Security Challenges in future NDN-Enabled VANETs

Salvatore Signorello and Maria Rita Palattella
SnT, University of Luxembourg
Email: firstname.lastname@uni.lu

Luigi Alfredo Grieco
DEI, Politecnico di Bari
Email:a.grieco@poliba.it

***Abstract*—Originally envisioned to tackle the massive content distribution in today's Internet, the Information-Centric Networking (ICN) has turned out to be a promising paradigm for different network scenarios, including Vehicular Ad Hoc Networks (VANETs). Data retrieval independent from specific recipients bound to fixed physical locations could be a key enabler for future vehicular networks, fixing old unsolved issues of mobility management in classical IP-based systems. As an evidence, several preliminary investigations have been performed on a widely known ICN instance, i.e., the Named-Data Networking (NDN). Nevertheless, the NDN architecture presents a new set of security vulnerabilities. Interest flooding attacks, cache poisoning attacks and privacy violation attacks by means of content names represent concrete NDN threats. While the benefits offered by NDN to vehicular networks have been partially investigated, the impact of major security threats stays unclear. Therefore, this paper opens a more comprehensive discussion of the security risks brought by the application of NDN solutions in VANETs. This is a fundamental first step toward the future design of suitable related countermeasures.**

I. Introduction

The design of network protocols for Vehicular Ad Hoc Networks (VANETs) is extremely challenging as proved by analysis conducted on real traffic traces [1]. Usually, VANETs exhibit highly partitioned networks, leading to short inter-vehicle communications dominating the exchanged traffic. Therefore, the main issues in VANETs revolve around delivery of data in presence of nodes mobility, and routing consistence in presence of constant topology changes. Classical IP-based solutions, relaying on network addresses, can be easily broken by mobile nodes and intermittent links. Thus, an interest in alternative networking paradigms has recently emerged.

The Information-Centric Networking (ICN) [2] seems to be a promising network solution for VANET infrastructure-less scenarios. It proposes a different semantics for the packets at the network layer together with a wide use of in-network caches, mainly to address massive content distribution scenarios. In particular, ICNs use content names, rather than IP addresses, to route and fetch cached copies of the content by any possible source. Its native support to multicast and mobile communication, makes it suitable for Mobile Ad hoc Networks (MANETs), including VANETs. As a consequence, seminal works have investigated the applicability of specific ICN instances, e.g., the Named Data Networking (NDN) [3], to vehicular scenarios. However, despite promising preliminary results, a seamless application of NDN to the VANET domain is far reaching and, as a consequence, ad-hoc customizations proliferate. Yet worse, there is no concern about how the intrinsic security/privacy threats of ICN/NDN-based solutions could be eventually magnified once this network paradigm is applied in VANETs. By design, the NDN architecture is immune to many of the common DDoS attacks affecting today's IP-based networks [4]. However, NDN brings a new class of vulnerabilities for which universally efficient countermeasures have not been proved to exist yet. For example, flooding of unnecessary content requests and wide dissemination of fake contents both constitute a serious menace to NDN. The former attack may exhaust both content producers' and infrastructure's resources. The latter attack may pollute in-network storages. In the end, legitimate content requests cannot be processed and valid contents can not be easily fetched. Furthermore, there exist a major concern about the semantic correlation between the human-readable names and the contents in NDN, since this link can be exploited to trace back content consumers as well as to censor produced contents.

This work aims to raise awareness on the security vulnerabilities that NDN can introduce when the ICN paradigm is applied in vehicular scenarios. The rest of the paper is organized as follows: Section II overviews related works which have proved the relevance of ICN-NDN features for data dissemination in mobile ad-hoc environments, and in VANETs in particular. Section III presents the most serious security vulnerabilities that affect ICN solutions in general; and then, analyzes how some of these weaknesses can influence the adoption of NDN in VANETs. Finally, Section IV summarizes the open challenges to address in our future works.

II. Advantages of NDN in mobile settings

The Named-Data Networking (NDN) [3] is a well-known ICN instance. The NDN protocol is based on the exchange of two different named packets, one for a content request and the other for the content itself, namely respectively, the *Interest* and the *Data*. Both packets carry a human-readable URL-like name, which is used to route the *Interests* first, and to forward back the *Data* later, from a content requester to a source of contents. As any ICN instantiation, NDN supports named contents, in-network caching, name-based routing, asynchronous communication, and in-data security.

