2020 IEEE 14th International Conference on Big Data Science and Engineering (BigDataSE) | 978-0-7381-1114-8/20/$31.00 ©2020 IEEE | DOI: 10.1109/BigDataSE50710.2020.00023

Reputation-based Trust: A robust mechanism for Dynamic Adaptive Streaming over Named Data Networking

1st Ioanna Angeliki Kapetanidou
ATHENA Research and Innovation Center
Xanthi, Greece
ikapetan@athenarc.gr

2nd Muhammad Hassan
University of Padua
Padua, Italy
hassan@math.unipd.it

3rd Christos-Alexandros Sarros
ATHENA Research and Innovation Center
Xanthi, Greece
alexcsarros@athenarc.gr

4th Mauro Conti
University of Padua
Padua, Italy
conti@math.unipd.it

5th Vassilis Tsaoussidis
ATHENA Research and Innovation Center
Xanthi, Greece
tsaousi@athenarc.gr

***Abstract*—Information Centric Networking (ICN), emerges as a suitable networking paradigm to address functional challenges of today's overloaded Internet. Named Data Networking (NDN) architecture, as an ICN instance, appears as a promising candidate for next-generation Internet architecture. In addition, due to its reduced bandwidth requirements, NDN facilitates efficient content distribution, and hence, it is deemed suitable for supporting critical services such as multimedia streaming using standards like Dynamic Adaptive Streaming (DAS).**

Security and trust management in NDN are built on credential-based methods, i.e., based on cryptographic operations. However, the deployment of the default NDN defense means is restricted to the consumer-side, and it is insufficient against some attacks, such as bitrate oscillation attacks (BOAs). In this paper, we focus on investigating reputation-based trust as a means to reinforce the existing NDN security system. We present a novel reputation-based trust scheme which aims at mitigating BOAs. Evaluation results show that our proposed model manages to efficiently mitigate this type of attacks which cannot be alleviated by relying solely on NDN's default security system.

***Index Terms*—Named Data Networking, reputation-based trust, security, Dynamic Adaptive Streaming**

I. Introduction

The massive growth of traffic, witnessed during the last few years, calls for novel architectural solutions to better assist in content distribution. By grafting content at the core of its design, Information Centric Networking (ICN), and especially the Named Data Networking (NDN) paradigm [1], has arisen as a prominent candidate for the future Internet. NDN also appears to be beneficial for resource-consuming services, such as multimedia streaming, and particularly, when investigated in combination with the Dynamic Adaptive Streaming (DAS) standard [2], [3]. One of the NDN's fundamental features is in-network caching by routers. Although this feature contributes to reduced overall latency and bandwidth requirements, it also raises new security issues [4].

In NDN, security is a built-in feature, premised on public key cryptography and digital certificates [5], [6]. NDN ensures data integrity and authenticity by requiring content publishers to seal data with public key signatures and consumers to verify the signature to validate the received content. In addition, trust management in NDN has also been addressed by establishing trust in keys [7]. By using the so-called *trust schemas* [8], NDN entities are capable of determining which keys are authorized to sign each specific content piece.

Although performing signature verification is obligatory for NDN consumers, it constitutes a deterrent policy for intermediate routers given the prohibitive cost it introduces [9]. Therefore, most of the DoS attacks in NDN target routers which are susceptible to security threats because of their caching capability and are left with little defense means against malicious behaviors [4], [9], [10]. In this light, alternate methods need to be leveraged to consolidate the NDN security framework.

In this paper, we investigate a reputation-based trust mechanism as means to complement the NDN's current credential-based security in a specific use case, i.e. multimedia streaming. More specifically, we examine the mitigation of bitrate oscillation attacks (BOAs) [11], which are launched during video streaming using the DAS protocol over NDN. In BOAs, the adversary forces a benign DAS client to experience redundant bitrate oscillations during video streaming and eventually, to perceive degraded Quality of Experience (QoE) [12].

Traditional NDN security schemes fail to safeguard the

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the NGI_TRUST grant agreement no 825618 and partly from the Greek State Scholarships Foundation (IKY) action "Supporting human research resources through doctoral research", Operational Programme "Developing human Resources, Education and Lifelong Learning", 2014–2020.

I.A.Kapetanidou, C.A. Sarros and V.Tsaoussidis are with ATHENA Research and Innovation Center, Xanthi, Greece and and also with the Department of Electrical and Computer Engineering, Democritus University of Thrace, Xanthi, Greece.

978-0-7381-1114-8/20/$31.00 ©2020 IEEE
DOI 10.1109/BigDataSE50710.2020.00023

network from BOAs. Although some mitigation methods have been proposed, they either do not prevent the attack [11], or require continues network monitoring which introduces additional signalling overhead [13]. Motivated by this, we propose and implement a reputation-based trust mechanism, which overcomes the vulnerabilities identified in previous methods, and assists NDN in mitigating the attack's impact. Moreover, aiming to evaluate our approach under realistic conditions, we experiment with an on-off attack model [14], [15]. The results show that our technique efficiently shields the network from BOAs. Anticipated contributions are:

- To the best of our knowledge, this is the first work which, starting from evidently proving that reputation-based trust can be efficiently utilized in a specific use case, aims to generalize these results and argue that reinforcing the overall NDN's security framework by leveraging reputation-based trust, is doable.
- We enhance an existing reputation-based trust protocol and evaluate its efficiency in a multimedia streaming scenario. Our refined model, thanks to our design modifications, is also resistant against Sybil attacks.
- Unlike previous works concerning BOA mitigation, in our evaluation we have considered an on-off attack model, which is more complicated and realistic. Furthermore, our approach suppresses ongoing attacks without introducing communication overhead.

The rest of the paper is organized as follows: In Section 2, we provide an overview of the DAS protocol over NDN, as well as, of the BOA model. The design of our reputation-based trust scheme is delineated in Sections 3, while related evaluation results are presented in Section 4. Finally, in Section 5, we present previous reputation-based trust approaches in NDN, as well as, countermeasures for BOAs.

II. Background and Related work

A. NDN Overview

NDN architecture positions itself as a perfect applicant in the design space of receiver-driven multimedia streaming systems due to its implicit features such as receiver-driven mechanism, in-network caching, multi-cast routing, native mobility support, and so on. Contrary to the host-centric communication model, in NDN, a client directly requests for the content instead of addressing the location of content provider. In particular, for consuming specific *content*, it issues an exclusive *interest* related to that content. The interest represents a Uniform Resource Identifier (URI) by means of a routable name arrangement, e.g., `/UNIPD.IT/video4u/examples.mp3` [1]. Correspondingly, security follows a data-centric security model, in which each piece of content is signed by the provider, and which ensures content integrity and data-origin authentication [16]. The design of NDN entrusts extra responsibilities to the network by introducing router-side content caching and interest aggregation [7]. When receiving an interest, a router initially checks if the requested content is available in the *cache* (i.e., Content Store). If not, it performs a lookup in the *Pending Interest Table* (PIT) for outstanding forwarded interests, and aggregates closely spaced interests for the same content. Later, when the requested content arrives at the router, all pending interests are satisfied just by sending the content copies back to all consumers. Only when a PIT miss occurs, the router forwards the interest to *Forwarding Information Base* (FIB), which is responsible to route interests towards the origin content provider(s).

B. Dynamic Adaptive Streaming over NDN

As NDN has proven to be a promising candidate for replacing the existing Internet architecture, DAS over NDN has reasonably gained significant attention from the academic and research community. Numerous authors in their works [2], [3], [17]–[20] have shown ICN's native support for in-network caching and content-oriented delivery as a provision for DAS. Unlike HTTP-based multimedia streaming, in DAS over NDN, the Multimedia Presentation Description (MPD [1]) file lists the NDN names (i.e., Uniform Resource Identifier (URI)) for the segments as URL alternatives [21]. In addition, the hierarchical naming structure of NDN explicitly supports versioning and segmentation which indicates various representations of DASH-based multimedia content. In particular, NDN interest packets are issued to retrieve multimedia segments, which are provided either by the original content source or by in-network caches of routers.

Compared with HTTP- based adaptive streaming, the work in [17], [18] confirms that DASH over ICN is able to provide enhanced performance in terms of average download bitrate, smooth streaming session and reduced bandwidth requirements for the origin server. Also, the outcome of [3] demonstrates the effectiveness of in-network caching in case where multiple clients request the same content, subsequently showing improved video quality over time. Furthermore, authors in [19] highlight the gain of NDN-based dynamic adaptive streaming in the case of using Scalable Video Coding (SVC) [19], and prove that the integration of layered data approach with in-network caching increases the performance of bitrate adaptation process and allows for smooth playback without stalling.

However, despite the claims that NDN's explicit features are advantageous for adaptive multimedia streaming in terms of reduced bandwidth requirement and higher quality experience, DAS also exposes new security vulnerabilities when it is used over the NDN architecture [12]. In particular, the attacker is able to adversely exploit the two fundamental characteristics of NDN, i.e., *in-network caching* and *interest aggregation*. That way, the adversary is able to damage the adaptive behaviors of DASH streaming control system, resulting in the degradation of benign users' perceived QoE [12].

C. Reputation-based trust in NDN

As involving routers in the specifics of trust management is cumbersome, reputation-based trust schemes, owing to their

[1] XML document containing information about media segments

lightweight design, have been investigated as an alternate means to mitigate attacks in NDN [9].

In the case of a cache poisoning attack, NDN inherently supports no other way to flush content from router caches than cache replacement policies, which rely on eventual natural cache aging [4]. In this light, authors of both [22] and [23] propose reputation-based techniques based on explicit exclusion filters (i.e., exploiting the optional ”Exclude” field[2] included in Interest packets). In the former, consumers, who normally verify signatures, are able to identify invalid content and, subsequently, notify routers by issuing a new Interest to exclude certain content. Based on the exclusion information provided by consumers, routers prioritize valid over fake content. In the latter, besides the trust value assigned to each content object, a credibility value is also specified for each content provider. When a consumer issues an Interest excluding fake content, the content's trust value will be decreased, impacting the credibility of the sender, as well. Routers, thereafter, cache the received content and accept the incoming Interests with a probability which is equal to the content's trust value and to the credibility value of the consumer who sent the Interest, respectively. However, the exclusion functionality is no longer available in NDN [3], rendering the previous methods infeasible.

Furthermore, reputation-based trust has been leveraged in [24] for cache snooping detection. Users are rated based on the assumption that high interest, exclusion and cache hit rates' measurements in a specified short time period, are indicative of a cache snooper's behavior. Adversaries are identified by comparing the trust values to a threshold.

