

# Sicherheitsaspekte bei Deployment virtueller Netzwerkinfrastrukturen

Gerhard Gröschl, Miran Mizani  
{gerhard.groeschl, miran.mizani}@campus.lmu.de

Seminar: Trends in Mobilen und Verteilten Systemen  
Wintersemester 2016/2017

Lehrstuhl für Mobile und Verteilte Systeme  
Institut für Informatik  
Ludwig-Maximilians-Universität München

Betreuer: Michael T. Beck  
*eingereicht am 19. Januar 2017*

FEHLT [GG]: Optimierung der Grafiken, farbliches Herausheben der Sicherheitskriterien in mathematischen Modellen

TODO [MM]: Übergänge zwischen den Texten beider Autoren

TODO [MM]: Unterstrichene Passagen überarbeiten oder löschen. Kommentare entfernen

TODO [MM]: Graphiken erstellen / überarbeiten.

**Abstract:** Durch die äußerst effiziente Nutzung von Hardware mittels Virtualisierung steigt die Nachfrage nach virtualisierten Infrastrukturen enorm. Serviceprovider müssen die Hardwarebasis für ihre Dienste nicht mehr selbst unterhalten und geben ihre dahingehende Verantwortung an Infrastrukturanbieter weiter. Um die Sicherheit dieser Strukturen nicht zu vernachlässigen, arbeiten viele Forscher in diesem Bereich und versuchen effiziente Algorithmen mit integrierter Beachtung der Sicherheitsaspekte zu finden. Diese Arbeit soll einen Überblick und eine Klassifizierung der Gefahren, die solche Konstrukte betreffen, sowie eine Analyse zweier unterschiedlicher Ansätze zur Vermeidung möglichst vieler Risiken zum Zeitpunkt der Planung übermitteln.

## **Inhaltsverzeichnis**

|          |  |           |
|----------|--|-----------|
| <b>1</b> | <b>Einleitung</b>  | <b>3</b>  |
| <b>2</b> | <b>Das Virtual Network Embedding Problem</b>                       | <b>4</b>  |
| <b>3</b> | <b>Sicherheitsaspekte virtueller Netzinfrastrukturen</b>           | <b>6</b>  |
| 3.1      | (Sicherheits-)Anforderungen an virtualisierte Umgebungen . . . . . | 6         |
| 3.2      | Verwundbarkeiten in virtualisierten Umgebungen . . . . .           | 8         |
| 3.2.1    | Technischer Art . . . . .  | 9         |
| 3.2.2    | Organisatorischer Art . . . . .                                    | 12        |
| 3.2.3    | Rechtlicher Art . . . . .  | 12        |
| 3.3      | VNE-Relevante Gefahren . . . . .                                   | 13        |
| <b>4</b> | <b>Vermeidung von Gefahren via Secure VNE (SVNE)</b>               | <b>13</b> |
| 4.1      | Ansatz 1 . . . . .   | 13        |
| 4.2      | Ansatz 2 . . . . .   | 18        |
| 4.3      | Vergleich . . . . .  | 25        |
| <b>5</b> | <b>Schlussfolgerung und Ausblick</b>                               | <b>26</b> |

## 1 Einleitung

Ein Konzept dem Internet Impasse mit flexibler Architektur [WAS IST DAS?] und Handhabbarkeit zu begegnen, wurde in der Netzwerkvirtualisierung (NV) gefunden. [APST05, BOB<sup>+</sup>12, FBB<sup>+</sup>13] Sie basiert auf Knoten- (z.B. Xen) und Linkvirtualisierung [ANGABE ZU BEIDEM?] und erlaubt so von der tatsächlichen physischen Hardware und Netzinfrastruktur (NI) beinahe unabhängige logische bzw. virtuelle Netzwerke einzurichten, welche nach außen hin den Anschein physischer Netzwerke erwecken. Die Möglichkeit mehrere virtuelle Maschinen (VMs) pro physischem Host und verschiedene heterogene virtuelle Netzwerke (VNs) auf demselben physischen Substratnetz zu betreiben befördert die Flexibilität der Netzwerkarchitektur und wirkt dem Internet Ossification Problem [APST05] entgegen.

Die großen Vorteile der NV liegen in der Abstraktion von der eingesetzten Hardware. Das Erstellen, Verändern, Migrieren, Zurücksetzen und Löschen von Maschinen funktioniert genauso einfach wie der Umgang mit Dateien, was eine dynamische Nutzung des Netzwerkes erlaubt. Virtuelle Maschinen und Netzwerke eignen sich auch als Testumgebung. Einerseits werden bestehende Systeme im Fehlerfall nicht direkt beeinträchtigt. Andererseits kann neuer Code leicht in verschiedenen Umgebungen (Windows, Linux, verschiedene großer RAM, mit oder ohne Software-Developer-Kits etc.) ohne zusätzliche Hardware getestet und später einfach ausgerollt werden.

NV eröffnet eine Unterteilung des klassischen Internetserviceproviders (ISP) in Service-Provider (SP) und Infrastructure-Provider (InP). Damit gewonnene Freiheiten durch z.B. jeweils unabhängige Technologieentscheidungen sind besonders für Unternehmen interessant, die die Hardwarebasis ihrer Dienste nicht selbst unterhalten wollen. [WCC16]

Das Anbieten von Software und Hardware als on-demand Ressourcen wird wegen des geringen Wartungsaufwand, verminderter Hardwarekosten durch Koexistenz mehrerer Mieter, aber v.a. wegen Automatisierbarkeit in der Programmierung der Netzwerkumgebung vereinfacht. Dass InPs nicht mehr streng durch Hardware limitiert sind, begünstigt Skalierbarkeit und bspw. lastbedingte Migration von VMs auf andere physische Hosts.

Auch für den Kunden bietet NV Vorteile: Unternehmen bezahlen nur noch für diejenigen Ressourcen, die gerade in Anspruch genommen werden. Hochqualitative Hardware kann so zu einem Bruchteil ihres Preises erworben und ungenutzte Hardware reduziert werden. Durch dynamisches Skalieren (z.B. in Zeiten hoher Last) kann die eigene IT-Landschaft mühelos vergrößert werden.

Die durch NV gewonnene Flexibilität und Kostenreduzierung begünstigen z.B. auch das Outsourcing von Rechenleistung, Speicher, Inhalten und Netzwerk. Dadurch wird Soft- und Hardware einfacher nutzbar gemacht und Geschäftsprozesse befördert. Die damit einhergehende Verantwortungsübertragung erfordert eine Anpassung des Risikomanagements und IT-Sicherheitstechnische Arbeiten zur Erhaltung der klassischen C.I.A.-Aspekte. Wegen der gemeinsam genutzten Hardware kommt aus Sicht des Kunden besonders der Isolation und dem Datenschutz eine wichtige Rolle zu.

Bekannte Sicherheitsmechanismen wie Verschlüsselung, Firewalls, Intrusion Detection Systeme etc. können zwar auf den virtuellen Komponenten des Netzwerks implementiert werden. Die Sicherheit von Nutzerdaten könne dadurch aber wegen der heterogenen und stark dynamischen Struktur virtueller Umgebungen jedoch nicht garantiert werden.

Zusätzlich gehen Vorteile der Netzwerkvirtualisierung durch den zusätzlichen Overhead verloren. [GCH<sup>+</sup>16]

Eine mögliche Lösung hierzu ist das Integrieren von Sicherheitsaspekten bereits in die Zuordnung von virtuellen zu physischen Knoten und Links. Dieser Virtual Network Embedding (VNE) Prozess stellt eine der größten Herausforderungen in der Netzwerkvirtualisierung dar. [FBB<sup>+</sup>13] Werden virtuelle Netzwerke entsprechend ihrer Sicherheitsanforderungen bereits auf Substratknoten mit hinreichender Schutzfunktion wie beispielsweise Firewall abgebildet, so kann Overhead durch zusätzliche Sicherheitstechnik im laufenden Betrieb des VNs reduziert werden.

[TODO] Derzeit wird versucht [BOB<sup>+</sup>12, GCH<sup>+</sup>16, WCC16] derartige Probleme bereits im VNE-Algorithmus anzugehen [SVNE Security-aware VNE—security by design]. Nicht allen Problemen bzw. Sicherheitsrisiken kann aber auf diese Weise begegnet werden.

Diese Arbeit klassifiziert Gefahren im Kontext virtualisierter Netzwerke und analysiert zwei unterschiedliche Ansätze zur Schaffung eines möglichst hohen Sicherheitsniveaus bereits zum Zeitpunkt des VNE-Prozesses.

Dazu wird zuerst das VNE-Problem in Kapitel 2 dargestellt. Kapitel 3 untersucht Sicherheitsanforderungen an virtuelle Netzwerkstrukturen und klassifiziert Sicherheitsrisiken, die sich in deren Kontext ergeben. Zwei Möglichkeiten zur Vermeidung von Gefahren, denen bereits im VNE-Prozess begegnet werden kann, werden im Kapitel 4 betrachtet. Nach einer Diskussion in dieser Arbeit offengebliebener Probleme in Kapitel 5 wird mit einem Ausblick abgeschlossen.

