Projektvorstellung

Implementierung einer Testsuite zur Untersuchung von Möglichkeiten für DoS-Angriffe auf DTN-Protokollimplementierungen

Tim Krieg,
Tobias Nöthlich,
Florian Richter

Betreuer: Dr.-Ing Marius Feldmann

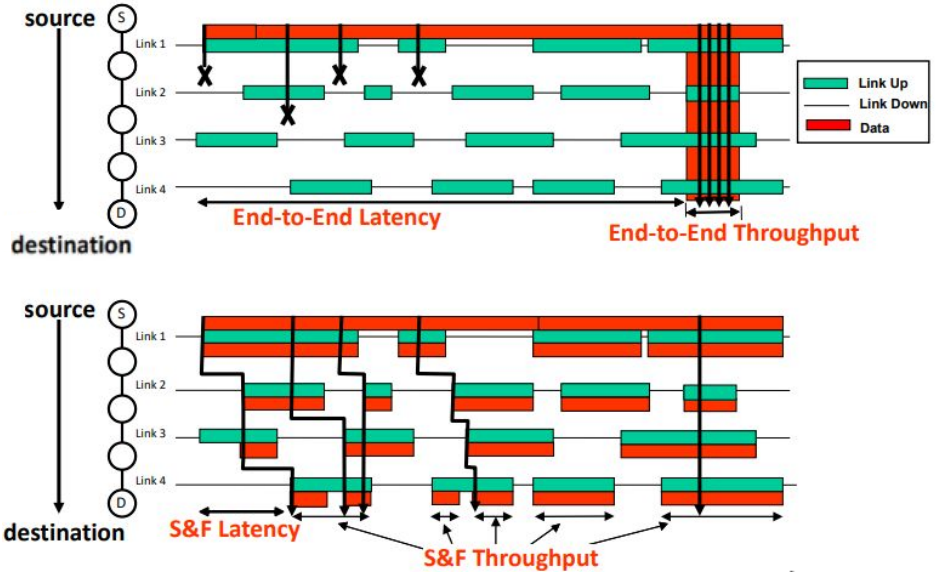
Dresden, 05.02.2021

Delay-Tolerant Networking

Für Verbindungen mit langen und variablen Verzögerungen, asymmetrischen Datenraten und häufigen Disruptionen

Umsetzung mit Datenpaketen (Bundles), die mittels Store-and-Forward von Node zu Node zum Ziel geschickt werden, ohne dass eine Ende-zu-Ende-Verbindung bestehen muss

Anforderungen an Bundle Protokolle vorgegeben durch RFC 4838 und RFC 5050



© NASA, ION IMPLEMENTATION OF THE DTN ARCHITECTURE

Aufgabenbeschreibung

Lokale Untersuchung von Auswirkungen verschiedener Denial-of-Service-Angriffe auf Netzwerke, welche Delay-Tolerant Networking Protokolle einsetzen und Entwicklung eines Toolkits zum Ausführen verschiedener Testszenarien.

Anforderungen

- Das Toolkit soll auf Linux ausführbar sein
- Es sollen verschiedene Szenarien mitgeliefert werden
- Erweiterung um weitere Szenarien muss möglich sein
- Es muss ein Setup beiliegen, um das Toolkit problemlos installieren zu können
- Schreiben einer vollständigen Dokumentation

Herausforderungen im Laufe der Entwicklung

- spärliche Dokumentationen der einzelnen DTN-Implementierungen
- Implementierungen teilweise veraltet und nicht aktiv gepflegt
- automatischer Build und Install der einzelnen Komponenten im Setup-Skript
- Verbindung von ION und CORE, sodass die einzelnen CORE-Router als ION-Knoten genutzt werden können