Apart from cache-related attacks, [14] proposes the ICRP mechanism to mitigate Interest Flooding attacks. In ICRP, edge routers assign reputation values to their adjacent consumers, which represent the transmission degree of Interests requiring existing content objects. ICRP identifies the malicious users by comparing the consumers' reputation values against a threshold, while it records non-existent content names and thus, limits the flow of malevolent Interests in the network.

D. Existing countermeasures for Bitrate Oscillation Attacks

Recent proposals aim to address BOA by proposing robust countermeasures, however, not highly effective. Conti et al. [11] were the first to address BOA by proposing a receiver-driven approach called Fair-RTT-DAS to mitigate the attack. Fair-RTT-DAS uses a scalable adaptive rate control technique at the user-end to assure high perceived QoE despite the presence of an adversary. Fair-RTT-DAS aims to maintain fairness when uneven round trip time (RTT) values are triggered by the adversary and due to the ICN's features. However, since it is a robust application running on the user-end, it does not protect network caches from being abused by the attacker.

he CoMon-DAS [13] aims to eliminate the deficiencies of the ICN architectural features against BOA. More specifically, the Coordination with lightweight Monitoring for DAS (CoMon-DAS) approach enables network-wide coordinated caching and cache-aware routing. CoMon-DAS aims to reduce bitrate oscillations and cache content redundancy considering both the presence of a BOA adversary and the ICN's inherent content source variations. However, continuous network monitoring and controlling of each network node by a single domain controller creates additional signalling overhead in the network. Moreover, it is prone to DDoS attacks as the central domain constitutes also a single point of failure.

III. Vulnerability in DAS over NDN

To illustrate the vulnerability in DAS over NDN, we consider the multimedia streaming scenario, as illustrated in Figure 1. The DAS-compatible multimedia data (S) is provided by a server, denoted as *producer* (P). S consists of n number of equal-length segments. Moreover, each segment is available in various representations, i.e., visual qualities. The *client* (C) streams each segment in the most optimal representation. We also consider that S is publicly available, and thus accessible by the adversary Adv. Furthermore, each request from Adv and C traverses one or more ICN routers before being satisfied by P or by an on-path CS. For adaptive bitrate streaming C, Adv and P utilize the DAS over ICN protocol, e.g., [3], [17].

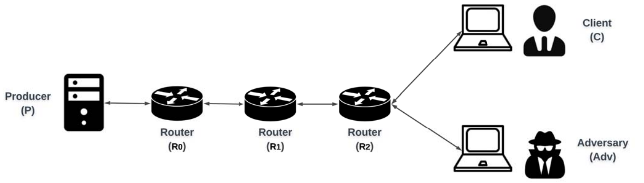

Fig. 1. Topology

A. Adversary model

For the adversarial model, we firstly assume that Adv is attached to at least one on-path router between C and P. Existing techniques, such as the one presented in [25], could be used by the Adv to identify the router closest to the victim and simply connect to it. We also consider that Adv has prior knowledge of the video (S) that C is about to stream. This assumption is rational, since there are various techniques which can be used by the Adv to obtain this information. For instance, Adv could exploit the timing attacks [26] and probe the MPD of the video, to discover S. Also, in case of identical wireless links, eavesdropping techniques [27] on the exposed traffic traces could be exploited as well, to analyze the online activities of C and predict S and its source location [28]. Lastly, we consider that the video is publicly available by Internet Service Providers (ISPs).

B. A Bitrate Oscillation Attack in DAS over NDN

In this section, we outline the proposed Bitrate Oscillation Attack (BOA) in NDN, which harms the adaptive behavior of the DAS streaming protocol, resulting in the degradation of

[2] contains information about name components that must not occur in the name of the returned content

[3] since version 0.3

the perceived QoE. In particular, an Adv forces the C into frequently switching between high and low bitrates.

At the beginning of the streaming session, the Adv obtains the MPD file containing the list of all available segments (S_n) and the associated representations [3]. To trigger oscillations for C, the Adv exploits the information included in the MPD to request a non-sequential subset of S. For each selected segment of S, Adv requests all the available representations to assure that the representation requested by C will be cached in an intermediate router. In particular, Adv issues a series of interests following an ascending order, i.e., $S(n + \gamma)$, where γ is the consecutive gap between the requested segments. As a result, when C subsequently requests all the segments of S, each segment has either been previously requested or skipped by the Adv. For instance, let us assume that a specific segment S_n requested by C, has been already requested by the Adv and a copy of S_n is then available in the CS of R_2. This segment would be delivered to C in the round-trip time between R_2 and C. In case that the earlier requested S_n has not yet reached R_2, the interest of C is aggregated at R_2, and it will be satisfied by R_2 in the round trip time a bit less than the round trip time between C and P. Finally, if S_n has been skipped by the Adv, C's interest will be forwarded all the way to P and S_n will be retrieved after the round trip time between P and C.

C, consequently, interprets short delivery times for the segments pre-issued by Adv as indicative of high network bandwidth availability. In contrast, C interprets longer delivery times for the remaining segments as indicative of lower bandwidth availability. Based on this assumption, by pre-issuing specific segments of S with the consecutive gaps, the Adv makes the DAS adaptation strategy at C to frequently switch between varying bitrates, e.g. from low to high. Therefore, the Adv accomplishes to cause unwanted bitrate oscillations to C, and eventually, degrade C's perceived QoE.

