Authenticated Communication in Crises: Toward an Infrastructureless Trust Model for Challenged Networks

Pouyan Fotouhi Tehrani
Weizenbaum Institute / Fraunhofer Fokus
pft@ieee.org

Eric Osterweil
George Mason University
eoster@gmu.edu

Jochen H. Schiller
Freie Universität Berlin
jochen.schiller@fu-berlin.de

Thomas C. Schmidt
HAW Hamburg
t.schmidt@haw-hamburg.de

Matthias Wählisch
Freie Universität Berlin
m.waehlisch@fu-berlin.de

***Abstract*—Natural as well as human-caused disasters and catastrophes easily lead to chaos. Effective crisis communication and informing the public about the ongoing situation can reduce chaos and maintain social resiliency. Communication, however, relies on a working physical infrastructure, which usually is broken in the incident area. Whereas first response teams and authorities benefit from special communication equipment, civilians do not and experience longer periods of being disconnected from the outside world. Even if messages come through occasionally, the communication is too intermittent to allow for channel-based trust models. TLS, for example, requires access to trusted third parties to authenticate data.**

In this position paper, we argue that end-to-end communication conflicts with disaster scenarios. We propose an approach that leverages information-centric networking (ICN) to authenticate risk and crisis communication in loosely connected communication systems. Our proposal makes use of spatiotemporal decoupling of data from their producers based on ICN for optimal message propagation in fragmented networks, while introducing a trust bootstrapping phase to enable off-line authentication. The data-oriented security model of ICN is used to tailor a trust model specifically for scenarios during which access to trusted third parties or data owners is not given and messages are relayed through untrusted parties.

***Index Terms*—Information-centric Networking, Disaster Management, Data-origin Authentication, Trust**

I. Introduction

Severe disasters and catastrophes almost always lead to communication disturbances by damaging the infrastructure, by causing power outages, or due to delayed and unattainable repairing efforts [1]. Whereas disaster relief teams are in advantage in terms of communication means through special equipment such as satellite phones and long range radio systems, civilians are susceptible of becoming isolated and getting cutoff from external communication. Due to the extra ordinary state of the situation during such incidents, it is as critical as ever to guarantee *risk and crisis communication* in face of disasters to maintain social resiliency [2], [3].

Effective crisis communication requires, among others, timely information provision from trusted and credible sources. In challenged or fragmented networks, however, it is unreliable to utilize existing Internet infrastructure, as targeted endpoints might be unreachable or down altogether. Simply put, the end-to-end paradigm of the Internet does not adapt well in disaster and crisis response phase. Even if limited communication is made possible, *e.g.,* through ad hoc, delay and disturbance tolerant, or software defined networks, typical security measures such as public key infrastructure (PKI) require access to trusted third parties (TPP), which cannot be guaranteed. Nonetheless, authenticating messages in such scenarios remains a crucial and necessary step.

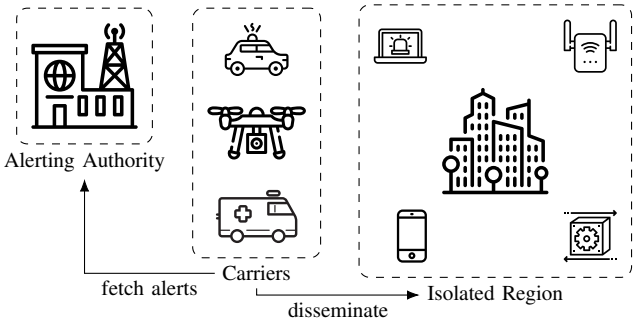

Fig. 1. Use case Scenario: Alert Dissemination

In this paper, we focus on securing messages, *e.g.,* warnings, issued by authorities which can be authenticated off-line regardless of how a message is retrieved (see Figure 1).

The remainder of this paper is structured as follows: a brief overview of ICN and respective trust management is given in **§ II** followed by a general concept on how to realize off-line authentication for disaster response in ICN in **§ IV**. A concrete solution based on named-data networking (NDN) [4] is introduced in **§ V**. § VI discusses related work, and § VII summarizes our findings.