Die Testsuite

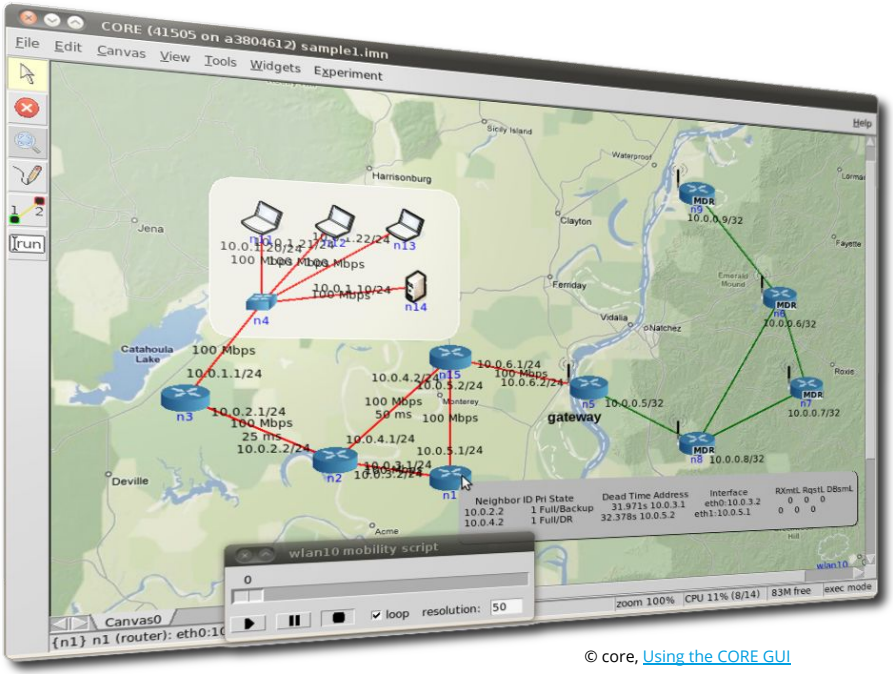
ION-DTN

Überblick

- von NASA entwickelt
- Implementation der Delay-Tolerant Networking (DTN) Architektur wie in RFC 4838 beschrieben
- vorgesehen für den Einsatz in eingebetteten Umgebungen, einschließlich Flugcomputern für Raumfahrzeuge
- enthält Implementierungen der folgenden Protokolle:
  - DTN Bundle Protocol (v6 und v7)
  - Licklider Transmission Protocol
  - 2 CCSDS application protocols welche an den BP/LTP stack angepasst wurden:
    - CCSDS File Delivery Protocol
    - Asynchronous Message Service