## 2 Das Virtual Network Embedding Problem

Um den Anforderungen der heutigen Gefahren zu genügen, ist es unumgänglich sämtliche Grundsätze der IT-Sicherheit möglichst früh in die Planung der gewünschten Infrastruktur miteinzubeziehen. Nicht nur, weil das nachträgliche Schließen von Sicherheitslücken und Hinzufügen von Sicherheitskomponenten in finanzieller und zeitlicher Hinsicht zehnmal so teuer ist wie die initiale Beachtung dieser Aspekte, sondern weil die vollständige Sicherheit eines nachgerüsteten Systems kaum gewährleistet werden kann [Col11]. „Security-by-Design“ ist einer der wichtigsten Begriffe bei der Planung öffentlich zugänglicher Netzwerkstrukturen. Dementsprechend groß ist die Nachfrage nach VNE-Algorithmen, die bereits beim Prozess des Mappings möglichst viele Sicherheitsaspekte beachten und abdecken. Die vorausgehende Klassifizierung der bekannten Gefahren in „VNE-relevant“ und „nicht-VNE-relevant“ bildet die Grundlage für unsere weiteren Untersuchungen. Um zuvor noch einen genaueren Einblick in die Problematik von VNE zu gewähren, beginnen wir zunächst mit der Erläuterung des VNE-Problems sowie einem Überblick über die verschiedenen erfolgreichen Strategien bestehender VNE-Algorithmen, welche die Sicherheitsaspekte noch nicht beachten.

Betrachtet man das zugrundeliegende physische System als einen ungerichteten Graphen



und extrahiert die vorhandenen Elemente sowie deren Werte, erhält man die Basismenge

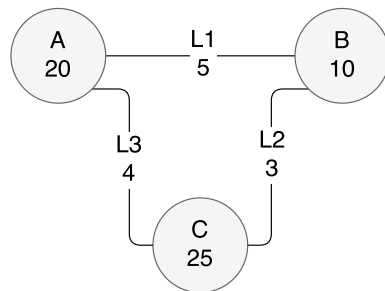
$$G^S = \{N^S, L^S\}$$

(N steht für die Menge der physischen Knoten, L für die Menge der physischen Links)

$$G^S = \{ \{ (A^S, 50), (B^S, 30), (C^S, 70), (D^S, 40), (E^S, 20) \}, \\ \{ (L1^S, 3), (L2^S, 9), (L3^S, 8), (L4^S, 10), (L5^S, 4), (L6^S, 7) \} \}$$

in welche die virtuellen Strukturen eingebettet werden sollen.

Ein „virtual network request“ (in Folge „VNR“ genannt) kann hierbei ebenfalls als ein ungerichteter Graph gesehen



und genauso in eine Menge übersetzt werden.

$$G^V = \{N^V, L^V\}$$

(N steht für die Menge der virtuellen Knoten, L für die Menge der virtuellen Links)

$$G^V = \{ \{ (A^V, 20), (B^V, 10), (C^V, 25) \}, \{ (L1^V, 5), (L2^V, 3), (L3^V, 4) \} \}$$

Gesucht ist nun eine Abbildungsfunktion  $f : G^V \rightarrow G^S$

In der Regel ist es üblich, nicht nur eine einzelne VNRs auf ein physisches System abzubilden, sondern gleich mehrere auf einmal. Ebenso wäre es theoretisch möglich, dass ein Infrastruktur-Provider gleich mehrere getrennte unabhängige physische Strukturen betreibt, und somit mittels VNE das beste System für die Abbildung der Menge von VNRs erörtern möchte. Dies könnte beispielsweise der Fall sein, wenn ein Serviceprovider ein VNR mit der Bedingung „alle Elemente mögen sich am selben Standort befinden, egal an welchem“ in Auftrag gibt, und der Infrastruktur-Provider über mehrere Hardware-Standorte verfügt.

Die Attributmenge bei den grundlegenden VNE-Algorithmen beschränkt sich zumeist auf Rechnerleistung und Bandbreite. Lokalität, GPU-Leistung und RAM-Menge wären einige weitere mögliche Standard-Attribute. Ein großes Problem bei der Berechnung des optimalen Mappings findet sich bei der Berechnungszeit. Die endliche Beschränkung der Knoten- sowie Link-Ressourcen und die „on-line nature“ von VNRs stellen zusätzliche Hindernisse dar. Da selbst Lösungen für einfache Anfragen (geringe Anzahl von Knoten und Links), welche wenige Attribute beinhalten, exponentiellen Rechenaufwand benötigen, steigt der Aufwand sowohl mit der Anzahl der abzubildenden Knoten und Links, als auch mit steigender Attributanzahl dementsprechend. Teilweise gilt das Problem als rechnerisch unlösbar, grundsätzlich aber befinden wir uns im Komplexitätsbereich der NP-Vollständigkeit [MRR13]. Da die Erhöhung der Attributmenge - wie bereits genannt - grundsätzlich nicht positiv zur Laufzeit der existierenden Algorithmen beiträgt, werden wir den Komplexitätsbereich beim Hinzufügen von Sicherheitsanforderungen nicht verlassen. Dennoch gibt es Möglichkeiten, die den Rechenaufwand reduzieren können. Im Folgenden widmen wir uns allerdings zuerst einer Übersicht über die Gefahren, welche bei VNE eine Rolle spielen.

### 3 Sicherheitsaspekte virtueller Netzinfrastrukturen

#### 3.1 (Sicherheits-)Anforderungen an virtualisierte Umgebungen

[FALLS NÖTIG / GEWÜNSCHT. SONST WIRD DIESES KAPITEL NICHT AUSGEARBEITET UND ENTFÄLLT] Netzwerkvirtualisierung ist eine Methode unabhängige und voneinander isolierte logische Netzwerke auf einem gemeinsamen physischen Netzwerk zu betreiben. Dieses Kapitel widmet sich möglichen Anforderungen, die an ein so solches System gestellt werden könnten.

- Anonymität und Privatsphäre von Nutzern (vertrauenswürdige Paketweiterleitung, wenn das virt. Netzwerk bei einem Drittanbieter gehostet ist)
- VM Interkonnektivität

- Möglichkeit zur Zusammenarbeit mit nicht-virtualisierten Netzen und Anwendungen  
Bsp. Günstige Webhosting-Lösungen auf vServern sollen auch von nicht-virt. Maschinen aus erreichbar sein.
- Angriffe von Endnutzern sollten nicht in der Lage sein das Substratnetz zu beeinträchtigen, während Attackenverkehr hingegen identifiziert und gefiltert werden können soll.
- Substratnetz sollte nicht VN-Verkehr monitoren, sniffen, manipulieren, stören/unterbrechen (können).
- Umgekehrt sollte auch das VN keine Informationen über das Substratnetz sammeln (können).
- Substratnetz sollte effektive Kontrollmechanismen gegen unerlaubte Erlangung von Infos aus/über das VN bereitstellen.
- ...

### **Mögliche Richtlinien**

- [IN DIESER ARBEIT WERDEN FOLGENDE BEGRIFFE IN DIESEM SINNE VERSTANDEN / KURZE BEGRIFFSDEFINITION]
- Isolation ist Hauptaufgabe / Kernpunkt [-> Ausbauen]
  - Keine gegenseitige Beeinflussung der VMs oder VNs
  - Keine Beeinflussung zwischen VMs verschiedener Mieter / VNs.
  - Von zwei VMs gemeinsam genutzte Ressourcen sind logisch voneinander getrennt. Kein ungewollter direkter Informationsfluss.[Fußnote: Ausführliche Betrachtung indirekten Informationsflusses z.B. via verdeckter Kanäle oder side channel Attacken würde den Umfang dieser Arbeit übersteigen.]
  - Problem: Kunde weiß nicht, ob die „Nachbar-VM“ vertrauenswürdig ist.
  - Die gehosteten VNs sollten keine Attacken gegen privilegierte Informationen der Substratinfrastruktur fahren.
- Datenschutz
- Vertraulichkeit, Integrität, Verfügbarkeit (CIA)
  - Vertraulichkeit: Zwei VMs innerhalb desselben VNs sollen in der Lage sein frei miteinander zu kommunizieren, ohne dann dabei ein Dritter durch Belauschung an Kommunikationsinhalte gelangen kann.
  - Integrität: Ein virt. Knoten / VM soll nicht in der Lage sein, (Kommunikations-)Daten Anderer zu manipulieren und die eigene Urheberschaft der Veränderungen einer anderen Instanz zuzuschreiben.

- Informationsflusskontrolle
- Mitglieder- und Zulassungsverwaltung in Virt. Netzen.

### Herausforderungen:

- Kann das Substratnetz Paketvermittlung effektiv durchführen, ohne Informationen über das VN zu sammeln oder Privatsphäre zu verletzen?
- ...

