Lightweight Authentication for Fault-Tolerant Topic-Channels in Ad Hoc Distributed Systems*

Hans Walter Behrens
Arizona State University
Tempe, AZ, USA
hwb@asu.edu

K. Selçuk Candan
Arizona State University
Tempe, AZ, USA
candan@asu.edu

ABSTRACT

Many distributed systems assume participants are both performant and secure, characteristics offered by many cloud-based systems. However, scaling distributed techniques down to highly resource- or power-constrained contexts may require alternative approaches. One such context is the deployment of ad hoc distributed systems in insecure or uncontrolled areas, for example during disaster response activities. Providing reliable and secure service is exacerbated by the computational and power constraints imposed on these devices. In this work, we first introduce the concept of on-demand topic-channels. Then, we describe three message authentication protocols which provide secure, authenticated communication between participants and a coordinator, while also providing resilience from adversarial or accidental disruption. We leverage homomorphic hashing primitives to trade message secrecy against communication and computational costs. Finally, we assess these protocols, and show that our hash-based protocols provide significant efficiency improvements over traditional encryption-based approaches.

KEYWORDS

distributed systems, homomorphic hashing, messaging protocols

ACM Reference Format:
Hans Walter Behrens and K. Selçuk Candan. 2018. Lightweight Authentication for Fault-Tolerant Topic-Channels in Ad Hoc Distributed Systems. In *HPDC '18: The 27th International Symposium on High-Performance Parallel and Distributed Computing, June 11–15, 2018, Tempe, AZ, USA.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3220192.3220458

1 INTRODUCTION

Efficient, low-power, and fault-tolerant distributed protocols are ideally suited for applications in disaster response. Rapid deployments of ad hoc devices in natural disaster response provides emergency personnel with a much better situational understanding in areas where underlying infrastructure may be damaged or nonexistent.

Such deployments are intrinsically ephemeral, as nodes may fail for a number of reasons: battery depletion, hardware failure, or communication interruption. Criminals seeking to exploit a disaster may serve in an adversarial role, attempting to subvert or compromise sensor coverage. The deployed network should therefore be resilient, remaining available for readings despite such failures or attacks while also rejecting unauthorized queries.

Furthermore, disaster response activities may necessitate layered, heterogeneous deployments of different sensors. Not all data will be relevant to all responders; by compartmentalizing information and releasing only to users who are both relevant and authorized, operational security and communication efficiency can both be improved. These "topic-channels" have thus far been associated with publish-subscribe frameworks, yet event-driven approaches do not account for changing user demands. By adapting the concept of topic-channels to an on-demand paradigm, the number of sensor readings and network transmissions may be drastically reduced.

2 BACKGROUND & RELATED WORK

Many aspects of providing secure communication in low-power ad hoc systems have been extensively studied in the literature, both from a security and efficiency perspective. For example, [3] proposed a grouped aggregation scheme for distributed systems to reduce network load, but did not address adversarial resilience.

Message routing itself provides a sensitive attack surface for adversaries to exploit. In their benchmark paper, [4] proposed Ariadne, a distributed protocol for securing message routing for ad hoc networks. However, their approach is restricted to the routing messages themselves, which are used to 'learn' the topology of the network. Additionally, it requires either time synchronization or shared secret keys; the former is rarely possible in low-power deployments, and the latter is sensitive to node capture attacks.

The authentication of message content is highly important in sensor systems, as improper messages may distort the semantic conclusions of users. The power savings of hashing over encryption in low-power systems are supported by the work of [7]; [2] proposes a protocol to leverage this, and provide efficient message authentication. However, it relies on a secure setup phase for handshaking, which makes post-deployment changes difficult or impossible.

To address this drawback, we make use of homomorphic hashing, a class of collision-resistant hash functions initially introduced by [1], and later extended by [5] and [6]. Given a hash function $H(x)$, we can say that H is homomorphic if for some operation $|$, $H(a)|H(b) = H(a|b)$. We leverage this class of functions to provide node capture resilience while also permitting queries to target specific topic-channels.

*Funding for this research was provided by the National Science Foundation under the proposal "DataStorm: A Data Enabled System for End-to-End Disaster Planning and Response" (NSF Award No. 1610282). Primary author is a PhD student.

HPDC '18, June 11–15, 2018, Tempe, AZ, USA

ACM ISBN 978-1-4503-5899-6/18/06…$15.00
https://doi.org/10.1145/3220192.3220458

3 RESEARCH CONTRIBUTIONS

We first define the concept of *topic-channels*: semantically-distinct node groupings used to address context-sensitive subsets of nodes within a heterogeneous network. For example, certain types of participant nodes or specific sensor families may be selectively queried according to user requirements, reducing communication and computational load without impacting functional performance.

We then aim to answer the following questions: **(1)** Can we provide a protocol for on-demand querying of topic-channels within a heterogeneous, ad hoc distributed system? **(2)** Can the security of the protocol be guaranteed against a variety of attacks and adversarial scenarios, while also maintaining availability and fault tolerance throughout? **(3)** Can the protocol support post-deployment modifications to topic-channel assignment, without compromising the security of the network? **(4)** Can the efficiency of our protocol be ensured through the use of less computationally-intensive methods? **(5)** Can we minimize transmissions, to reduce energy usage?

