Revisiting Colored Networks and Privacy Preserving Censorship

Yvo Desmedt[1,3,⋆], Yongge Wang[2], and Mike Burmester[3,⋆⋆]

[1] University College London, UK
y.desmedt@cs.ucl.ac.uk
[2] UNC Charlotte, USA
yonwang@uncc.edu
[3] Florida State University, USA
burmester@cs.fsu.edu

Abstract. Reliable networks are obviously an important aspect of critical information infrastructures. *Dolev-Dwork-Waarts-Yung* linked research on reliable point-to-point networks with privacy and authenticity. In their threat model the adversary can only take over a number of nodes bounded by a threshold k. Hirt-Maurer introduced the concept of an adversary structure (i.e. the complement of an access structure). Kumar-Goundan-Srinathan-Rangan and Desmedt-Wang-Burmester generalized Dolev-Dwork-Waarts-Yung scenarios to the case of a general adversary structure.

Burmester-Desmedt introduced a special adversary structure, now called a color based adversary structure. Their argument in favor of their model is that using automated attacks (such as worms), a vulnerability can be exploited on all computers in the network running the same platform (color). In their model the adversary can control all nodes that use up to k different platforms (or colors).

We will demonstrate one of the limitations of their model. Although the family of color based adversary structures has a trivial representation which size grows polynomial in the size of the graph, we will demonstrate in this paper that deciding reliability issues and security issues are co-**NP**-complete.

In most societies censorship is common. Indeed, for centuries it has often been viewed by authorities as an essential security tool. We apply the computational complexity result to study censorship. Authorities may require network designers to demonstrate the capability to censor the internet. We present a zero-knowledge interactive proof for the case of a color based adversary structure.

Keywords: network security, Byzantine threats, secret sharing, adversary structure, censorship, unconditional security, zero-knowledge.

⋆ A part of this work has been funded by CCR-0209092. The author is BT Professor of Information Security. He is also courtesy professor at Florida State University.
⋆⋆ A part of this work has been funded by CCR-0209092.

J. Lopez (Ed.): CRITIS 2006, LNCS 4347, pp. 140–150, 2006.

1 Introduction

The research on how to achieve reliable networks is well known [11,20]. After Dolev-Dwork-Waarts-Yung [12] extended the research on reliable networks by also addressing privacy issues, a lot of research has been done on this topic (see e.g. [15,1,13,27,9,23,2,7,8]). This research has been partially motivated by the importance of securing networks both against a denial of service attack as well how to achieve privacy and authenticity at the same time.

Another important issue is to guarantee that the infrastructure built cannot be exploited to undermine society. Although, the topic of censorship is taboo in the West, it has been used extensively during centuries. There are many examples over the centuries, and even today, that censorship was used in Western societies. As a first example, consider the recently recovered "Gospel of Judas" [24]. It has been used as an occasion to reflect back on how the church censored "non-traditional" gospels [19]. As a second example, today in many countries books remain censored. A well known example is Hitler's "Mein Kampf." As a third example, in the US, the Rolling Stones performance during the 2006 superbowl on February 5 was censored. Finally, texts describing in details the construction of atomic bombs, or other classified information, are also censored.

Whether censorship in a limited format is in the benefit of mankind or not, is a non-scientific topic, and therefore not discussed. Information, such as books, are passed on through a network, e.g. a distribution network, involving bookstores, etc. The communication of gossip can be modeled using social networks [26]. Whether the edges in this network are virtual or physical communication links seems irrelevant. However, as we now discuss, this conclusion may be wrong.

In the *classical model* for communication networks nodes are treated equally. So when a limited adversary (or a censor in our prior example) wants to undermine communication, it is natural to assume that there is an upperbound k of the number of nodes the adversary (or censor) can control. The first to dispute this homogeneous viewpoint was Hirt and Maurer [21]. Their paper introduces the concept of an adversary structure (i.e. the complement of an access structure [22]). An adversary structure is a list of subsets the adversary can control. Before performing the attack the adversary must choose one of these subsets. However, Hirt and Maurer do not specify how to choose such an adversary structure. Burmester-Desmedt [5] introduced a method to address this, we now discuss. Burmester-Desmedt partition the nodes in a network based on the platform used to operate the node, e.g. the router. The mapping from node to platform is modeled using a node coloring. To take into account the ease of automated attacks using computer viruses and worms, they view that the difficulty for an adversary to control one node running one platform is approximately the same as the difficulty to control all nodes running the same platform. A limited adversary corresponds in their setting to one that can control all nodes that have up to k different colors. The resulting adversary structure is called a color based adversary structure.

We believe that color based adversary structures are worth studying in more details for the following reasons: