FORSCHUNGSPROJEKT WS21/22

FORMAL VERIFIZIERTE FIREWALL-OPTIMIERUNG

Samuel Müller

HOCHSCHULE ESSLINGEN

Nah an Mensch und Technik.

1. Einleitung

In automatisierten Fertigungsanlagen sind Verzögerungen bei der Übertragung von zeitkritischen Steuerungsdaten für Roboter sehr problematisch. Unter anderem können Sicherheitsmaßnahmen wie Firewalls für solche Verzögerungen verantwortlich sein. [1]

Die Zielsetzung dieses Projektes ist es die Leistung von Firewalls für solche Anlagen zu optimieren, ohne deren Semantik zu verändern.

Da die Optimierung nach der Zertifizierung eines Auditors automatisiert erfolgt, ist ein formaler Beweis für den Funktionserhalt der Firewall zwingend notwendig.

2. Firewall-Regeln

Das Verhalten einer Firewall wird durch eine Vielzahl verschiedener Regeln – einem Regelsatz – bestimmt. Welche Regel mit welchem Paket auf welche Weise interagiert wird durch deren Parameter und Aktion bestimmt. [2]

Darüberhinaus sind folgende Beobachtungen für dieses Projekt von Relevanz:

- Wie lange eine Firewall benötigt, um ein Paket zu verarbeiten, hängt von der Position der auf das Paket zutreffenden Regel innerhalb des Regelsatzes ab.
- Solange ausschließlich Regeln derselben Aktion aufeinander folgen, können diese untereinander beliebig verschoben werden. In diesem Projekt werden solche Mengen an Regeln als Regelgruppe bezeichnet. (Andere Regelparameter können hierbei auch ausschlaggebend sein, werden in diesem Projekt allerdings vorerst nicht mit in die Gruppenbildung einbezogen.)

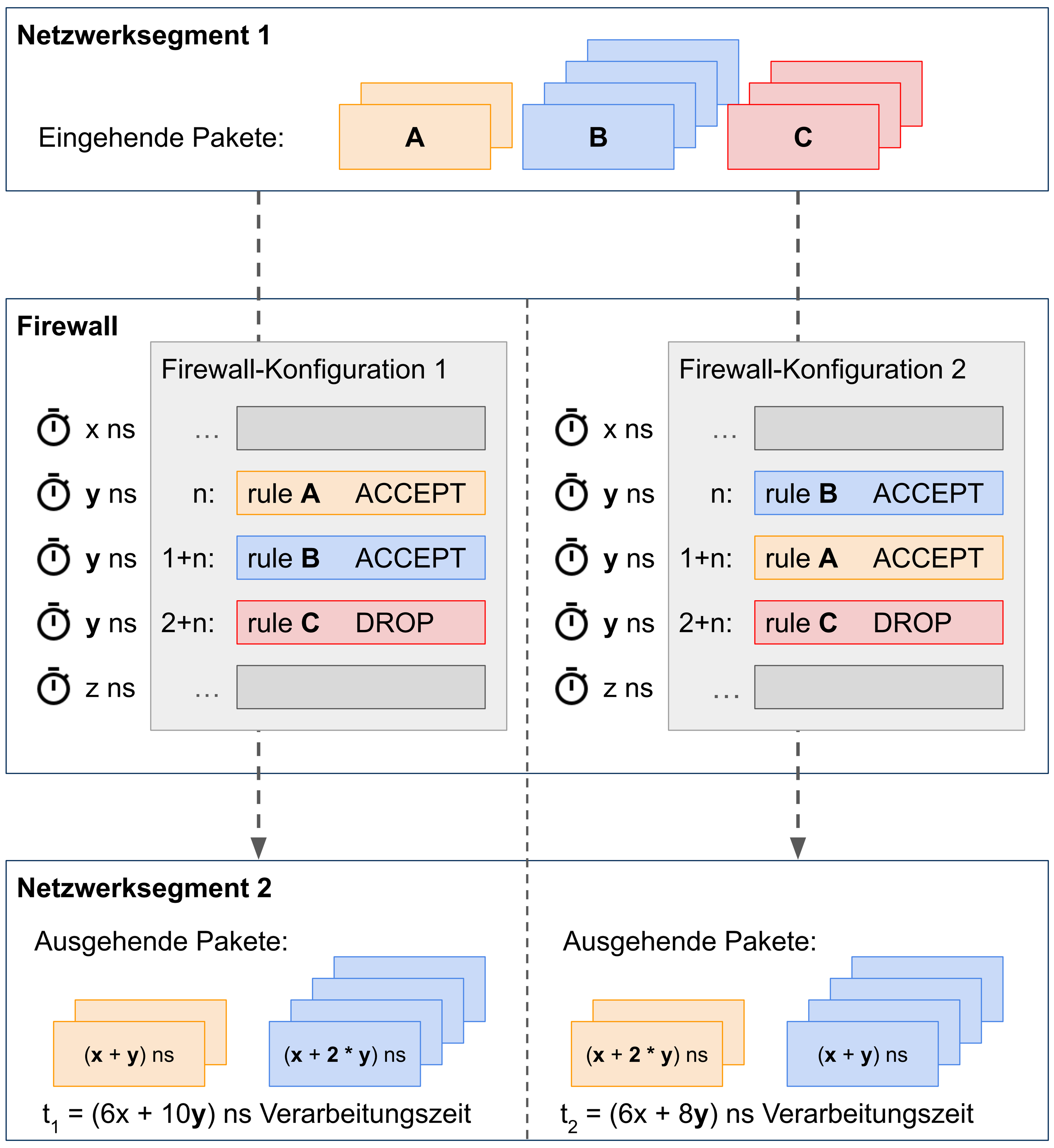

Abbildung 1: Aufruforientiertes Umsortieren von Firewall-Regelsätzen zur Minimierung der Verarbeitungszeit

