the occurrences of the loops and show how they can affect the overall service of the network.**

***Keywords—Content Centric Networks, Forwarding Loops***

## I. INTRODUCTION

Today the Internet is mainly used for data dissemination to interested users, rather than for connecting hosts. The user is interested in data itself, while the location of data is of minor importance. However, the Internet was formerly designed and has evolved according to the host-centric communication paradigm. Recent studies have shown that the poor performance of the traditional Internet, in the areas of security, efficient content dissemination, content delivery etc., lies in its host-centric nature.

Information Centric Networking (ICN) is a new effort that aims to eliminate the traditional Internet's limitations. Content Centric Networking (CCN) is one of the proposed ICN approaches.

In CCN the content or data is requested by the Client in the form of an "Interest" packet and the host, which can either be the primary source or the intermediate nodes who have cache capability, provide the data in the form of a "Content Object". Thus in this new paradigm focus is shifted from location specifications of the content to the content delivery and encryption. As any new network protocol CCN is not free from malicious attacks. Interest Flooding attacks and Cache Poisoning attacks are more common and well explored.

In this work we present "forwarding-loop" attacks, which allow malicious CCN customers to attack CCN availability by creating looping requests within a single CCN domain(Intra-cluster) or across multiple CCN domains (Inter-cluster). Forwarding-loop attacks allow attackers to immensely consume CCN resources by building up a large number of requests (or responses) circling between CCN nodes. Although many CCN nodes have internal mechanisms to drop repeated content requests when they circle back, the attacker can ask for unique content request

In this paper we firstly define Content Centric Networking and its core principles and strategies We also discuss its implementation in Mobile Networks. Previous related work on the security issues and attacks in CCN are surveyed. We then present the forwarding loop attacks in CCN and discuss the three stages of its implementation in static, mobile-ad hoc and mobile-infrastructure networks. Later we describe a few strategies to mitigate these attacks. Finally, we use ndnSIM software tool to simulate and examine the impact of these looping attacks in single and multiple compromised node networks.

## II. CONTENT CENTRIC NETWORKING

In the CCN architecture, a CCN node model is comparable to an IP node model. CCN nodes receive and send packets over multiple faces. A face in CCN is a connection to an application, or another CCN node, or some other kind of interface. A face may have attributes that indicate broadcast or multicast capability, expected latency and bandwidth, or other useful features.

A CCN node accepts Interest packets and either sends them out on an outgoing face, or directly replies with a matching Content object. If the node has forwarded an Interest packet, then it should normally receive a corresponding Content object which will be send to the original requesting face. A Content Consumer issues an Interest request for data over the network. The Interest is transmitted through a set of intermediate Forwarders until the Content Object is found or the Interest's Life time expires.

A CCN node has three main data structures:

1) Content Store (CS)

2) Forwarding Information Base (FIB)

3) Pending Interest Table (PIT)

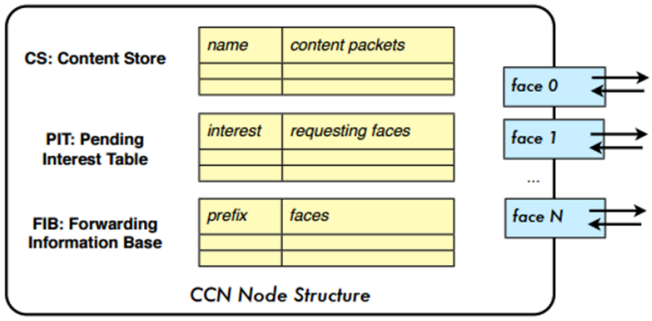


Fig. 1. CCN Node Structure

The *Content Store (CS)* holds a table of previously seen (and optionally cached) Content objects indexed by the Name field of the packet. Besides providing communication buffering, the Content store also serves as a content cache. The CS is similar to the buffer memory of an IP node but has a different replacement policy. Since each IP packet corresponds to a single point-to-point conversation, it has no further value after it has been forwarded. Unlike IP, CCN packets are self-authenticating and self-identifying and can potentially be useful to many users. Thus, in order to optimize the use of network bandwidth, and reduce user-perceived latency, CCN nodes store the Content objects in their CS. In CCN, only Interests are routed. Matching Content objects follow the reverse-path of the corresponding Interest packet.

