This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TNSM.2018.2811944, IEEE Transactions on Network and Service Management

Enhancing Information Resilience in Disruptive Information-Centric Networks

Vasilis Sourlas*, Onur Ascigil†, Ioannis Psaras† and George Pavlou†
* ICCS-NTUA, GR. † University College London (UCL), UK.
Email: v.sourlas@iccs.gr, {o.ascigil, i.psaras, g.pavlou}@ucl.ac.uk

***Abstract*—We argue that data communications in dynamic and potentially fragmented networks should not and cannot rely on network-centric resilience schemes, as is the case in today's networks, but should take advantage of techniques that focus on *information-centric* resilience. We make the case that management and control in disruptive environments should take advantage of information-centricity, rather than focus on node-oriented path recovery routing. This is also essential in the Information-Centric Networking (ICN) paradigm, which is by nature oblivious to network locations. In this context, we build on ICN and enhance the Named Data Networking (NDN) architecture with extra functionality in order to make it resilient to network failures. We introduce an extra *Interest management routing table*, which we call the *"Satisfied Interest Table"* (SIT) and which points to the direction of already satisfied interests. This way, upon failure of links/nodes towards the content origin, the SIT table can redirect Interests towards caches and end-users that have recently received the requested content. Our extensive performance evaluation shows that our simple, yet efficient *information resilience scheme* can serve most requests made after disruptive effects, *e.g.,* natural disasters, where users are interested in latest updates, dissemination of warnings from first responders and evacuation plans. More generally, we believe that our proposed approach should become part of the main NDN architecture as it can support service resilience in the case of network failures.**

***Index Terms*—Information-Centric Networks, Information Resilience, Fault Management, Disruptive Scenarios.**

I. Introduction

Resilience in telecommunications refers to the ability of a given network architecture to provide and maintain acceptable quality of service levels to end users when nodes and/or links fail. Given the host-centric nature of the current Internet architecture, research has so far naturally focused on *network-centric* resilience in order to allow uninterrupted content delivery, ignoring *information-centric* aspects [2]. Resilience is achieved by performing path recovery and traffic re-routing through alternative unaffected paths, *e.g.,* [3] for IP-specific network resilience. The management plane configures provisioned alternative paths *e.g.,* disjoint LSPs in MPLS or alternative non-shortest paths in IP fast re-routing, and the control plane activates these paths as soon as a relevant failure is detected. However, if connectivity to the content origin is lost due to network fragmentation, or the origin server itself fails, all the node-centric network architectures fail to resume the content delivery process.

In this work, *we argue that the type of communication required during a disruptive scenario is primarily of information-centric nature* [4], *e.g.,* quick dissemination of warnings and evacuation plans, or crucial content from legal authorities to reach all users in time. The need for information-centricity combined with the inherent support for mobility, security and in-network opportunistic caching provided by the Information-Centric Networking (ICN) paradigm, makes it a natural fit for communication in disruptive networking scenarios.

Interestingly, despite the sizable amount of work in the area of ICN routing, all current architectural proposals forward by default requests/interests directly towards the primary content source. That said, even if cached copies of requested content exist in the network, they will eventually "dry out" when the server itself is not replicated.

In this work, we investigate the potential to exploit the in-network caching capabilities of the NDN architecture [5] together with user-assisted caching in order to prolong content lifetime, and therefore improve information resilience when fragmentation happens and the origin server is unreachable. For instance, in a dynamic/disruptive environment, during the aftermath of a natural disaster, or a human-generated network breakdown, both users and content servers may dynamically join and leave the network (due to mobility or network fragmentation). Thus, users may request and retrieve content when the network is fragmented and the corresponding content origin is unreachable, by taking advantage of similar interests issued by neighboring users and their cached content.

In order to deal with network fragmentation or, more generally, with network failures that prohibit interest forwarding towards the origin server, we propose a simple, yet novel and efficient *Interest forwarding management* scheme, whose focus is to search and discover content cached by both routers and end-users. In this scheme, routers maintain an Interest management routing table, denoted as *"Satisfied Interest Table" (SIT)*, which maps the names of the recently satisfied interests to the interface(s) the corresponding interests arrived from. The routers use the information stored in the SIT table as a "hint" of where cached content may reside and, in case of disruptions, forward content requests towards users who have recently obtained the same content. This approach effectively uses data plane information to substitute the centrally-configured management and control information in current node-centric network architectures. In other words, the proposed scheme uses a part of the data plane, *i.e.,* the SIT, to replace the equivalent functionality of the management and control planes.

Our results show that our simple, yet efficient information resilience scheme can serve most requests made after disruptive effects, *e.g.,* natural disasters, where users are interested in latest updates, dissemination of warnings from first responders and evacuation plans. The proposed approach is general

Part of this work appeared in the proc. of IFIP NETWORKING 2015 conference [1] and has been awarded the BEST PAPER AWARD.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TNSM.2018.2811944, IEEE Transactions on Network and Service Management

enough to be used in every ICN environment (both fixed and dynamic) so as to cater for single or even multiple link and node failures.

In this paper we:

- Enhance the Interest packet management and forwarding mechanism of the NDN [5] architecture with a new component called "*Satisfied Interest Table*" (*SIT*) so that interests can be forwarded towards neighbouring users with similar interests. Entries in the SIT point to both off-path caches and end-users, and these entries can be exploited to retrieve cached content when the network is fragmented (*i.e.,* the content origin is temporarily unreachable).
- Decompose the proposed information resilience scheme in a set of basic policies (*i.e.,* forwarding, caching and placement policies) and propose combinations of them that lead to different resilience strategies.
- Provide an analytical expression with the use of continuous time, discrete state, Markov processes for the computation of the probability that an item will disappear (be absorbed) from the network. We also provide an expression for the corresponding *time to absorption* upon the fragmentation of the network, when the cache capacity of each router is equal to zero. These expressions are used to obtain lower bounds for the proposed information resilience scheme.
- Enhance the publicly available Icarus simulator [6] to support the proposed resilience scheme, and validate and evaluate it through extensive simulations using realistic network topologies for various system parameters.

The rest of the paper is organized as follows. In Section II we survey related work, whereas in Section III we present the functionality of the proposed information resilience scheme and the necessary augmentations to the original NDN router design to support it. Section IV is devoted to the description of the management policies that constitute the various information resilience strategies, whereas in Section V we derive the analytical expressions for the absorption probability and the time to absorption of an item. Finally, in Section VI we evaluate the performance of the proposed information resilience scheme, while we conclude the paper in Section VII.

II. Related Work

One of the core elements of the ICN paradigm is the exploitation of network devices (*i.e.,* routers), as content caches. The challenges of placing content in caches and resolving the location of the caches upon subsequent requests have attracted considerable attention from the research community [7].

A. Content Placement

The majority of ICN architectures follow reactive, opportunistic content placement strategies. As such, most works in this area have focused on placing content in in-network caches in order to optimize traditional metrics such as *delivery latency* based on content popularity assessment [8], content locality [9], or cache redundancy and cache resource management [10]. Generally, ICN architectures enable caching of addressable information items, in every cache-equipped node. However, this *leave copy everywhere* scheme [5] has already raised doubts and several researchers have already questioned this aggressive strategy [11]. In that direction, a plethora of caching algorithms have been proposed according to which on-path routers decide probabilistically whether or not to cache passing-by content [12].

B. Request to Cache Routing

Besides making content placement decisions, the network should also have the right mechanism in place in order to direct content requests to the right cache. Given the location-independent nature of ICN, this constitutes a central and challenging part of the communication system. By and large, request-to-cache routing can follow one of two approaches: either *opportunistic on-path*, where content is searched on-path as the request is travelling towards the content source, or *co-ordinated off-path*, where requests are forwarded off the shortest path to the content source or some designated caches that are likely to hold this content.

At the data plane, the most prominent solution to the *"request-to-cache" routing* challenge is to maintain an extra routing table which matches requests to information items cached in nearby nodes [13][14]. The techniques proposed in [15][16][17] involve also the control plane and use co-ordination techniques between the data and control plane to place content and re-direct requests to the corresponding caches. In [18] two methods are proposed to route requests to the nearest replica of a content by either flooding requests or meta-requests to discover the content location. In [19], the authors utilize hash-routing techniques, which have been proposed in the past for mapping requests to physically co-located servers. Each router in the network is assigned a part of the hash space and caches the items whose hashed identifiers fall within that space. This way, hash-routing avoids all the complex request-to-cache resolution steps of similar proposals and minimizes the corresponding signalling overhead. Finally, the authors in [20] have proposed a scoped flooding-based content discovery mechanism. The proposal includes a ring model, which limits the spread of the flood to the immediate neighbourhood. The results show that although scoped-flooding introduces some overhead, it is far from prohibitive and can scale and achieve considerable gains.

C. ICN in Disruptive Environments

Despite the large body of work in the area of ICN caching and content retrieval, research efforts have largely assumed that the content origin is always present. In that sense, caching is only used to boost performance. Furthermore, all the aforementioned research attempts did not explore the caching capabilities of end-users and the possibility of exploiting them to further assist content retrieval and delivery. To the best of our knowledge, [21] is the only work which integrates end-users in the content delivery process and proposes a "*user-assisted in-network caching*" scheme. In contrast to our approach though, the work in [21] also assumes the presence of the content origin (uninterrupted connectivity) and user-assisted caching is only used to improve network performance in terms of cache hit ratio and not as an information resilience scheme in disruptive scenarios.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TNSM.2018.2811944, IEEE Transactions on Network and Service Management

In terms of project efforts, the GreenICN EU-Japan project [22] has exploited the ICN architectural paradigm to support the aftermath of a disaster. A major part of the project's vision/objective is *"the aftermath of a disaster, e.g., hurricane or tsunami, when communication resources are at a premium and it is critical to efficiently distribute disaster notification and rescue information. Key to this is the ability to exploit fragmented networks with only intermittent connectivity"*. This is also one of the main technical challenges according to the IETF ICNRG working group [23][24], regarding the use of ICN in disaster scenarios, namely to exploit management and control techniques in order to enable the use of the functional parts of the infrastructure, even when these are disconnected from the rest of the network. In that direction, the authors in [25] developed a distributed serverless social networking service based on NDN for sharing information among users before and after a disaster. Moreover, in [26] the authors presented the "*Name-based Replication*" (NREP) system for scope-based prioritisation of ICN messages in disasters, where ICN messages carry attributes such as user-defined priority, space, and temporal-validity. These attributes are then taken into account when prioritizing messages. This system is orthogonal to our approach here and can be used as an alternative to determine information items' importance, as well as to differentiate between emergency-related and normal traffic content.