We need to note here that it is possible that a legitimate user also requests the non sequential segments. However, as the requests of each of the benign users are adapted to their individual network conditions, the chances of the representations of the segments requested by the two users coinciding, are extremely low. Therefore, many interests will be satisfied by the initial content provider. In contrast, our work focuses on the case in which an attacker intentionally mis-exploits NDN's native in-network caching and interest aggregation characteristics to inject all the representations of the non-consecutive segments in the network and thus, ensures that the victim will be forced to experience redundant oscillations.

IV. Reputation-based trust scheme design

In this section, we detail the design of the proposed reputation-based trust scheme. As the key to the attacker's success is his/hers capability to misuse the NDN's native in-networking caching property, the main objective of our countermeasure is to allow routers for controlling and limiting caching if they find out that it is being mis-exploited.

A. Design overview

The fundamental idea of our reputation-based approach is to allow NDN routers for adjusting their caching policy. More specifically, routers compute a reputation value for each multimedia content object based on the level of consecutiveness of its received segments. By relying on the inferred reputation values routers decide whether they will cache the following segments of the specific multimedia content or not. In summary, our reputation-based model is divided in four distinct phases:

1) The rating process of a specific multimedia file is initialized upon the arrival of an MPD file at the router. Once a router receives a multimedia content object's MPD file, it firstly checks whether it is the first time that the specific content is received. If so, the router, thereafter, assigns a default initial reputation value to it. In other words, routers keep a record of the multimedia content that has passed through them, along with their corresponding reputation values.
2) Once the MPD file has been parsed, the following data packets received, are expected to concern the segments of the multimedia content. Upon each segment receipt, the router checks if there is a gap between the segment that just arrived and the latest received segment, by comparing their segment numbers. The router provides a negative rating if a gap is detected, or a positive one, otherwise.
3) A certain time interval is defined and once it expires, the segment ratings calculated during this time interval are aggregated. The updated reputation value is computed by considering both the current ratings' aggregation result and the past reputation value. Therefore, the multimedia content's reputation value is updated on a periodic basis.
4) By relying on the derived reputation values, routers make suitable caching decisions, determining whether the upcoming segments should be cached or excluded from routers' caches.

The above-described design is captured in Algorithm 1. It is important to note here that we propose a decentralized framework where no coordination between routers is needed, i.e. each router calculates and stores its individual reputation values. By making this design choice, we avoid the undesirable overhead introduced by an exchange protocol required in a centralized framework [9].

As it is implied by the design analysis, the effectiveness of our model is premised on two key features: the proper calculation of the reputation values and the adaptation of a suitable caching policy in order to weaken the attacker. In the following subsections we provide a thorough description of those two features.

B. Reputation values

Regarding the updating process of the reputation values, we have adopted the rationale of the reputation-based trust protocol, presented in [29]. Nonetheless, we have made any

Algorithm 1: Reputation-based trust scheme

```
Require: Incoming Data Packet
if Incoming Data packet corresponds to MPD file then
    if Multimedia file has not been received before then
        $reputation\ value \leftarrow default\ initial\ reputation\ value$
        Record content & its $reputation\ value$;
    end if
else if Incoming Data packet corresponds to video segment then
    Rate the segment;
end if
if Time interval $[t-1, t]$ expired then
    for each content object do
        for $j = t-1$ to $j = t$ do
            Aggregate segment $ratings$;
        end for
        Update content $reputation\ value$;
        Adjust caching policy;
    end for
end if
```

necessary adjustments so that the initial primitives become suitable for our BOA mitigation method.

At this point, it is noteworthy that our refinements have rendered the used reputation-based protocol resistant against Sybil attack [15]. In the initial protocol, which is designed for cache poisoning attack mitigation, every router assigns a reputation value to each of its adjacent routers. By relying on the inferred reputation values, routers choose their well-regarded neighbors as the next hops towards which they forward Interests, and thus, malicious routers are temporarily excluded from the transmission path. However, an attacker can act by creating multiple identities, which are attached to multiple routers, at least one of which is likely to be included in the transmission path, and hence accomplish to inject poisonous content in the network. Unlike [29], we have chosen to assign reputation values to the disseminated multimedia content itself instead of the interface where malicious requests come from. That way, our model becomes invulnerable to Sybil attacks.

We define three modified metrics which replace the initial ones defined in [29]: the *skipping ratio*, the *rating* and the *reputation value*.

Skipping ratio. We define the *skipping ratio* $(SR(C_i))$ as the ratio of the number of detected gaps between received segments of the certain multimedia content to the segment number of the last received segment. Therefore, the skipping ratio can be calculated by:

$$SR(C_i) = \frac{G(C_i)}{L(C_i)} \tag{1}$$

In this equation, $C_i, G(C_i)$ and $L(C_i)$ denote the multimedia content object, the number of detected gaps and the segment number of the last received segment, respectively. We use the segment number of the last received segment as the denominator because it specifies the total number of segments that would have been received if there were no gaps. The skipping ratio metric, consequently, indicates the frequency of the detected gaps.