CORE - Common Open Research Emulator

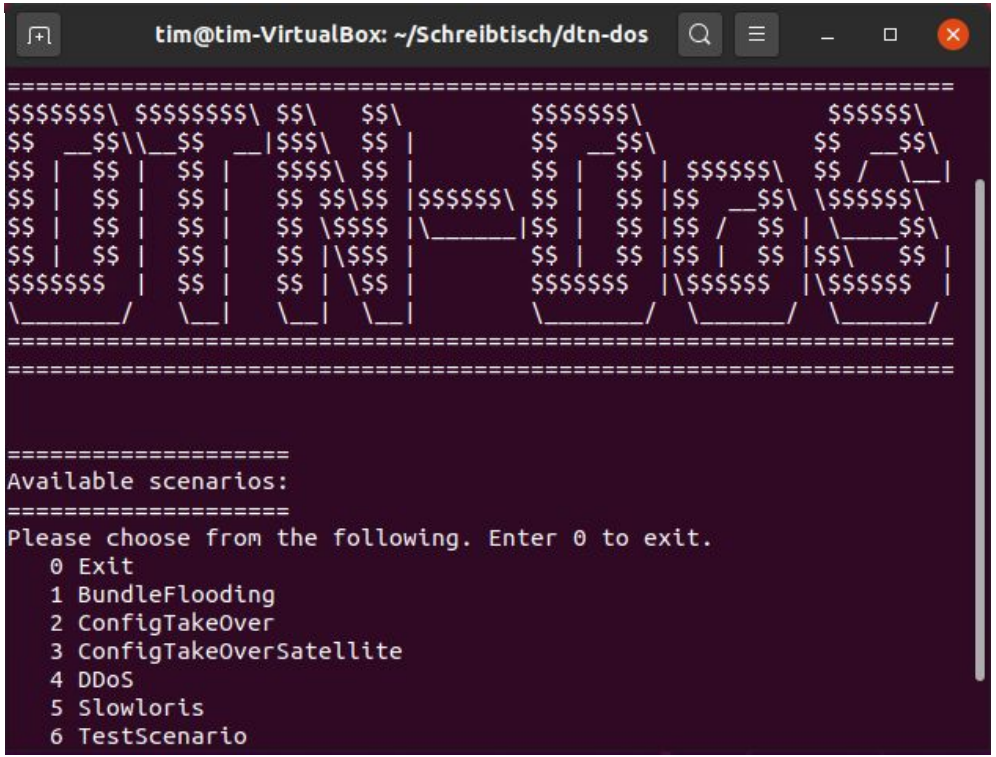
- Tool zum Aufbau virtueller Netzwerke
- baut Repräsentation eines in Echtzeit laufenden realen Computernetzwerks auf
- kann auch mit physischen Netzwerken und Routern verbunden werden
- besitzt grafische Oberfläche zum leichteren Bedienen
- wird verwendet, um ION sowie das Shellskript auf jeder DTN-Node laufen zu lassen



© core, Using the CORE GUI

DTN-DoS

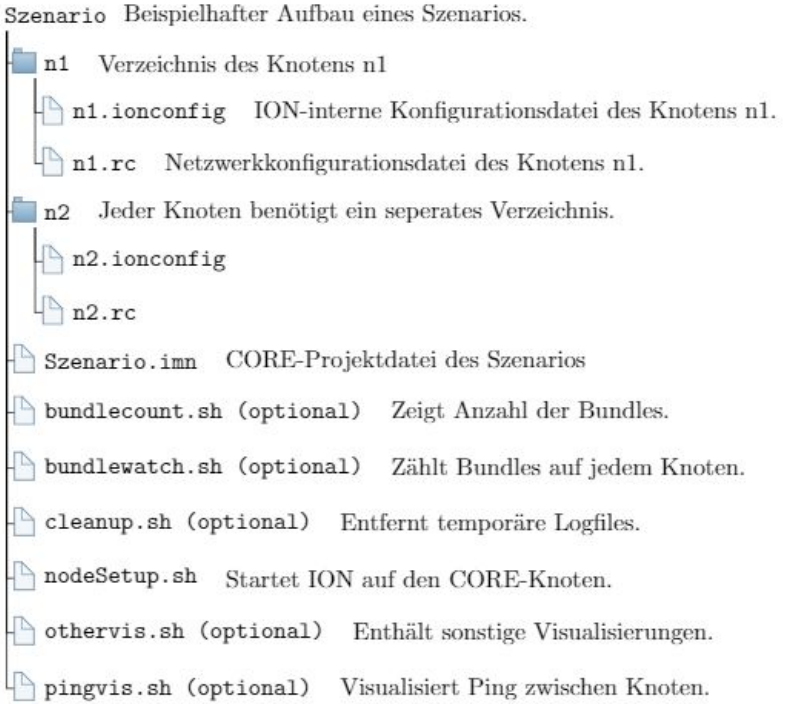
dtn-dos
- Documentation
  - img — Enthält die in der Dokumentation verwendeten Bilder.
  - Documentation_dtndos.pdf
  - main.tex
  - readme.txt
  - references.bib
- Scenarios
  - ion — Verzeichnis wird beim Setup nach /home/user/.core/configs kopiert.
    - BundleFlooding
    - ConfigTakeOver
    - ConfigTakeOverSatellite
    - DDoS
    - Slowloris
    - TestScenario
- ion-open-source-4.0.0
- core
- .gitignore
- README.md
- setup.sh
- start_dtndos.sh
- test.rc