In [27], the authors propose an information resilience scheme for the PURSUIT [28] ICN architecture. They introduce a resilience management function that supports link failure detection and usage of alternative sources for a given information item. Nodes publish periodically link state notifications and depending on whether messages are delivered or not, the network can detect link removals or additions. Furthermore, upon the detection of a link failure the proposed resilience function identifies if any delivery tree was affected by the failure and establishes a new tree for any broken one. This work also assumes the presence of multiple content origins/publishers in the form of CDN-like replication points in the network and aims at re-establishment of the connectivity between the users and an alternative origin.

Generally speaking, delay-tolerance is a desirable feature in case of network fragmentation. This has led over the past few years to an attempt to combine the capabilities of Delay Tolerant Networks (DTN) with those of the information-centric communication paradigm in order to assist content delivery in disaster situations. In [29], the authors proposed an enhanced ICN approach, where data mules are used for the dissemination of information between the fragments of the network. Since the paths followed by the interests might be different from the paths followed by the returned data due to the uncoordinated movement of the data mules, the authors propose the separation of the logical faces from the actual physical interfaces, since the data mules behave as mobile routers. The work in [29] is also orthogonal to our work, since we consider information resilience within a fragment when the content origin (or data mule) is not reachable.

A protocol stack which integrates the DTN architecture in native NDN to deal with network disruptions is presented in [30]. In particular, the authors in [30] extend NDN routing strategies to integrate the Bundle protocol (BP) of the DTN architecture. Integrating BP in NDN, enhances the connectivity options of NDN and allows it to deal with network disruptions. Finally, in [31], the authors propose a disruption-tolerant information-centric ad-hoc network to provide low-cost, bandwidth-efficient operations for Vehicular ad-hoc networks (VANET). Their solution is inspired by the family of peer-to-peer data dissemination networks (*e.g.,* Haggle [32]) and the use of specialized interest and cache summary messages to synchronize the nodes of the VANET. The work in [31] is also orthogonal to our proposed information resilience scheme. In [31], authors assume a vehicular network and users use special Bloom filter-based broadcast control messages to indicate the data objects a node wants. In contrast, we assume a scheme to retrieve information when a part of the network is still functional and the connectivity to content origin is missing. However, the underlying network is connected and users utilize the SIT entries to search for matching content.

The work presented here is an extension of the work presented in [1] and is the first attempt to exploit the caching capabilities of NDN routers and of end-users to support content retrieval in disruptive scenarios, where the network is fragmented and the content origin is not reachable. In addition, it provides the basis to address resilience in ICN in general. Compared to [1], apart from various enhancements and a new implementation in the Icarus simulator, the proposed resilience scheme is augmented with a limited scoped flooding mechanism to minimize the edge router effect that is described in Section III. Also, a new set of alternative policies and resilience strategies are proposed here. This was done for completeness, and in order to align the proposed resilience scheme with the new findings in the area of caching and forwarding strategies in ICN.

III. Enhanced NDN Router Design

In this section, we present the functionality of the proposed information resilience scheme. The rationale behind our design is to increase information resilience by leveraging the caching capabilities of both network routers and end-users.

A. NDN router

As shown in Fig. 1, we augment the original NDN content router design presented in [5] with the *Satisfied Interest Table (SIT)*, while the functionality of the other router components, namely the Content Store (CS), the Pending Interest Table (PIT) and the Forwarding Information Base (FIB) remain the same.

We introduce SIT to reap the benefits of name-based routing and search for available content whenever the content origin is not reachable (or differently the data mule in [29] is not connected to the examined network fragment). Specifically, SIT keeps track of the Data packets that are heading towards users. In the event that Interest packets cannot reach the content origin following the FIB entries, they can be forwarded based on the SIT entries towards users that issued similar interests in the past. SIT entries also allow for a list of outgoing faces, supporting multiple sources of data, which can

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TNSM.2018.2811944, IEEE Transactions on Network and Service Management

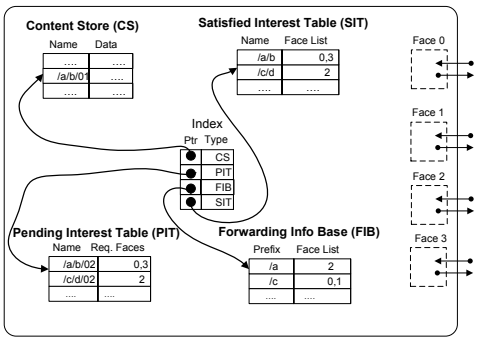

Fig. 1. Content Router design with the new Satisfied Interest Table (SIT).

be queried in parallel or sequentially depending on the chosen forwarding mechanism (see Section IV).

A SIT entry is triggered by a returning Data packet and comprises a trail of "*bread crumbs*" for a matching Interest packet that leads back to users with similar satisfied interests. Following the hierarchical naming scheme of NDN, an information item is segmented into chunks and each chunk is uniquely identified (*e.g.,* `Emergency/Police/Flooding/EvacPlan/chunkID`). Whereas each PIT entry follows the chunk based granularity, in this paper SIT entries are compiled in a file/object/information item basis instead of chunk/packet IDs to speed up the opportunistic retrieval mechanism and reduce the size of the SIT. This means that a returning Data packet "carrying" any of the chunks of the above item, *e.g.,* `Emergency/Police/Flooding/EvacPlan/CID-01` will trigger an entry in the SIT of the corresponding router of the form `Emergency/Police/Flooding/EvacPlan/`, coupled with the interfaces pointing towards the users that previously requested the aforementioned item[1] .

SIT entries store information concerning emergency related content only. This implies that each router should differentiate between emergency-related and normal traffic content. Without focusing on this aspect of the mechanism we consider that each router use a mechanism similar to [26] to register the prefixes of emergency-related content. Each time that the network is fragmented and items registered as emergency-related the routers will trigger the exploitation of their SIT (*i.e.,* create and/or follow entries).

We assume that users cache and can reproduce the entire content item. This is a reasonable assumption in disruptive networks set after a disaster scenario, where information items are smaller compared to other types of content that is requested during the normal operation of the network (*e.g.,* video streaming)[2] . The state maintained by the SIT table is negligible in size compared to the other NDN router components (*i.e.,* FIB, CS, PIT) since it contains information concerning only emergency-related content, whereas FIB should store state information for the whole Internet catalogue and PIT is using chunk-level entries as opposed to item-level. In case of storage constraints in the router a fixed capacity can be assumed for the SIT accompanied with a placement/replacement scheme (*e.g.,* LRU or LFU).

Because connections and disconnections are expected to be frequent among users during a disaster (*e.g.,* to conserve battery), the SIT table lookups return the "freshest" outgoing face(s) to avoid the usage of obsolete entries. This is achieved by maintaining the Face List component (see Fig. 1) of the SIT table as an LRU cache and by returning the head (*i.e.,* most recently added or used face) and the subsequent entries of the cache as the result of a lookup. In order to further avoid returning obsolete but most recently looked up entries, we additionally use an *invalidation mechanism*. According to this mechanism an outgoing face returned from a SIT lookup is removed from the Face List, if sending an Interest to the face does not lead to the response of a matching Data packet. The failure to retrieve a matching Data packet is detected by either PIT expiry or the arrival of negative acknowledgement (NACK).

B. Packet format and Processing

We introduce an *Interest Destination flag (IDF)* bit to the Interest packet in order to distinguish whether the packet is heading towards the content origin (IDF is set to zero), following a FIB entry, or is heading towards users with similar satisfied interests (IDF is set to one). In the second case, the Interest packet follows matching entries in the SIT of each router along the path. We also introduce a *Scoped-Flooding Counter (SFC)* to further enhance the information retrieval capabilities of the proposed resilience scheme in some special cases that we describe in the next section. We assume that the FIB entries for all items will be removed simultaneously from a router upon the "disappearance" of the content origin[3] . This means that an Interest packet will have to visit only one network router (the one that the user is attached to) until the IDF is set to one, upon fragmentation of the network. In case there is a delay for the update of the FIB entries, the proposed resilience mechanism can be enabled after a NACK is returned by the router which first identifies the content origin as unreachable or after the expiration of a timeout interval from the moment the user issued an interest.

C. Interest packet processing

1) ***IDF=0****:* Whenever a user issues an Interest packet the IDF bit is, by default, set to zero (*i.e.,* the router processes the packet in the exact same way as in NDN, and the packet heads towards the content origin). In particular, if a matching chunk is found in the CS (Step 1 in Fig. 2), the router initiates the transmission of the cached Data packet. The router sends the Data packet to the face the interest arrived on and discards the Interest packet. Also, the router creates a new SIT entry from the Interest packet and its arrival face. This entry points

[1] In the SIT entries, prefix aggregation occurs only at the chunk numbering level. Different versions of the same item with different timestamps are considered as different information items and separate SIT entries will be installed for each one of them.

[2] We leave for future investigation the scenario where users can reproduce only a subset of the chunks of an item as in P2P systems.