II. Background

Information-centric networking introduces a paradigm shift from *host-centric* networking to information by decoupling data from its producer both in temporal and spatial dimensions. Instead of assigning names to addresses and addresses to hosts to forward packets between them, in ICN the network is responsible for discovery and retrieval of data packets which are identified through unique names. ICN nodes are able to cache content for future provision without relying on the original producer.

The new networking paradigm of ICN requires new security perspectives. In contrast to securing channels between hosts such as in *HTTP secure* (HTTPS) or *secure shell* (SSH), ICN secures content independent of communication participants.

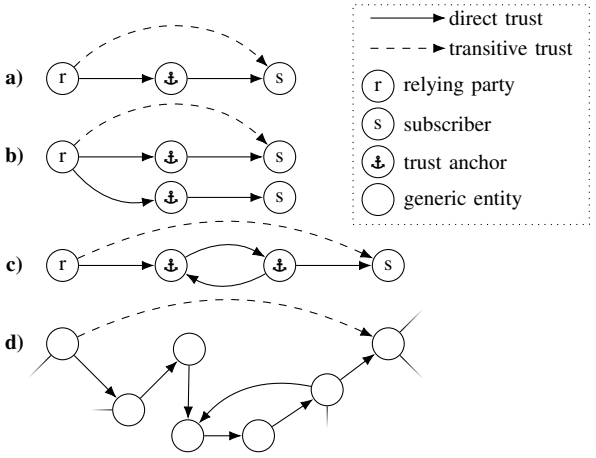

Fig. 2. Trust models—a) Basic Trust Model, b) Multiple Trust Anchors, c) Cross Certified Trust Anchors, d) Web of Trust.

A common approach in securing data is to use digital signatures over secure hashes of the data. To achieve authenticity, asymmetric cryptography signs data using a private key and verifies the signature using the corresponding public key. Public keys are commonly available in form of certificates. A certificate comprises a public key and metadata signed either by the owner (self-signed) or by a trusted third party (TPP) and is leveraged for signature verification and consequently data origin and non-repudiation authentication. To simplify key management tasks and policy enforcement, a *trust management framework* [5] can be used. Such framework defines trust relations by specifying which parties can issue and certify credentials. *i.e.,* TPPs, and enforces policies by putting constraints on actions of credential holders. Respectively, trust is established transitively through a TPP between a *relying party* and a *subscriber*, which uses the services of the TPP [6]. Beside the simple trust model, depicted in Figure 2a, alternative models such as multiple trusted parties, Figure 2b, and cross-certified trust anchors, Figure 2c, are possible. A generalization of these models is given in *Web-of-Trust* (WOT) [7] in which each party acts both as an authority and a relying party, see Figure 2d. Trust is considered to be established (to some degree) between two parties if there can be found a trust relation between them.

III. Requirement Analysis

Before eliciting functional and non-functional requirements, the following scenario is used to illustrate a typical use case of our proposed approach: given a geographically restricted disaster-stricken area in which communication channels between authorities and civilians are disturbed or cutoff altogether, it should be possible to (*i*) carry messages from authorities to civilians over multiple hops, and (*ii*) provide authentication mechanisms which are infrastructure-independent and only require information fetched in a preceding trust bootstrapping phase. Figure 1 visualizes such use case in its simplest form.

Stakeholders in this scenario are (*i*) alerting authorities as data producers, (*ii*) off-line and out-of-band data carriers , and (*iii*) data consumers ranging from consumer electronics to IoT devices and local network routers. Functional requirements are respectively defined as follows:

R1 Decoupling data from respective publishers.

R2 On and off-path caching.

R3 Passive and active data discovery.

R4 Data retrieval by its name (and not through its host).

Non-functional requirements are given below:

N1 Compatibility.
N2 Integrability.
N3 Scalability.
N4 Security.
N5 Resilience.
N6 Fault-tolerance.