Szenarien

Aufbau der Szenarien

- Szenarien müssen in einem eigenen Verzeichnis unter **/home/User/.core/config/ion/** liegen
- Aufbau eines solchen Szenarioverzeichnisses ⟶ siehe rechts
- Integration von ION in CORE und Erstellung eigener Szenarien ist in der Dokumentation erklärt



Bundle Flooding

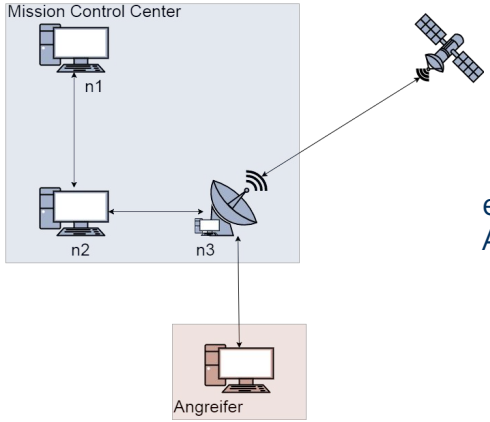
Szenario

Angriff auf die Kommunikationsinfrastruktur eines Mission Control Center, um die Verbindung zu einem Satelliten zu stören.

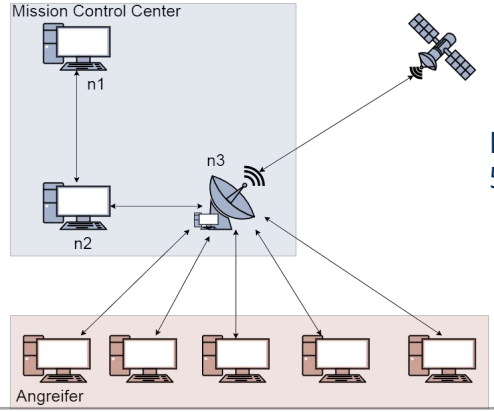
Angriffsmethode

Durch in Masse gesendete Bundle Ping Anfragen an den Satelliten (Flooding) ist der Zwischenknoten n3 mit der Bearbeitung der Bundles des Angreifers vollkommen ausgelastet.

Es folgt, dass von n1 verschickte Anfragen nicht (rechtzeitig) zugestellt werden können.



einzelner Angreifer



DDoS-Angriff mit 5 Angreifern

Config Take Over & Config Take Over Satellite

Szenario

Zwei Simulationen eines Angriffs auf die Konfiguration eines Knotens:

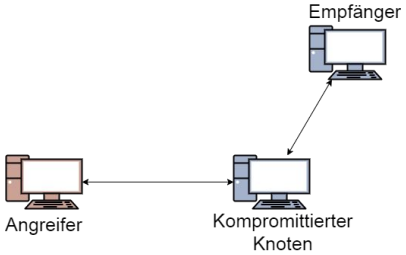
- direkt auf einen kompromittierten Knoten
- über einen kompromittierten Knoten (n3) auf einen Satellit

Angriffsmethode

Mittels ncat Zugriff auf den kompromittierten Knoten, bzw. n3

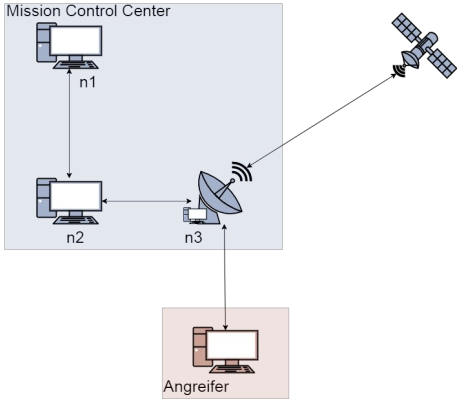
CTO: Abschalten des Zugriffs von BP auf Transportprotokoll-Schicht und nach 10s Reaktivierung