[3] The procedure followed by the network operator in order to detect a network fragmentation and update the FIB entries (remove entries in order to enable the proposed resilience scheme) is out of the scope of this paper. However, a scheme similar to the one presented in [27] for the PURSUIT architecture or the Named-data Link State Routing protocol (NLSR) presented in [33] for the NDN architecture could be adopted.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TNSM.2018.2811944, IEEE Transactions on Network and Service Management

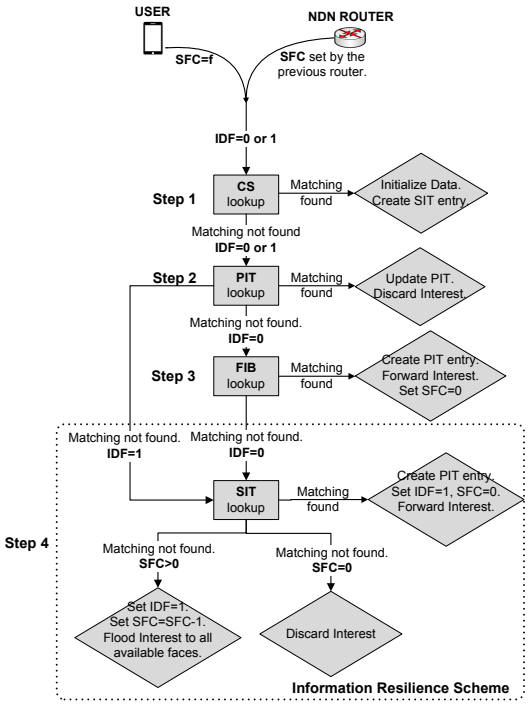

Fig. 2. Interest processing at an NDN router.

towards the user (or the next hop towards the user) that issued the interest. On the other hand, if the router does not find matching content in CS and there is an exact-match PIT entry (Step 2 in Fig. 2), the interest's arrival face is added to the PIT entry's Requesting Faces list and the Interest packet is discarded. Otherwise, if there is a matching FIB entry (Step 3 in Fig. 2), the Interest packet is sent upstream towards the content origin. In particular, the arrival face is removed from the face list of the matching FIB entry, and if the resulting list is not empty, the packet is sent out to all the remaining faces and a new PIT entry is created from the interest and its arrival face.

The above procedure is identical to the functionality of NDN [5]. However, in NDN, when an Interest packet does not find a match in any of the CS, PIT and FIB it is discarded, since this router has neither the data in its CS to respond nor the information in its FIB to forward the packet. On the other hand, in our proposed resilience scheme (Step 4; dotted box in Fig. 2), when the router does not find a match in any of the CS, PIT and FIB it checks for a matching SIT entry; this implies that the network connectivity has been interrupted either due to the mobility of the content origin or the fragmentation of the network. If such a match is found, a new PIT entry is created from the interest and its arrival face and the Interest packet is sent out to the corresponding face(s) with the IDF flag set to one.

*2) **IDF=1**:* When an Interest packet arrives on some face of a router and its IDF bit is set to one, the router checks for a matching content in its CS. If a matching content is found, the router, as above, initiates a Data Packet, creates a new SIT entry and discards the interest. If the router does not find a matching content in CS, it searches the PIT as normally done. If a matching entry is found, the interest's arrival face is added to the PIT entry's Requesting Faces list. Otherwise, it skips searching the FIB and checks for a matching SIT entry (goes

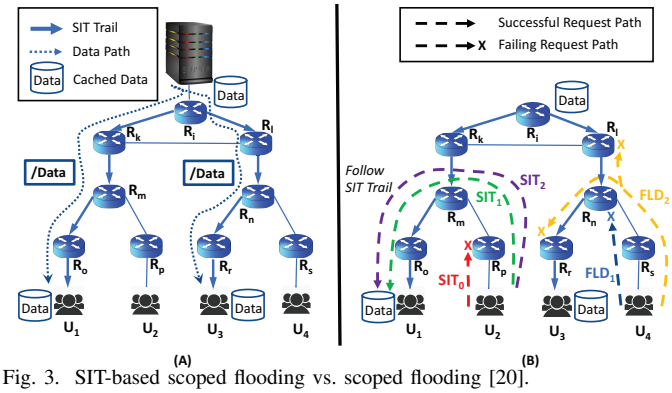

Fig. 3. SIT-based scoped flooding vs. scoped flooding [20].

from Step 2 to Step 4 in Fig. 2). If no such entry is found in the SIT, the router discards the Interest packet. This means that the user(s) who created the SIT entry is no longer reachable (or the SIT entry towards that user has expired).

When an Interest packet arrives on some face of a user, the user initiates a Data packet with the requested cached chunk and satisfies the interest. In this paper, we assume that users are willing to assist in the dissemination of the data and respond to incoming interests following a disaster. This of course assumes that users are connected to the same fragment of the network and have previously cached the requested information item.

*3) **Scoped Interest Flooding**:* In the case of "edge" (*i.e.,* adjacent to users) routers, the majority of SIT entries usually points only towards end-users connected to the *same* router (*i.e.,* common in ISP topologies with core and edge components). This means that even if there are other potential users connected to other routers of the network that can be exploited for content retrieval, there might be no SIT entries pointing towards them at the corresponding edge router. As an example, consider part A of Fig. 3, where the SIT entries (shown with arrowed lines between routers) are formed along the data retrieval path as a result of U_1 and U_3 retrieving content named `/Data` from an origin server attached to router R_i. Assuming that the content is cached at R_i and at users U_1 and U_3 and that the content origin disconnects (part B of Fig. 3), then user U_2 (U_4) has to exploit the SIT trails to retrieve the cached content at U_1 (U_3) and its request needs to travel upstream to R_m (R_n), where a SIT entry points downstream towards the user. Therefore, to better exploit end-users connected to nearby routers, we combine our SIT forwarding scheme with an Interest scoped flooding mechanism, similar to [20].

In this combined forwarding scheme, when a first-hop (*i.e.,* edge) router receives an Interest packet from a user and does not find a match in its SIT, it initiates scoped flooding instead of discarding the interest. The scoped flooding mechanism introduced here includes a Scoped-Flooding Counter (SFC) parameter set at a given predetermined value (the router also sets the IDF to one). The scope of flooding presents a trade-off with respect to the incurred signalling overhead; its effectiveness is also related to the availability of users with cached matching content in the fragmented network, *i.e.,* the more the users, the smaller the required flooding scope to discover SIT entries pointing towards them. As we show in the Evaluation section, in most cases, a small scope value (*e.g.,* equal to two) is enough to discover the corresponding SIT entries, a finding in agreement to [34]. Finally, when an Interest with SFC value

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TNSM.2018.2811944, IEEE Transactions on Network and Service Management

greater than one (in a flooding mode) reaches a router with matching SIT entries, it terminates flooding by setting SFC to zero and follows the default forwarding policy (*i.e.,* follow matching SIT entries).

In part B of Fig. 3, we depict the processing of the scoped flooding (shown as FLD_{scope}) and the scoped flooding enhanced with our SIT forwarding scheme (shown with SIT_{scope}), where the network of part A is now disconnected from the origin server. As discussed above, the interest from user U_2 (for `/Data`) is unable to find SIT entries in the nearby router R_p and has to reach router R_m in order to find a corresponding SIT entry and follow the path towards user U_1 to retrieve the requested content. Note that when the interest reaches router R_m with matching SIT entries, it terminates its flooding process (*i.e.,* not forwarded towards router R_k) and follows only SIT entries. The scoped flooding with scope values one and two (*i.e.,* SIT_1 and SIT_2) manages to reach R_m by simply flooding one hop upstream (counting from the adjacent router R_p of U_2), while the SIT forwarding scheme without scoped flooding (*i.e.,* SIT_0) terminates at R_p failing to retrieve the content. On the other hand, the scoped flooding [20] scheme, unable to take advantage of SIT trails, does not manage to retrieve cached content since its scope is not enough to reach user U_3. Even worse, the scheme with scope equal to two (*i.e.,* FLD_2) generates a redundant interest towards R_l. This simple example shows the effect of the limited scoped flooding scheme in our SIT-based approach, as well as its superiority against the scoped flooding scheme in [20]. This will be further quantified in the Evaluation section.

Alternative interest forwarding mechanisms can also be considered, where for instance Interest packets are heading both towards other users and the content origin, similar to [21] and [35], in order to satisfy them faster. Furthermore, in a non-disaster scenario, where end-users are more likely to stay connected for longer periods, a router can also add FIB entries (instead or in addition to SIT entries) whenever end-users with satisfied interests are attached to it. In this case, the edge-router would play the role of a replication point (alternative origin).

D. Data packet processing

The Data packet processing procedure is identical to NDN [5]. That is, a Data packet simply follows the chain of PIT entries back to the requesting user(s). A longest-match lookup of a Data packet's Content Name takes place upon the arrival of the packet at each router. A CS match means that the Data packet is a duplicate so it is discarded. A PIT match (there may be more than one) means that the Data packet was solicited by interest(s) forwarded by this router. A list is created, that is the union of the Requesting Faces list of each PIT match minus the arrival face of the Data packet. The Data packet is sent out on each face on this list, the PIT entries are removed, no further lookups with the rest of the router components are performed and for each face a new SIT entry is created. The new SIT entries are exactly the same as the PIT entries matching the Data packet (*i.e.,* without the chunk Id part as described in Section III-A). Obviously, the new SIT entries might be identical to existing entries. In that case, a SIT entry points towards more than one users (faces to reach those users), just like the PIT and FIB entries in NDN. Also, the Data packet is (optionally - see Section IV-B) cached in the Content Store of the router.

IV. Policies and Information Resilience Strategies

In this section, we present the family of policies the combination of which result the different information resilience strategies that we will evaluate later on.

A. Interest forwarding policies

The *Interest forwarding policy* dictates how the Interest packet is forwarded in the network when the content origin is not reachable. An Interest packet that has its Destination flag (IDF) bit set to one is propagated following the entries found in the SIT of each router, until a matching Data packet is found. Furthermore, we have integrated a scoped-flooding interest forwarding mechanism to reach routers with matching SIT entries (if any in the vicinity) in the special case described in Section III-C3. The scope value (*i.e., SFC* parameter) of this mechanism allows to search deeper into the network, albeit by increasing the control overhead. Of course, it is possible to flood the network with Interest packets (SFC is set to ∞ or to a value larger than the network diameter, and the flooding is not terminated at a router with matching SIT entries) in order to make sure that a Data packet is retrieved at the cost of even higher overhead.