### 3.2 Verwundbarkeiten in virtualisierten Umgebungen

Wie in der Einleitung angedeutet bietet Netzwerkvirtualisierung einige Vorteile gegenüber bisherigen Netzarchitekturen. Durch die Einführung einer weiteren Schicht zwischen Hardware und Anwendungssoftware (Abbildung 1) und dem gemeinsamen Hosten verschiedener virtueller Netzwerke auf gemeinsamen Substratnetz tun sich aber auch verschiedene neue Verwundbarkeiten auf. [GCH<sup>+</sup>16, NW, WDWY10, GR05, DMT11] haben bereits einige Sicherheitsrisiken analysiert, welche im Folgenden klassifiziert und ergänzt werden.

<WOHL EINE MISCHUNG AUS DIESEN BEIDEN>

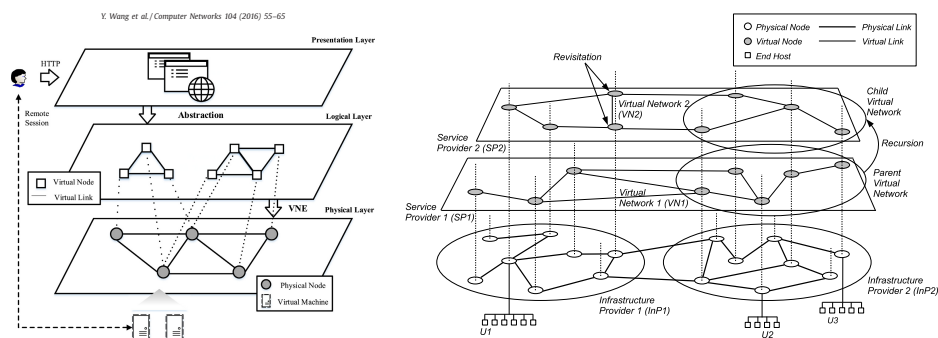


Abbildung 1: Drei-Schichtenarchitektur der Netzwerkvirtualisierung.  
Substratnetz hostet zwei virtuelle Netze

Sicherheitsrisiken in virtualisierten Netzinfrastrukturen lassen sich auf verschiedene Weisen wie z.B. nach ISO/OSI-Schicht, nach Verletzung der klassischen C.I.A.-Aspekte, [nach Schicht in der NV-Architektur,] oder aus Sicht des SPs bzw. InPs klassifizieren. Da dieses Kapitel sich aber auf durch Netzvirtualisierung gegenüber herkömmlichen Netzinfrastrukturen neu hinzukommende Risiken konzentriert, liegt der folgenden Klassifizierung zur



Verdeutlichung der Angriffswege die in Abbildung 2 dargestellte Struktur zugrunde, die sich auf der Drei-Schichtenarchitektur virtualisierter Netze (Abbildung 1) ableitet.

Sicherheitsrisiken werden zunächst nach solchen technischer, organisatorischer bzw. unternehmerischer und rechtlicher Art geordnet. Im Zentrum der Betrachtung stehen dabei die technischen Risiken, welche wiederum nach Angriffsrichtungen ‚von NI ausgehend‘, ‚vom VN ausgehend‘ und ‚vom User ausgehend‘ gegliedert werden sollen. In jeder dieser Kategorien wird nach Angriffsziel ‚gegen NI‘, ‚gegen VN/VM‘ und ‚gegen User‘ unterteilt. Da die Kategorien ‚I.1 von NI ausgehend gegen NI‘ und ‚III.3 vom User ausgehend gegen User‘ in virtualisierten Netzwerkumgebungen keine neuen Angriffsszenarien zu eröffnen scheinen, werden sie hier dem Ziel des Kapitels entsprechend nicht tiefergehend ausgeführt.

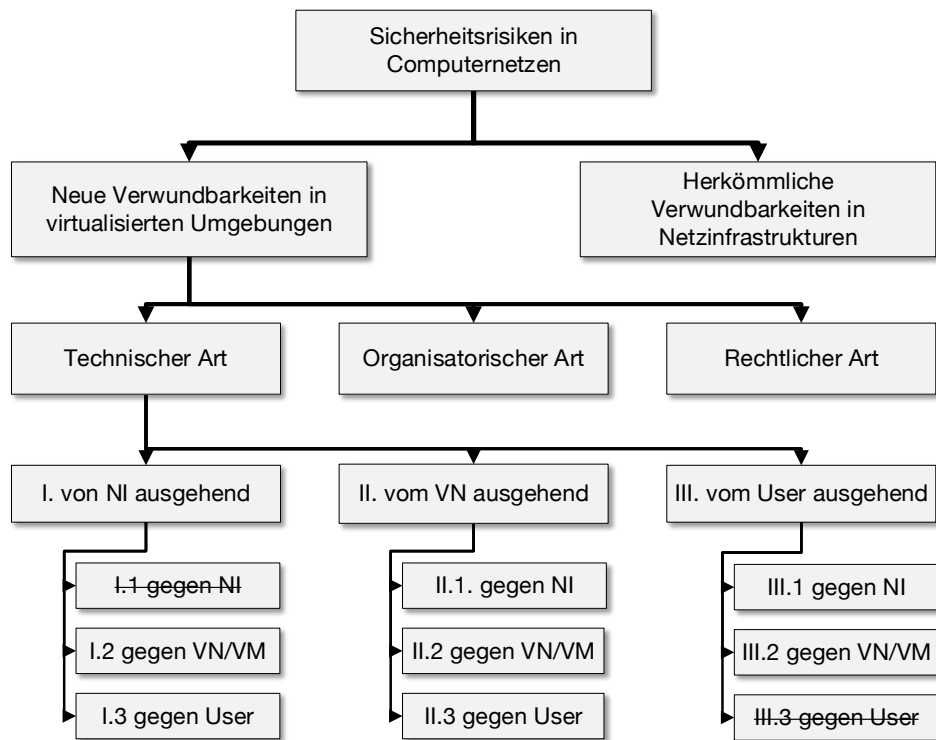


Abbildung 2: Klassifizierung von Gefahren in virtualisierten Netzwerken.

NI = Netzwerkinfrastruktur / Substratnetz. Der physische Host einer VM ist Teil der NI.

User = Endsystem bzw. in VNs implementierter Service oder Nutzer.

### 3.2.1 Technischer Art

[KURZE EINLEITUNG?]

**I.2 & I.3 Von NI ausgehend gegen VN und User.** Physische Hosts bieten ihren VMs Ressourcen an. Alle Dienste und Anwendungen der VMs werden letztlich auf dem physischen Host ausgeführt und auch alle Daten auf ihm gespeichert. Dies eröffnet für den physischen Host prinzipiell die Möglichkeit eines Monitorings der VM-Aktivitäten, was ab einer gewissen Intensität sicherlich über Verwaltungsbelange hinausgehen und Privatsphärenanforderungen widersprechen dürfte. Auf demselben Weg lassen sich auch vertraulichkeitsverletzende Sniffing- oder Spoofing-Attacken gegen VM bzw. VN starten.

Da alle ihre Rechenoperationen letztlich auf dem physischen Host ausgeführt werden, ist es für eine VM nur schwer möglich sich gegen solche Angriffe zu wehren. [VER-SCHLÜSSELUNG ALS AUSWEG?]

Auch Manipulation des legitimen Datenverkehrs, (gezieltes) Verwerfen von empfangenen Paketen bzw. das Einschleusen schadhafter Nachrichten bieten eine weitere Möglichkeit der Kompromittierung, gegen die VNs und Endsysteme wohl schutzlos ausgeliefert ist. [AUSFÜHRLICHER?]

Durch derartige Aktionen oder auch unzureichende Sicherungsmaßnahmen gegen Datenabfluss kann der physische Host in den SLAs vereinbarte Bestimmungen verletzen, was gerade bei Drittanbietern als Hostingpartner eine Rolle spielt.

#### **Von VN/VM ausgehend [MINI EINLEITUNG]**

- **II.1 Von VM/VM ausgehend gegen NI/ihren physischen Host.** Das Bereitstellen von Ressourcen für VMs ist aber auch für den physischen Host nicht ohne Risiko. Schadhafte oder bösartige VMs können Verwundbarkeiten ihres physischen Host über zugeteilte Ressourcen angreifen. Ohne hinreichende Restriktionen könnte eine VM dann über ihr zugeteiltes Kontingent hinaus bspw. wichtige Speicherbereiche manipulieren oder durch übermäßige Reservierung von CPU-Zeiten eine Denial of Service Attacke gegen den physischen Host bzw. das Substratnetz fahren. Da Host und virtuelle Netztopologie aus der Ferne konfigurierbar sind, stellt das Einschleusen von konstruierten Nachrichten des verwendeten Netzwerkmanagementprotokolls auf oder durch die Netzwerkkarte des physischen Hosts einen weiteren gefährlichen Angriffsvektor dar.

Nach Eindringen in oder Übernahme des Hosts, einem „break of isolation“ im ersten Sinne [WDWY10], könnte eine schadhafte VM dann ihr Kontingent an Ressourcen beeinflussen, netztopologische Informationen sammeln, andere Netzwerkressourcen oder -infrastrukturkomponenten angreifen und so beispielsweise Dienste anderer VMs oder VNs behindern.