TABLE I
NAMES FOR NDN INTERESTS IN V2X SCENARIOS

Goal	Interest Name
Traffic dissemination [5]	”/traffic/geolocation/timestamp/data_type” e.g.: /traffic/highwayA31/north/400,410/146431644,1464366644/speed
Geographic forwarding [6]	”/content/MilitaryGridReferenceSystem(MGRS)” e.g.: /music/lkravitz/cd1/track2/4QFJ123678
Service discovery [7]	”/domain/mainService/subService/typeOfQuery/options” e.g.: /luxembourgCity/transportation/parking/discover/placeGlacis

Hereafter we highlight how each of these features can be beneficial in vehicular scenarios.

1) Naming Contents: It has a multi-facet benefit, well beyond the simple match of requests and contents that names enable in NDN-enabled nodes. In fact, the rich semantics of human-readable NDN names has also proved to be useful for sorting information with different granularity [8], [5] and forwarding Interests [6] in V2X scenarios. Safety messages, traffic information, and other infotainment services can be easily described and retrieved by using human-readable names. Spatio-temporal coordinates may be embedded in those names to seamlessly express further preferences in terms of time validity and area of provenance for a content. In addition to the semantic potential, names may help the propagation of Interests towards geographical areas where fetching data is more likely. In fact, this can be done trailing name components obtained through successfully fetched Data in future *Interests* name. Naming harnesses applications to achieve important tasks in V2V settings, like geographical and temporal scoping of the information [8] or service discovery [7], and so its design is quite critical. Further, while some resource-constrained devices pay for too much semantics embedded in names, today's cars may be equipped with computational units able to process smoothly more complex naming schemes. Table I. summarizes some illustrative Interest names which belong to naming schema designed for different purposes in V2X scenarios.

2) In-Network Caching: It can reduce traffic overhead independently from the application scenario; this may happen, for instance when exchanging traffic information between vehicles [9]. Indeed, the investigation of caching in ICN for MANETs has a few additional implications. First, mobile nodes may bring content copies close to prospective consumers, so reducing both average data retrieval time and the overall network traffic. In particular, this fastens the dissemination of critical information in V2X scenarios. For example, vehicles entering a critical/congested area may obtain fresh traffic/safety report from vehicles leaving the same, as shown in Fig. 1. Second, nodes may keep content copies in their caches, even when the original producer of such information is no longer available. A content producer may move to a different portion of networks (e.g, a mobile vehicle), or, it may cease to work (e.g., a base station) or be temporary unavailable (e.g., an information point shut down for maintenance or fault). Given that vehicles do not suffer from resources scarcity, they can easily support intensive computations and a considerable amount of fast main memory. The use of NDN caching mechanisms in VANETs has been already investigating in some preliminary work [10], and it has been recognized to be valuable for several purposes. In fact, caching bring additional advantages beyond shorter download times and overall reduced network traffic. For example, content cached by vehicles may be moved into different areas to improve the dissemination of special event notifications, like cars accidents or congestion [5], to link temporary disconnected areas in emergency or post-disaster situations [11], to prevent frame collisions by overhearing the communication on the broadcast medium [12].

3) Routing by name: It does not enforce steady sessions on the same network interface. In fact, NDN-enabled nodes can natively exploit different physical media at the same time thanks to the adaptive forwarding logic they implement [13]. Hence, an NDN node may easily switch to another physical interface when the current one either stops working or starts performing poorly. Thus, this adaptive forwarding behavior could be easily leveraged to relax routing constraints in highly dynamic scenarios and to exploit the broadcast inherent nature of the wireless medium. In VANETs content names could further be designed to tackle the mobility of vehicular scenarios. The key-observation is that vehicles often move meanwhile communicating, hence, most of the time a vehicle which issues a request for a certain content is the less-informed one about the potential sources for that information than others around it. Following this assumption, many approaches [14] strive to move the forwarding decision to either the receiver or the intermediate nodes, because those nodes may be in a better position to provide a timed information. Such forwarding decision may be taken looking at the Interest name. The decision may later be enforced either using defer/back-off timers or by looking at additional information piggybacked into previous processed Data packets.