In addition, as mentioned in Section III-A, a SIT entry allows for a list of outgoing faces, where the interest can be forwarded. Particularly, an interest can be forwarded to one of the outgoing faces (the "freshest" one using an LRU replacement policy in the Face List of the SIT table), or to any number, *i.e.,* the top k freshest faces in the list. Here we assume that an interest is either forwarded to only one (*i.e.,* freshest) of the outgoing faces (*i.e.,* noted as *One* next to the used forwarding policy), or is forwarded (multicasted) to all the available faces (*i.e.,* noted as *All* next to the used forwarding policy). Particularly, we will investigate the following forwarding policies:

- Interest forwarding based on SIT entries with ($SFC > 0$) or without ($SFC = 0$) the scoped flooding mechanism–*SIT-based forwarding policy, SIT_{SFC}-One and SIT_{SFC}-All.*
- Interest forwarding based on a scoped flooding mechanism–*Scoped-flooding forwarding policy, FLD_{SFC}.*
- Interest flooded to the network–*Flooding forwarding policy, FLD_{∞}.*

Note that the *SFC* variable determines the initial scope value of the Interest packet. An *SFC* value equal to zero in the SIT-based mechanisms means that the Interest packet follows only SIT entries, whereas the FLD_{SFC} mechanisms are similar to the flooding mechanism with the exception that the flooding is constrained by a hop scope/radius [20]. For completeness we also present results in the Evaluation section for the native NDN forwarding policy, where an Interest packet follows the FIB entries (despite that the content origin is not accessible) in an attempt to retrieve content from the on-path caches. For this policy we assume that FIB entries are not erased when the content origin/data mule disconnects from the network.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TNSM.2018.2811944, IEEE Transactions on Network and Service Management

TABLE I
INFORMATION RETRIEVAL POLICIES

Policies		
Forwarding	Caching	Placement/Replacement
1. SIT_{SFC}-One 2. SIT_{SFC}-All 3. FLD_{SFC} 4. FLD_{∞} 5. NDN	1. LCE 2. PRB_p	1. LRU

B. Caching policies

A *caching policy* dictates where a Data packet heading towards a user will be cached in the caches/routers along the path. In NDN, every router along the delivery path cache the passing-by Data packet. Due to the inefficiency of this ubiquitous caching mechanism we also assume an opportunistic caching policy, where each router caches a passing by item with some probability p, regardless of whether the item is cached elsewhere along the path or not. We will therefore investigate the following caching policies:

- Cache in all routers along the path/route – *Leave copy everywhere caching policy, LCE.*
- Cache Probabilistically at each router along the path/route – *Probabilistic caching policy, PRB_p*

C. Placement/Replacement policies

The *placement/replacement policy* decides a position in the Content Store where a Data packet will be inserted and which packet will be discarded in case of an overflow. Due to space limitations, we will only examine the *Least Recently Used, LRU* placement/replacement policy. There exist more sophisticated placement/replacement policies in the literature (*e.g.,* [36][37]), but their additive impact to the overall performance is negligible since in most cases they require additional functionality, which is not supported by the NDN router.

D. Information Resilience Strategies

Table I depicts the whole spectrum of the policies considered in this paper. The combinations of those policies result in different information resilience strategies for the retrieval of cached content when the network is fragmented and the content origin is not reachable. From Table I, there exist ten different basic combinations of resilience strategies, which with different values for *SFC* regarding the scoped flooding, and for p regarding the caching probability at each router, could lead to a large set of available resilience strategies. In the Evaluation section we evaluate and compare a subset of this set.

V. PROBLEM FORMULATION AND PERFORMANCE BOUNDS

In this section we provide an analytical expression with the use of continuous time, discrete state, Markov processes for the computation of the probability that an item will disappear from the network (be absorbed) and the corresponding time to absorption, when the cache capacity of each router in the fragmented network is equal to zero. The computed absorption time serves as the theoretical lower bound for the resilience strategies described above, and depicts the capability of the network to sustain and deliver content when the network is fragmented and only users can opportunistically respond to the demand for content. The lower bound on the absorption time can be extremely useful for the first responders to determine how often and for how long the information items need to be disseminated in order to ensure their survival, assuming that the first responders know roughly the mobility patterns of the users and the state of the fragmented network topology.

A. System model

We consider a network of arbitrary topology, where $\mathcal{V}$ denotes the set of cache-enabled routers/nodes in the network[4] . We denote with $\mathcal{M}$ a set of M equally sized items. Each one of these items is served by a data mule that plays the role of the content server/origin and we assume that all items are served by the same data mule, which is arbitrarily connected to a random router of the network. Without loss of generality we normalize the size of each item to one unit with respect to the node's storage capacity C_v, and we assume that all nodes have the same caching capacity ($C_v = C$, $\forall v \in \mathcal{V}$). Hence, each node can hold up to C different unit-sized items[5] .

We also assume that new users randomly connect to a node of the network with rate ζ, always request an information item, remain connected for a random time period and disconnect. Particularly, we assume that each user connected to the network disconnects from it with rate ϕ. This implies that on average a user remains connected to the network for $1/\phi$ time units (*i.e.,* here seconds). The requested item is determined by its *popularity*. Here we approximate the popularity of the items by a Zipf law of exponent z. Literature provides ample evidence that the file popularity in the Internet follows such a distribution [38]. We denote by ϑ_m, $m \in \mathcal{M}$ the popularity of item m in the Zipf distribution. In that way the aggregate incoming request rate r_m (in requests per second) for an information item $m \in \mathcal{M}$ is given by:

$$r_m = \zeta \cdot \vartheta_m = \zeta \cdot \frac{1/k^z}{\sum_{i=1}^{M} 1/i^z}, \tag{1}$$

assuming that the particular item is ranked k-th out of the M items within the Zipf distribution.

B. Absorption time and absorption probability

The probability of retrieving a requested item $m \in \mathcal{M}$ at time $t > 0$, assuming that at time $t = 0$ the network fragments and the content origin for that particular item is not reachable, depends only on the probability that another user has already retrieved that item in the past and is still connected to the network (*i.e.,* assuming zero router cache capacity). Note that here we assume (*i.e.,* Section III-A) that a user downloads, caches and reproduces the entirety of an information item and not fractions of it.

We define as $\{X_m(t),\ 0 \leq t < \infty\}$ the Markov process with stationary transition probabilities (where the possible values of $X_m(t)$ are non-negative integers), that depicts the number of users (*population*) which have already retrieved item m and are connected to the network at time t *i.e.,* the actual state

[4] We are using the calligraphic letters to denote sets and the corresponding capitals for cardinality (*e.g.,* $|\mathcal{V}| = V$).

[5] For the absorption time and probability analysis in Section V-B we assume $C = 0$.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TNSM.2018.2811944, IEEE Transactions on Network and Service Management

of the Markov process corresponds to that number of users. Clearly, if at any time instance $t' \geq 0$, $X_m(t') = 0$, the requested item can no longer be retrieved, since *(i)* it is not cached in the network, *(ii)* the content origin is not reachable and *(iii)* there are no connected users who have previously retrieved the item and can assist in content retrieval.

According to the stochastic modelling theory $X_m(t)$ is a *birth and death* process with one absorbing state. We define as the zero state, the state at which $X_m(t) = 0$. This is an absorbing state (no user with a cached copy of item m is attached at a router of the network), since after that state the requested item cannot be retrieved. Of course, new users can arrive at a network node, but they cannot retrieve the requested item, until a data mule reconnects to the network, or the network re-establishes connectivity with the server/Internet.

We define as $\lambda_m(n)$ the birth rate of the process when the process is at state n (n connected users in the network who have the item m) and as $\mu_m(n)$ the death rate of the same process. Clearly $\lambda_m(0) = 0$. In our case we have for $\lambda_m(n)$:

$$\lambda_m(n) = \begin{cases} 0 & \text{if } n = 0, \\ r_m & \text{if } n > 0. \end{cases} \tag{2}$$

Note that the birth rate of the process is independent of its actual state when $n > 0$ and it depends only on the popularity of the corresponding item.

For the death rate of the process we have:

$$\mu_m(n) = n \cdot \phi. \tag{3}$$

From the stochastic modelling theory we derive the following theorem:

THEOREM 1. *Consider the birth and death process that depicts the number of mobile users (population) which have already retrieved item m and are connected to the network with birth and death parameters $\lambda_m(n)$ and $\mu_m(n)$. The probability of absorption into state 0 from the initial state $s > 0$ is:*

$$u_m(s) = \begin{cases} 1 & \text{if } \sum_{n=1}^{\infty} \rho_m(n) = \infty, \\ \dfrac{\sum_{n=s}^{\infty} \rho_m(n)}{1 + \sum_{n=1}^{\infty} \rho_m(n)} & \text{if } \sum_{n=1}^{\infty} \rho_m(n) < \infty. \end{cases} \tag{4}$$

where

$$\rho_m(n) = \begin{cases} 1 & \text{if } n = 0, \\ \dfrac{\mu_m(1) \cdots \mu_m(n)}{\lambda_m(1) \cdots \lambda_m(n)} = \dfrac{\phi \cdot 2\phi \cdots i\phi}{\lambda_m \lambda \cdots \lambda_m} = \left(\dfrac{\phi}{r_m}\right)^n \cdot n! & \text{if } n > 0. \end{cases} \tag{5}$$

The corresponding mean time to absorption is:

$$T_m(s) = \begin{cases} \infty & \text{if } \sum_{n=1}^{\infty} \dfrac{1}{\lambda_m(n) \cdot \rho_m(n)} = \infty, \\ \sum_{n=1}^{\infty} \dfrac{1}{\lambda_m(n) \cdot \rho_m(n)} + & \\ + \sum_{k=1}^{s-1} \rho_m(k) \sum_{j=k+1}^{\infty} \dfrac{1}{\lambda_m(j) \cdot \rho_m(j)} & \text{if } \sum_{n=1}^{\infty} \dfrac{1}{\lambda_m(n) \cdot \rho_m(n)} < \infty, \end{cases} \tag{6}$$

Proof. Due to limited space the detailed derivation of Eq.(4) and Eq.(6) is omitted, but the proof which is similar in rationale to [39] can be found in https://github.com/oascigil/sit_icarus/blob/master/TNSM_theory_proof.pdf. ■

The time and the probability of absorption depends on the initial state, that is, the number/population of users that both possess item m and are connected to the network when the network gets fragmented. Obviously, when new users arrive faster than those disconnecting, an item never gets absorbed and the proposed information resilience scheme allows the retrieval of content infinitely. In the Evaluation section we analyse the performance of various resilience strategies when almost all of the items are to be finally absorbed and examine how those strategies and the corresponding policies further enhance information resilience.