- **II.2 Von VM/VN ausgehend gegen VM/VN.** Neben den herkömmlichen Angriffsszenarien zwischen Maschinen im selben Netzwerk, ergeben sich v. a. aus der gemeinsamen Nutzung von Ressourcen neue Angriffsvektoren.<sup>1</sup> Ein Angreifer kann sich nun gezielt Ressourcen auf denjenigen physischen Maschinen mieten, von denen auch sein Angriffsziel gehostet wird, um so erleichterten Zugang zu deren

---

<sup>1</sup>Da die Angriffstechniken von VMs gegen VMs auf anderen physischen Hosts vergleichbar mit herkömmlichen Angriffen in nicht-virtualisierten Netzinfrastrukturen sein dürften, werden hier hauptsächlich VMs auf demselben physischen Host betrachtet.

Verwundbarkeiten zu erlangen. Durch Eindringen oder Übernehmen gewisser Ressourcen des gemeinsamen physischen Hosts kann eine schadhafte VM dann ggfs. Verwundbarkeiten ausnutzen oder durch Cross-VN-side-channel-Attacken vertrauliche Informationen gewinnen und Daten manipulieren. Ein Beispiel einer Integritätsverletzung mittels einer solchen Attacke findet sich in [RTSS09].

Da i.d.R. [ANGABE?] werden nur virtuelle Netzwerkkarten zugeteilt, kann jede VM potentiell den gesamten Datenverkehr aller VMs bzw. VNs auf derselben physischen Netzwerkkarte lesen. Ein Monitoring anderer VMs auch aus anderen VNs, ein „break of Isolation“ im zweiten Sinne bedroht deren Vertraulichkeit. Durch Belauschen des Netzwerkverkehrs lassen sich ggfs. auch Dienste gemeinsam gehosteter VN reproduzieren und dadurch bspw. ein live Videostreaming breiter zugänglich machen.[NW]

Sollte es einer VM gelingen kritische Teile ihres physischen Hosts zu übernehmen, so stehen ihr zusätzlich die im Abschnitt *I.2 & I.3 Von NI ausgehend gegen VN und User* aufgeführten Angriffsvektoren offen.

- **II.3 Von VM ausgehend gegen User.** Auch ein virtuelles Netzwerk kann mit herkömmlichen Methoden wie Monitoring der Nutzeraktivitäten oder dem Einschleusen von konstruierten Nachrichten zur Störung oder Abbruch von Peer-to-Peer-Verbindungen Einfluss auf den Nutzverkehr seiner User nehmen.

**Vom User ausgehend** Einem Benutzer oder schadhafte Anwendungsprogramm stehen auch in virtualisierten Netzwerkumgebungen die bekannten Methoden der Störung durch z.B. Herbeiführen von Überlastsituationen in NV oder NI offen.

- **III.1 Vom User ausgehend gegen NI.** Da sich die virtuelle Netztopologie im VNE laufend ändert, müssen Netzwerkkomponenten wie Switches und Router dynamisch umprogrammierbar sein. Dies ermächtigt Angreifer aber solche ggfs. mit Codeexploits wie Bufferoverflows o. Ä. zu kompromittieren und für ihre Zwecke zu nutzen oder einen Denail of Service herbeizuführen.  
Daneben besteht die Chance auch Netzwerkknoten anzugreifen. Gelingt es z.B. mit einem Rootkit wie BluePill [RT08] (als Vorbereitung für weitere Angriffe) einen Hypervisor zu übernehmen, wird so gleichzeitig die Kontrolle über alle gehosteten VMs erlangt. Auch eine VM lässt sich als Rootkit instrumentalisieren.[WDWY10]
- **III.2 Vom User ausgehend gegen VN.** Aus der dynamischen Natur virtueller Netzwerktopologien ergeben sich neue Verwundbarkeiten: Während der Migration im Livebetrieb eines VNs ist eine Man-in-the-Middle-Attacke möglich, mit der Informationen über und Inhalte des migrierenden VNs erlangt werden können. [NW] Auch die Manipulation von Speicherbereichen der VMs ist während der Migration möglich und lässt sich sogar automatisieren. [OCJ08]  
Die Notwendigkeit die gesamte virtuelle Netzwerkstruktur aus der Ferne umkonfigurieren zu können, erschließt weitere Angriffsziele: Attacken auf die VN-Managementtools durch z.B. Cross-Site-Scripting, SQL-Injection etc. werden lohnend, da auf diese Weise effizient Kontrolle über das gesamte Netzwerk gewonnen werden kann.

[UNTERKAPITELZUSAMMENFASSUNG]

### 3.2.2 Organisatorischer Art

[TODO / AUSFORMULIEREN]

Unter ‚organisatorischen‘ Risiken werden hier Risiken für Unternehmen oder im menschlichen Umgang betrachtet, die im Zusammenhang mit Virtualisierung stehen.

Wie im Kapitel Technischer Art dargestellt, eröffnet Netzvirtualisierung eine Reihe neuer Verwundbarkeiten für gehostete Systeme. Gerade für Unternehmen dürfte die teils deutliche Gefährdung der Vertraulichkeit und Integrität von Firmen- oder Kundendaten ein ernstzunehmendes Problem darstellen. Da Netzvirtualisierung oftmals via Cloudcomputing abgewickelt wird, erhöht sich das Risiko eines Datenlecks nochmals durch den Up- und Downloadprozess von Daten.

Substratnetzprovider ist auch ein Unternehmen/Dienstleister, der sich organisatorisch verändert oder z.B. Insolvenz anmelden kann.

Snapshot-Problem. Momentanaufnahme der virt. Maschine für Backup- oder Migrationszwecke.

- Einfachheit dessen ist großer Vorteil von VMs.
- Nachteil: Nach dem Wiedereinspielen werden ggfs. zwischenzeitlich deaktivierte Accounts oder veraltete Sicherheitsrichtlinien wieder produktiv gesetzt.
- Virtuelle Maschinen entstehen schnell. Probleme bei Patchmanagement
- VMs zeitweise/Häufig deaktiviert/offline
  - Erhalten keine Patches am Patchday.
  - Würmer infizieren meist relativ schnell alle verwundbaren Systeme. Geht die VM danach offline wird Malware darin nicht entfernt und die Wurminfektionswelle startet beim erneuten Onlinegehen der VM.
- Rücksetzen/rollback einer VM kann zwischenzeitlich gepatchte Schwachstellen wieder offenbaren (Snapshot-Problem)

### 3.2.3 Rechtlicher Art

[TODO] Da Substratnetze nicht zwingend räumlich eng beschränkt sein müssen, könnte es passieren, dass gewisse Teile des virtuellen Netzes dynamisch auf Knoten in einem anderen Land abgebildet werden, welches mit den Auflagen des Unternehmens zu Datenschutz, Privatsphäre oder IT-Securitystandards nicht vereinbar ist.

Aus technischen Gefahren resultierende Risiken (Sniffing vs. Datenschutz, Leaks, ...)

### 3.3 VNE-Relevante Gefahren

[TODO] Benennung von (Kategorien an) Gefahren aus dem vorherigen Kapitel, denen mit dem VNE-Prozess begegnet werden kann.

## 4 Vermeidung von Gefahren via Secure VNE (SVNE)

Da wir nun einen Überblick zu VNE sowie den bestehenden Gefahren gegeben haben, widmen wir uns nun zwei verschiedenen SVNE-Lösungsansätzen. Der Detailgrad wurde so gewählt, dass man einen guten Einblick in die Arbeitsweise der Ansätze bekommt und die Problematik der zusätzlichen Last der Sicherheitsaspekte erkennt.

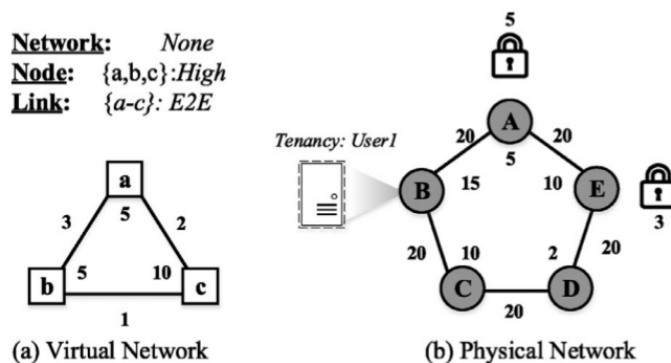
### 4.1 Ansatz 1

Hierbei beschäftigen wir uns mit dem Lösungsansatz aus [WCC16]. Das Hauptaugenmerk bezüglich der Sicherheitsaspekte legen Wang et. al. auf Traffic-Verschlüsselung und die Separierung von VMs unterschiedlicher Trust-Levels. Mittels „Security plan design“ werden die drei folgenden strukturellen Aspekte betrachtet und in dementsprechende Levels eingeteilt.