The *Pending Interest Table (PIT)* is used to keep track of Interests forwarded upstream by that CCN node to- ward the content source so that Content objects later received can be sent back to their requestor(s). The PIT holds a set of entries, each entry containing a previously seen Interest packet and a list of the faces that received the interests. There may be additional information, such as timeout values, that affect the entries.

The *Forwarding Information Base (FIB*) forwards Interest packets towards potential data sources and is analogous to the FIB in IP routers. The FIB holds a set of entries, each entry containing a name prefix and a list of the faces that might provide content for that prefix. The FIB may be populated by an overlay routing protocol or with static routes There may be additional control information that affects forwarding.

### *A. Flooding and Forwrding Strategies*

i) Arrival of New Interest:

At the initial stage, the FIB on each CCN node is empty. An incoming Interest packet at Face 0 is propagated to all Faces (1, 2, and 3) except the incoming Face 0. This is an initial flooding.

ii) Arrival of the First Data Packet:

When the first Data packet arrives, the corresponding FIB entry is created. The prefix of the Data name is stored in the Prefix field and the arrival face of the Data is recorded in the Face(s) field, which can maintain N maximum elements (faces).

iii) Arrival of Data Packet with the Same Prefix:

When there is the second Data packet with the same prefix as an existing packet in the FIB, the arrival face will be added to the corresponding Face(s). If N faces are already stored in the set of Face(s), a FIFO operation is performed. That means that the first oldest arrival face will be deleted.

iv) Interest Forwarding Principle:

When a new Interest packet arrives that matches Prefix entries in the FIB, Interest forwarding is performed by selecting one face among the elements in Face(s) according to the occurrence ratio of the faces. That is, the most successful face is selected. Since the FIB can maintain at most N faces, the learning mechanism adjusts the face selection according to the recent data retrievals. In the case of link failure or packet loss, Data does not return in time; therefore, the data requester or consumer returns to step [a], flooding the Interest to all available connected faces to discover a working path quickly

### *B. Mobility in CCN*

Machines today typically have multiple network interfaces and are increasingly mobile. Since IP is restricted to forwarding on spanning trees, it is difficult for IP to take advantage of more than one interface or adapt to the changes produced by rapid mobility. CCN packets cannot loop so CCN can take full advantage of multiple interfaces. CCN talks about data, not to nodes, so it does not need to obtain or bind a layer 3 identity (IP address) to a layer 2 identity such as a MAC address. Even when connectivity is rapidly changing, CCN can always exchange data as soon as it is physically possible to do so. They can be broadly classified as mobile ad hoc and infrastructure networks. In the mobile ad hoc networks there is no central entity to oversee the transactions between the mobile nodes. Nodes join and leave the network in a random fashion. On the other hand, in the mobile-ad hoc networks, the central entity (generally the Access point) manages the interaction and movements of the mobile nodes. Mobile CCN networks are further discussed in the Chapter 5.

## III. Related Work

### *A. Interest Flooding Attacks (IFA)*

Denial-of-service (DoS) attack is an old phenomenon of computer networks. Traditional Internet is vulnerable to DoS attacks that primarily aim to degrade or completely deny the services of network devices and servers to legitimate users. For this purpose, different schemes and techniques have been tested by attackers to launch attacks, whereas many countermeasures have been pro- posed by network professionals and researchers to fight against DoS attacks. DoS attacks have not been vanished in the Internet, and even some sophisticated systems of recent times have been observed being under DoS attacks.

The interest propagation technique in CCN makes it capable to fight against DoS attacks. An adversary finds it more difficult to launch DoS attacks in CCN environment than TCP/IP. The balance between interest and data makes DoS attack very difficult for an attacker. The attacker can try flooding the network through interest packets. If zombies behind an attack generate large amount of interest packets with the same content name, an aggregation of interests takes place and only one pending interest is ever forwarded on the available link; hence, the flooding does not occur. If zombies use different content names with the same target prefix, the cached copies of interest- satisfying data are available at various places in the net- work. As soon as an interest packet finds a content copy that satisfies it at the nearest possible location of attacking source, the interest is cleared. Hence, it still makes the flooding very difficult to occur in a CCN environment.