VI. Performance Evaluation

In this section, we evaluate the performance of various resilience strategies based on a wide range of parameters. The objective is to evaluate their performance in terms of content retrieval efficiency and incurred cost/overhead. Overhead in our case refers to the duplicate copies of data that travel through the network, as well as the number of Interest packets generated, and processed by intermediate routers, for each unique user request. Extra responded data and interest overhead consumes precious bandwidth resources, but more importantly resources (*e.g.,* energy) of network components and end-user devices.

A. Evaluation Setup and Metrics

For the evaluation of the proposed resilience scheme, we used the Icarus simulator [6]—a Python-based discrete-event simulator for ICNs. Icarus allows users to evaluate caching strategies for any ICN implementation and also provides modelling tools useful for caching research. Given that by design Icarus is not bound to any specific ICN architecture, we made extensions to the simulator to support the NDN architecture with the new functionalities described in Section III and Section IV. The simulator code with our extensions is publicly available [40].

We use the Tiscali (AS 3257) network topology as provided through the Rocketfuel dataset [41]. This topology has $V = 161$ routers and 328 bidirectional links. We consider a scenario where the information item population is $M = |\mathcal{M}| = 10^4$ items. Although 10^4 items may not seem representative of the current Internet content space, here we focus on a disruptive/disaster case, where emergency-related information is distributed by first responders and users request for updates. That is, first responders (*e.g.,* fire brigade, police, *etc.*) are publishing information in specific places, utilising mobile data mules (*e.g.,* ambulances, drones, *etc.*). As the authorities move in the disaster area, the origin server (here represented by a mobile data mule) becomes inaccessible. In turn, users asynchronously request for updates on the state of the emergency. In this case, information has to be retrieved from either in-network caches, or from other users who have already downloaded the updated information. Given that authorities publish new content/information every some tens of minutes [26], we experiment with an average size content population and evaluate whether users can get access to important data.

We assume a warm-up period of one hour during which the content origin (*i.e.,* data mule) of every item is reachable, and we call this the *"initialisation period"*. During the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TNSM.2018.2811944, IEEE Transactions on Network and Service Management

TABLE II
SUMMARY OF THE EVALUATION PARAMETER SETTINGS.

Parameter	Value
Number of nodes V	161
Number of items M	10^4
Aggregate routers' cache capacity C	$0.90 \cdot M$
Users connection rate (overall) per second ζ	100
Connected user's disconnection rate per second ϕ	0.005
Popularity exponent z	0.7

initialisation period, the network processes Interest packets according to NDN (*i.e.,* requests follow FIB entries towards the content origin and routers follow LCE caching policy), but Data packets are processed as explained in Section III-D by adding new entries to the SIT table. We assume $\zeta = 100$ and $\phi = 0.005$ for the user connection and disconnection rates, respectively. A disconnection rate of 0.005 corresponds to an average end-user connection duration of 200 seconds. After the end of the initialisation period, we assume that the data mule disconnects from the corresponding network fragment and monitor the performance of the resilience strategies for a period of one hour (we call this the *"observation period"*). This is assumed to be the time interval until the data mules revisit the fragmented network and publish updated data. Extensive experiments show that the duration of the initialisation period does not affect results. We therefore, set this parameter equal to 1 hour. Finally, we assume that during the observation period the content popularity is stable, and we also leave for future work the evaluation of scenarios where popularity alterations exist after the fragmentation of the network.

Our evaluation is based on the following metrics:

- *Satisfaction* (in % of issued interests): The percentage of the interests that have been satisfied (*i.e.,* found the requested item) during the observation period.
- *Traffic Cost* (in *hops*): The total number of hops that the responded Data packets per satisfied interest travel in the network until they are either discarded by a router or consumed by a user.
- *Interest Overhead* (in *hops*): The total number of hops that a user's request travels in the network until it is either discarded or satisfied. This number is also equal to the number of Interest packets generated and processed per each unique user request, satisfied or not.
- *Absorbed Items* (in % of information items): The percentage of the $\tilde{M} = |\tilde{\mathcal{M}}|$ items that have been absorbed (*i.e.,* disappeared) during the observation period.
- *Absorption Time* (in *sec*): The time between network fragmentation and item absorption averaged over all items $\tilde{M}$.
- *Average Minimum Data Hops* (in *hops*): The minimum number of hops between the closest responding router or user and the user that issued the Interest packet. This metric is indicative of the transfer delay as a function of hops in the network.
- *Percentage from Users* (in % of satisfied interests): The percentage of interests satisfied by the users during the observation period. If a request returns duplicate data, this metric takes into account the origin of only the first Data packet arriving at the user.

Note that $\tilde{\mathcal{M}}$ is the set of the items that are cached in the network or at the connected users when the fragmentation occurs. As shown later, this set might be smaller than the initial set of items provided by the server/data mules. Table II gives the default values for the various system parameters.

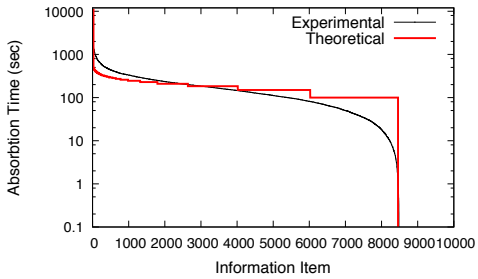

Fig. 4. Experimental and theoretical absorption time for the case where each router has zero cache capacity.

B. Model validation

In Fig. 4, we depict the actual absorption time for each information item using Eq.(6) (red line) and using the Icarus simulator (black line). We observe that the theoretical results are inline with the output of the simulator. In particular, we see that the vast majority of the items $\approx 85\%$ are absorbed in $200-500$ seconds after the fragmentation of the network when routers have zero caching capacity and for the given users' connection and disconnection rates. We also notice that there is a very small portion of the item population, approximately $\approx 0.25\%$, that never gets absorbed (*i.e.,* can be retrieved throughout the observation period). Finally, a significant amount of items, roughly $\approx 15\%$ (*i.e.,* $\tilde{M} = 0.85 \cdot M$), whose absorption time is equal to zero, did not manage to make it through the initialisation period. This means that they were never requested during the initialisation period or the users who have requested those items disconnected from the network before the beginning of the observation period.

C. Impact of the caching probability

Since the performance of the LCE caching policy is questionable, various alternative probabilistic caching schemes have been proposed. Here, we adopt a simple yet effective caching scheme according to which a router that lies on the delivery path of an item decides, based on some probability p, whether or not to cache passing-by content. Particularly, in this section we compare various combinations of the proposed resilience strategies against various values of caching probability p. The performance of the various strategies is depicted in Fig. 5, where p varies between 0.1 and 1. We observe that the probability of caching has negligible impact on the satisfaction rates of all the strategies. This is because of the correlation between an information item's popularity—i.e., its likelihood of being cached within the network—and the number of connected users storing the item. Increasing the probability of caching merely increases the replication of the popular items in the network of caches, which were already retrievable (possibly from a network cache) and already stored at the nearby users. As a result, we observe that increasing the probability of caching has negligible impact on the overall satisfaction rate of the strategies. In the rest of the experiments, we use the median value of $p = 0.5$.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TNSM.2018.2811944, IEEE Transactions on Network and Service Management

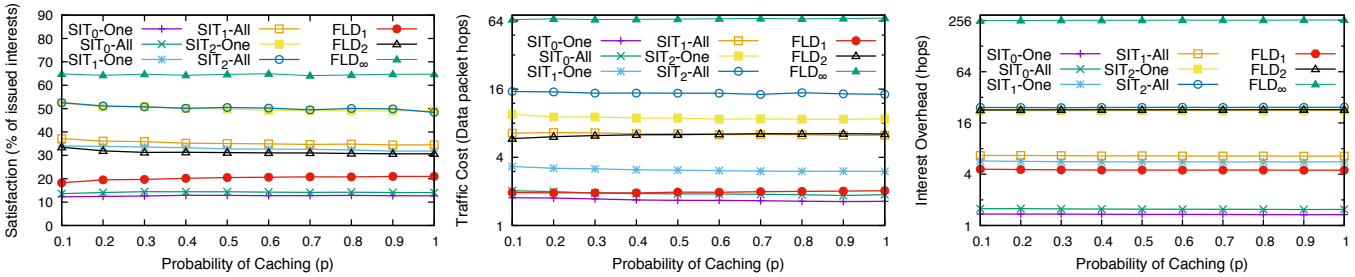

Fig. 5. The impact of the caching probability in the satisfaction, traffic cost and the interest overhead of various resilience strategies.

From the comparison of the different resilience strategies, we observe that the basic SIT_0 (*i.e.,* SFC value is set to zero) forwarding policy performs the worst with respect to the satisfaction rate. This is due to the edge router effect (described in Section III-C3), where routers with low connectivity typically have SIT entries only pointing towards end-users connected to the same router. Because the majority ($\approx 90\%$) of the nodes are edge routers in a typical ISP topology such as the Tiscali network, the basic SIT_0 strategy performs rather poorly. This drove us to introduce the hybrid mechanism combining scoped flooding and SIT-based forwarding. We observe in Fig. 5, that both SIT_1-All and SIT_1-One forwarding policies result in roughly three-fold increase in the satisfaction rate compared to SIT_0-All and SIT_0-One policies, respectively. Additionally, the SIT_2-One and SIT_2-All policies further improve the satisfaction rate and results in nearly five-fold increase in the satisfaction rate compared to the SIT_0 policies. While the scope parameter (SFC) has considerable impact on the satisfaction rate, the difference between One and All policies with the same scope parameter is negligible.

Overall from Fig. 5, we observe that the SIT-based strategies significantly improve on the scoped-flooding strategies (*i.e.,* FLD_{SFC}) for the scope values of one and two. For instance, SIT_1 can satisfy 15% more requests compared to FLD_1, whereas SIT_2 results in 25% more satisfied requests compared to FLD_2. This is an overall increase of 75% and 70% in the performance (*i.e.,* satisfaction rate) of the system. Note that SIT_1 policy with only one hop flooding scope achieves slightly better satisfaction compared to FLD_2, which allows two hops of flooding scope. The satisfaction rate performance of the proposed SIT-based policy with limited flooding over the native scoped flooding policy for various scopes is better illustrated in Fig. 6. We find that the exploitation of the SIT tables leads to higher satisfaction rates even when scoped flooding is enabled for smaller radius. Of course, when the scope is large enough to reach the network diameter the extra benefit is diminished since both policies act as the unscoped flooding scheme (*i.e., FLD_∞*).