4) Asynchronous Communication: In NDN, the traditional 1-to-1 IP communication model can be replaced by multiple

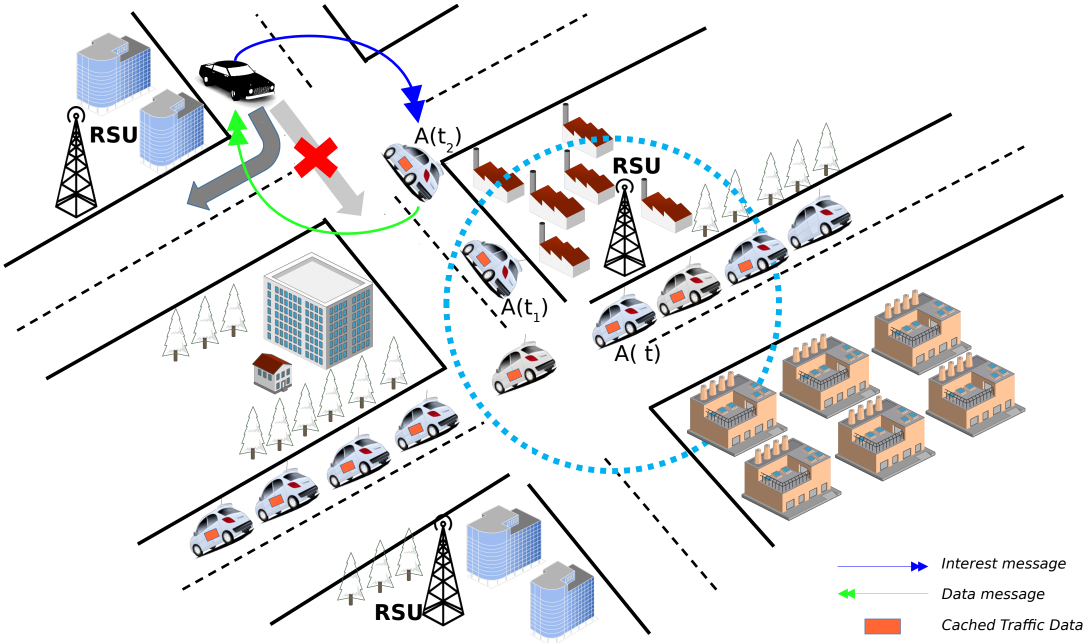

Fig. 1. Cached traffic information disseminated by vehicles leaving a congested area may prevent upcoming vehicles to experience the same congestion.

ones: 1-to-any, 1-to-many, and many-to-many, which can be very useful in vehicular scenarios. For example, a car driving in a city district may be interested in the latest traffic report about a close highway, not minding who is going to provide such information (1-to-any). An information panel may need the same content by different vehicles to compute the average speed over a certain city area (1-to-many); and, finally, vehicles experiencing congestion may want to exchange information each other to reroute towards the destination so to get around the jams (many-to-many). NDN serves natively the anycast model, because the data exchange is not based on any specific content source to retrieve content from. However, all the other communication patterns can be implemented with a careful design of the naming scheme and/or with some minor add-ons.

5) In-Data Security: Since no communication channel is established between two fixed end-points, in NDN the security cannot be anymore provided with mechanisms that secure the channel itself and thus, it has to be embedded in the network packets. Assuming content can be stored anywhere in the network, the assessment of security properties associated to the content must be independent from the storage location. Therefore, in-data security must guarantee a secure binding between the content name and the object this refers to. In NDN, every *Data* packet contains a signature that binds the name and the payload together. The so computed signature guarantees name and data integrity, while for provenance (the identity behind the original source) a trust management schema is needed. Despite the natively enforced data integrity, NDN does not prevent the networks from different classes of attacks, as discussed in the following section.

III. NDN Security Challenges

Nowadays, security on Internet is provided by creating and maintaining secure channels between endpoints. In practice, the security of the information exchanged is bound to the session that hosts establish and it cannot be used anymore once the session expires. On the contrary, ICN aims to secure the data itself by detaching the security of every single unit of information from the entity that has generated it. This can be done in several ways; in NDN for instance, a cryptographic signature and some auxiliary meta-data are embedded in the *Data* packet together with the actual payload.

ICN approach to the security may solve many of the problems that have been harming the actual Internet infrastructure. For example, distributed denial of service (DDoS) attacks that benefit from knowing the IP address of a specific target are harder to be performed against an ICN network, because ICN hosts are not directly addressable. NDN's further immunity comes thanks to a combination of stateful routing mechanisms, to the absence of addresses and of name resolution systems, to the lack of communication sessions [4].