Interest flooding attack is the most common source of DoS attacks in CCN. Therefore, many countermeasures proposed against CCN DoS attacks primarily focus on mitigating the flooding attack. In CCN, flooding attacks are triggered to degrade a router's performance, network's responsiveness, or the performance of a content source. This CCN-DoS classification is different from traditional DoS classifications because of some of CCN's distinguished characteristics (flow balance, content integrity with publisher's sig- nature, etc.). We classify CCN- DoS attacks considering three main attack methods, that is, (i) flooding, (ii) forced computation, and (iii) cache/con- tent manipulation under which different forms of attacks are possible.

### *B. Undetected Interest Loops in CCN*

The author in [2] defines an Interest loop in CCN and has postulated two theorems based on the loops.
Interest Loop: An Interest loop of h hops for NDO with name n(j) occurs when one or more Interests asking for n(j) are forwarded and aggregated by routers along a cycle L = {v1, v2, ..., vh, v1} such that router vk receives an Interest
for NDO n(j) from vk−1 while waiting for a response to the Interest it has forwarded to vk+1 for the same NDO, with 1 $\leqslant$ k $\leqslant$ h, vh+1 = v1, and v0 = vh.

## IV. FORWARDING ATTACKS IN CCN

Malicious customers of nodes (Consumers, Publishers or Routers) can deliberately manipulate the forwarding to create forwarding loops inside CCNs. Forwarding loops can cause CCNs to process one client request repetitively or even indefinitely. The consequent amplification effect allows malicious customers to launch, with little resources and cost, resource-consuming DoS attacks (Interest Flooding Attacks) against CCNs. In this thesis, we have identified approaches to create forwarding loops in the following kinds of CCN network systems:

A) Static Networks

B) Mobile-ad-hoc network

C) Mobile-Infrastructure

The process of Forwarding Loop is described in three main stages at each network system:

(i) Identification of the loop

(ii) Creation and Sustenance of the loop

(iii) Exploitation of the loop

### *A. Forwarding Loop Attacks in Static CCN*

We assume the physical topology of the underlying closed-static network is Mesh type and that we have a Compromised Router (CR) or Rogue-router (both terms used interchangeably) which is actively listening or transmitting on two or more faces. CR assisted by an independent set of consumer and producers adjacent to the router (one-hop away). This set of compromised producers (CP) and consumers (CC) aid in creating the required malicious Interest and Content objects to be routed by the compromised router (CR). We have identified loops with one and two compromised routers, which can also be generalized to n-compromised nodes.

#### *a) Loop traversing one compromised router*

*Step 1: Identification of the Loop*

The forwarding loop can either be identified by the CR independently or with the aid of another malicious consumer node, which is located in the same domain as that of the CR.

In the first scenario, the CC sends out a fake Interest packet to the which in turn forwards it only on one of its outgoing faces. The specific face chosen can based on prior strategic analysis of the incoming interests on multiple interfaces of the routers, which is beyond the scope of this thesis. In the default case, as described in the previous sections, an Interest packet for unknown content is sent on all the broadcast capable faces (and later on the remaining faces). This fake interest packet is generated for a unique content name such that it can only be satisfied by the content object generated by the CP (or the inherent producer). The prefix of this unique content is purposefully not registered by the CR (can also be considered as the content being invoked/created for the Interest on the fly) in its CCN domain so as to trigger a broadcast flooding of the interest, in search of the satisfying content.

After a couple of iterations, the CR may receive the Interest back on one or more of its remaining faces, excluding the one it had previously sent the Interest out on. Figure 6 shows a simple scenario with a loop comprising of 6 nodes: CR → R1→R2→R3→R4→R5→CR. This proves the existence of a loop, traversing the CR, in the CCN domain. We can also assume that the loop created by the Interest packet received last on one of the faces, is the longest or has the highest cost,

among all the loops detected and either of these properties can be further exploited by the attacker.

In the second scenario, another malicious consumer node, located in the same domain as that of the CR sends out the interest for unique content name which only be satisfied by the content object generated by the CP. This Interest packet is flooded in the domain and may be received on one or more faces of the CR. If the interest is indeed received on two or more faces of the CR, we can safely assume the existence of the loop traversing the CR, which can be created and exploited as described below. The above scenario can also aid in the identification and creation of longer loops.

*Step 2: Creation of the Loop*

Now the attacker asks for an Interest with the same unique prefix as before, but with a different segment name, on the same router node. The router checks its FIB, and identifies the prefix name and the interface. It creates an entry in the PIT and forwards it along the interface on which the CO was received earlier. The Interest is forwarded along the singular path of nodes until it finally reaches the rogue router.

