ETH zürich Research Collection

Doctoral Thesis

Generalized communication and security models in Byzantine agreement

Author(s):
Fitzi, Matthias

Publication Date:
2002

Permanent Link:

https://doi.org/10.3929/ethz-a-004521924 →

Rights / License:

In Copyright - Non-Commercial Use Permitted →

This page was generated automatically upon download from the ETH Zurich Research Collection. For more information please consult the Terms of use.

ETH Library

Diss. ETH No. 14761

Generalized Communication and Security Models in Byzantine Agreement

A dissertation submitted to

ETH ZÜRICH
(SWISS FEDERAL INSTITUTE OF TECHNOLOGY)

for the degree of
Doctor of Technical Sciences

presented by

Matthias Fitzi
Dipl. Informatik-Ing. ETH

born April 29, 1970, in Basel
citizen of Gais AR, Switzerland

Prof. Dr. Ueli Maurer, examiner
Dr. Michael Waidner, co-examiner

2002

Abstract

Byzantine agreement (BA) is a primitive of fundamental importance for fault-tolerant distributed computing and cryptographic protocols. BA among a set of n players allows them to reach agreement about a value even if some of the players are malicious and try to prevent agreement among the non-faulty players by distributing false information.

Since the initial statement of the BA problem, a small number of widely accepted standard models have established, distinguishing between aspects such as what means of communication are given among the players or how powerful the faulty players are. Both in research on Byzantine agreement and its applications, these standard models are obstinately followed.

Besides a selective overview on some standard models in Byzantine agreement, this thesis gives a broader view on the problem by considering natural generalizations of these models and generalizations of the problem definition itself. Thereby the main focus is on synchronous networks and active adversaries. It turns out that some of these generalizations, without restricting the adversarial power, allow for BA protocols that achieve a level of security that is provably unachievable in their corresponding standard models. The main contributions are described in the following paragraphs whereby n denotes the number of players and t the number of cheaters among the players.

Security. Standard BA provides either unconditional or computational security. Unconditionally secure protocols for BA are provably secure but can only tolerate a relatively small number of cheaters, typically $t < n/3$. Computationally secure ones often tolerate any number of cheaters, $t < n$, but their security is based on unproven intractability assumptions. So far, every previous computationally secure protocol from the literature has the property that, in case its underlying intractability assumption is

false, it does not withstand one single cheater, $t = 0$. In contrast, we show that computational and unconditional security can be combined by presenting protocols computationally secure against some large number t_1 of cheaters but, at the same time, still unconditionally secure against some smaller number $t_0 > 0$ of cheaters. It is shown that BA of this flavor is achievable if and only if $2t_0 + t_1 < n$ and $t_1 \geq t_0$.

Communication. Standard communication models assume either pairwise authenticated or pairwise secure channels among the players. In these models, unconditional BA is achievable if and only if $t < n/3$. A natural generalization of these models is to assume partial broadcast among the players to be possible, i.e., that for some number $b \geq 2$, broadcast is achievable among each set of b players. It is shown that for any b, $2 \leq b \leq n$, BA is achievable if and only if $t < \frac{b-1}{b+1}n$.

New threshold paradigm. The security of standard BA is defined with respect to one threshold t meaning that BA is achieved in the presence of up to $f \leq t$ cheaters but that no security is guaranteed at all if $f > t$. In particular, unconditionally secure protocols are completely insecure in the presence of $f \geq n/3 > t$ cheaters. However, in reality, nothing would really guarantee that $f \leq t$ and thus the usefulness of non-fully resilient protocols is questionable. Preferably, a non-fully resilient protocol should guarantee BA for some threshold t — but in case that more than t players are cheating, $f > t$, and BA cannot be achieved, it should be guaranteed that all players safely abort the protocol in unison. We show that this is possible if and only if $t = 0$. More generally, we introduce the notion of two-threshold BA, involving two different thresholds t_v and t_c: if at most t_v players cheat then the "validity condition" of BA is achieved and, if at most t_c players cheat then the "consistency condition" of BA is achieved. We show that two-threshold BA is achievable if and only if both $t_v + 2t_c < n$ and $2t_v + t_c < n$, or $t_v = 0$, or $t_c = 0$.

Zusammenfassung

Byzantine Agreement (BA) ist eine Primitive von fundamentaler Wichtigkeit für fehlertolerante verteilte Berechnungen oder kryptographische Protokolle. BA unter n Spielern erlaubt ihnen, sich auf einen Wert zu einigen, auch wenn einige der Spieler betrügerisch sind und versuchen, durch das Versenden falscher Information zu verhindern, dass sich die ehrlichen Spieler auf den selben Wert einigen.