N1 and **N2** emphasize the importance of compatibility with established and common protocols, *e.g., common alerting protocol* (CAP) [8], **N3** foresees the need for scalability in face of increasing data publishing frequency and consumer count, **N4** denotes the need for mechanisms to secure data, **N5** is derived from the fragile nature of given situation immediately after disaster and crises, and finally **N6** caters for failures in involved networking nodes.

IV. Concept

The goal of this work is to conceptualize an approach which allows securing messages, their dissemination in challenged networks, and finally providing means for off-line authentication. All functional requirements are already covered when using ICN as networking infrastructure (see section II). Regarding non-functional requirements, we focus on **N4**, namely security, while leaving the rest for future work.

We consider a data packet to be secured if the following can be guaranteed: (*i*) data integrity, (*ii*) data origin authentication, and (*iii*) non-repudiation verification. In other words, it should be possible to confirm that data has not been modified during transmission, its origin is traceable, and it can only be originating from its producer and no one else. A producer in this context is a real-world entity, *e.g.,* an alerting authority, identified by its digital credentials. Whereas mere technical solutions can be used to realize data integrity verification (by secure hashes) or non-repudiation attestation (by asymmetric cryptography), origin authentication requires organizational effort to bind digital credentials with real-world identities. To bind real-world identities to public keys, certificates are enhanced with metadata, *e.g.,* using *organization* field in X.509 certificates [9], and the authenticity of the binding can be attested by a TPP.

As the emphasis of this work lies within off-line authentication, consumers need to fetch *all* necessary certificates during the bootstrapping phase *before* a disaster strikes. This way no on-line communication is required during authentication to fetch missing certificates. This turns out to be a non-trivial task, since a wide spectrum of non-governmental, private, and international entities are involved in disaster management (DM) beside the local major parties, such as police forces, fire departments, and emergency medical services.

Adequate trust bootstrapping would entail two phases: (*i*) a discovery, and (*ii*) a certificate retrieval phase. In discovery phase, a consumer should be able to fetch a list of DM organization which in turn maintain a set of certificates of their authorized producers. The inquiry is context-aware and results in discovery of only spatially related authorities, including both local and global organizations with a mandate for DM in that specific region. Finally, the retrieval phase is an iterative process by the consumer through which the set of certificates for authorized producers is fetched from the discovered organizations. To be practical for consumers, we propose the highest civil protection body of each country, *e.g., Sécurité*

Interest Packet
Name
Guiders
Nonce
Application Params

Data Packet
Name
Metadata
Content
Data Signature

Fig. 3. NDN Interest and Data Packets

Civile in France, *BBK* in Germany, or *FEMA* in the USA, to maintain the list of top-tier DM organizations. It would suffice for consumers to obtain the certificate of civil protection organization securely to initiate the trust bootstrapping phase.

V. Proposed Solution

In this section, we introduce a proof of concept that fulfills all functional and non-functional requirements leveraging *named-data networks* (NDN) [4] as ICN core and NDNSSEC [10] for namespace management.

NDN is a popular ICN approach supporting a hierarchical naming scheme. Data packets in NDN are identified by their names, *e.g.,* `/com/example/index.html`, and can be retrieved using *interest messages*. Intermediate nodes forward interest messages to producers or hosts, which may have cached copies of the desired data. Data packets can be secured using asymmetric cryptography, and a signed packet contains all information necessary to fetch the corresponding certificate(s) required for authentication. For this NDN introduces the `KeyLocator` field (part of Digital Signature). A certificate in NDN is an ordinary data packet which carries a public key. To distinguish certificates from ordinary data packets, NDN adds special constraints on the naming of the certificate packets. The standard naming convention for certificates in NDN is as follows: `/<prefix>/KEY/<id>/<issuer>/<ver>` [11] where `prefix` denotes the certificate namespace, `id` the ID of key it carries, `issuer` the ID of the issuer, and `ver` the certificate version. The structure of interest and data packets in NDN is depicted in Figure 3.