Rating. Upon the receipt of a new segment, there are two potential scenarios. In the first one, the segment number of the received segment is the expected one, i.e. received segments are consecutive. In the second case, the received segment number is greater than expected, i.e. some segments have been skipped.

Based on this assumption, the router rates the received segment either positively or negatively. Similar to [29], routers utilize a rating system which follows the "linear increase, exponential decrease" principle. The skipping ratio metric, is factored into the calculation of the *rating* in time t, as indicated by the following equation:

$$R(C_i) = \begin{cases} 1 & \text{if segments are consecutive} \\ -\theta e^{\alpha}(1 - SR(C_i) & \text{if a gap is detected} \end{cases} \tag{2}$$

As described in [29], θ is a penalty factor representing the strength of the punishment and α is an adjustment factor.

We have adopted this rating system in order to detect content which causes suspicious oscillations and thus, it is likely that the specific content is being requested by an attacker. The computed rating is included in the calculation of the updated *reputation value*, increasing it if there no gaps have been detected or decreasing it otherwise.

Reputation value. The *reputation value* $(RV(t))$ represents an assessment of the trustworthiness of a certain multimedia file. In particular, a low *reputation value* means that segments are usually skipped and thus, it is possible for an adversary to utilize the content as weapon, while high reputation scores signal requests of consecutive segments. The updated *reputation value* is calculated by:

$$RV(t) = \delta RV(t-1) + \sum_{1}^{N} R(C_i) \tag{3}$$

In the equation (3), N denotes the number of segments received in the time interval [t − 1 , t]. It is, also, clear that we incorporate both the past and the current inference regarding the multimedia content's trustworthiness. By taking into account both the past (multiplied by a time decay factor δ) and current inferences, the mechanism becomes capable of lessening the impact of on-off attacks [14].

By relying on the *reputation value*, each router decides whether it should allow for caching the incoming video segments or not.

C. Caching policies

Based on the *reputation values*, routers determine the caching policy they will follow. We examine three different potential caching policies:

- **Threshold-based.** The derived *reputation values* are being compared to a predefined threshold value T. In the beginning, the caching of segments is not granted. In order for the segments to get cached, the content's *reputation value* needs to reach the threshold. In other words, the caching of video segments is enabled as soon as the content gains the reputation of the routers.

$$Caching(C_i) = \begin{cases} Permitted & \text{if } RV(t) \geq T \\ Denied & \text{if } RV(t) < T \end{cases} \quad (4)$$

However, exceeding the threshold value does not guarantee caching the rest of the segments. If punishing the multimedia content according to equation (2) results in an updated *reputation value* value below the threshold, then the caching of the content segments is explicitly disabled until the *reputation value* recovers.

- **Probabilistic.** In that case, a drop probability (DP) tied to the *reputation value* is introduced. As the *reputation value* decreases, the drop probability increases.

$$DP(t) = 10 - RV(t)$$

The drop probability defines how likely it is for the incoming segments to get accepted to routers' caches.

- **Hybrid.** In this approach we define two threshold values, the lower (LT) and the upper (UT) threshold. When a segment is received there are three potential cases:

1) The *reputation value* is below the lower threshold.

$$RV(t) < LT$$

2) The *reputation value* is equal to or greater than the lower threshold and less than the upper threshold.

$$LT \leq RV(t) < UT$$

3) The *reputation value* is equal to or greater than the upper threshold.

$$UT \leq RV(t)$$

If the *reputation value* is less than the lower threshold value, then the router explicitly avoids caching the video segments. If the *reputation value* falls under the second case, then the router decides to cache or not to cache the incoming segments according to a drop probability (the lower the *reputation value*, the higher the drop probability). In the last case, routers cache all incoming segments without exception.

V. Reputation-based trust scheme evaluation

A. Simulation setup

In this section, we evaluate the effectiveness of our proposed reputation-based trust countermeasure for bitrate oscillation attacks by using the AMuSt-ndnSIM simulator framework [30]. AMuSt-ndnSIM is a modified version of the Named Data Networking Simulator (ndnSIM [31]), which supports adaptive multimedia streaming over NDN by integrating the libdash software [32] (i.e., an open-source library of the MPEG-DASH standard).

TABLE I
Simulation Configurations

Parameter	Value
Link Bandwidth	10 Mbps
Point-to-point link delay	2 ms
Link between Producer and edge router delay	350 ms
Content Store size	0 (unlimited)
Cache replacement policy	LRU
Forwarding Strategy	BestRoute
Video codec	AVC
No. of video segments	299
No. of available representations	20
Segment duration	2 s
Adaptation Logic	RB
Start up delay	0.1 s
Max. buffered seconds	30
Consecutive gap γ	5
Default initial reputation value	3.5
Penalty factor θ	0.5
Adjustment factor α	1
Time decay factor δ	0.75
Time interval $[t-1, t]$	100 s
On-off attack time interval	250 s

The topology considered in our simulations is the one depicted in Fig.1, while corresponding configurations are included in Table I. Both the adversary and the legitimate multimedia consumer request the AVC-encoded Big Buck Bunny clip from the DASH/AVC Dataset [33]. The multimedia consumer uses the Rate-based adaptation logic (RB), i.e. he/she adapts the best possible representation based on throughput estimations. We have chosen this adaptation logic in order to maximize the attack impact [12]. Intermediate routers use the BestRoute forwarding strategy (i.e. they forward the Interests to the upstream with lowest routing cost) and the Least Recently Used (LRU) cache replacement policy to update the Content Stores' entries.