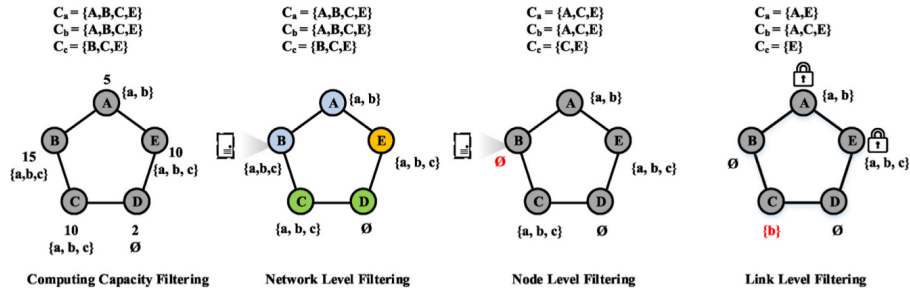
- The Network plan:  
Ein VNR wird als Netzwerk betrachtet und seinem Level entsprechend isoliert. „High“ fordert und beansprucht ein gesamtes Netz bzw. Subnetz der physischen Infrastruktur für sich. Hiermit soll die Wahrscheinlichkeit für DOS-Angriffe oder ähnliche vermindert werden, da „Mehr-Parteien-Netzwerke“ die Hauptschwachstellen für solche Angriffe darstellen [Liu10]. Auch Sniffing durch kompromittierte Hosts im selben Netz wird durch diese Maßnahme verhindert. Während „high“ Ressourcenteilung somit komplett verweigert, lässt der Level „medium“ zumindest ein gemeinsam genutztes Netz für VNRs vom selben Eigentümer zu.
- The Node plan:  
Die einzelnen virtuellen Knoten eines VNR stellen Isolierungsanforderungen an die physischen Knoten. Wie auch beim „network plan“, werden die Levels „high“, „medium“ und „none“ definiert und umgesetzt. „high“ fordert die alleinige Existenz eines VNR-Knotens, „medium“ lässt VNR-Knoten vom selben Eigentümer auf ein und demselben physischen Knoten zu. Durch diesen Plan sollen Angriffe von VM zu VM über gemeinsam genutzte Ressourcen unterbunden werden. Zusätzlich wird das Risiko eines Angriffs vom physischen Host verringert, da der Angriffsvektor „VM zu physischem Host“ eliminiert wird.
- The Link plan:  
End-to-End(E2E), Point-to-Point(P2P) und „none“ sind die hier wählbaren Levels.

Während E2E nur an den Endpunkten Verschlüsselungskapazitäten zu Verfügung stellen muss, benötigt P2P diese Kapazitäten an allen Hops des abgebildeten Links. Die heutzutage sehr gängigen man-in-the-middle Angriffe sollen dadurch wesentlich erschwert werden.

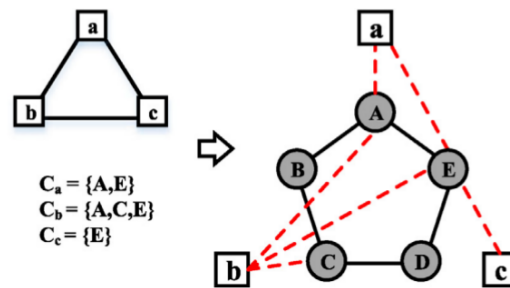
VNRs werden nun, wie in Kapitel 2 bereits gezeigt, in ungerichtete Graphen mit Standardanforderungstransformiert. Zusätzlich werden hier auch noch Sicherheitsanforderungen integriert.



Nun wird ein vier-stufiges Pre-Processing durchgeführt, um die Berechnung der optimalen Abbildung der VNRs zu vereinfachen. Hierbei werden als ersten die Standardanforderungen der virtuellen Knoten mit den zu Verfügung stehenden Kapazitäten der physischen Knoten verglichen. Sollten physische Knoten bestimmte Anforderungen nicht erfüllen, werden sie aus der Berechnung ausgeschlossen. Der zweite Schritt ist dem „Network plan“ gewidmet. Sollte ein physischer Knoten, welcher den Anforderungen des „Network plan“ nicht genügt sich in einem Kandidaten-Netzwerk befinden, wird das Subnetz aus den Berechnungen ausgeschlossen. Im dritten Schritt werden die Sicherheitsanforderungen der einzelnen Knoten betrachtet und nicht entsprechende physischen Knoten werden abermals entfernt. Der letzte Schritt widmet sich den Sicherheitsanforderungen aus dem „Link plan“ und streicht Links aus den weiteren Berechnungen, welche den Verschlüsselungsanforderungen der virtuellen Links nicht genüge tun.



Mit den aus dem Pre-Processing gewonnenen Information bildet man nun einen Hilfsgraphen, welcher die übrig gebliebenen Möglichkeiten der Einbettung zeigt.



Dieses Pre-Processing reduziert das SVNE-Problem auf ein „multi-commodity-flow“ Problem. [RA93] Im weiteren Vorgehen werden nun zwei Fälle unterschieden, „Path-splitting“, im weiteren SVNE-PS und „no-path-splitting“, im weiteren SVNE-NPS, sind zusätzliche Sicherheitsvorgaben, welche im Vorfeld definiert werden müssen, um die Wahl des Algorithmus zu ermöglichen. Sollte SVNE-PS gewählt werden, beziehen sich die Gleichungen nur auf die Erfüllung der geforderten Attribute. Sollte SVNE-NPS gewählt werden, werden die für Link-Abbildungen verantwortlichen Gleichungen ersetzt.

$$\text{Min} \sum_{p \in \psi} sf_p * ct_p + \sum_{(V,s) \in AL} cn_s * E_{V,s} * cr_V + ct_L \quad (1)$$

$$\sum_{V:(V,s) \in AL} E_{V,s} \leq 1, \quad \forall s \in N^S \quad (2)$$

$$\sum_{s:(V,s) \in AL} E_{V,s} = 1, \quad \forall V \in N^V \quad (3)$$

$$\sum_{p:x \in p} sf_p \leq \beta c_x, \quad \forall x \in L^S \quad (4)$$

$$\sum_{p \in \psi^c} sf_p = \beta r_c, \quad \forall c \in L^V \quad (5)$$

$$\sum_{p \in \psi_s^c} sf_p = \beta r_c, \quad \forall c \in L^V \quad (6)$$

$$\sum_{p \in \psi} \alpha_{p,(V,s)} * sf_p \leq E_{V,s} * T_V, \quad \forall (V,s) \in AL, V \in N^V, s \in N^S \quad (7)$$

$$sf_p \leq x_p * \beta r_c \quad \forall p \in \psi_s^c, c \in L^V \quad (8)$$

$$\sum_{p:x \in p, p \in \psi^c} x_p * \beta r_c \leq \beta c_x, \quad \forall x \in L^S \quad (9)$$

$$\sum_{p \in \psi^c} x_p = 1 \quad \forall c \in L^V \quad (10)$$

$$\sum_{p \in \psi_s^c} x_p = 1 \quad \forall c \in L^V \quad (11)$$

$$\sum_{p \in \psi} \alpha_{p,(V,s)} * x_p \leq E_{V,s} * D_V \quad \forall (V,s) \in AL, V \in N^V, s \in N^S \quad (12)$$

$$\sum_{p \in \psi} x_p * \theta_{p,i} \leq nc_i \quad \forall i \in N^S \quad (13)$$



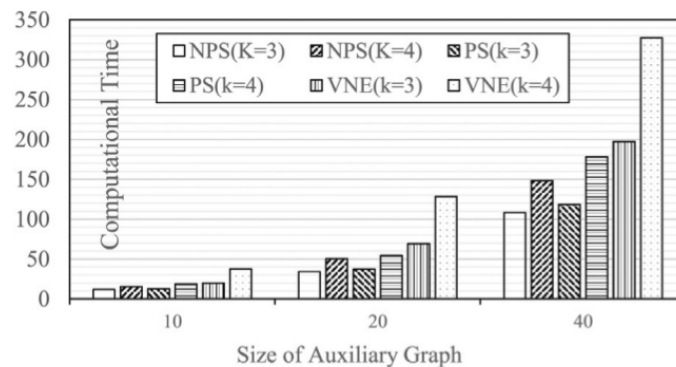
|                      |   |
|----------------------|---|
| $ct_p$ :             | The unit cost of flow on path $p$ , $ct_p \geq 0$ ;   |
| $H_p$ :              | The hop number of path $p$ , $H_p \geq 1$ ;   |
| $cn_s$ :             | The unit cost of computing resources at physical node $s$ , $cn_s \geq 0$ ;                             |
| $\psi$               | The set of all the paths for the model;   |
| $\psi^c$             | The set of paths for virtual link $c$ ;   |
| $\psi_s^c$           | The set of paths for virtual link $c$ that consists of physical nodes all with cryptography capability; |
| $cr_V$               | The computing capacity requirement of each virtual node $V$ ;   |
| $\beta r_c$          | The bandwidth requirement of virtual link $c$ ;   |
| $\beta c_x$ :        | The bandwidth capacity of physical link $x$ ;   |
| $nc_i$ :             | The number of cryptography instances that physical node $i$ can support;                                |
| $\alpha_{p, (V, s)}$ | 1 if auxiliary link $(V, s)$ is on the path $p$ , and 0 otherwise;                                      |
| $\theta_{p, i}$      | 1 if node $i$ is contained in path $p$ , and 0 otherwise;   |
| $ct_L$ :             | The cost of selected link security plan;  |
| $ct_L^c$ :           | The cost of selected link security plan for virtual link $c$ ;  |
| $ct_{ED}$ :          | The cost per cryptography instance;   |
| $AL$ :               | The set of auxiliary links;   |
| $D_V$ :              | The node degree of virtual node $V$ in the virtual network;   |
| $T_V$ :              | The summation of the bandwidth requirements of all incident virtual links of virtual node $V$ .         |
| $E_{V, s}$ :         | 1 if virtual node $V$ is embedded to physical node $s$ , and 0 otherwise;                               |
| $sf_p$ :             | The size of the flow on path $p$ , $sf_p \geq 0$ ;  |
| $x_p$ :              | 1 if there is a non-zero flow on path $p$ , 0 otherwise.  |