Despite reducing the effectiveness of DDoS attacks targeting IP networks, ICN proposals may introduce several new architecture-specific vulnerabilities. For example, two novel classes of attacks hindering the NDN architecture are: (i) attacks overwhelming routers with content request state to exhausting their forwarding resources [15], i.e., Interest flooding attacks [16]; and (ii) attacks disseminating fake content into the network by means of either advertising fake name-prefixes or polluting the network caches, i.e., cache poisoning attacks [17]. Moreover, the use of human-readable URL-like names for contents raises major concerns since it gives ground to potential effortless privacy-violation tools.

In this Section we describe in more details each class of attack, and the few countermeasures, which have been proposed so far. We then analyze if the aforementioned attacks can be still operated when applying the NDN Architecture in VANETs. If it is the case, we investigate if the related solutions may be still suitable for mobile networks, or there is need of new methods, to make NDN-enabled VANETs secure against such attacks.

A. Interest Flooding Attacks

An *Interest flooding* attack floods the network with a huge amount of fake content requests to saturate either the network's resources or the content provider ones. The goal of the attack is to make the network or a content provider unable to process and to serve legitimate requests. Legitimate requests and malicious ones are quite similar, with the exception that the latter ones ask for non-existing content or exceed the content delivery rate. For this reason, Interest flooding attacks are often extremely difficult to identify. Several countermeasures against this kind of attacks have already been proposed and they are based on different heuristics [16]. These countermeasures can be roughly classified in three major categories according to what they monitor: traffic on incoming interfaces, consumption of router resources, frequency of content names. Recent findings in [18] claim that no single solution can be totally efficient, while hybrid solutions may look promising once tuned to the network settings.

Vehicular scenarios exhibit high mobility that reduces the effectiveness of this kind of attack. An Interest flooding attack has been proved to affect mainly content sources serving the attacked namespace (original source or cached replicas) and/or network devices on the path to those sources. However, most information in VANETs is mainly served on 1-hop basis by broadcasting Interests on the wireless medium. Such short-range dissemination allows to notify several potential content providers with a single *Interest* that is no further propagated. Moreover, proposed schemes for NDN in VANETs usually adopt additional strategies to limit the propagation of *Interests* in order to reduce the risk of collisions. Those forwarding strategies tend not to forward *Interests* when many similar requests are overheard in the node's radio range, or the *Data* retrieval performs poorly. Therefore, this reduces the efficacy of flooding attacks in NDN-based VANETs.

B. Cache Poisoning attacks

A *cache poisoning* attack consists of injecting either fake or corrupted contents[1] into the caches of the network devices so to prevent or delay the download of legitimate contents. In theory, the signatures of *Data* packets are native countermeasures to this attack, but in practice they cannot prevent this attack from happening. Besides, the verification of a signature is a computation intensive operation, so NDN-enabled nodes will likely be designed to verify only a small portion of signatures over the totality of the traffic processed. This is particularly true for devices that perform forwarding operations, like routers. A way to reduce the number of signature verifications performed is to create and distribute a manifest file, i.e., a signed collection of content hashes as a certified list of content names. The idea of manifest has already being acknowledged and leveraged by CCNx[2]. Unfortunately, manifest files suit well only scenarios in which large long-lived contents are produced by either known or certified entities.

Traffic in many V2X scenarios is made of small-size volatile contents that are dynamically generated by many transient vehicles. These conditions make the manifest-based countermeasures not applicable. However, preliminary investigation on ICN VANETs has extensively relied on caching for many purposes, ranging from efficient ways to reduce the amount of traffic by moving information close to the place where may be needed. Hence, it is critical to design NDN nodes that are resilient to the cache poisoning attack to use them in VANETs. There exist ICN features that provide immunity against such kind of attacks: the use of Self-Certifying Names (SCNs) [19] to identify contents and the verification of signatures provided in contents. However, the former requires including the content hash in the request name and this value cannot be computed for dynamically-generated contents. The latter could be easily performed by vehicles equipped with the necessary computational resources and with a set of keys deployed by certified authorities, e.g., car manufacturers or city administrations. Unfortunately, a valid signature does neither guarantee that the retrieved information is readable nor prevent the consumer avoiding the signature verification or the caching of fake content. Indeed, promising countermeasures for the cache poisoning threat are based on shared ranking metrics [17]. In other words, to prevent caches to be polluted, content should be cached only if a device has a fair understanding of the content's validity by means of either a signature verification or some ranking feedback provided by the surrounding environment.