Consider the following scenario with a compromised router. The initial adjacent node (R1 in Figure 6) to which the attacker had asked for content, will be unable to find any cached content for this unique Interest in the CS. There wouldn't be any similar pending interests in the PIT nor any entries for the prefix in the FIB. According to the current methods, the initial edge node, floods the Interest on all its faces and adds an entry in its PIT for the same. The interest propagates in the network along the core nodes, following the above flooding strategy, until it reaches the rouge router node (CR → R1→R2→R3→R4→R5→CR ). The rouge router is the only one which can satisfy the specific interest, such that it may receive the same interest on multiple interfaces from adjacent nodes in the same network. This strategy aids in interpreting the "loops" to the starting node on which the Attacker had asked for an interest.

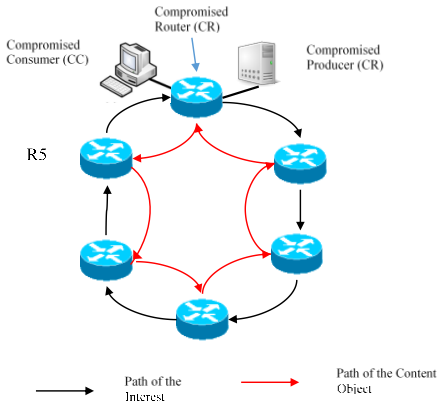


Fig. 2. Forwarding Loop with one CR in Static CCN

But the Rogue node instead of sending back the Content Object on all the interfaces on which the interest was received (CR → R5→R4→R3→R2→R1→CR), it sends it only one particular face (of the so-formed loop). The CO is passed along all nodes on one singular path until it reaches the final node and forwarded to the Attacker. When the CO is received, the PIT entry for the unique interest is eliminated and an entry is added for that unique prefix in the FIBs (along with the ingress interface on which the CO was received) of all the nodes along that singular path. The content may also be cached in the CS of the nodes along the path. The PIT entry for the unique interest for the all other adjacent nodes, on which the CO was not received, will expire and no entry is added to the FIB or CS.

Instead of creating fake Interest packets, the compromised producer can also anticipate popular content and is ready with the content, before any other node can provide it. Now without the help of the attacker, the Rogue router may send another Interest with the same prefix along the reverse loop. Next rogue router can send the same Interest with same name but a different nonce and with an Interest lifetime more than specified before.

So according to the strategy, the previous entry's Lifetime is increased. The routers keep increasing the Interest Lifetime of the Interest in the PIT entry, and this is propagated throughout the loop and the whole operation is stalled. In this scenario the genuine Interests packets get dropped and the attacker may employ Bots to increase the miss rate. CC may also send out other many more Interests packets (either requesting unique fake content or a huge file which has multiple segments). These fake interest entries can then over-flow the PIT table, which will subsequently drop the legitimate Interest packets from legitimate users, having reached the hardware memory capacity, thus leading to Interest flood attacks.

*Step 3: Exploitation of the Loop*

Now without the help of the attacker, the Rogue router may send another Interest with the same prefix along the reverse loop. Next rogue router can send the same Interest with same name but a different nonce and with an Interest lifetime more than specified before. So according to the strategy, the previous entry's Lifetime is increased. The routers keep increasing the Interest Lifetime of the Interest in the PIT entry, and this is propagated throughout the loop and the whole operation is stalled. In this scenario the genuine Interests packets get dropped and the attacker may employ Bots to increase the miss rate. CC may also send out other many more Interests packets (either requesting unique fake content or a huge file which has multiple segments). These fake interest entries can then over-flow the PIT table, which will subsequently drop the legitimate Interest packets from legitimate users, having reached the hardware memory capacity, thus leading to Interest flood attacks.

*b) Loop traversing two compromised routers*

In this scenario, we assume we have two compromised routers (CR1 and CR2) that are located in the same domain preferably located multiple-hops apart from each other. First

step would be to identify the presence of each other, by sending each other Interests messages for unique content which can only be satisfied by the other counter-part.

Both the CRs are listening on two or more faces. Initially one of the CRs sends an Interest on all its faces, for a prefix which has not been registered in the domain. By the default strategy for ad hoc networks the Interest packet is broadcasted to all the nodes in the domain, including the other CR. If the other CR receives the Interest on one or more of its faces, we can safely assume that they are multiple routes to the other CR.