Die Berechnungen wurden mittels induktiver logischer Programmierung unter Verwendung von CPLE [hi] und durch k-shortest-path anhand aller abzubildenden Elemente limitiert. Für die Testumgebungen wurden zufällig erzeugte VNRs mit 2 bis 10 Knoten und halbsovielen Links erzeugt. Auch die Rechenkapazität wie Bandbreite wurden durch Zufallsgeneratoren mit Werten im Bereich von 1 bis 10 gewählt und verteilt. Die Anzahl der VNRs beträgt einer Poisson-Verteilung nach einen Durchschnitt von 4 VNR pro 100 Zeiteinheiten, mit einer jeweiligen durchschnittlichen Einsatzzeit von 1000 Zeiteinheiten.

Die zugrundeliegenden physischen Netze wurden ebenfalls zufällig erzeugt und beinhalteten 10 bis 50 Knoten, sowie halbsoviele Links. Die Rechen- sowie Bandbreiten-Kapazitäten wurden gleichmäßig verteilt und enthielten Werte zwischen 1 und 50. Die Verschlüsselungskapazitäten der Knoten wurde über die gesamte Testreihe ebenfalls gleichmäßig verteilt.

Die folgende Statistik zeigt einen Durchschnittsvergleich zwischen dem, als Standard gewählten, VNE-Algorithmus [QH13] und den beiden SVNE-Varianten PS und NPS. Dazu sei gesagt

dass sämtliche Algorithmen ihre Berechnungen anhand des Hilfsgraphen durchgeführt haben und durch  $k=3$  bzw.  $k=4$  limitiert wurden.



Man sieht hier einen deutlichen Zeitvorsprung von PS und NPS gegenüber dem Standard-Algorithmus. Da hier jedoch auch der Standard-Algorithmus vom Pre-Processing profitiert, wäre ein Vergleich, welcher die Dauer des Pre-Processings mit aufnimmt und den Standard-Algorithmus ohne Pre-Processing arbeiten ließe, anschaulicher und aussagekräftiger. Dennoch ist ein Punkt durchaus überraschend und bemerkenswert: Der Standard-Algorithmus benötigt deutlich länger, obwohl er keine Sicherheitsaspekte mitbeurteilt, im Gegenzug zu seinen Kontrahenten.

In welchem Komplexitätsbereich sich das Pre-Processing befindet wird hier leider nicht erwähnt.

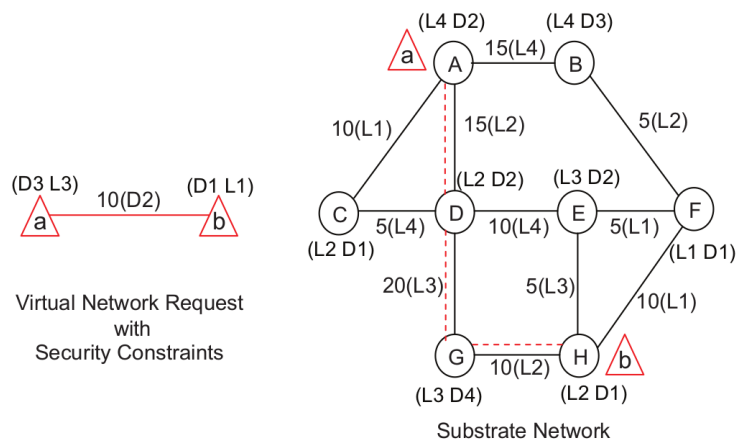
## 4.2 Ansatz 2

Im zweiten Ansatz widmen wir uns dem Modell aus [SL15]. Dieser Ansatz arbeitet mit abstrakten Sicherheitslevels. Im Folgenden werden zwar Skalare hierfür verwendet, was allerdings nicht zwingend so vorgesehen ist. Stattdessen wäre eine Verwendung komplexerer Sicherheitsvektoren möglich, welche bei weitem detailliertere Sicherheitsmerkmale beschreiben könnten. Des weiteren verfügt jeder physische wie auch virtuelle Knoten über zwei Sicherheitswerte: Anforderungslevel und (eigenes) Sicherheitslevel. Der Anforderungslevel definiert das Minimum-Level des Gegenübers, der Sicherheitslevel definiert die eigenen gewünschten Sicherheitsmerkmale. Virtuelle Links verfügen über Anforderungslevels, physische Links nur über Sicherheitslevels. Die vorausgesetzten Basisanforderungen, welchen alle VNRs unterliegen, beschränken sich auf 4 Regeln, welche mittels der zuvor genannten Merkmale umgesetzt werden:

- Ein physischer Knoten sollte einen Sicherheitslevel garantieren, der höher ist als die

Anforderungen der darauf abzubildenden virtuellen Knoten.

- Der Sicherheitslevel des virtuellen Knotens sollte höher sein, als das Anforderungslevel des physischen Knotens.
- Alle virtuellen Knoten, welche auf den selben physischen Knoten abgebildet werden, sollten über einen ausreichenden Sicherheitslevel verfügen.
- Der Anforderungslevel des virtuellen Links sollte stets niedriger sein, als das Sicherheitslevel des physischen Links.



Wie man in Abbildung X sieht, werden auch bei diesem Modell VNRs und physische Netze in ungerichtete Graphen transformiert. Die in Klammern gestellten Parameter beschreiben Anforderungslevel(D) und Sicherheitslevel(L). Die hier durchgeführte Abbildung berücksichtigt nicht nur die Sicherheitsanforderungen aller Parteien unter Berücksichtigung der Basisanforderungen, sondern achtet zusätzlich noch auf Kostenminimierung. Insgesamt existieren drei Abbildungsmöglichkeiten, die gewählte ist jedoch die günstigste, unter dem Aspekt keine Sicherheitsressourcen zu verschwenden. Dieser VNR hätte auch auf EDGH abgebildet werden können, wobei der Link ED über einen Sicherheitslevel verfügt, welcher höher als nötig ist. Würde dies nicht beachtet werden, könnte es zu unnötigen Engpässen bei der Behandlung von VNRs mit höheren Anforderungslevels kommen. Um ein solches Verhalten zu erreichen, wurden zusätzlich Kosten- und Nutzen-Funktionen in die Berechnung integriert.

$$\rho(i) = \begin{cases} 1, & \text{if request No. } i \text{ is accepted.} \\ 0, & \text{if request No. } i \text{ is denied.} \end{cases}, \forall i \in \{1, 2, \dots, |M|\}. \quad (1)$$

$$Rev(M_i) = \rho(i) \times Dur_i^V \times \left[ \sum_{n_i^V \in N_i^V} dem^V(n_i^V) \times cpu^V(n_i^V) + \sum_{l_i^V \in L_i^V} dem^V(l_i^V) \times bw^V(l_i^V) \right]. \quad (2)$$

$$Cost(M_i) = \rho(i) \times Dur_i^V \times \left[ \sum_{n_i^V \in N_i^V} lev^S(M_{i,N}(n_i^V)) \times cpu^V(n_i^V) + \sum_{l_i^V \in L_i^V} lev^S(M_{i,L}(l_i^V)) \times len(M_{i,L}(l_i^V)) \times bw^V(l_i^V) \right]. \quad (3)$$

$$\max \lim_{n \rightarrow \infty} \frac{\sum_{i=1}^n \rho(i)}{n}, \text{ where } \rho(i) = \begin{cases} 1, & \text{if } VNR_i \text{ accepted.} \\ 0, & \text{if } VNR_i \text{ denied.} \end{cases}, \quad (4)$$

$$\max \lim_{T \rightarrow \infty} \frac{\sum_{i=1}^{|M|} Rev(M_i)}{T}, \quad (5)$$

$$\max \lim_{T \rightarrow \infty} \frac{Rev(\mathbf{M})}{T} / \lim_{T \rightarrow \infty} \frac{Cost(\mathbf{M})}{T}. \quad (6)$$