NDNSSEC is a security extension which relies on DNS to realize namespace management in NDN. It partitions the global NDN namespace into smaller management units, *zones*, and provides mechanisms to verify if a producer is authorized to publish under a zone or not. To this mean, a DNS zone apex, *e.g.,* `example.com.`, is *ndnified* [12] into its equivalent *reverse slash separated* notation, *e.g.,* `/com/example`, and is used as name prefix for names published under that zone in NDN. The possibility of representings a DNS zone apex in its equivalent NDN notation and vice versa enables the outsourcing of zone management in NDN onto existing DNS ecosystem. This way not only technical aspects of namespace management, but also non-technical issues, such as binding names to real-world identities or solving trademark conflicts, are taken care for by DNS related organizations, such as ICANN. To authorize an NDN publisher to publish under a given zone, the respective zone owner must register a public key of a producer as a `DNSKEY` record under its authoritative name server. Prior to publishing a packet, the producer would sign it using its private key, and set the `KeyLocator` respectively, that is with zone apex as `<prefix>` and its public key digest as `<id>`. To authenticate a packet, consumers consult the DNS to check if any of the listed public keys by the zone owner has been used to sign the packet or not [10].

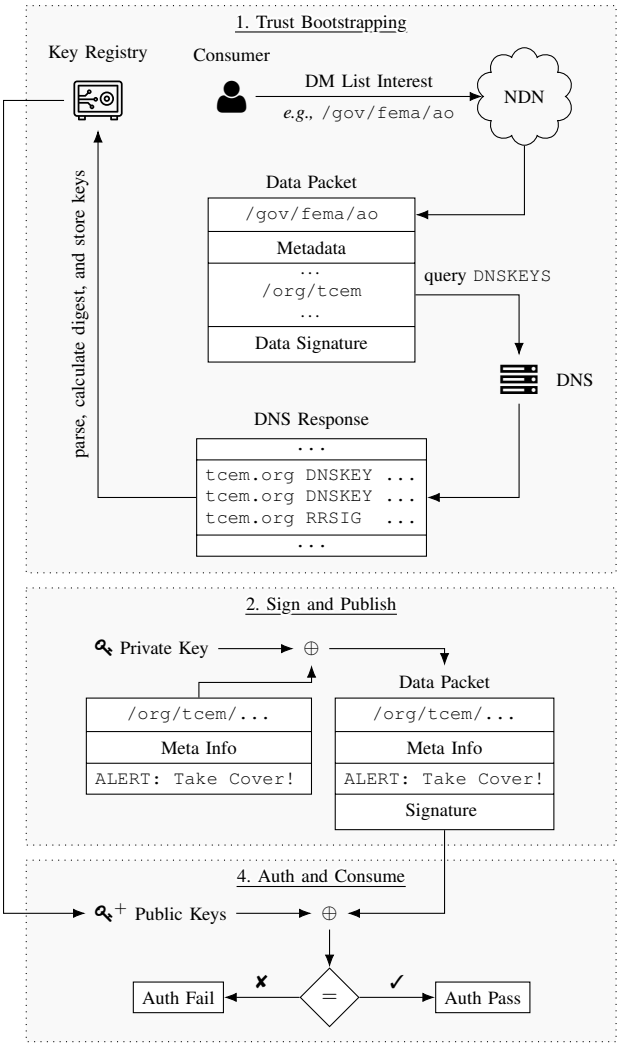

Fig. 4. Overview of Workflow: from Bootstrapping to Authentication

Our proposed solution presupposes the following as given: (*i*) both data producers and consumers have access to the same logical NDN instance, (*ii*) consumers access the network through a designated application which is already preconfigured with zone apexes, *e.g.,* `/gov/fema`, and certificates of the highest civil protection bodies for each country, and (*iii*) participating DM organizations follow NDNSSEC policies to authorize producers under their respective zones.