Furthermore, we assume that we have to deal with a rogue adversary who realizes that following the simple BOA model, i.e. simply skipping segments with a consecutive gap γ, would result in repeated punishments (according to equation (2)) and thus, a very low *reputation value*. In that case, incoming segments would be rejected from routers' caches and hence, the attack would fail. Therefore, the adversary attempts to launch an on-off attack, mixing normal and malicious behavior, aiming to render the attack hard to detect [15]. This assumption is reasonable, since on-off attacks are more realistic [14]. Hence, we assume that the adversary who launches the BOA, changes his/hers behavior from requesting consecutive segments for a certain period of time to requesting segments with a consecutive gap γ, and vice versa. In our simulations, we set this time interval to 250 seconds.

B. Results

Motivated by previous works [34], [35], we evaluate the performance of our mechanism, and thus, the QoE perceived by the DAS client, using the following metrics:

- Number of switches

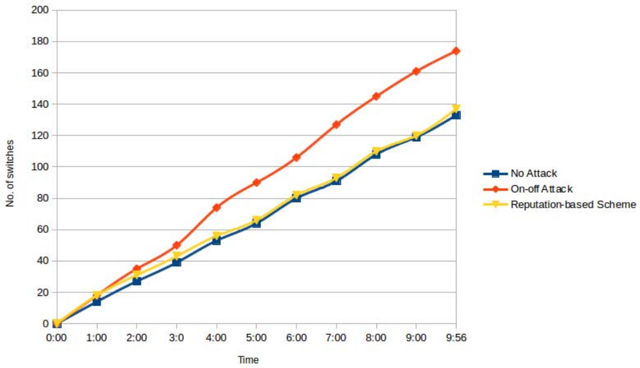

Fig. 2. Reputation-based countermeasure efficiency: No. of switches

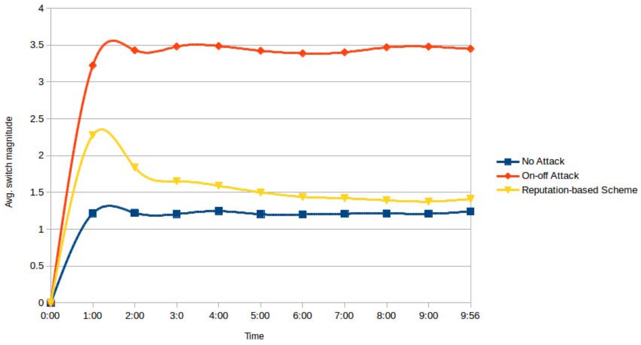

Fig. 3. Reputation-based countermeasure efficiency: Avg. magnitude

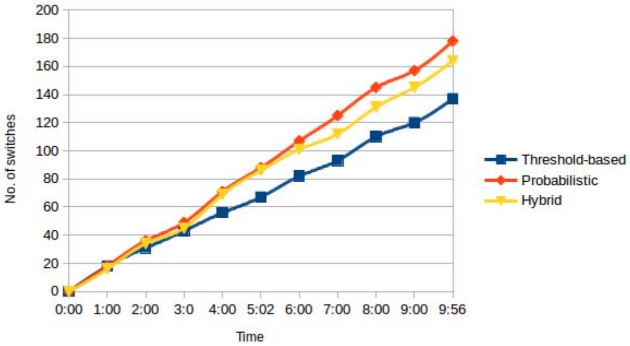

Fig. 4. Caching policies evaluation: No. of switches

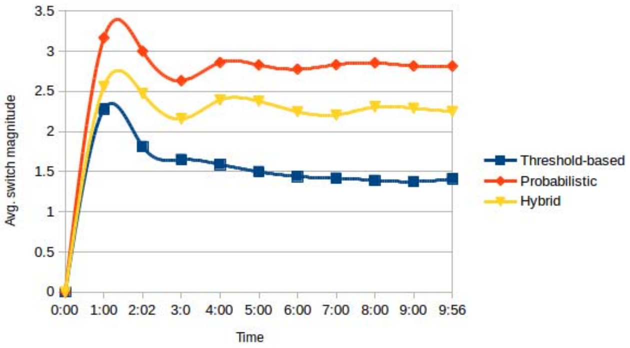

Fig. 5. Caching policies evaluation: Avg. magnitude

- Average switch magnitude (i.e., the average amplitude of video quality switches)

1) Reputation-based countermeasure efficiency: We firstly evaluate the performance of our proposed reputation-based countermeasure. We assume that intermediate routers have adopted the threshold-based caching policy and set the threshold value to 7.

The simulation results are illustrated in Figs. 2 and 3. We compare our results against both the results of the on-off attack model and the absence of an attacker.

According to the simulation results, even though the adversary behaves legitimately for a long period of time and strives to confuse the reputation-based trust system, our countermeasure efficiently mitigates the impact of an ongoing BOA. In the beginning, the adversary accomplishes to hide his/hers malicious behavior and cause some redundant oscillations. However, due to the punishments enforced by the trust model, the attack's impact is rapidly eliminated. In particular, the number of the switches is decreased by 21%, while the average switch amplitude is decreased by 60%. The aforementioned percentages are very satisfactory since the final number of the switches and the average switch amplitude are only 3% and 13% greater than the respective values of the ”No Attack” case. Overall, the proposed framework maintains both the number of the switches and the average switch amplitude at a reasonable level, despite the tactic adopted by the attacker.