CTOS: Abschalten des Zugriffs von BP auf Transportprotokolle beim Satelliten



Config Take Over (CTO)

Config Take Over Satellite (CTOS)



Slowloris

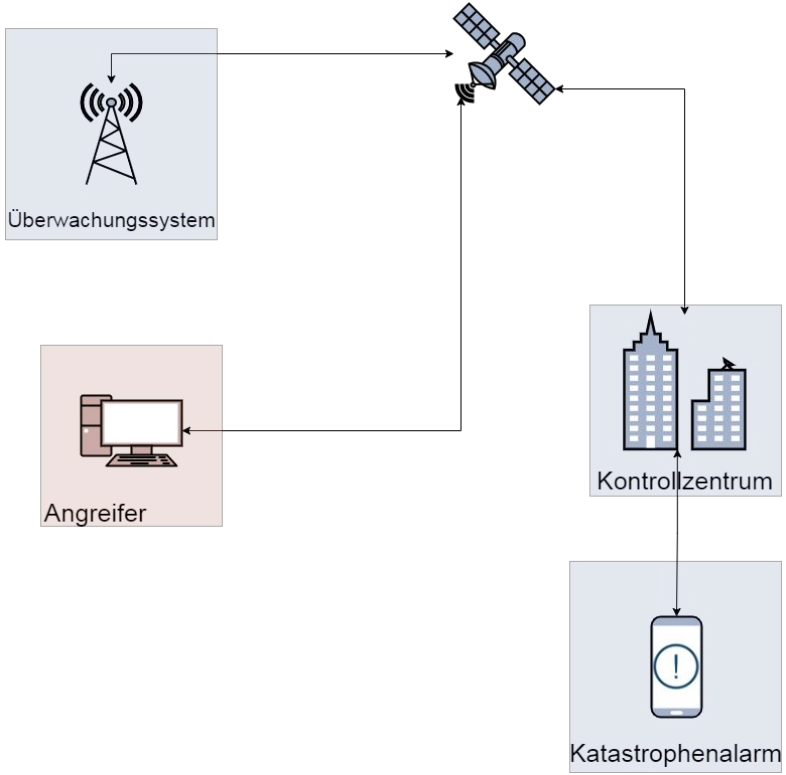
Szenario

Angriff auf ein Emergency Warning System mit dem Ziel, die Kommunikation zwischen Überwachungssystem und Kontrollzentrum zu stören.

Angriffsmethode

Der Angreifer öffnet möglichst viele Verbindungen zum Satelliten durch Versenden von Teilanfragen und versucht diese lange offen zu halten.

Da die maximale Anzahl an offenen Verbindungen begrenzt ist, muss der Satellit die legitimen Verbindungsversuche des Überwachungssystems ablehnen



Präsentation der Anwendung

Zukünftige Erweiterungsmöglichkeiten

- Anzeigen detaillierter Statistiken eines Szenarios
- Simulation weiterer Szenarien von DoS-Angriffen
- grafische Auswertung des Netzwerkverkehrs während der Ausführung der Testsuite
- möglicherweise Integration von anderen DTN-Implementierungen

Referenzen

- Scott Burleigh, Patricia Lindner, Shawn Ostermann, Hans Kruse; ION-DTN; Version 4.0.0; 01. Februar 2021; https://sourceforge.net/projects/ion-dtn/
- Gokberk Yaltirakli; ”Slowloris“; github.com (2015); https://github.com/gkbrk/slowlorishttps://github.com/gkbrk/slowloris
- Jeff Ahrenholz; CORE Documentation; https://coreemu.github.io/core/ (besucht am 17. 01. 2021)
- Tim Krieg, Tobias Nöthlich, Florian Richter, DTN-DoS, https://github.com/tobinatore/dtn-dos

Diskussion und Fragen