Seit der Erstformulierung des BA-Problems hat sich eine kleine Zahl weit akzeptierter Standardmodelle etabliert, die Aspekte wie Mächtigkeit der Betrüger oder Art der Kommunikation zwischen den Spielern unterscheidet. In der Erforschung von Byzantine Agreement und dessen Anwendungsgebieten werden diese Standardmodelle stur verfolgt.

Nebst einer selektiven Übersicht solcher Standardmodelle für BA bietet diese Dissertation eine umfassendere Sicht auf das Problem, indem natürliche Verallgemeinerungen dieser Modelle und auch der Problemstellung selbt untersucht werden. Von Hauptinteresse sind dabei synchrone Netzwerke und aktive Gegner. Es stellt sich heraus, dass gewisse dieser Verallgemeinerungen, ohne dabei die Macht des Gegners einzuschränken, BA-Protokolle ermöglichen, deren Sicherheitsniveau im entsprechenden Standardmodell beweisbar unmöglich ist. Die Hauptbeiträge dieser Dissertation sind in den folgenden Abschnitten beschrieben. Dabei sei n die Anzahl der Spieler und t die Anzahl der Betrüger unter den Spielern.

Sicherheit. Standard-BA bietet entweder unbeschränkte oder berechenmässige Sicherheit. Unbeschränkt sichere BA-Protokolle sind beweisbar sicher, können aber nur verhältnismässig wenige Betrüger tolerieren, üblicherweise $t < n/3$. Berechenmässig sichere Protokolle tolerieren häufig beliebig viele Betrüger, $t < n$, aber deren Sicherheit basiert auf unbewiesenen Schwierigkeitsannahmen. Jedes bisherige solche Protokoll

aus der Literatur hat die Eigenschaft, dass es keinen einzigen Betrüger toleriert, $t = 0$, falls die zu Grunde liegende Schwierigkeitsannahme falsch ist. Im Gegensatz dazu zeigen wir, dass berechenmässige und unbeschränkte Sicherheit kombiniert werden können, indem wir Protokolle präsentieren mit berechenmässiger Sicherheit gegen eine grössere Zahl t_1 von Betrügern und zusätzlicher unbeschränkter Sicherheit gegen eine kleinere Anzahl $t_0 > 0$ von Betrügern. Es wird gezeigt, dass BA dieser Art genau dann möglich ist, wenn $2t_0 + t_1 < n$ und $t_1 \geq t_0$ gilt.

Kommunikation. Standard-Kommunikationsmodelle setzen entweder paarweise authentische Kanäle oder paarwiese sichere Kanäle unter den Spielern voraus. In diesen Modellen ist unbeschränkt sicheres BA genau dann möglich, wenn $t < n/3$ gilt. Eine natürliche Verallgemeinerung besteht daraus, partiellen Broadcast unter den Spielern vorauszusetzen, d.h., dass für eine bestimmte Zahl $b \geq 2$ Broadcast unter jeder Menge von b Spielern möglich ist. Es wird gezeigt, dass für beliebiges b, $2 \leq b \leq n$, BA genau dann möglich ist, wenn $t < \frac{b-1}{b+1}n$.

Neues Schwellen-Paradigma. Die Sicherheit von Standard-BA ist bezüglich einer Schwelle t definiert mit der Bedeutung, dass BA erreicht wird, falls bis zu $f \leq t$ Betrüger unter den Spielern sind, dass aber nicht die geringste Sicherheit garantiert ist, falls $f > t$. Insbesondere sind unbeschränkt sichere Protokolle völlig unsicher, falls $f \geq n/3 > t$ Betrüger anwesend sind. In der Realität würde jedoch nichts garantieren, dass tatsächlich nur $f \leq t$ Spieler betrügen, und deshalb ist der Nutzen von Protokollen, die nicht beliebig viele Betrüger tolerieren, fragwürdig. Vorzugsweise sollte ein solches Protokoll für eine bestimmte Schwelle t BA erreichen aber im Falle, dass mehr als t Spieler betrügen, $f > t$, und BA nicht erreicht werden kann, sollte garantiert sein, dass alle Spieler zusammen das Protokoll wohlbehalten abbrechen. Es wird gezeigt, dass dies genau dann möglich ist, wenn $t = 0$. Allgemeiner noch wird der Begriff des Zwei-Schwellen-BA eingeführt, das bezüglich zweier Schwellen t_v und t_c definiert ist: falls höchstens t_v Spieler betrügen, erreicht das Protokoll die "Validity-Bedingung" von BA, und falls höchstens t_c Spieler betrügen, errreicht das Protokoll die "Consistency-Bedingung" von BA. Es wird gezeigt, dass Zwei-Schwellen-BA genau dann möglich ist, wenn $t_v + 2t_c < n$ und $2t_v + t_c < n$ gilt, oder $t_v = 0$, oder $t_c = 0$.