Information Sciences 318 (2015) 144–156

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

Universal designated verifier transitive signatures for graph-based big data

Shuquan Hou [a,b], Xinyi Huang [a,b,*], Joseph K. Liu [c], Jin Li [d], Li Xu [a]

[a] Fujian Provincial Key Laboratory of Network Security and Cryptology, School of Mathematics and Computer Science, Fujian Normal University, China
[b] The State Key Laboratory of Integrated Services Networks, Xidian University, China
[c] Faculty of Information Technology, Monash University, Australia
[d] School of Computer Science, Guangzhou University, China

ARTICLE INFO

Article history:
Received 25 January 2014
Received in revised form 3 February 2015
Accepted 9 February 2015
Available online 5 March 2015

Keywords:
Big data
Transitive signature
Universal designated verifier signature
Privacy

ABSTRACT

In this paper, we propose a new type of digital signatures which is specifically designed for graph-based big data system. The properties of the proposed signatures are twofold. On one side it possesses the features of transitive signatures: One can sign a graph in such a way that, given two signatures on adjacent edges (i,j) and (j,k), anyone with public information can compute a signature on edge (i,k). The efficiency advancement ($O(1)$ communication overhead) in transitive signatures is especially important in big data paradigm. On the other side, it is universal designated verifiable: It allows any signature holder to prove to a designated verifier that a message has been signed by the signer, but the verifier cannot convince (even sharing all secret information) any other third party of this fact. The new notion is called Universal Designated Verifier Transitive Signatures (UDVTS for short). As an integration of transitive signatures and universal designated verifier signatures, UDVTS can efficiently address privacy issues associated with dissemination of transitive signatures of graph-based big data. We further prove that our proposed design is secure in the random oracle model.

1. Introduction

According to the research by MGI and McKinsey's Business Technology Office [22], *"The amount of data in our world has been exploding, and analyzing large data sets – so-called big data – will become a key basis of competition, underpinning new waves of productivity growth, innovation, and consumer surplus."* As the volume of data becomes larger, it is more difficult to process or analyze. This is understandable as the speed of data increment is a lot faster than the increment of the machine processing speed, as stated by IBM [18]. This is mainly due to the rapid exploiture of various pervasive hand-held devices and mobile social networks. Thus the traditional approach to manage or analyze data may not work in the big data era. Mechanisms should be specifically designed for big data in order to work efficiently. This create great challenges for scientists and researchers to re-design various tools suitable for this era.

* Corresponding author at: Fujian Provincial Key Laboratory of Network Security and Cryptology, School of Mathematics and Computer Science, Fujian Normal University, China.
E-mail address: xyhuang81@gmail.com (X. Huang).

http://dx.doi.org/10.1016/j.ins.2015.02.033
0020-0255/

Among all areas in big data, security is one of the most important issues that takes precedence over the others. Without security, privacy will be lost and sensitive data will be leaked. Un-authenticated entity may break into the system and does whatever he likes. Hence security mechanism is an essential ingredient in implementing every big data system.

In this paper, we narrow the problem into the authentication of graph-based big data. We consider the big data system is formed by a set of administrative domain and is represented by a graph. The vertices represent computers and an edge (i,j) means that i and j are in the same administrative domain. It is clear that if i and j are in the same administrative domain, and if j and k are in the same administrative domain, then i and k are in the same administrative domain. Thus, transitive undirected graphs represent equivalence relations. Fig. 1 provides a system overview of our concern.

Now, someone wishes to publish a transitive graph which allows others to know that they are working with authentic components of the graph.

1. Sign the Entire Graph: One could just sign a representation of the entire graph as a single signed message. However, this approach may be awkward in practice if the graph grows frequently or the components are large. Unfortunately, these are the usual cases in big data paradigm! Regarding the efficiency of representation, we observe that a graph with n vertices may have $O(n^2)$ edges. That means the signing complexity of the above naive method is $O(n^2)$ (e.g., one signature for one edge), though the communication overhead is a constant (e.g., only one signature to prove there is an edge between two nodes).
2. Sign the Transitive Reduction: Because we are focussing on the situation where the graph is transitive, the signer need only sign the transitive reduction which has the minimum subset of edges with the same transitive closure as the intended graph. In this case, the signer only needs to sign no more than $O(n)$ edges. To this point, it seems that this alternative solution is a perfect replacement of the naive method mentioned at the beginning. However, to prove there is an edge between two nodes, one may need to present all edge signatures on the path between two nodes on the transitive reduction, which would lead to two issues: (1) the growth in signature size and (2) the loss of privacy incurred by having signatures carry information about their history.
3. Transitive Signature: Transitive signatures solve this issue in such a way that given two signatures on adjacent edges (i,j) and (j,k), anyone with the signer's public key can compute a signature on edge (i,k). Thus, one can calculate an edge signature for two nodes as long as there is a path between those two nodes on the transitive reduction. This leads to the signing complexity as $O(n)$ and the communication complexity as $O(1)$. As introduced by Micali and Rivest [23], transitive signatures can be used to authenticate undirected graphs (in which (i,j) and (j,i) represent the same edge and thereby have the same edge signature) and directed graphs (in which (i,j) and (j,i) represent distinct edges and thereby have distinct edge signatures).

Table 1 shows the comparison among the three mentioned approaches, and a thorough study can be found in [23]. We compare the overall signing complexity and the communication overhead to represent a signature for an edge connected with any two transitive vertices. We note that the efficiency advancement in transitive signature is especially important in big data paradigm.

Universal designated verifier signatures. Universal designated verifier signatures (UDVS for short), first introduced by Steinfeld et al. [27] in 2003, is an efficient method to protect the privacy of the signature holder from dissemination of signatures by verifiers. Given a publicly verifiable signature from the signer, a signature holder can transform it into a UDVS for any desired designated verifier, who can be convinced that the message has been signed by the signer. However, any other third party cannot believe it because the designated verifier can use his/her private key to create a valid UDVS, which is indistinguishable from the one created by the signature holder. Therefore, one cannot distinguish whether the UDVS is created by the signature holder or by the designated verifier.

Motivation. As introduced in [23], transitive signatures for undirected graphs can be used to authenticate administrative domains, where vertices represent computers and an undirected edge (i,j) means that i and j are in the same administrative domain. Now, we assume Alice's computer and Bob's computer are in the same administrative domain. Then, Alice receives a transitive signature from the signer, which can prove that their computers are in the same administrative domain. We are interested in such a situation where Alice wishes to send a transitive signature to Cindy (not in the same administrative domain with Alice) to state that her computer and Bob's computer are in the same administrative domain, but she does not wish Cindy to convince any third party about the truth of this message (maybe due to some contract agreement, some political reasons, or privacy concerns). Situations like this call for the need of Universal Designated Verifier Transitive Signatures. It is normal that this computing domain will be very big (e.g. if the unit of the administrative domain is a country). Thus transitive signature should be a good candidate to tackle this problem as we have discussed above.

1.1. Our contributions

The contributions of this paper lie in the following aspects:

1. We integrate the notions of transitive signatures and UDVS, and propose a new type of digital signatures called Universal Designated Verifier Transitive Signatures (UDVTS) which is particularly suitable for graph-based big data system.