Byzantinische Fehler

Matthias Reumann

7. April 2020

Inhaltsverzeichnis

1 Problem der byzantinischen Generäle

Mehrere Truppen mit jeweils einem General umzingeln eine feindliche Stadt und kommunizieren direkt über Boten miteinander. Jeder der Generäle beobachtet den Feind und schlussendlich müssen die Generäle eine gemeinsame Entscheidung treffen. Jedoch kann es unter den Generälen Verräter geben, deren Ziel es ist eine gemeinsame Entscheidung der loyalen Generäle zu unterbinden.

Die Generäle müssen einen Algorithmus finden der garantiert, dass

(a) Alle loyalen Generäle die gleiche Entscheidung treffen

(b) Eine geringe Anzahl an Verrätern die loyalen Generäle nicht zu einer Fehlentscheidung führt

Eine Entscheidung unter den Generälen wird gefällt indem jeder General den Feind beobachtet und seine Informationen an die anderen Generäle weitergibt. *v(i)* ist die Nachricht gesendet vom i.ten General. Jeder General erhält die Nachrichten *v(1)* bis *v(n)*, wobei n die Anzahl der Generäle darstellt. Die finale Entscheidung wird durch die absolute Mehrheit der Werte dieser Nachrichten bestimmt. Allerdings könnte es sein, dass loyale Generäle unterschiedliche *v(i)* erhalten, da ein Verräter unterschiedliche Werte zu unterschiedlichen Generälen sendet, was widerum Punkt A widerspricht.

Deshalb müssen sogennante *interactive consistency*-Bedingungen gelten. Ein führender General, auch Commander gennant, sendet einen Befehl an seine $n-1$ Leutnant Generäle so, dass:

IC1 Alle loyalen Leutants den gleichen Befehl ausführen
IC2 Wenn der Commander loyal ist, dann befolgt jeder loyale Leutnant seinen Befehl

In Abbildung 1 wird die Situtation beschrieben, in der Leutnant 2 der Verräter ist. Dabei sendet der loyale Commander den Befehl *ANGRIFF* an beide Leutnants. L2 sendet L1 die Nachricht, er habe den Befehl *RÜCKZUG* erhalten. Um IC2 zu erfüllen, muss L1 jedoch den Befehl des Commanders ausführen.

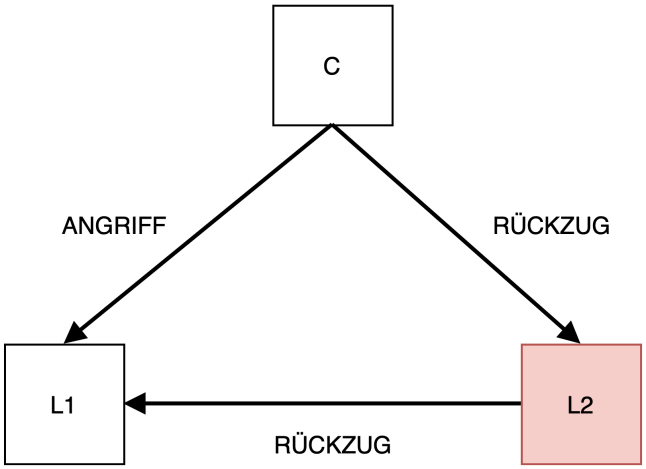

Abbildung 1: todo

Im nächsten Szenario (Abbildung 2) ist der Commander der Verräter. Dieser sendet unterschiedliche Befehle an seine Leutnants. Für L1 ist es die exakt selbe Situation wie in Abbildung 1 beschrieben: Um IC2 zu erfüllen muss er den Befehl *ANGRIFF* ausführen.

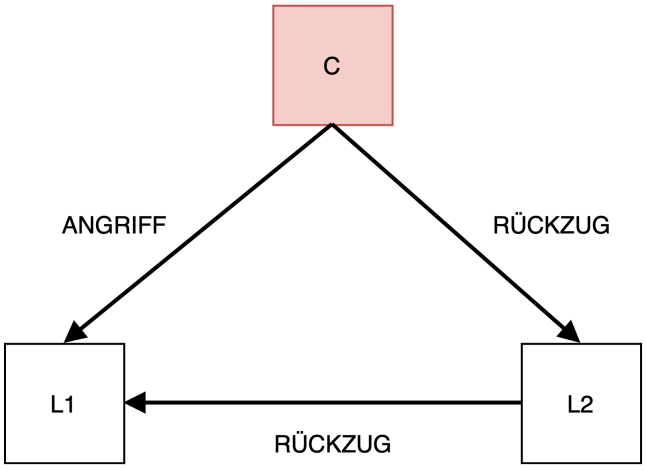

Abbildung 2: todo

Hierbei liegt aber das Problem. Die gleiche Argumentation muss demnach für L2 verwendet werden, der den Befehl *RÜCKZUG* ausführt. Dies widerspricht jedoch IC1. Es existiert daher keine Lösung für drei Generäle mit einem Verräter.