2) Caching policies evaluation: In our simulations, we also experiment with the three different caching policies. For the threshold-based policy, T value is set to 7, while for the hybrid one, the upper threshold (UT) is set to 7 and the lower (LT) is set to 4.

Figs. 4 and 5 show the values of the evaluation metrics over time for the threshold-based, the probabilistic and the hybrid caching policy.

Although all three policies produce results up to the mark, they have distinct differences. As observed, the threshold-based method seems to generate the best results. This is rational since it is the strictest method, explicitly excluding the content which does not meet the criteria from routers' caches and hence, weakening the attacker. Instead, the probabilistic policy due to its flexibility, produces the least satisfactory results. It neither explicitly allows the caching of well-reputed content in the network nor it prevents the attacker from injecting segments of suspicious content. Moreover, since caching is associated with some probability, a specific segment might be cached only by certain routers of the path. As a consequence, retrieving segments from different locations increases the number of fluctuations. Finally, the results generated by the hybrid method are expected, since it combines the logic of the other two policies, gradually shifting from explicit caching decisions to probabilistic caching.

VI. Conclusions

The current credential-based NDN security framework is inherently insufficient against particular security threats, such as BOAs. In this paper, we argued that reputation-based trust should be leveraged in order to assist securing the NDN architecture. We further supported our argument by implementing a reputation-based trust mechanism which mitigates BOAs in NDN, while it is also invulnerable to Sybil attacks. As shown by the evaluation, reputation-based trust has the potential to efficiently complement the NDN security mechanisms.

References

[1] L. Zhang, A. Afanasyev, J. Burke, V. Jacobson, P. Crowley, C. Papadopoulos, L. Wang, B. Zhang *et al.*, "Named data networking," *ACM SIGCOMM Computer Communication Review*, vol. 44, no. 3, pp. 66–73, 2014.

[2] J. Samain, G. Carofiglio, L. Muscariello, M. Papalini, M. Sardara, M. Tortelli, and D. Rossi, "Dynamic adaptive video streaming: Towards a systematic comparison of icn and tcp/ip," *IEEE Transactions on Multimedia*, vol. 19, no. 10, pp. 2166–2181, Oct 2017.

[3] Y. Liu, J. Geurts, J. C. Point, S. Lederer, B. Rainer, C. Müller, C. Timmerer, and H. Hellwagner, "Dynamic adaptive streaming over ccn: A caching and overhead analysis," in *2013 IEEE International Conference on Communications (ICC)*, June 2013, pp. 3629–3633.

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

[5] Z. Zhang, Y. Yu, H. Zhang, E. Newberry, S. Mastorakis, Y. Li, A. Afanasyev, and L. Zhang, "An overview of security support in named data networking," *IEEE Communications Magazine*, vol. 56, no. 11, pp. 62–68, 2018.

[6] Z. Zhang, A. Afanasyev, and L. Zhang, "Ndncert: universal usable trust management for ndn," in *Proceedings of the 4th ACM Conference on Information-Centric Networking*. ACM, 2017, pp. 178–179.

[7] V. Jacobson, D. K. Smetters, J. D. Thornton, M. Plass, N. Briggs, and R. Braynard, "Networking named content," *Commun. ACM*, vol. 55, no. 1, p. 117–124, Jan. 2012. [Online]. Available: https://doi.org/10.1145/2063176.2063204

[8] Y. Yu, A. Afanasyev, D. Clark, V. Jacobson, L. Zhang *et al.*, "Schematizing trust in named data networking," in *Proceedings of the 2nd ACM Conference on Information-Centric Networking*. ACM, 2015, pp. 177–186.

[9] I. A. Kapetanidou, C.-A. Sarros, and V. Tsaoussidis, "Reputation-based trust approaches in named data networking," *Future Internet*, vol. 11, no. 11, p. 241, 2019.

[10] P. Gasti, G. Tsudik, E. Uzun, and L. Zhang, "Dos and ddos in named data networking," in *2013 22nd International Conference on Computer Communication and Networks (ICCCN)*. IEEE, 2013, pp. 1–7.

[11] M. Conti, R. Droms, M. Hassan, and C. Lal, "Fair-rtt-das: A robust and efficient dynamic adaptive streaming over icn," *Computer Communications*, vol. 129, pp. 209–225, 2018.

[12] M. Conti, R. Droms, M. Hassan, and S. Valle, "Qoe degradation attack in dynamic adaptive streaming over icn," in *2018 IEEE 19th International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM)*. IEEE, 2018, pp. 1–9.

[13] M. Hassan, H. Salah, M. Conti, F. H. P. Fitzek, and T. Sturfe, " CoMon-DAS: A Framework for Efficient and Robust Dynamic Adaptive Streaming over NDN," *In proceedings of 24th IEEE Symposium on Computers and Communications (ISCC).*

[14] S. Umeda, T. Kamimoto, Y. Ohata, and H. Shigeno, "Interest flow control method based on user reputation and content name prefixes in named data networking," in *2015 IEEE Trustcom/BigDataSE/ISPA*, vol. 1. IEEE, 2015, pp. 710–717.

