

Informatik I: Einführung in die Programmierung

23. Kleiner Exkurs: Daten-Übertragungen über unzuverlässige Medien

Albert-Ludwigs-Universität Freiburg



**UNI
FREIBURG**

Bernhard Nebel

16. Januar 2018

1 Motivation



**UNI
FREIBURG**

Motivation

Das Problem
der zwei
Generäle

- Wir wollen ein **verteiltes System**/Spiel implementieren, bei denen die Radio-Schnittstelle des micro!bit als Kommunikationskanal dienen soll.
- Man könnte annehmen, dass dieser Kommunikationskanal **zuverlässig** ist (und alle gesendeten Nachrichten überträgt).
- Ist er aber nicht.
- Es können **Nachrichten verloren** gehen!
- Können wir aus einem unzuverlässigen nicht einen zuverlässigen Kommunikationskanal machen?

2 Das Problem der zwei Generäle



**UNI
FREIBURG**

Motivation

Das Problem
der zwei
Generäle



- Zwei byzantinische Generäle liegen mit ihren Armeen vor Konstantinopel (so um 1453 herum), und können die Stadt nur besiegen, wenn sie zur gleichen Zeit losschlagen.
- Sie können sich nur indirekt über Boten unterhalten, die vom Gegner **abgefangen** werden können.
- Gibt es eine Möglichkeit für sie, sich so abzusprechen, dass sie beider sicher sein können, dass sie beide gleichzeitig losschlagen.

- General A schickt General B eine Nachricht, morgen um 11 Uhr loszuschlagen.
- Er wird aber nur angreifen, wenn er sich 100% **sicher** ist, das der andere auch angreift, und wartet deshalb auf eine Bestätigung.
- Wenn General B die Nachricht erhält, wird er eine Bestätigung schicken.
- B wird aber nur angreifen, wenn er weiß, dass auch General A angreift, er also weiß, dass die Bestätigung angekommen ist.
- Deshalb wird A die Bestätigung bestätigen.
- A wird aber nur angreifen, wenn er weiß, dass B angreift, d.h. die Bestätigung der Bestätigung erhalten hat.
- ...

Motivation

Das Problem
der zwei
Generäle

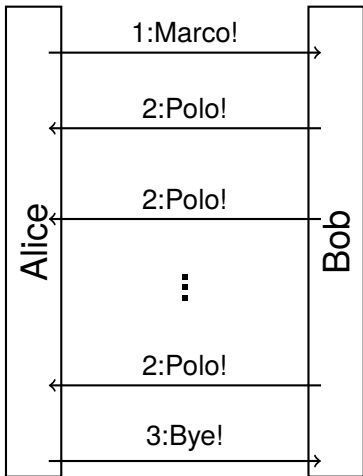


- Die Generäle müssen offensichtlich unendlich oft sich gegenseitig bestätigen um sich 100% sicher zu sein, dass sie tatsächlich koordiniert attackieren.
- Tatsächlich ist beweisbar, dass kein **gemeinsames Wissen** aufbaubar ist.
- Allerdings benötigt man das auch nicht immer.
- Oft reicht zu wissen, dass meine Nachricht angekommen ist.

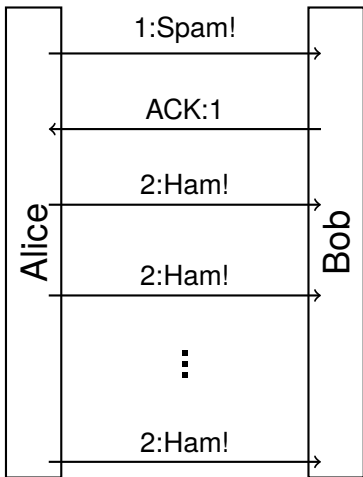
- Wenn man keine koordinierte Aktion vereinbaren will, sondern nur dafür sorgen will, dass der andere einen nicht stört, dann reicht, dass ich weiß, dass der andere meine Nachricht erhalten hat.
- General A schickt eine Nachricht, dass er morgen um 11 Uhr angreifen will und dass der andere General bitte **nicht** zur gleichen Zeit aktiv werden soll.
- General B empfängt die Nachricht und sendet eine Bsetzung.
- Kommt die bei A an, kann er beruhigt die Attacke beginnen (wobei B nicht weiß, ob seine Bestätigung angekommen ist).

Motivation

Das Problem
der zwei
Generäle



- Idee: Man schickt immer seinen eigenen Zug und wartet dann auf den Gegenzug des Mitspielers, was gleichzeitig die Bestätigung der eigenen Nachricht ist.
- Da man bis zu dieser Bestätigung nicht weiß, ob der eigene Zug angekommen ist, schickt man ihn wiederholt.
- Erhält man den nächsten Zug, kann man ab da auch wieder eine neue Nachricht schicken.



- Der Erhalt einer Nachricht wird **immer** bestätigt (acknowledgment)
- Wurde die letzte Nachricht bestätigt, kann die nächste Nachricht gesendet werden.
- Unbestätigte Pakete werden in Intervallen erneut gesendet.
- Vermeidet überflüssige Wiederholungen.



- Über unzuverlässige Leitungen ist kein **gemeinsames Wissen** aufbaubar.
- Man kann aber garantieren, dass der Sender weiß, dass seine Nachricht angekommen ist.
- Das ist i.W. ausreichend, um ein ein verteiltes Spiel zu realisieren.