Now the Rogue router does not send the CO for the new interest along the face on which it was received. Instead it floods an interest, with the same Interest name but with a different Nonce, along the other interface(s) to the adjacent nodes of the loop previously detected. Since the adjacent nodes still perceive the Interest to be unique, flood the Interest on all their respective faces and add an entry in their respective PITs for the same. This Interest is probated along the loop until it reaches the Initial edge node on which the attacker is asking for content, so completing the loop.

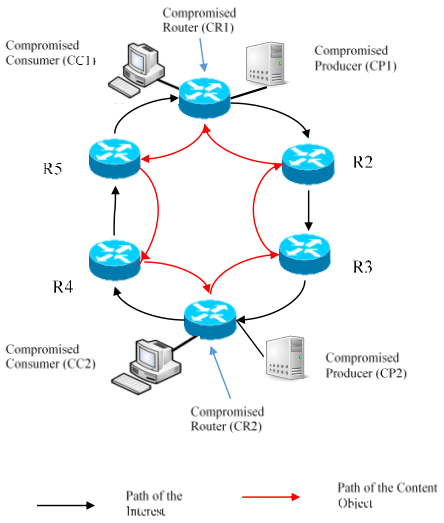


Fig. 3. Forwarding Loop with two CRs in Static CCN

Now when the initial edge node receives the Interest with the same name but different nonce, it adds the ingress face to the PIT entry already waiting for the CO on the same name and deletes the interest. The rogue router now sends a CO along the initial singular path and this CO is satisfied along the loop, with the creation of the FIB entry and/or cache entry. This confirms the loop.

### *B. Forwarding Loops in Mobile Ad hoc CCN Networks*

We assume the compromised node (CN) in the Ad Hoc networks has the feature of inherently creating both Interest and Content Objects, thus acting as the consumer, the producer (or publisher) and router independently as is the case in a standard Ad hoc environment.

In Fig 4 the forwarding loop in a simple ad-hoc network with a single compromised node is depicted. We observe that the CN acts as both the CC and the CP. The loop follows similar stages as previously discussed in the Static CCNs in the above section. The loop in this case traverses through Node 1 through Node 5 and back to the CR.

The implementation of two Compromised nodes CN1 and CN2 is depicted in Fig 5. Both the nodes establish a connection and exploit the resources of the intermediate nodes. The loop can be initiated by either of the CRs and traverses all the intermediate nodes.

We can extend this further to loops created by the multiple compromised routers, which can identify larger loops extended between domains thus exploiting larger set of resources.

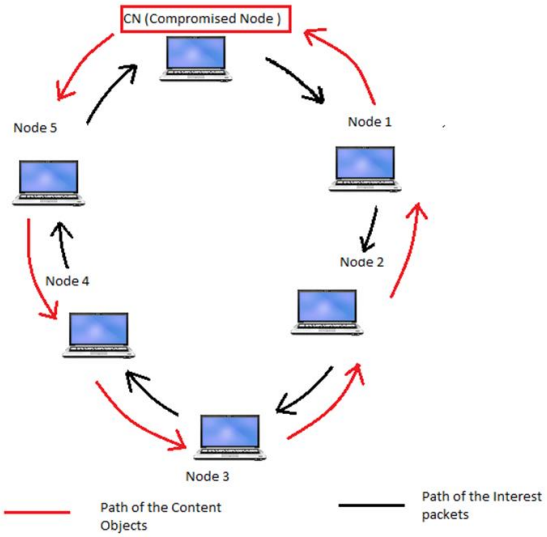


Fig. 4. Forwarding Loop with one CR in Ad hoc CCN

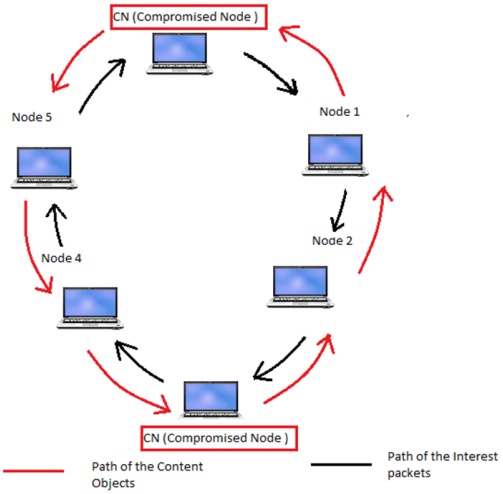


Fig. 5. Forwarding Loop with two CRs in Ad hoc CCN

### C. Detection and Mitigation Techniques

In this section we discuss the possible detection and mitigation strategies of Forwarding Loops. The implementation and impact of these loops is studied in the Chapter 6.