At the same time, we observe that the traffic cost of SIT_{SFC}-One strategies is slightly higher than its counterpart FLD_{SFC}, whereas those strategies have the same Interest overhead for the same used scope value. On the other hand, the traffic cost of the "All" strategies are much higher than the "One" strategies, whereas "All" strategies only provide marginal increase in the satisfaction rate compared to "One" strategies with equal scope of flooding. In the remainder of this section, we do not consider the "All" strategies and only depict the resilience strategies presented in Table III. Apart from the strategies above, we also examine the unscoped flooding mechanism (FLD_∞) and the NDN forwarding policy presented in Section IV-A. We investigate the performance of those schemes for benchmarking purposes (lower/upper-bounds for the used metrics).

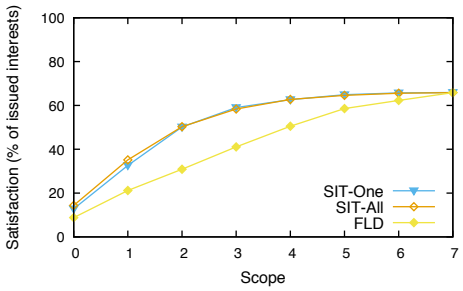

Fig. 6. The performance of SIT-based and Scoped flooding forwarding policies for different scopes of flooding.

TABLE III
EXAMINED INFORMATION RESILIENCE STRATEGIES.

Strategy	Notes
SIT_1-One - $PRB_{0.5}$ - LRU	SFC set to one
SIT_2-One - $PRB_{0.5}$ - LRU	SFC set to two
FLD_2 - $PRB_{0.5}$ - LRU	Scoped Flooding with SFC set to two
FLD_∞ - $PRB_{0.5}$ - LRU	Unscoped flooding
NDN - LCE - LRU	Native NDN mechanism

D. Impact of the router's cache size

In Fig. 7, we depict the impact of the cache capacity on performance, expressed as the fraction of the item population that can be stored in the entire network's cache storage space.

As can be seen in the top left plot of Fig. 7, an increase in the cache capacity of the network improves the end-users' satisfaction rate for all the strategies except for the unscoped flooding strategy (FLD_∞), whose satisfaction rate remains almost stable around 63%. Consistent with the previous results, the satisfaction rate of the SIT-based strategies are higher than the scoped flooding strategy (FLD_2) for all the cache capacity values. Even the basic NDN strategy is able to satisfy an increasing percentage of requests through the caches along the default path to the disconnected data mule. This results in a small increase in the average data hops metric of this scheme, because a larger percentage of requests are able to find content further away from the user. However, a ten times increase in the cache capacity of a router results in an increase of the NDN satisfaction by a factor of 11 (in top left plot of Fig. 7), whereas the average data hops are only increased by 8% (in bottom center plot of Fig. 7).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TNSM.2018.2811944, IEEE Transactions on Network and Service Management

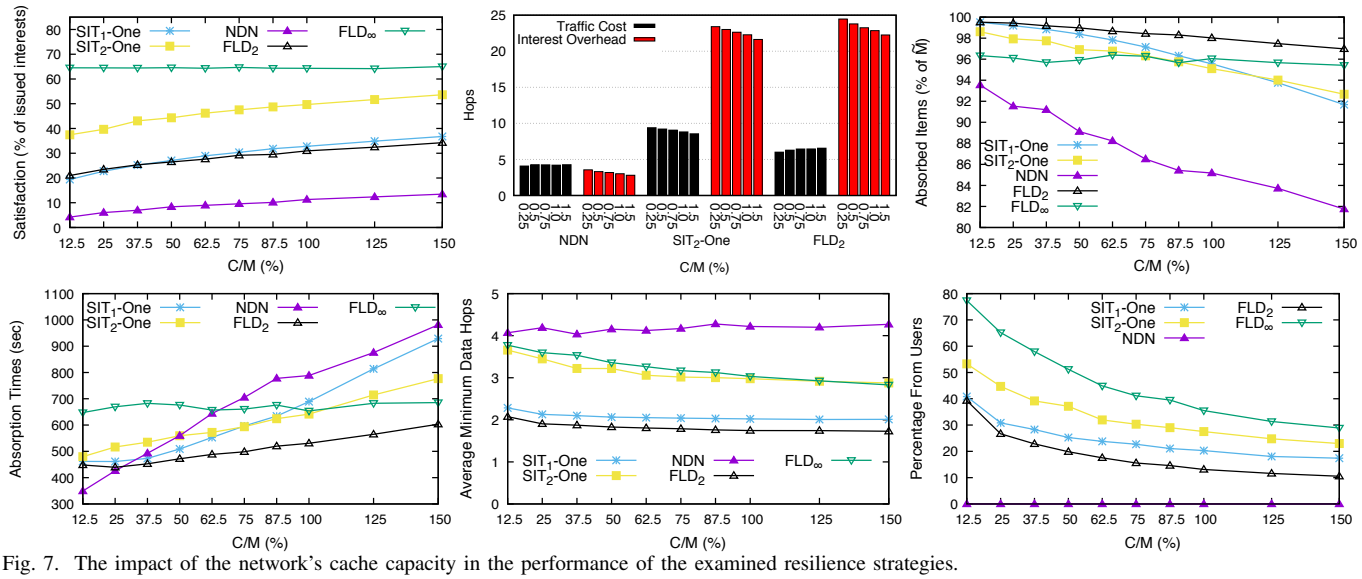

Fig. 7. The impact of the network's cache capacity in the performance of the examined resilience strategies.

In order to understand the satisfaction rate results, one should consider several other metrics together, particularly the *Absorbed Items* (top right plot) metric. Consistent with the satisfaction rate, the percentage of absorbed items remains roughly constant with increasing cache capacity for the unscoped flooding (FLD_∞). This is because the unscoped flooding fetches all the available (*i.e.,* duplicate) copies of matching data across the network for each request and thus, severely increases the replacement rate in the router caches. As a result, the CS of each router only retains a very small portion of the most popular items, the majority of which are also stored and are available at the connected end-users too. Consistent with the absorbed items plot, we observe that the *Absorption Time* (bottom left plot) of the unscoped flooding strategy stays roughly constant. The constant absorption rates results with a constant satisfaction rate for the unscoped flooding.

Again from the Absorbed Items (top right) and Absorption Time (bottom left) plots in Fig. 7, we observe that the SIT-based strategies are able to retain a higher percentage of content for longer time periods than the unscoped flooding as the overall network cache capacity increases beyond 100% of the content catalogue. The increasing trend in the absorption time leads to an increasing trend in the satisfaction rates of the SIT-based strategies.

The percentage of content retrieved from end-users tends to decrease for all strategies as the cache storage of the network increases as shown in the bottom right plot in Fig. 7. This is because more items become available in the nearby routers' caches with increasing storage capacity. The effectiveness of SIT_2-One in retrieving content from distant end-users can be also observed in this plot, where it is shown to retrieve between $25\% - 55\%$ of the responses from end-users. Its scoped flooding counter-part FLD_2, on the other hand, retrieves $\approx 35\%$ less data from end-users than SIT_2-One for all cache sizes considered. These results indicate that not only the introduction of the SIT table, but also the exploitation of end-users' storage is important to increase the satisfaction rate. Of course, as we relax the storage capacity constraint, the majority of the interests are satisfied by network caches.

Moreover, we observe from the average minimum data hops plot (bottom center plot of Fig. 7) that increasing cache capacity of the network reduces the minimum hop distance traveled by Data packets, especially for strategies that have wider reach (not for NDN as mentioned above). As shown in the plot, SIT_2-One strategy can effectively discover information items beyond three hops away from users by taking advantage of the trails leading to end-users. Also, few additional (intra-domain) hops usually translates to negligible amount of latency in practice so we do not consider this extra path stretch as a serious drawback.

The NDN strategy achieves the worst satisfaction rate despite retaining the highest percentage of items in the network (see top right plot of Fig. 7). This strategy is unable to exploit end-user storage and can only retrieve content from router caches. That said, there are very few cache hits and very limited cache replacement. Caches, therefore, remain almost idle.

Although unscoped flooding may seem appropriate for smaller network cache capacities based on these results, we stress here that it leads to heavy duplication of Data packets originating mostly from users. This translates to *heavy consumption of end-users' resources* (*e.g.,* battery—a scarce resource under a disaster scenario). Therefore, we consider unscoped flooding an extremely poor cache management practice. For larger cache capacities, the SIT-based strategy SIT_2-One achieves comparably well with much less overhead and traffic cost.