$$\sum_{r=1}^{|N^S|} x_{i,qr} = 1, \quad \forall n_{i,q} \in N_i^V, \quad (7)$$

$$\sum_{r=1}^{|P^S|} y_{i,qr} = 1, \quad \forall l_{i,q} \in L_i^V, \quad (8)$$

$$\sum_{i=1}^{|N|} x_{i,qr} cpu_i^V(n_{i,q}) \leq cpu^S(n_r), \quad \forall n_{i,q} \in N_i^V, n_r \in N^S, \quad (9)$$

$$\sum_{i=1}^{|N|} y_{i,qr} bw_i^V(l_{i,q}) \leq \min_{l_j \in p_r} bw^S(l_j), \quad \forall l_{i,q} \in L_i^V, p_r \in P^S, \quad (10)$$

$$x_{qr} dem^S(n_r) \leq lev^V(n_q), \quad \forall n_q \in N_i^V, n_r \in N^S, \quad (11)$$

$$x_{qr} dem^V(n_q) \leq lev^S(n_r), \quad \forall n_q \in N_i^V, n_r \in N^S, \quad (12)$$

$$\max\{dem^S(n_r), \max_{x_{qr}=1} dem^V(n_q)\} \leq \min\{lev^S(n_r), \min_{x_{qr}=1} lev^V(n_q)\}, \quad \forall n_q \in N_i^V, n_r \in N^S, \quad (13)$$

$$dem^V(l_q) \leq \min_{l_i \in p_r, y_{qr} > 0} lev^S(l_i), \quad \forall l_q \in L_i^V, p_r \in P^S. \quad (14)$$

$$H^{(t+1)}(n, k) = \lambda \sum_{(m,n) \in Link(n)} PC((m, n), k) H^{(t)}(m, k) + (1 - \lambda) H^{(t)}(n, k), \quad (16)$$

Das außergewöhnliche bei diesem Ansatz ist die Verwendung zweier unterschiedlicher Algorithmen, welche sich gegenseitig ergänzen: uSAV und cSAV.

- **uSAV**  
uSAV, der unkoordinierte zwei-Phasen-Algorithmus, behandelt Knoten- und Link-Abbildungen getrennt voneinander. Dementsprechend liegt die Schwäche von uSAV in der Abbildung von non-splittable-links. uSAV ist ein terminierender Algorithmus, welcher die Abbildung der Knoten priorisiert und dahingehend ein sehr gutes Ergebnis mit wenig Aufwand erzielt. Jedoch kann es, durch die Priorisierung der Knoten, zu hohen Kosten bei der Link-Abbildung kommen.
- **cSAV**  
cSAV, der koordinierte Algorithmus, behandelt Knoten und Links gemeinsam, und kann zur Optimierung, des bereits von uSAV gelieferten Ergebnisses verwendet werden. cSAV liefert zwar optimalere Ergebnisse als uSAV, benötigt aber auch mehr Zeit. Hier muss Zeitaufwand mit gelieferter Leistung abgewogen werden.

Beide Varianten nutzen die selben Heuristiken. Der Author schlägt für ideale Ergebnisse eine kombinierte Benutzung der beiden Varianten vor.

#### uSAV

```

1: For all requests in the time window, set the ones that did not expire yet but
   classified with MAP_FAILED to NEW.
2: Release the substrate resources that were occupied by DONE requests. Re-
   fresh the redundant network.
3: repeat
4:   Get  $G_i^V$  that has the maximum revenue from all NEW requests in the time
   window.
5:   Map the nodes of  $G_i^V$  using the node mapping algorithm.
6:   if MAP_NODE.SUCCESS then
7:     Map the links of  $G_i^V$  using the link mapping algorithm.
8:     if MAP_SUCCESS then
9:       Occupy the substrate resources. Refresh the redundant network.
10:      Set the state of  $G_i^V$  to MAP_SUCCESS.
11:    return
12:   Set the state of  $G_i^V$  to MAP_FAILED.
13:   Release the occupied resources of  $G_i^V$ .
14: until There is no more NEW requests in the time window
15: return

```

### cSAV

**Input:** The redundant substrate network as  $G^S$ . The current interested virtual network request as  $G^V$ .

- 1: Initialize variables:  $N$  for maximum back-off times; two empty stacks  $S$  (for mapped nodes) and  $Q$  (for unmapped nodes).
- 2: Apply the heuristic computation in the virtual network. Find the virtual node  $m$  with the highest heuristic value  $H(m)$ . Let node  $m' = m$ .
- 3: **repeat**
- 4:   Try to map  $m$  to  $n \in G_S$ , starting from substrate node with higher heuristic value.
- 5:   **if** No applicable substrate node  $n$  to host virtual node  $m$  and corresponding virtual link  $mm'$  **then**
- 6:     **if**  $N == 0$  **then**
- 7:       **return** MAP\_FAILED
- 8:     **else**
- 9:        $N \leftarrow N - 1$
- 10:       $Q.push(m)$ ,  $m = S.pop()$ .
- 11:       $S.push(m)$ .
- 12:    Update the redundant network, recalculating heuristics.
- 13:    **for all** Virtual node  $m' \in Adj(m)$  in the decreasing order of  $H(m')$  **do**
- 14:       $Q.push(m')$
- 15:       $m' = m$ .  $m = Q.pop()$ .
- 16: **until**  $Empty(Q) == \text{true}$
- 17: **return** MAP\_SUCCESS

### Sub-Algorithmus 1: Knoten-Abbildungen

```

1: For each possible security demand  $k$ , sort all substrate nodes in a candidate
   node queue  $queue(k)$  in descending order of heuristic value  $H$ .
2: For all nodes  $m \in G_i^S$ , initialize their state by setting  $Occupied(m) =$ 
   FALSE.
3: repeat
4:   Get an unmapped node  $n$  randomly from  $G_i^V$ .
5:    $k = dem^V(n)$ .
6:   if  $\exists$  node  $m \in queue(k)$  s.t.  $Occupied(m) = \text{FALSE}$  and  $dem^S(m) \leq$ 
      $lev^V(n)$  and  $cpu^S(m) \geq cpu^V(n)$  then
7:      $Occupied(m) = \text{TRUE}$ .
8:     Map the virtual node  $n$  onto the substrate node  $m$ .
9:   else
10:    Release all resources occupied by  $G_i^V$ .
11:   return MAP_FAILED.
12: until all nodes in  $G_i^V$  are mapped successfully.
13: return NODE_MAP_SUCCESS.

```

### Sub-Algorithmus 2: Link-Abbildungen

```

1: for each unmapped virtual link  $l \in G_i^V$  do
2:    $bw_r = bw^V(l), k = lev^V(l), flag = 0.$ 
3:   if  $l$  is splittable then
4:      $split = 1.$ 
5:   else
6:      $split = MAX\_SPLIT\_TIME.$ 
7:   Let  $m_1, m_2 \in G^S$  be the hosts of both ends of  $l.$ 
8:   repeat
9:     if  $\exists p \in P^S$  s.t.  $p : m_1 \rightarrow m_2$  has the minimum  $PCC(p, k)$  then
10:       $bw^S(p) = \min_{t \in p} bw^S(t), t \in L^S.$ 
11:      Map the remaining resources of  $l$  onto  $p.$ 
12:       $bw_r = bw_r - bw^S(p).$ 
13:      if  $bw_r \geq 0$  then
14:         $flag = 1.$ 
15:      else
16:         $split = MAX\_SPLIT\_TIME + 1.$ 
17:    until  $flag = 1$  or  $split > MAX\_SPLIT\_TIME$ 
18:    if  $flag = 0$  then
19:      return MAP_FAILED.
20: return MAP_SUCCESS.

```

Die Testumgebung dieses Ansatzes wurde mittels GT-ITM-Tool [cite-missing!](#) erstellt.

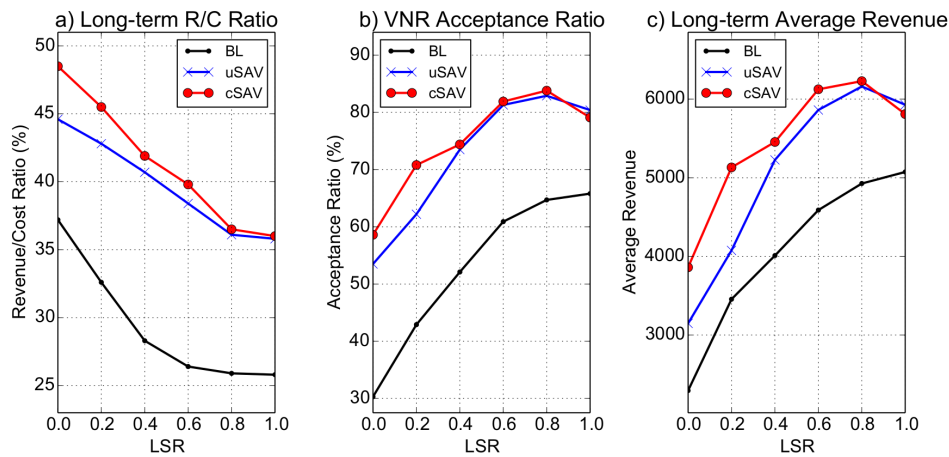
Die physischen Netze wurden in der Größenordnung eines mittleres ISP angesetzt, und betrugen 100 Knoten und 500 Links. Die Bandbreite und Rechenkapazität wurden, wie auch im vorherigen Ansatz, gleichmäßig verteilt und betrugen Werte zwischen 50 und 100. Die abstrakten Sicherheitslevels der physischen Elemente wurden zwischen 0 und 4 gleichmäßig verteilt. Die Anforderungslevels wurden ebenfalls aus dem Bereich 0-4 gewählt, und so verteilt, dass kein physisches Element ein höheres Anforderungslevel als Sicherheitslevel besitzt.