Detection Strategies include the implementation of a Node ID (N-ID) or a Router ID (R-ID) and detection of malicious nodes, causing harm to the overall network.

#### *a) Node ID/ Router ID fields*

One of the main reasons for the creation of the forwarding loop is the re-transmission of the Interest back to the to the compromised node. This can be avoided by the implementation of a Router-ID field. Using a Router-ID. along with the Interest packet. R-IDs are assigned when a node joins the Ad-Hoc network and identifies itself to the nearby node by sending a PROBE request and every node is aware of the R-IDs of its one-hop neighbors. When forwarding the Interest for the unknown content, a particular node checks the R-ID of the Interest packet. If the R-ID matches to its one-hop neighbors it drops the packet, thus avoiding the formation of the loop.

#### *b) Maximum Interest Life-time (MIL)*

The Maximum Interest Life-time (MIL) assumed by a router before it deletes an Interest from its PIT should be large enough to preclude an excessive number of retransmissions. On the other hand, MIL should not be too large to cause the PITs to store too many Interests for which no NDO messages or NACKs will be sent due to failures or transmission errors. A few seconds would be a viable value for MIL. In practice, however, the consumer submitting an Interest to its local router could provide an initial value for the Interest lifetime estimated over a number of Interests submitted for NDOs in the same NDO group corresponding to a large piece of content (e.g., a movie). This is specially the case given our assumption that Interest retransmissions are carried out by content consumers, rather than by routers. Furthermore, because the CCN forwarding strategy does not detect loops when Interests are aggregated, many Interest entries in PITs may have to be stored until their lifetimes expire.

#### *c) Suppression of Malicious Nodes*

Below we employ the methods of detecting and mitigating Interest Flood Attacks. The suspicious compromised router can be detected using the below techniques:

1) Attack detection:

During the detection phase, the edge router keeps statistics about the expired PIT entries per each user. Two thresholds are used to classify users into: legitimate, suspicious (possible attackers), and malicious (attackers). If the number of expired PIT entries per time unit, N of a user u is below the low threshold, T-low, user u is considered legitimate. If N is above T-low but below the high threshold, T-high, user u is considered suspicious. Finally, if N> T-high, user u is considered malicious.

2) Rate reduction and blocking phase:

During this phase, any user that has been classified as malicious, will be blocked, whereas the suspicious users will receive reduced data rate.

3)Attack notification phase:

If an edge router detects an ongoing attack, after blocking this user, it will notify other routers about the identity of the malicious user, by sending the attack notification packet. This is done to prevent the Mobile Interest Flooding Attack, where a mobile user periodically visits different routers and floods them with Interest packets. In this context, the notion of router is extended and refers to any data-forwarding network element, such as a Wi-Fi Access Point (AP) or a Base Station (BS) in a cellular network.

## V. Performance Evaluation

The fundamental departure of the CCN communication paradigm from the Internet Protocol principles requires extensive evaluation through experimentation, and simulation is an essential tool to enable the experimentation at scale. For this purpose, we rely on the open source simulation software ndnSIM.

We consider a fixed set of nodes in the network. In the first scenario we evaluate the packet dropping probability of the entire network, with respect to the length of the forwarding loop involving a single compromised router (Self-loop). We consider a mesh network in matrix representation of 5X5, with 24 ordinary routers and 1 compromised router. The CR has both the CP and CC assisting it in administering the forwarding loop. We consider a simple scenario where we have 9 consumer nodes (C1-C9) and 9 producer nodes (P1=P9). Each of these consumer nodes sends Interests requesting content that can be satisfied by the corresponding Producer node (C1 for P1, C2 for P2 and so on). The producers listen on specific prefixes (we chose a random prefix: /producer*n*/ for each of the n- producers) previously announced in the network.