We propose and compare three novel messaging protocols that support desired on-demand topic-channel structures:

(1) The first is a novel protocol based on homomorphic hashing primitives. This approach offers efficiency improvements over standard encryption protocols, but sacrifices the secrecy of the messages. However, limitations on authentication in this protocol may leave the network open to some types of exhaustion attacks during the response phase.
(2) The second protocol introduces the concept of *channel validation* through additional hashing, and leverages on-node decision making to provide stronger response validation at the expense of slightly increased computational costs.
(3) The third protocol builds upon the previous ideas by introducing *chain validation*, which incorporates structural properties of the network to constrain and shape message propagation. This further reduces communication overhead during the response phase, at the expense of increased hashing.

Routing for these protocols is implemented through multicasting, for additional fault tolerance in message delivery.

4 PRELIMINARY RESULTS

In evaluating these results, simulated deployments with different topologies were tested. The total, network-wide count of response transmissions triggered by a valid query is shown in Fig. 1(a); the total, network-wide count of erroneous transmissions triggered by a coordinated adversarial attack is shown in Fig. 1(b).

For deployments with high centrality, where messages must pass through several intermediate nodes, channel validation provides reductions in adversarial propagation, shown in Fig. 1(b). These attacks are filtered out by non-compromised intermediate nodes during the forwarding process. In particular, the channel filtering approach is most effective in topologies where the number of paths among source and destination nodes are relatively small, as there are fewer routes for the adversarial broadcast to take.

Under chain validation, systems with lower diameters see efficiency improvements in both message transmission, shown in Fig. 1(a), and adversarial impact, shown in Fig. 1(b). By bounding broadcast depth, total message count can be reduced regardless of source, producing synergistic effects with channel validation due to pruning of overly circuitous routes.

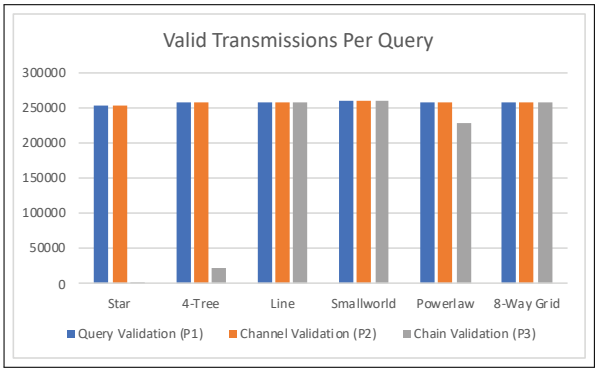

Fig. 1(a): Number of transmissions per query for a topic-channel with a 10% membership rate.

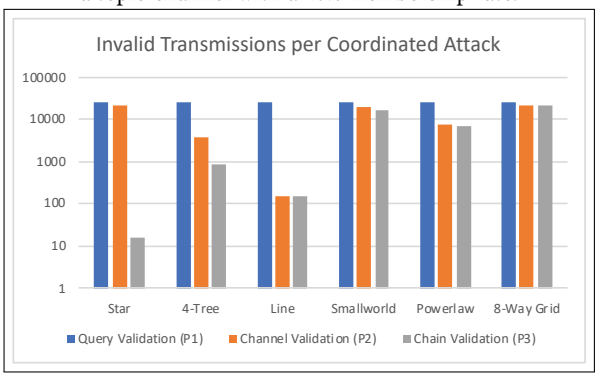

Fig. 1(b): Number of transmissions incurred by a single, coordinated attack for a network with a 1% adversarial rate.

Figure 1: Comparison of three proposed protocols under varying topologies, with an ad hoc system size of 1600 nodes.

5 CONCLUSION & FUTURE WORK

In this work, we introduced on-demand authenticated topic-channels, and presented three alternative protocols to provide both fault-tolerant, authenticated communication and resilience from adversarial or accidental disruption for ad hoc distributed systems. Potential future work includes evaluating messaging performance under additional attack models, topological structures, or network partitioning. Additionally, intelligent message aggregation, routing, and forwarding strategies provide several promising alternatives to further reduce communication load.

REFERENCES

[1] M Bellare and D Micciancio. 1997. A new paradigm for collision-free hashing: Incrementality at reduced cost. In *EUROCRYPT '97*. Springer.
[2] O Delgado-Mohatar, A Fúster-Sabater, and JM Sierra. 2011. A light-weight authentication scheme for wireless sensor networks. *Ad Hoc Networks* (2011).
[3] Benjamin Heintz, Abhishek Chandra, and Ramesh K Sitaraman. 2015. Optimizing grouped aggregation in geo-distributed streaming analytics. In *International Symposium on High-Performance Parallel and Distributed Computing (HPDC)*. ACM.
[4] Y Hu, A Perrig, and DB Johnson. 2005. Ariadne: A secure on-demand routing protocol for ad hoc networks. *Wireless networks* 11, 1-2 (2005), 21–38.
[5] MN Krohn, MJ Freedman, and D Mazieres. 2004. On-the-fly verification of rateless erasure codes for efficient content distribution. In *Security and Privacy (S&P)*.
[6] Jeremy Maitin-Shepard, Mehdi Tibouchi, and Diego F Aranha. 2016. Elliptic curve multiset hash. *Comput. J.* 60, 4 (2016), 476–490.
[7] GCCF Pereira, RCA Alves, F Silva, RM Azevedo, BC Albertini, and CB Margi. 2017. Performance Evaluation of Cryptographic Algorithms over IoT Platforms and Operating Systems. *Security and Communication Networks* (2017).