As a final note, we observe in the top right plot of Fig. 7 that all the strategies retain a very small percentage of the items at the end of the observation period, during which data mules are not available in the network. For instance, the SIT_1-One retains only $\approx 8\%$ of the information items at the end of the one hour long observation period, for the highest cache capacity. This indicates that the disconnection rate of 0.005 considered in these results requires shorter durations between subsequent visits of data mules (*i.e.,* publishing of data) to the network than one hour. Next, we examine the impact of disconnection rate on the performance metrics.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TNSM.2018.2811944, IEEE Transactions on Network and Service Management

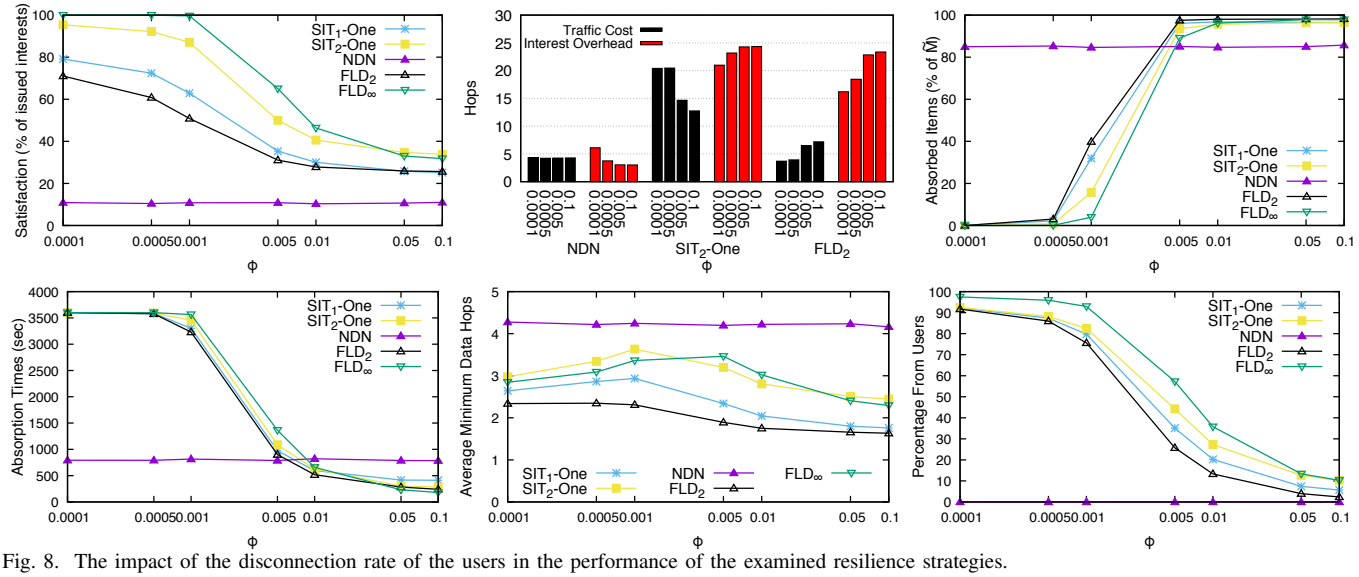

Fig. 8. The impact of the disconnection rate of the users in the performance of the examined resilience strategies.

E. Impact of the users' disconnection rate

Fig. 8 depicts the impact of users' disconnection rate on the performance of the examined resilience strategies. Starting from the *Percentage From Users* metric (bottom right plot), we observe for all strategies that most of the requests are satisfied from users for low disconnection rates. In particular, when users remain connected for at least 100 seconds on average (*i.e.,* $\phi \leq 0.01$), user-based content retrieval significantly improves the system performance as can be seen in the top left plot of Fig. 8.

Generally, we observe that when the mobility of users is low (*i.e.,* disconnection rate below 0.001), the satisfaction is more than 50% for all the strategies (except NDN where user-assisted content retrieval is not supported). This means that the data mules can spend less and less time connected to the network. However, for larger disconnection rates the duration of data mule connection (*i.e.,* warmup period) has no impact on the performance of the system, since users tend to stay connected for a very small amount of time, and therefore the content is eventually absorbed very quickly. Instead, the mule should revisit the fragment of the network more often in the case of high mobility.

From Fig. 8 (bottom right plot) we also see that even the unscoped flooding (FLD_∞) strategy obtains more than 40% of the content from users for $\phi < 0.01$. As ϕ increases beyond 0.01, the number of users available to assist in the content retrieval process drops significantly, and consequently the satisfaction rate drops for all strategies (see top left plot in Fig. 8). From that point on, the interests are mostly satisfied from network caches. This trend is also visible in the *Average Minimum Data Hops* metric (bottom center plot in Fig. 8), where we notice a slightly increasing trend initially, followed by a decreasing trend for the unscoped flooding and SIT-based strategies. The initial increasing trend is a combined effect of the large percentage of unabsorbed items (see top right plot in Fig. 8) and the increasing difficulty of finding nearby end-users having the same item. As a result, the requests have to travel deeper in the network to retrieve content or find connected users (also noticeable from the increased trend of the Interest Overhead metric). Once ϕ exceeds 0.005, the majority of the content comes from network caches closer to users as observed in the decreasing trend of the average minimum data hops metric.

For larger disconnection rates, the time that each user stays in the network is not sufficient for any resilience strategy to exploit them in order to retrieve cached content. This observation is especially useful and could be used by network managers operating a network after a disruptive scenario to either provide incentives and compensate users to remain connected to the network for longer periods, or schedule more frequent "visits" of data mules to the network (*i.e.,* in timescales smaller than the one hour period assumed here).

F. Impact of the popularity distribution

In the above scenarios, we used a default Zipf exponent value of $z = 0.7$ when determining the items' popularity. Measurement-based studies, such as [42], suggest that the Zipf exponent z for web traffic lies in the range of $0.64 - 0.84$, while other types of traffic (*e.g.,* P2P or video) may follow different popularity patterns [38].

In Fig. 9, we examine a wider range of values for the Zipf distribution. In the top left plot, we observe a rapid increase in the satisfaction rate with increase in z for all the strategies. For $z \approx 0$, each content is almost equally likely to be requested, *i.e.,* the locality of reference in the set of requested items is very low. As a consequence, all strategies, with the exception of NDN, exploit end-users' storage, as can be seen from the Percentage From Users (bottom right) plot. As z increases beyond zero, requests are increasingly satisfied from nearby network caches. This is also obvious from the Interest overhead metric, where we observe that the number of interests circulated in the network is significantly smaller as the exponent of the Zipf distribution increases.

In the Absorbed Items (top right) plot of Fig. 9 we see that the percentage of absorbed items increases slightly as z increases from 0 to 1 for all the strategies. Once z increases beyond 1, the network is able to retain a larger portion of the items and consequently the average absorption time increases

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TNSM.2018.2811944, IEEE Transactions on Network and Service Management

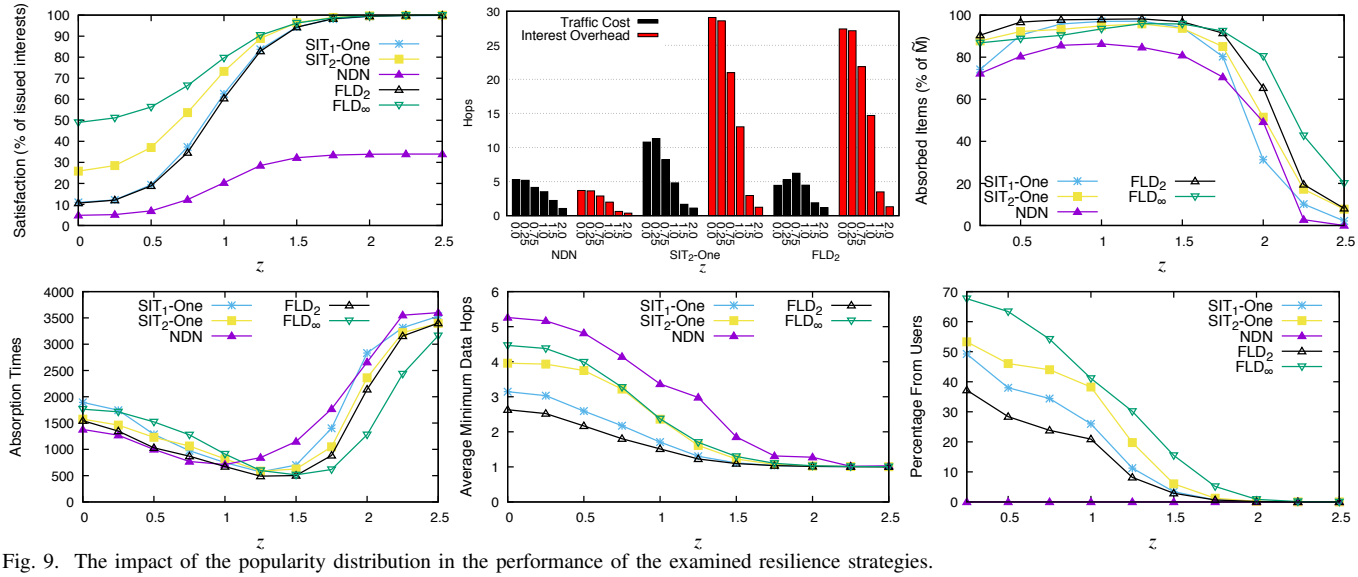

Fig. 9. The impact of the popularity distribution in the performance of the examined resilience strategies.

TABLE IV
SIZE OF $\tilde{M}$ FOR DIFFERENT z VALUES.

Zipf Parameter	0	0.25	0.5	0.75	1.0	1.25	1.5	1.75	2.0	2.25	2.50
$\tilde{M}$	10000	10000	10000	10000	9954	8403	4445	1813	833	387	230

(see bottom right plot). In order to understand this trend in the absorption rate, consider Table IV, where we show the total number of items that are found in the network at the end of the initialization phase (*i.e.,* $\tilde{M}$) for different z values. As can be seen in this table, the number of items available in the network in the end of the initialisation period decreases very rapidly, as z increases above 1.25. In general, the rate of requests for items belonging to the long tail of the Zipf distribution reduces as z increases. As z approaches 1.0, the size of $\tilde{M}$ only slightly decreases below the content population catalogue size, while the rate of requests for the tail items reduces. This leads to an increase in the percentage of absorbed items as z increases from 0 to 1.25. Because the size of $\tilde{M}$ shrinks very rapidly as z increases above 1.25, the network cache can store (and retain) an increasingly large percentage of $\tilde{M}$.

Evaluation take away points: The SIT-based approach combined with scoped flooding is very effective in fragmented networks and achieves better satisfaction rate than pure scoped flooding strategies (*i.e.,* FLD_{SFC}). Although the unscoped flooding (FLD_∞) strategy has a higher satisfaction rate than the SIT-based strategies for small network cache capacities, its traffic cost and interest overhead is significantly higher. Because traffic cost and overhead means resource consumption (*e.g.,* bandwidth, energy, *etc.*), we consider unscoped flooding unsuitable for disaster scenarios. Also, the default NDN strategy is unable to retrieve content from end-users and is also not effective in retrieving content from off-path network caches. Finally, for very large values of the popularity Zipf exponent, all strategies (with the exception of NDN) perform nearly the same since the network caches can store almost the entire content in $\tilde{M}$, whereas for very large user disconnection rates (*i.e.,* user mobility), all strategies are ineffective in retrieving content from users. Instead, the proposed SIT-based strategy (SIT_2) is able to achieve slightly higher satisfaction rate than FLD_∞, albeit with much less overhead.