The duration of the simulation is 50s. A large number of legitimate requests will not be satisfied, since the corresponding PIT entry of each request will expire before the content arrives. In Figure 10, we observe that during the first 5-10 seconds, when only legitimate users are active, the required PIT size is relatively small (20MB). The required size of the PIT of the edge router grows over time due to the launched attack However, shortly after the attack starts, the PIT size increases rapidly. These results show that it is relatively easy even for attacking nodes of limited capabilities to quickly occupy large amounts of router's storage and processing resources.

To show the negative impact of the forwarding loops, we evaluate the packet dropping probability of actual users (producers and consumers) due to PIT overflow. We consider the PIT capacity equal to 250 MB and use PIT expiration time as 50ms. The rest of the simulation parameters remain the same as described in the previous paragraph.

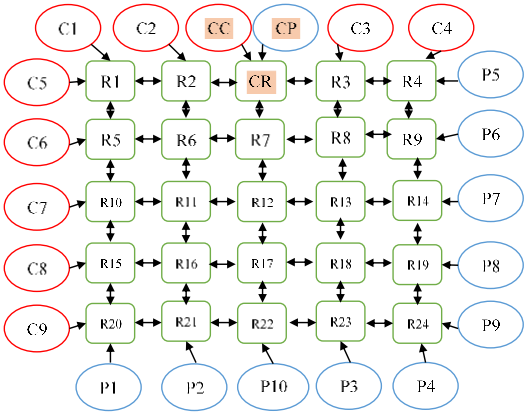


Fig. 6. Experimental setup for evaluating the impact of Forwarding Loops in Static CCN with one compromised node

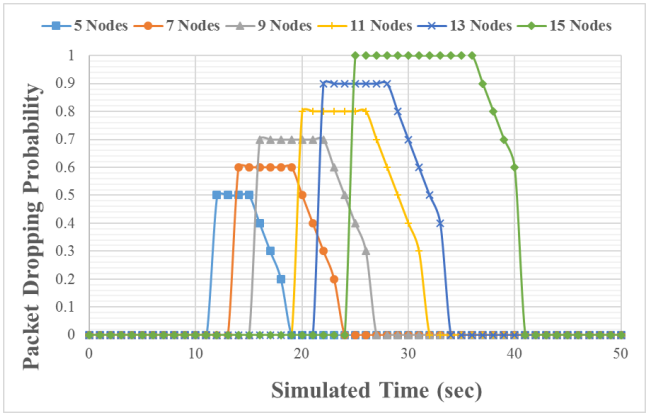


Fig. 7. Graph depicting the Packet Dropping Probability in multiple one CR loops

In the second scenario we extend the above evaluation to involve four compromised routers (CR1,CR2,CR3,CR4) equipped with their corresponding compromised consumers and producers (CCs and CPs) in the same network with the same number of nodes. As in the above scenario, the packet dropping probability of the entire network, with respect to the length of the forwarding loop involving the compromised routers is considered. We then try to evaluate the Rate reduction and blocking phase of Interest flooding attacks. This is carried out after the compromised routers are detected and labeled as being 'suspicious' or 'malicious'.

The above scenario can further be extended to a bipartite graph G = (C ∪ P, E) where the vertex set is composed of two parts Consumer set C and Producer set P and every edge has one end point in C and the other in P. That is there is no edge with both its endpoints in C or P. The set R depicts the various combinations of the intermediate paths (of nodes) that can be traversed to reach from the consumer set to the producer set. A simple case of this implementation is depicted in Fig 9.

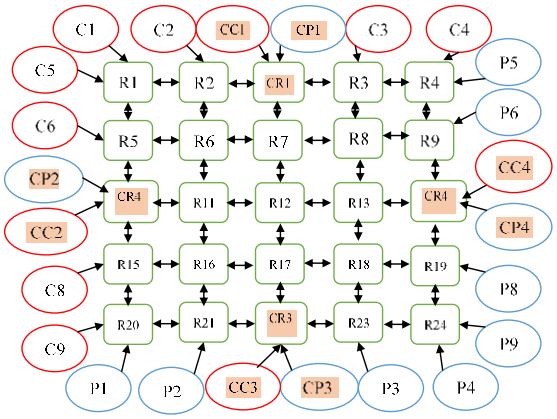


Fig. 7. Experimental setup for evaluating the impact of Forwarding Loops in Static CCN with four Compromised nodes

