Brief Announcement: Byzantine Agreement with Homonyms

Carole Delporte-Gallet
LIðA, Université Paris Diderot
cd@liafajussieu.fr

Hugues Fauconnier
LIðA, Université Paris Diderot
hf@liafajussieu.fr

Rachid Guerraoui
Ecole Polytechnique Fédérale de Lausanne
Rachid.Guerraoui@epfl.ch

Anne-Marie Kermarrec
INRIA Rennes
Anne-Marie.Kermarrec@inria.fr

ABSTRACT
In this work, we address Byzantine agreement in a message passing system with homonyms, i.e., a system with a number \( l \) of authenticated identities that is independent of the total number of processes \( n \), in the presence of \( t < n \) Byzantine processes.

We prove the following results: (i) agreement is possible if (and only if) \( l > 3t \) in a synchronous model; (ii) agreement is impossible, independently of the number of failures, in an eventually synchronous model; (iii) eventual agreement is possible, if (and only if) \( l > 3t \), in an asynchronous model.

Categories and Subject Descriptors

General Terms
Algorithms, Theory, Reliability

Keywords
Consensus, Message-Passing, Byzantine Agreement, Authentication.

1. INTRODUCTION
We study Byzantine agreement in a message passing system with a limited number of authenticated identities, i.e., a system with homonyms. Basically, there is a set of \( l \) different identities used to identify processes. This set can be much smaller than the set of processes and hence several processes may have the same identity. Such processes can be considered as homonyms. Identities are authenticated in the sense that if a process \( p \) receives a message from a process \( q \) with identity \( id \), \( p \) knows that the message does not come from a process with name \( id' \neq id \). The message could however come from a homonym process \( q' \neq q \), also with identity \( id \).

In this context, we ask whether Byzantine agreement can be solved if \( l \) is independent of the total number of processes \( n \). Beyond intellectual curiosity, the motivation of addressing this question is twofold.

Firstly, the assumption, underlying many distributed systems, e.g. [12, 14], that all processes have unique (unforgeable) identities might, we believe, be considered too strong. More specifically, authenticated unique identities are typically achieved through collision-free hash functions. Yet, such functions are potentially breakable, e.g., [15], namely they may lead to the same output with different inputs. Even the ones that have not been broken yet, such as SHA-256, might be in a near future.

Secondly, in many cases, processes (users) do care about their privacy and would rather not reveal their identity. In a fully anonymous system where processes do not have identities [2], reaching agreement is simply impossible in the face of Byzantine players. With a limited number of identities, one can preserve some level of anonymity and hide, to some extent, the association between every user and every identity. A limited number of identities, may render some agreement possible, as we will show in the sequel.

2. RESULTS
Assuming a system of \( n \) processes, \( t \) potential Byzantine failures and \( l \) identities, we prove the three following main results:

1. In a synchronous model [9], Byzantine agreement is possible if (and only if) \( l > 3t \). This result is to be contrasted with the classical impossibility of Byzantine agreement if \( n \leq 3t \): in a sense, we show that what really matters is the ratio between the number of Byzantine processes and the number of authenticated identities rather than the one between the number of Byzantine processes and the total number of processes.

We prove the existence of our algorithm by simulation: we show how to transform any synchronous Byzantine agreement protocol, where all processes have uniquely authenticated identities (i.e., \( n = l \), into a Byzantine agreement protocol using only \( l \) (\( n \geq l > 3t \)) au-
thenticated identities. In short, we do so by adding a communication round between any two communication rounds of the original agreement protocol. The added rounds are used by the processes with the same identities to agree on the same message to send in the next round of the original protocol.

2. In an eventually synchronous model [5] agreement is impossible. More specifically, we show, using a partitioning argument, that processes can decide on different values if \( n \geq 3l \). The proof does not require any failure, which might be surprising at first glance.

Interestingly, this highlights the very fact that, in a setting with limited identities, the demarcation line between the possibility and impossibility of agreement is different that in a model where all processes have identities [6].

3. In an asynchronous model, eventual agreement is possible, if (and only if) \( l > 3t \). In eventual agreement (also called stabilizing consensus [1]), processes can decide several times, possibly on different values, but eventually converge to the same value.

We first present a binary eventual agreement protocol and then show how to use a transformation close to [2, 10] to obtain a multi-valued agreement.

3. CONCLUDING REMARKS

To the best of our knowledge, this paper is the first to study a distributed system model with a limited number of identities, i.e., homonyms. In a sense, the model unifies both classical non-anonymous [3, 9] and anonymous models [1, 2, 4, 7, 8, 11, 13]. As we argued in the introduction, we believe this model to be interesting for both intellectual and practical considerations.

While studying the spectrum of possibilities for Byzantine agreement in a system with homonyms, we shed a different light on this problem. Whereas the traditional agreement impossibility result holds only in a fully asynchronous model only, we show than in a system with homonyms, the impossibility holds as soon as there is some (even partial) asynchrony. In addition, in a synchronous setting, the relevant crucial ratio turns out to be between the number of identities \( l \) and the number of Byzantine processes \( t \), while the classical result considers a ratio between \( n \) and \( t \).

It is important to note that we only scratched the surface of what can be computed with homonyms: many challenging issues are open. For instance, we considered a message passing model and it would be interesting to explore the impact of a shared memory. Also, we focused on agreement and many other problems should be considered. Finally, we focused on computability, complexity is yet to be explored.

Acknowledgments

We are grateful to Christian Cachin for his useful comments on our model with homonyms and to the reviewers for their helpful comments.

4. REFERENCES