The general workflow of our solution comprises three stages as follows:

1) **Trust Bootstrapping**: The optimal phase to initiate trust bootstrapping is prior to disaster, *e.g.,* in disaster preparedness phase. Depending on its current location, a consumer would first need to fetch the list of authorized DM organizations. To this mean an interest message is dispatched for the list of zone apexes of authorized organizations under the name `/ao` prefixed with the namespace of respective civil protection organization. For example the list of authorized DM organizations within the United States can be retrieved by dispatching an interest for `/gov/fema/ao`. Note that the response is not necessarily provisioned by the data owner but any other reachable node which happens to have a copy of that packet. The authenticity of the response can be verified using the preloaded certificates in the application of the

consumer.
Iteratively, the consumer fetches the list of public keys authorized by each organization using NDNSSEC. This step can be done using a single round trip per organization by simply querying all `DNSKEY` records listed under its authoritative name server. Finally, the digest of public key for each entry is calculated and is stored in a local key registry alongside the zone apex and the key itself.

2) **Data Publishing**: Published data must conform to the NDNSSEC workflow and policy. An authorized producer must sign its data and set the `KeyLocator` prior to publishing.
3) **Data Consumption and Authentication**: During disaster response it is expected for consumers to retrieve messages from DM organizations relayed through untrustworthy parties. Given a data packet, a consumer uses NDNSSEC to extract the respective zone apex from packet's name and its signature info block. The zone apex is used to search the local key registry, which is propagated during the trust bootstrapping phase, for authorized keys. The key digest included in the packets `KeyLocator` field is used to filter available keys in the registry.

The general overflow is summarized in Figure 4.

VI. Related Works

The benefits of utilizing ICN in disaster management has been a subject of attention in recent years. Tyson et al., for example, highlight improved resiliency and superior disruption tolerance [13], while Seedorf et al. emphasize the spatiotemporal decoupling and data-oriented security schemes of ICN [14] as beneficial for disaster management. Projects such as *GreenICN* [15] and *UMobile* [16] are a few examples which leverage ICN specifically for disaster management use cases.

At the same time and in spite of widely recognized need for suitable trust models in disaster scenarios [13], [14], [17], only a few approaches have been proposed so far which address both origin authentication and identification. Seedorf et al. [18] propose a decentralized mechanism based on WOT (see Figure 2d) to bind names to real-world identities in fragmented mobile networks. The objective here is to assess trustworthiness of *on-behalf-of* messages which are received from unknown third parties. Tagami et al. [19] leverage *identity-based cryptography* to avoid the need for persistent access to TTPs for authentication. In this approach, the identity of a producer is used to generate its public key using only public parameters retrieved from a trusted *private key generator* (PKG) (see [20]). A consumer can then generate public keys for an arbitrary producer on the fly, given that the corresponding private key is generated by a PKG known to and trusted by the consumer.

VII. Conclusion

In this paper, we proposed a solution for message propagation and off-line data-origin authentication in fragmented and intermittent networks. Whereas the end-to-end principles of the Internet are considered as an obstacle, the spatiotemporal decoupling of data from hosts and the data-oriented security paradigm of ICN are enablers for quick message propagation and authentication in scenarios with impaired communication infrastructure.

Our future work comprises the implementation of the proposed solution and its evaluation. An analysis of time and space complexity of trust bootstrapping phase as well as the authentication process is to be undertaken. Furthermore, the organizational overhead for involved parties has to be studied to assess the integrability and interoperability of our approach in existing workflows of DM organizations.

References

[1] G. O'Reilly, A. Jrad, R. Nagarajan, T. Brown, and S. Conrad, "Critical Infrastructure Analysis of Telecom for Natural Disasters," in *Networks 2006. 12th International Telecommunications Network Strategy and Planning Symposium*, pp. 1–6, IEEE, 2006.

[2] P. H. Longstaff and S.-U. Yang, "Communication Management and Trust: Their Role in Building Resilience to "Surprises" Such As Natural Disasters, Pandemic Flu, and Terrorism," *Ecology and Society*, vol. 13, no. 1, pp. 1–14, 2008.

[3] B. Reynolds and M. W. Seeger, "Crisis and emergency risk communication as an integrative model," *Journal of Health Communication*, vol. 10, no. 1, pp. 43–55, 2005.

[4] L. Zhang, A. Afanasyev, J. Burke, V. Jacobson, K. Claffy, P. Crowley, C. Papadopoulos, L. Wang, and B. Zhang, "Named data networking," *ACM SIGCOMM Computer Communication Review*, vol. 44, pp. 66–73, jul 2014.

[5] M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized trust management," in *Proceedings 1996 IEEE Symposium on Security and Privacy*, pp. 164–173, IEEE Comput. Soc. Press, 1996.

[6] H. van Tilborg and S. Jajodia, *Encyclopedia of Cryptography and Security*. Encyclopedia of Cryptography and Security, Springer US, 2011.

[7] P. R. Zimmermann, *The Official PGP User's Guide*. Cambridge, MA, USA: MIT Press, 1995.

[8] J. Westfall, "Common Alerting Protocol Version 1.2," July 2010.

[9] S. Boeyen, S. Santesson, T. Polk, R. Housley, S. Farrell, and D. Cooper, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile." RFC 5280, 05 2008.

[10] P. F. Tehrani, E. Osterweil, J. Schiller, T. C. Schmidt, and M. Wählisch, "The Missing Piece: On Namespace Management in NDN and How DNSSEC Might Help," in *Proc. of 6th ACM ICN*, ACM, 2019.

[11] Z. Zhang, Y. Yu, H. Zhang, E. Newberry, S. Mastorakis, Y. Li, A. Afanasyev, and L. Zhang, "An Overview of Security Support in Named Data Networking," *IEEE Communications Magazine*, vol. 56, pp. 62–68, nov 2018.

[12] A. Afanasyev, *Addressing Operational Challenges in Named Data Networking Through NDNS Distributed Database*. PhD thesis, University of California Los Angeles, 2013.

[13] G. Tyson, E. Bodanese, J. Bigham, and A. Mauthe, "Beyond content delivery: can ICNs help emergency scenarios?," *IEEE Network*, vol. 28, pp. 44–49, may 2014.

[14] J. Seedorf, A. Tagami, M. Arumaithurai, Y. Koizumi, N. B. Melazzi, D. Kutscher, K. Sugiyama, T. Hasegawa, T. Asami, K. K. Ramakrishnan, T. Yagyu, and I. Psaras, "The Benefit of Information Centric Networking for Enabling Communications in Disaster Scenarios," in *2015 IEEE Globecom Workshops (GC Wkshps)*, pp. 1–7, IEEE, dec 2015.

[15] A. Tagami and M. Arumaithurai, "GreenICN Project: Architecture and Applications of Green Information Centric Networking," *IEICE Transactions on Communications*, vol. E99.B, no. 12, pp. 2470–2476, 2016.

[16] C.-A. Sarros, S. Diamantopoulos, S. Rene, I. Psaras, A. Lertsinsrubtavee, C. Molina-Jimenez, P. Mendes, R. Sofia, A. Sathiaseelan, G. Pavlou, J. Crowcroft, and V. Tsaoussidis, "Connecting the Edges: A Universal, Mobile-Centric, and Opportunistic Communications Architecture," *IEEE Communications Magazine*, vol. 56, pp. 136–143, feb 2018.

[17] J. Seedorf, M. Arumaithurai, A. Tagami, K. Ramakrishnan, and N. Blefari-Melazzi, "Research Directions for Using ICN in Disaster Scenarios," Internet-Draft draft-irtf-icnrg-disaster-07, Internet Engineering Task Force, June 2019. Work in Progress.

[18] 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 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 416–421, IEEE, apr 2014.

[19] A. Tagami, T. Yagyu, K. Sugiyama, M. Arumaithurai, K. Nakamura, T. Hasegawa, T. Asami, and K. K. Ramakrishnan, "Name-based push/pull message dissemination for disaster message board," *IEEE Workshop on Local and Metropolitan Area Networks*, pp. 1–6, 2016.

[20] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proceedings of CRYPTO 84 on Advances in Cryptology*, (New York, NY, USA), pp. 47–53, Springer-Verlag New York, Inc., 1985.