[15] D. Wang, T. Muller, Y. Liu, and J. Zhang, "Towards robust and effective trust management for security: A survey," in *2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications*, 2014, pp. 511–518.

[16] A. Compagno, M. Conti, and M. Hassan, *An ICN-Based Authentication Protocol for a Simplified LTE Architecture*. Cham: Springer International Publishing, 2018.

[17] S. Lederer, C. Mueller, C. Timmerer, and H. Hellwagner, "Adaptive multimedia streaming in information-centric networks," *IEEE Network*, vol. 28, no. 6, pp. 91–96, Nov 2014.

[18] S. Lederer, C. Mueller, B. Rainer, C. Timmerer, and H. Hellwagner, "Adaptive streaming over content centric networks in mobile networks using multiple links," in *2013 IEEE International Conference on Communications Workshops (ICC)*, June 2013, pp. 677–681.

[19] S. Petrangeli, N. Bouten, M. Claeys, and F. D. Turck, "Towards svc-based adaptive streaming in information centric networks," in *2015 IEEE International Conference on Multimedia Expo Workshops (ICMEW)*, June 2015, pp. 1–6.

[20] B. Rainer, D. Posch, and H. Hellwagner, "Investigating the performance of pull-based dynamic adaptive streaming in ndn," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 8, pp. 2130–2140, Aug 2016.

[21] S. Lederer, C. Mueller, B. Rainer, C. Timmerer, and H. Hellwagner, "An experimental analysis of dynamic adaptive streaming over http in content centric networks," in *2013 IEEE International Conference on Multimedia and Expo (ICME)*, July 2013, pp. 1–6.

[22] C. Ghali, G. Tsudik, and E. Uzun, "Needle in a haystack: Mitigating content poisoning in named-data networking," in *Proceedings of NDSS Workshop on Security of Emerging Networking Technologies (SENT)*, 2014.

[23] Z. Rezaeifar, J. Wang, and H. Oh, "A trust-based method for mitigating cache poisoning in name data networking," *Journal of Network and Computer Applications*, vol. 104, pp. 117–132, 2018.

[24] N. Ntuli and S. Han, "Detecting router cache snooping in named data networking," in *2012 International Conference on ICT Convergence (ICTC)*. IEEE, 2012, pp. 714–718.

[25] A. Compagno, M. Conti, P. Gasti, L. V. Mancini, and G. Tsudik, *Violating Consumer Anonymity: Geo-Locating Nodes in Named Data Networking*. Cham: Springer International Publishing, 2015, pp. 243–262.

[26] G. Acs, M. Conti, P. Gasti, C. Ghali, G. Tsudik, and C. Wood, "Privacy-aware caching in information-centric networking," *IEEE Transactions on Dependable and Secure Computing*, vol. PP, no. 99, 2017.

[27] F. Zhang, W. He, X. Liu, and P. G. Bridges, "Inferring users' online activities through traffic analysis," in *Proceedings of the Fourth ACM Conference on Wireless Network Security*, ser. WiSec '11. New York, NY, USA: ACM, 2011, pp. 59–70. [Online]. Available: http://doi.acm.org/10.1145/1998412.1998425

[28] M. Liberatore and B. N. Levine, "Inferring the source of encrypted http connections," in *Proceedings of the 13th ACM Conference on Computer and Communications Security*, ser. CCS '06. New York, NY, USA: ACM, 2006, pp. 255–263. [Online]. Available: http://doi.acm.org/10.1145/1180405.1180437

[29] D. Wu, Z. Xu, B. Chen, and Y. Zhang, "What if routers are malicious? mitigating content poisoning attack in ndn," in *2016 IEEE Trustcom/BigDataSE/ISPA*. IEEE, 2016, pp. 481–488.

[30] C. Kreuzberger, D. Posch, and H. Hellwagner, "Amust framework - adaptive multimedia streaming simulation framework for ns-3 and ndnsim," 2016.

[31] S. Mastorakis, A. Afanasyev, and L. Zhang, "On the evolution of ndnsim: An open-source simulator for ndn experimentation," *ACM SIGCOMM Computer Communication Review*, vol. 47, no. 3, pp. 19–33, 2017.

[32] C. Mueller, S. Lederer, J. Poecher, and C. Timmerer, "Demo paper: Libdash-an open source software library for the mpeg-dash standard," in *2013 IEEE International Conference on Multimedia and Expo Workshops (ICMEW)*. IEEE, 2013, pp. 1–2.

[33] S. Lederer, C. Müller, and C. Timmerer, "Dynamic adaptive streaming over http dataset," in *Proceedings of the 3rd Multimedia Systems Conference*, ser. MMSys '12. New York, NY, USA: ACM, 2012, pp. 89–94. [Online]. Available: http://doi.acm.org/10.1145/2155555.2155570

[34] Y. Liu, S. Dey, F. Ulupinar, M. Luby, and Y. Mao, "Deriving and validating user experience model for dash video streaming," *IEEE Transactions on Broadcasting*, vol. 61, no. 4, pp. 651–665, 2015.

[35] D. Z. Rodríguez, R. L. Rosa, E. C. Alfaia, J. I. Abrahão, and G. Bressan, "Video quality metric for streaming service using dash standard," *IEEE Transactions on broadcasting*, vol. 62, no. 3, pp. 628–639, 2016.