C. Name privacy

Another weak point of NDN resides in the use of human-readable names (HRNs) to identify the contents. Naming eases the design of NDN protocols, meanwhile it has strong implications on the network security and user privacy. Although HRNs may be treated opaquely by network devices, those names are visible by anyone who has access to the communication medium. Furthermore, HRNs have a strong semantic link with the contents they refer to, hence, they may reveal users' interests about the content consumed. For example, a malicious user may simply infer the content of a packet named as *"/luxembourg/highwayA1/10Oct2015/km10tokm50/listOfActiveRadars"* eavesdropping a link. Thus, content names requested in a certain area reveal critical information about the information consumed within it, as well as possible targets. Even worse then in today's IP networks, NDN names cannot be encrypted

[1] In this work we follow the definition of *fake and corrupted content* proposed in [4]

[2] www.ccnx.org.

to be intelligible, as done, for example, to the URLs in HTTPS connections.

The wireless medium opens the doors to massive and effortless sniffing of content requests in VANETs. The granularity of such analysis likely does not allow to identify single consumers of a certain content, but it gives a rough idea of the traffic generated and consumed in a certain area. This information is quite sensitive and it could be exploited for malicious purposes, e.g., censoring/tracking specific devices according to the contents they provide or request, spoofing popular contents, among others. Tentative countermeasures might be based on the adoption of encryption of the Data payload supported by a well-designed fine-grained trust models. Encrypting the payload prevents malicious user to understand the semantic link between the issued requests and the retrieved contents. While, fine-grained trust models can be created in certified entities, e.g., RSUs, needing ad-hoc security associations for the sake of data exchange in local areas. Both countermeasures can be implemented by using Hierarchical Identity Based Encryption (HIBE)-based schemes, as already proposed in previous works [20].

IV. Conclusion

The interest of the research community in alternative network solutions for VANETs is growing. Therefore, the time is ripe to showcase the ICN-NDN potential for those mobile ad-hoc environments. Nevertheless, leveraging NDN in VANET scenarios needs weighing up benefits and risks. Overall, future research works on NDN-based VANETs should investigate more lightweight mechanisms to avoid poisoned caches than mechanisms to prevent the network to be flooded with *Interests*. In fact, the former threat seems to be extremely relevant for a scenario in which caching is proposed as a paramount factor to improve data dissemination. While, the latter seems to be natively counteracted by the forwarding strategies applied to deal with the network dynamics in VANETs. As regard to the name privacy threat, Identity Based Cryptography may be used to hide Data packets content, so breaking the semantic link among name and content for unintended eavesdroppers. A further viable countermeasure could be the design of counter-intuitive naming spaces. These techniques strive for the camouflage of names' semantics in order not to reveal Data content unless the naming convention is known. We will investigate the aforementioned approaches in our future research work.

Acknowledgment

This work was undertaken under the IDSECOM project, /INTER/POLLUX/13/6450335, and the CONTACT project, CORE/SWISS/15/IS/10487418, both funded by the National Research Fund Luxembourg (FNR); and by the H2020 BON-VOYAGE project, funded from the European Union under grant agreement No 635867.

References

[1] A. Rowstron and G. Pau, "Characteristics of a vehicular network," UCLA, Tech. Rep., 2009.

[2] B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher, and B. Ohlman, "A survey of information-centric networking." *IEEE Communications Magazine*, vol. 50, no. 7, pp. 26–36, 2012.

[3] L. Zhang, A. Afanasyev, J. Burke, V. Jacobson, k. claffy, P. Crowley, C. Papadopoulos, L. Wang, and B. Zhang, "Named data networking," *SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 3, pp. 66–73, Jul. 2014.

[4] P. Gasti, G. Tsudik, E. Uzun, and L. Zhang, "Dos and ddos in named data networking," in *22nd International Conference on Computer Communication and Networks, ICCCN 2013, Nassau, Bahamas, July 30 - Aug. 2, 2013*, 2013, pp. 1–7.

[5] L. Wang, A. Afanasyev, R. Kuntz, R. Vuyyuru, R. Wakikawa, and L. Zhang, "Rapid traffic information dissemination using named data," in *Proceedings of the 1st ACM Workshop on Emerging Name-Oriented Mobile Networking Design - Architecture, Algorithms, and Applications*, ser. NoM '12. New York, NY, USA: ACM, 2012, pp. 7–12.