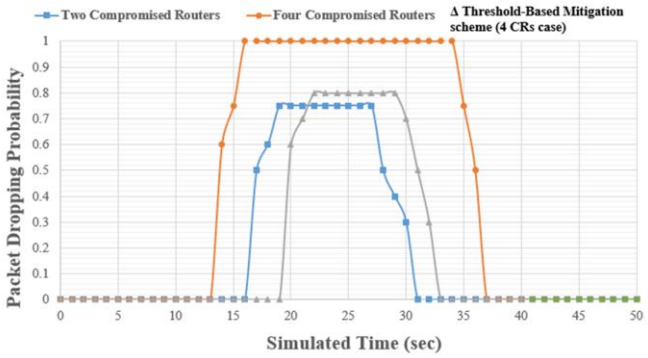


Fig. 8. Graph depicting the Packet Dropping Probability in with two pairs of CRs.

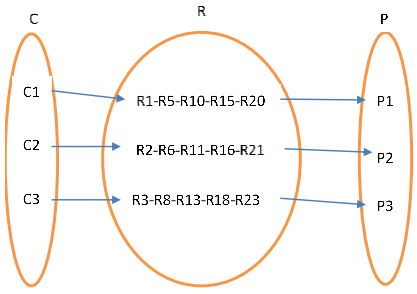


Fig. 9. Consumer and Producer sets in a bipartite graph

The above results clearly depict the extent of the impact the forwarding loops have on the Content Centric Networks. Various techniques discussed in Chapter 5, aid in mitigating these attacks. Occurrence of these attacks in other novel networking protocols can be further explored in the future.

## VI. Conclusion and future work

In this paper we have described how malicious customers can attack the availability of Content Centric Networks (CCNs) by creating forwarding loops inside one CCN cluster or across multiple Clusters. Such forwarding loops cause one request to be processed repeatedly or even indefinitely, resulting in undesired resource consumption and potential Denial-of-Service attacks. Next, we propose detection and mitigation techniques that will allow routers to identify and prevent the formation of such loops. To evaluate the practicality of such forwarding-loop attacks, we used the popular CCN simulation software, ndnSIM to simulate the occurrences of the loops and show how they can affect the overall service. We have observed that the Forwarding loops have a considerable impact on the normal services provided by the CCN. Forwarding loop attacks can also be evaluated further in other scenarios of ICN in the future.

## References


[1] A. Feldmann, “Internet clean-slate design: What and why?” ACM SIGCOMM Computer Commun. Review, vol. 37, 2007, pp. 59-64.

[2] J. J. Garcia-Luna-Aceves, "Eliminating undetected interest looping in content-centric networks," Network of the Future (NOF), 2015 6th International Conference on the, Montreal, QC, 2015, pp. 1-6.

[3] V. Jacobson, D. Smetters, J. Thornton, M. Plass, N. Briggs, and R.Braynard, “Networking named content,” Proc. CoNEXT, Rome, Italy, Dec. 2009, pp. 11-18.

[4] H. Yuan and P. Crowley, “Scalable pending interest table design: From principles to practice,” Proc. IEEE INFOCOM, 2014, pp. 2049-2057.

[5] S. Arianfar, T. Koponen, B. Raghavan, and S. Shenker, “On preserving privacy in content-oriented networks,” Proc. ACM SIGCOMM Workshop on Information-Centric Networking, 2011, pp. 19-24.

[6] C. Ghali, G. Tsudik, and E. Uzun, “Network-layer trust in named-data networking,” ACM SIGCOMM Computer Communication Review, vol.44, no. 5, 2014, pp. 12-19.

[7] M. Wa¨hlisch, T. Schmidt, and M. Vahlenkamp, “Lessons from the past: Why data-driven states harm future information-centric networking,” IFIP Networking Conference, 2013, pp. 1-9.

[8] S. Choi, K. Kim, S. Kim, and B. Roh, “Threat of DoS by interest flooding attack in content-centric networking,” Proc. IEEE International Conference on Information Networking (ICOIN), 2013, pp. 315-319.

[9] F. Li, F. Chen, J. Wu, and H. Xie, “Longest prefix lookup in named data networking: How fast can it be?,” Proc. 9th IEEE NAS, 2014, pp.186-190.

[10] Amadeo, M., Campolo, C., & Molinaro, A. (2014). Forwarding strategies in named data wireless ad hoc networks: Design and evaluation. Journal of Network and Computer Applications, doi:10.1016/j.jnca.2014.06.007