**LITERATURE SURVEY**

**1) Provable data possession at untrusted stores**

**AUTHORS:**  C. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song

We introduce a model for *provable data possession* (PDP) that allows a client that has stored data at an untrusted server to verify that the server possesses the original data without retrieving it. The model generates probabilistic proofs of possession by sampling random sets of blocks from the server, which drastically reduces I/O costs. The client maintains a constant amount of metadata to verify the proof. The challenge/response protocol transmits a small, constant amount of data, which minimizes network communication. Thus, the PDP model for remote data checking supports large data sets in widely-distributed storage system.

We present two provably-secure PDP schemes that are more efficient than previous solutions, even when compared with schemes that achieve weaker guarantees. In particular, the overhead at the server is low (or even constant), as opposed to linear in the size of the data. Experiments using our implementation verify the practicality of PDP and reveal that the performance of PDP is bounded by disk I/O and not by cryptographic computation.

**2) Proofs of storage from homomorphic identification protocols**

**AUTHORS:** G. Ateniese, S. Kamara, and J. Katz

Proofs of storage (PoS) are interactive protocols allowing a client to verify that a server faithfully stores a file. Previous work has shown that proofs of storage can be constructed from any homomorphic linear authenticator (HLA). The latter, roughly speaking, are signature/message authentication schemes where `tags' on multiple messages can be homomorphically combined to yield a `tag' on any linear combination of these messages.

We provide a framework for building public-key HLAs from any identification protocol satisfying certain homomorphic properties. We then show how to turn any public-key HLA into a publicly-verifiable PoS with communication complexity independent of the file length and supporting an unbounded number of verifications. We illustrate the use of our transformations by applying them to a variant of an identification protocol by Shoup, thus obtaining the first unbounded-use PoS based on factoring (in the random oracle model).

**3) ODSBR: An on-demand secure byzantine resilient routing protocol for wireless ad hoc networks**

**AUTHORS:** B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H.

Rubens

Ah hoc networks offer increased coverage by using multihop communication. This architecture makes services more vulnerable to internal attacks coming from compromised nodes that behave arbitrarily to disrupt the network, also referred to as Byzantine attacks. In this work, we examine the impact of several Byzantine attacks performed by individual or colluding attackers. We propose ODSBR, the first on-demand routing protocol for ad hoc wireless networks that provides resilience to Byzantine attacks caused by individual or colluding nodes. The protocol uses an adaptive probing technique that detects a malicious link after log *n* faults have occurred, where *n* is the length of the path. Problematic links are avoided by using a route discovery mechanism that relies on a new metric that captures adversarial behavior. Our protocol never partitions the network and bounds the amount of damage caused by attackers. We demonstrate through simulations ODSBR's effectiveness in mitigating Byzantine attacks. Our analysis of the impact of these attacks versus the adversary's effort gives insights into their relative strengths, their interaction, and their importance when designing multihop wireless routing protocols.

**4) TWOACK: Preventing selfishness in mobile ad hoc networks**

**AUTHORS:** K. Balakrishnan, J. Deng, and P. K. Varshney

Mobile ad hoc networks (MANETs) operate on the basic underlying assumption that all participating nodes fully collaborate in self-organizing functions. However, performing network functions consumes energy and other resources. Therefore, some network nodes may decide against cooperating with others. Providing these selfish nodes, also termed misbehaving nodes, with an incentive to cooperate has been an active research area recently. In this paper, we propose two network-layer acknowledgment-based schemes, termed the TWOACK and the S-TWOACK schemes, which can be simply added-on to any source routing protocol. The TWOACK scheme detects such misbehaving nodes, and then seeks to alleviate the problem by notifying the routing protocol to avoid them in future routes. Details of the two schemes and our evaluation results based on simulations are presented in this paper. We have found that, in a network where up to 40% of the nodes may be misbehaving, the TWOACK scheme results in 20% improvement in packet delivery ratio, with a reasonable additional routing overhead.

**5) Short signatures from the weil pairing**

**AUTHORS:** D. Boneh, B. Lynn, and H. Shacham

We introduce a short signature scheme based on the Computational Diffie–Hellman assumption on certain elliptic and hyperelliptic curves. For standard security parameters, the signature length is about half that of a DSA signature with a similar level of security. Our short signature scheme is designed for systems where signatures are typed in by a human or are sent over a low-bandwidth channel. We survey a number of properties of our signature scheme such as signature aggregation and batch verification.