[6] G. Grassi, D. Pesavento, G. Pau, L. Zhang, and S. Fdida, "Navigo: Interest forwarding by geolocations in vehicular named data networking." in *WOWMOM*, L. Bononi, G. Noubir, and V. Manfredi, Eds. IEEE Computer Society, 2015, pp. 1–10.

[7] G. Piro, I. Cianci, L. A. Grieco, G. Boggia, and P. Camarda, "Information centric services in smart cities," *J. Syst. Softw.*, vol. 88, pp. 169–188, Feb. 2014.

[8] L. Wang, R. Wakikawa, R. Kuntz, R. Vuyyuru, and L. Zhang, "Data naming in vehicle-to-vehicle communications," in *2012 Proceedings IEEE INFOCOM Workshops, Orlando, FL, USA, March 25-30, 2012*, 2012, pp. 328–333.

[9] G. Grassi, D. Pesavento, G. Pau, R. Vuyyuru, R. Wakikawa, and L. Zhang, "VANET via named data networking," in *2014 IEEE Conference on Computer Communications, INFOCOM 2014, Toronto, Canada, April 27 - May 2, 2014*, 2014, pp. 410–415.

[10] Y. Yu and M. Gerla, "Potential benefits of information-centric networks for vanets," 2014.

[11] J. Seedorf, D. Kutscher, and F. Schneider, "Decentralised binding of self-certifying names to real-world identities for assessment of third-party messages in fragmented mobile networks," in *2014 Proceedings IEEE INFOCOM Workshops, Toronto, ON, Canada, April 27 - May 2, 2014*, 2014, pp. 416–421.

[12] S. Oh, D. Lau, and M. Gerla, "Content centric networking in tactical and emergency manets," in *Proceedings of the 3rd IFIP Wireless Days Conference 2010, Venice, Italy, October 20-22, 2010*, 2010, pp. 1–5.

[13] C. Yi, A. Afanasyev, L. Wang, B. Zhang, and L. Zhang, "Adaptive forwarding in named data networking," *SIGCOMM Comput. Commun. Rev.*, vol. 42, no. 3, pp. 62–67, Jun. 2012.

[14] Y. Yu, R. B. Dilmaghani, S. B. Calo, M. Y. Sanadidi, and M. Gerla, "Interest propagation in named data manets," in *International Conference on Computing, Networking and Communications, ICNC 2013, San Diego, CA, USA, January 28-31, 2013*, 2013, pp. 1118–1122.

[15] M. Wählisch, T. C. Schmidt, and M. Vahlenkamp, "Backscatter from the data plane - threats to stability and security in information-centric network infrastructure," *Comput. Netw.*, vol. 57, no. 16, pp. 3192–3206, Nov. 2013.

[16] A. Afanasyev, P. Mahadevan, I. Moiseenko, E. Uzun, and L. Zhang, "Interest flooding attack and countermeasures in named data networking," in *IFIP Networking Conference, 2013, Brooklyn, New York, USA, 22-24 May, 2013*, 2013, pp. 1–9.

[17] C. Ghal, G. Tsudik, and E. Uzun, "Needle in a haystack: Mitigating content poisoning in named-data networking," in *Proceedings of the NDSS Workshop on Security of Emerging Network Technologies (SENT'14)*, Feb. 2014.

[18] S. Al-Sheikh, M. Wählisch, and T. C. Schmidt, "Revisiting countermeasures against ndn interest flooding," in *Proceedings of the 2Nd International Conference on Information-Centric Networking*, ser. ICN '15. New York, NY, USA: ACM, 2015, pp. 195–196.

[19] A. Ghodsi, T. Koponen, J. Rajahalme, P. Sarolahti, and S. Shenker, "Naming in content-oriented architectures," in *2011 ACM SIGCOMM Workshop on Information-Centric Networking, ICN 2011, Toronto, ON, Canada, August 19, 2011*, 2011, pp. 1–6.

[20] N. Fotiou and G. C. Polyzos, *Enabling NAME-Based Security and Trust*. Cham: Springer International Publishing, 2015, ch. Trust Management IX: 9th IFIP WG 11.11 International Conference, IFIPTM 2015, Hamburg, Germany, May 26-28, 2015, Proceedings, pp. 47–59.