Die VNRs beinhalteten 2 bis 20 Knoten sowie halbsoviele Links. Die Bandbreite- und Rechenkapazitäts-Forderungen wurden zwischen 0 und 50 gewählt und ebenfalls gleichmäßig verteilt. Die zeitlichen Parameter wurden auf durchschnittlich (Poisson-Verteilung) 5 Anforderungen pro 100 Zeiteinheiten begrenzt. Die Verwendungszeit eines VNRs folgt einer Exponential-Verteilung und beträgt im Durchschnitt 500 Zeiteinheiten. Eine einzelne Simulation erhielt 1500 VNRs und dauerte 30000 Zeiteinheiten.



Als Vergleichswert wurde der Algorithmus aus cite-6-missing verwendet. Die Tests wurden für drei, anhand der Link-Split-Ratio unterschiedenen Szenarien ausgelegt: High-LSR(mehr als 80% der Links dürfen gesplittet werden), Low-LSR(weniger als 20%) und VLSR(varied LSR). Da letzteres Testszenario am meisten Bezug zur Realität hat, werden wir hier nur diese Ergebnisse vorstellen.

Testergebnisse für VLSR



Man sieht hier die drei, am schwersten gewichteten Aspekte dieses Ansatzes. Der Kosten-/Nutzen-Wert sinkt mit zunehmender LSR, während die Akzeptanz und der Nutzen gegen- teiliges Verhalten zeigen. Die vorhandenen Laufzeitanalysen der Algorithmen bestätigen die Aussagen der Autoren. uSAV führt hier mit Werten zwischen 6 und 10 Minuten, während cSAV erst nach 14 bis 25 Minuten brauchbare Ergebnisse für einzelne VNRs liefert. Hinzuzufügen sei hier, dass für alle Simulationen der einfachste Sicherheitsvektor verwendet wurde und bei Verwendung eines ausgeprägten Vektors die Rechenzeit mit Sicherheit andere Maße annimmt.

#### 4.3 Vergleich

Um nun die beiden vorgestellten Ansätze in einen Vergleich zu bringen, möchten wir uns hier nicht auf die Ergebnisse der Testszenarien konzentrieren, sondern auf die unterschiedlichen Herangehensweisen.

Der - für uns wichtigste - Unterschied zwischen den beiden Ansätzen bezieht sich auf Granularität der Sicherheitsanforderungen. Ansatz 1 versucht hier mittels drei, auf Teil- elemente bezogene, Sicherheitspläne einen größtmöglichen Schutz zu bieten. Ein Vorteil dieses Vorgehens liegt klar in der Einfachheit der Umsetzungsmöglichkeit und der Limi- tierung zusätzlicher Parameter, durch welche die Rechenzeit der Algorithmen im Zaum

gehalten wird. Nachteile könnten sich aus der Starrheit des Sicherheitssystems und dem Kostenfaktor ergeben. Ansatz 2 bietet hier etwas mehr Flexibilität sowie Präzision. Die entsprechenden Vektoren müssten hierfür zwar erst definiert werden, bieten dafür aber Erweiterbarkeit, was ein Vorteil bezüglich Flexibilität und Nachteil bezüglich Rechen- sowie Zeit-Aufwand darstellen kann. [detailliertere Ausführungen für diesen Punkt folgen]

Ein weiterer Unterschied ist die Herangehensweise bei der Berechnung. Pre-Processing kann das Abbilden der VNRs deutlich verkürzen, muss jedoch sequenziell durchgeführt werden und benötigt bei komplexeren VNRs vermutlich auch eine nicht zu vernachlässigende Inanspruchnahme von Rechenzeit. Ansatz 2 versucht an dieser Stelle mittels Heuristiken und zweier unterschiedlicher Algorithmen das gewünschte Ziel zu erreichen.

## 5 Schlussfolgerung und Ausblick

Frage: Auf welcher Ebene wird virtualisiert? Auf IP-Ebene? Was ist dann aber mit IP-Support-Protokollen (ARP)? Oder nicht-IP-Protokollen? Will ich ein Netzwerk virtualisieren, oder nur den IP-Verkehr? Verkapselung führt zu Leistungseinbußen. [CDRS07]

Fragen aus den Herausforderungen, die sich aus Sicherheitsrisiken ergeben...

## Literatur

- [APST05] Thomas Anderson, Larry Peterson, Scott Shenker und Jonathan Turner. Overcoming the Internet impasse through virtualization. *Computer*, 38(4):34–41, 2005.
- [BOB<sup>+</sup>12] Leonardo Richter Bays, Rodrigo Ruas Oliveira, Luciana Salete Buriol, Marinho Pilla Barcellos und Luciano Paschoal Gaspary. Security-aware optimal resource allocation for virtual network embedding. In *Proceedings of the 8th International Conference on Network and Service Management*, Seiten 378–384. International Federation for Information Processing, 2012.
- [CDRS07] Serdar Cabuk, Chris I Dalton, HariGovind Ramasamy und Matthias Schunter. Towards automated provisioning of secure virtualized networks. In *Proceedings of the 14th ACM conference on Computer and communications security*, Seiten 235–245. ACM, 2007.
- [Col11] Eric Cole. Network Security Bible: Edition 2, 2011.
- [DMT11] Kamal Dahbur, Bassil Mohammad und Ahmad Bisher Tarakji. A survey of risks, threats and vulnerabilities in cloud computing. In *Proceedings of the 2011 International conference on intelligent semantic Web-services and applications*, Seite 12. ACM, 2011.
- [FBB<sup>+</sup>13] Andreas Fischer, Juan Felipe Botero, Michael Till Beck, Hermann De Meer und Xavier Hesselbach. Virtual network embedding: A survey. *IEEE Communications Surveys & Tutorials*, 15(4):1888–1906, 2013.

- [GCH<sup>+</sup>16] Shuiqing Gong, Jing Chen, Conghui Huang, Qingchao Zhu und Siyi Zhao. Virtual Network Embedding through Security Risk Awareness and Optimization. *KSI Transactions on Internet & Information Systems*, 10(7), 2016.
- [GR05] Tal Garfinkel und Mendel Rosenblum. When virtual is harder than real: Security challenges in virtual machine based computing environments. In *HotOS*, 2005.
- [hi] <http://www-01.ibm.com/software>. CPLEX.
- [Liu10] H. Liu. A new form of dos attack in a cloud and its avoidance mechanism, in: Proceedings of the 2010 ACM Workshop on Cloud Computing Security Workshop, 2010.
- [MRR13] Raouf Boutaba Muntasir Raihan Rahman. Survivable Virtual Network Embedding Algorithms for Network Virtualization, 2013.
- [NW] Sriram Natarajan und Tilman Wolf. Security Issues in Network Virtualization for the Future Internet.
- [OCJ08] Jon Oberheide, Evan Cooke und Farnam Jahanian. Empirical exploitation of live virtual machine migration. In *Proc. of BlackHat DC convention*. Citeseer, 2008.
- [QH13] X. Cao Q. Hu, Y. Wan. Resolve the virtual network embedding problem: a column generation approach. *INFOCOM, 2013 Proceedings IEEE*, 2013.
- [RA93] J.B. Orlin R.K. Ahuja, R.L. Magnanti. Network Flow: Theory, Algorithms and Applications, 1993.
- [RT08] Joanna Rutkowska und Alexander Tereshkin. Bluepillling the xen hypervisor. *Black Hat USA*, 2008.
- [RTSS09] Thomas Ristenpart, Eran Tromer, Hovav Shacham und Stefan Savage. Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. In *Proceedings of the 16th ACM conference on Computer and communications security*, Seiten 199–212. ACM, 2009.
- [SL15] Hong Xu Ming Xu Shuhao Liu, Zhiping Cai. Towards Security-aware Virtual Network Embedding, 2015.
- [WCC16] Yang Wang, Phanvu Chau und Fuyu Chen. Towards a secured network virtualization. *Computer Networks*, 104:55–65, 2016.
- [WDWY10] Hanqian Wu, Yi Ding, Chuck Winer und Li Yao. Network security for virtual machine in cloud computing. In *Computer Sciences and Convergence Information Technology (ICCIT), 2010 5th International Conference on*, Seiten 18–21. IEEE, 2010.