VII. SUMMARY AND CONCLUSIONS

Network resilience in current fixed networks is dealt with by pre-configuring alternative paths which the control plane is aware of and activates accordingly upon failures. In the case of dynamic networks, this is of course not possible and the control plane has to dynamically find alternative paths. Given that especially in case of disasters, content (*e.g.,* information from first responders) is more important than the actual node that content comes from, makes Information-Centric Networks a natural fit for such environments. In ICN, the notion of node and routing path are not explicitly present and resilience needs to be tackled at the information level. In this paper we have designed, presented and evaluated an approach for information resilience in disruptive, fragmented network situations for networks that follow the emerging ICN principles. We have proposed a necessary enhancement to the NDN router design, as well as to its Interest management forwarding scheme. According to our technique, which is realised through the *"Satisfied Interest Table"*, an extra routing component in the routing engine, users can retrieve cached content when the network is fragmented and the content origin not reachable. Our proposed scheme uses an additional part of the data plane, *i.e.,* the SIT, as indication of directions to network regions where the content may still reside.

The approach presented here is general enough to be applied with suitable modifications and enhancements to next generation ICNs, both fixed and infrastructure-less. In ICNs, the massive scale and dynamicity of content renders the pre-configuration of alternative routes-to-content non-scalable; in fact, end-to-end scalable inter-domain routing based on content names has yet to be satisfactorily addressed. Therefore, using the data plane itself to keep track of which network regions particular content objects have been found, can provide effective "alternative paths" in case of link/node failures. This is in line with the dynamic nature of cached content locations

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TNSM.2018.2811944, IEEE Transactions on Network and Service Management

and obviates the need for alternative route pre-configuration. It is in this direction that we plan to focus our future research in this area.

ACKNOWLEDGEMENTS

This work has been supported by the EC FP7 INACHUS project (GA no. 607522), the EC H2020 UMOBILE project (GA no. 645124), the EC H2020 ICN2020 project (GA no. 723014) and the EPSRC INSP fellowship (EP/M003787/1).

REFERENCES

[1] V. Sourlas *et al.*, "Information resilience through user-assisted caching in disruptive Content-Centric Networks," in *IFIP Networking*, 2015.
[2] J. Rak *et al.*, "Information-driven network resilience: Research challenges and perspectives," *Optical Switching and Networking*, 2016.
[3] A. Kvalbein *et al.*, "Multiple Routing Configurations for Fast IP Network Recovery," *IEEE/ACM Trans. Netw.*, vol. 17, 2009.
[4] G. Tyson *et al.*, "Beyond content delivery: can ICNs help emergency scenarios?" *IEEE Network*, vol. 28, 2014.
[5] V. Jacobson *et al.*, "Networking Named Content," in *ACM CoNEXT*, 2009.
[6] L. Saino *et al.*, "Icarus: A Caching Simulator for Information Centric Networking (ICN)," in *SIMUTools*, 2014.
[7] M. Zhang *et al.*, "A survey of caching mechanisms in information-centric networking," *IEEE Communications Surveys Tutorials*, vol. 17, 2015.
[8] J. Li *et al.*, "Popularity-driven Coordinated Caching in Named Data Networking," in *ACM/IEEE ANCS*, 2012.
[9] G. Tyson *et al.*, "A Trace-Driven Analysis of Caching in Content-Centric Networks," in *ICCCN*, 2012.
[10] I. Psaras *et al.*, "In-Network Cache Management and Resource Allocation for Information-Centric Networks," *IEEE TPDS*, vol. 25, 2014.
[11] A. Ghodsi *et al.*, "Information-centric Networking: Seeing the Forest for the Trees," in *ACM HotNets*, 2011.
[12] A. Ioannou *et al.*, "Towards on-path caching alternatives in Information-Centric Networks," in *IEEE LCN*, 2014.
[13] S. Guo *et al.*, "Collaborative Forwarding and Caching in Content Centric Networks," in *IFIP Networking*, 2012.
[14] V. Sourlas *et al.*, "A novel cache aware routing scheme for Information-Centric Networks," *Computer Networks*, vol. 59, pp. 44 – 61, 2014.
[15] Y. Wang *et al.*, "Advertising cached contents in the control plane: Necessity and feasibility," in *IEEE Computer Communications (INFOCOM WKSHPS)*, 2012.
[16] S. Eum *et al.*, "CATT: Potential Based Routing with Content Caching for ICN," in *ACM ICN Workshop*, 2012.
[17] V. Sourlas *et al.*, "Distributed Cache Management in Information-Centric Networks," *IEEE TNSM*, vol. 10, 2013.
[18] G. Rossini *et al.*, "Coupling Caching and Forwarding: Benefits, Analysis, and Implementation," in *ACM ICN Conference*, 2014.
[19] V. Sourlas *et al.*, "Efficient Hash-routing and Domain Clustering Techniques for Information-Centric Networks," *Computer Networks*, vol. 103, 2016.
[20] L. Wang *et al.*, "Pro-Diluvian: Understanding Scoped-Flooding for Content Discovery in Information-Centric Networking," in *ACM ICN Conference*, 2015.
[21] H. Lee *et al.*, "User-assisted in-network caching in information-centric networking," *Computer Networks*, vol. 57, 2013.
[22] "Architecture and Applications of Green Information Centric Networking (GreenICN)." [Online]. Available: http://www.greenicn.org/
[23] J. Seedorf *et al.*, "Using ICN in disaster scenarios," *IRTF*, 2015. [Online]. Available: https://datatracker.ietf.org/doc/draft-seedorf-icn-disaster/
[24] D. Kutscher *et al.*, "ICN Research Challenges," *IRTF, 2014*, August 2014.
[25] T. Ogawara *et al.*, "Information dissemination performance of a disaster-tolerant NDN-based distributed application in disrupted cellular networks," in *IEEE P2P*, 2013.
[26] I. Psaras *et al.*, "Name-based replication priorities in disaster cases," in *IEEE Computer Communications (INFOCOM WKSHPS)*, 2014.
[27] M. Al-Naday *et al.*, "Information resilience: source recovery in an information-centric network," *IEEE Network*, vol. 28, 2014.
[28] D. Trossen *et al.*, "Designing and realizing an information-centric internet," *IEEE Communications Magazine*, vol. 50, 2012.
[29] E. Monticelli *et al.*, "An information centric approach for communications in disaster situations," in *IEEE LANMAN*, 2014.
[30] H. M. A. Islam *et al.*, "Towards Disruption Tolerant ICN," *CoRR*, vol. abs/1510.04436, 2015. [Online]. Available: http://arxiv.org/abs/1510.04436
[31] Y.-T. Yu *et al.*, "DT-ICAN: A Disruption-Tolerant Information-centric Ad-Hoc Network," in *IEEE MILCOM*, 2014.
[32] J. Scott *et al.*, "Haggle: a Networking Architecture Designed Around Mobile Users," in *WONS*, 2006.
[33] A. K. M. M. Hoque *et al.*, "NLSR: Named-data Link State Routing Protocol," in *ACM ICN Workshop*, 2013.
[34] S. Bayhan *et al.*, "Two Hops or More: On Hop-Limited Search in Opportunistic Networks," in *ACM MSWIM*, 2015.
[35] O. Ascigil *et al.*, "Opportunistic off-path content discovery in information-centric networks," in *IEEE LANMAN*, 2016.
[36] S. U. Khan *et al.*, "Comparison and Analysis of Ten Static Heuristics-based Internet Data Replication Techniques," *Parallel Distrib. Comput.*, vol. 68, 2008.
[37] M. Diallo *et al.*, "A content-based publish/subscribe framework for large-scale content delivery," *Computer Networks*, vol. 57, 2013.
[38] G. Dán *et al.*, "Power-law Revisited: Large Scale Measurement Study of P2P Content Popularity," in *IPTPS*, 2010.
[39] H. Taylor *et al.*, *An Introduction to Stochastic Modeling*. Academic Press, 1998.
[40] "The extended Icarus Simulator." [Online]. Available: https://github.com/oascigil/sit_icarus
[41] N. Spring *et al.*, "Measuring ISP Topologies with Rocketfuel," in *ACM SIGCOMM*, 2002.
[42] L. Breslau *et al.*, "Web caching and Zipf-like distributions: evidence and implications," in *IEEE INFOCOM*, 1999.

Vasilis Sourlas received his Diploma degree from the Computer Engineering and Informatics Department, University of Patras, Greece, in 2004 and the M.Sc. degree in Computer Science from the same department in 2006. In 2013 he received his PhD from the Department of Electrical and Computer Engineering, University of Thessaly (Volos), Greece. In Jan. 2015 he joined the Electronic and Electrical Engineering Department, UCL, London to pursue his two years Marie Curie IEF fellowship.

Onur Ascigil received his PhD. degree from the Computer Science Department, University of Kentucky, Lexington, USA in 2014. From 2008 to 2014 he worked as a research assistant and from Jan. 2015 to Aug. 2015 as a Post-doctorate Research Associate at the Laboratory for Advanced Networking, University of Kentucky. In September 2015 he joined the Electronic and Electrical Engineering Department, UCL, London as a Research Associate.

Ioannis Psaras is an EPSRC Fellow at the Electrical and Electronic Engineering Department of UCL. He is interested in resource management techniques for current and future networking architectures with particular focus on routing, caching and congestion control. Before joining UCL in 2010, he held positions at the University of Surrey, and Democritus University of Thrace, Greece, where he also obtained his PhD in 2008. He has held research intern positions at DoCoMo Eurolabs and Ericsson Eurolabs.

George Pavlou is Professor of Communication Networks in the Department of Electronic and Electrical Engineering, University College London, UK. He received a Diploma in Engineering from the National Technical University of Athens, Greece and M.S. and Ph.D. degrees in Computer Science from University College London, UK. His research interests focus on networking and network management. In 2011 he received the Daniel Stokesbury award for "distinguished technical contribution to the growth of the network management field".