3. Umsetzung (erklärt anhand Abbildung 1)

Testdaten, Leistungsmessung und Optimierung

1. Testpakete für Testszenario erzeugen.
2. Trefferzahl jeder Regel für Testpakete aus Testszenario auswerten.
3. Manuelles Erstellen eines Iptables-Datensatzes durch Modifizierung des Originals, wobei Regeln innerhalb einer Regelgruppe nach Trefferzahl absteigend sortiert werden.

Original mit Trefferzahlen

Iptables-Exportdatei

```
:FORWARD REJECT
...
-A FORWARD -d [...] -j ACCEPT
(Trefferzahl: 1)
-A FORWARD -s [...] -j ACCEPT
(Trefferzahl: 4)
-A FORWARD -s [...] -j DROP
(Trefferzahl: 3)
...
```

Optimierung mit Trefferzahlen

Iptables-Exportdatei

```
:FORWARD REJECT
...
-A FORWARD -s [...] -j ACCEPT
(Trefferzahl: 4)
-A FORWARD -d [...] -j ACCEPT
(Trefferzahl: 1)
-A FORWARD -s [...] -j DROP
(Trefferzahl: 3)
...
```

Formaler Beweis der Äquivalenz mit Isabelle [3]

1. Parsen der beiden Iptables-Exportdateien.
2. Gruppieren der Regeln je Datensatz nach ihrer Kette und Aktion zu Regelgruppen.
3. Vergleichen der beiden Gruppenstrukturen nach folgenden Eigenschaften:
   a. existierenden Ketten,
   b. der Anzahl an Gruppen pro Kette und
   c. der Größe der bestehenden Gruppen

Prozessiertes und gruppiertes Original

Isabelle-interne Datenstruktur

```
...
(Chain ''FORWARD''),
[Group ''GROUP_ACCEPT_0''
[Rule (Dst ([...])) action.ACCEPT,
Rule (Src ([...])) action.ACCEPT],
Group ''GROUP_DROP_1''
[Rule (Match Src ([...])))
action.DROP]
...
```

Prozessierte und gruppierte Optimierung

Isabelle-interne Datenstruktur

```
...
(Chain ''FORWARD''),
[Group ''GROUP_ACCEPT_0''
[Rule (Src ([...])) action.ACCEPT,
Rule (Dst ([...])) action.ACCEPT],
Group ''GROUP_DROP_1''
[Rule (Match Src ([...])))
action.DROP]
...
```

Analyse der Firewall-Optimierung

1. Messen der benötigten Zeit des originalen Firewall-Regelsatzes für die Verarbeitung der Testpakete.
2. Messen der benötigten Zeit des optimierten Firewall-Regelsatzes für die Verarbeitung der Testpakete.
3. Ist die Verarbeitungszeit des optimierten Regelsatzes für die Testpakete kleiner als die des Originals, wurde die Leistung des Firewall-Regelsatzes optimiert.

4. Ergebnisse & Ausblick

In diesem Semester wurden aktions- und ausführungsbasierte Modifizierungen von Firewalls zur Minimierung der Verzögerungen erfolgreich umgesetzt, wobei der Erhalt der bestehenden Firewall-Semantik mit dem Theorembeweiser Isabelle formal bewiesen wurde.

Im weiteren Verlauf des Projektes soll die Gruppenbildung nicht nur auf Regelaktionen basieren, sondern andere Paketparameter mit einbeziehen. Gruppen werden in Zukunft somit nicht-lineare Abhängigkeiten besitzen, weshalb der Gruppierungsalgorithmus dahingehend optimiert werden muss. Für eine bessere Leistungssteigerung sollen Regeln darüber hinaus unabhängig von ihrer eigenen Regelgruppe verschoben werden. Um die ursprüngliche Semantik beizubehalten, sollen hierfür Helfer-Regeln implementiert werden, was allerdings eine Anpassung des Beweisverfahrens nach sich zieht.

Referenzen:
[1] Wüsteney, L., Menth, M., Hummen, R., & Heer, T. (2021, June). Impact of Packet Filtering on Time-Sensitive Networking Traffic. In 2021 17th IEEE International Conference on Factory Communication Systems (WFCS). IEEE.
[2] ubuntu Deutschland e.V. (2021, December) iptables. in: https://wiki.ubuntuusers.de/iptables/ (Zugriff am 04.02.2022)
[3] Nipkow et al. (2021, January) What is isabelle? in: https://isabelle.in.tum.de/overview.html (Zugriff am 04.02.2022)