Adversarial Trends in Mobile Communication Systems: From Attack Patterns to Potential Defenses Strategies

Hsin Yi Chen, Siddharth Prakash Rao

A! Aalto University

NOKIA Bell Labs

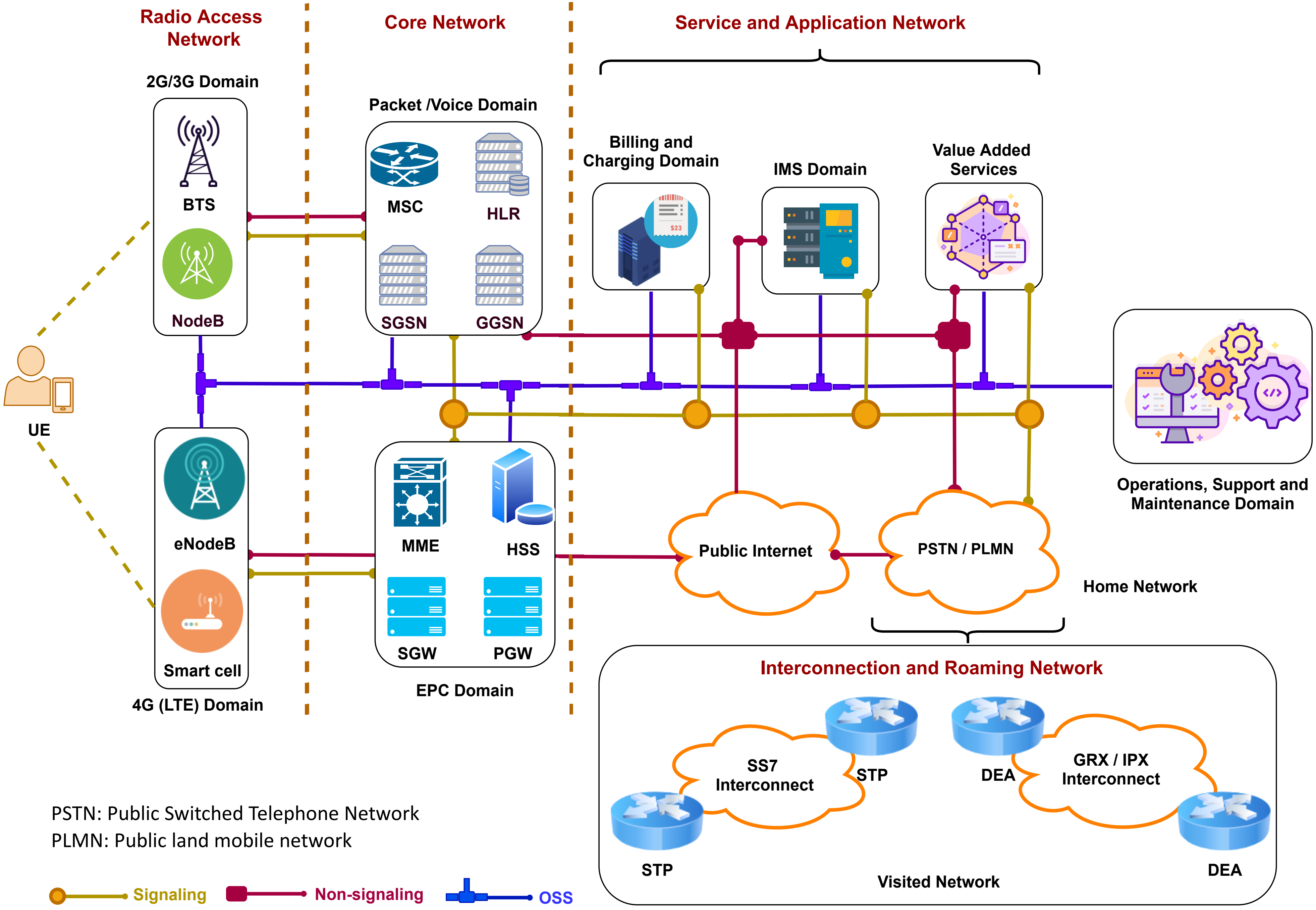
Agenda

- Problem Statement
- Background & Methodology
- Graph Analysis Results & Defense Strategies
- Discussion & Conclusion
- Future Direction

Understand adversarial behaviours in telco system

- Threat modeling
  - **Threat modeling** is the process of developing and applying a structured representation of adversarial threats
  - MITRE ATT&CK (Adversarial Tactics, Techniques, and Procedures - TTPs)
- Bhadra: domain-specific threat modelling framework for telco industry
- Modeling Attack/ Threat: Tag attack steps or threat with Bhadra conceptual framework to have a common representation

Background

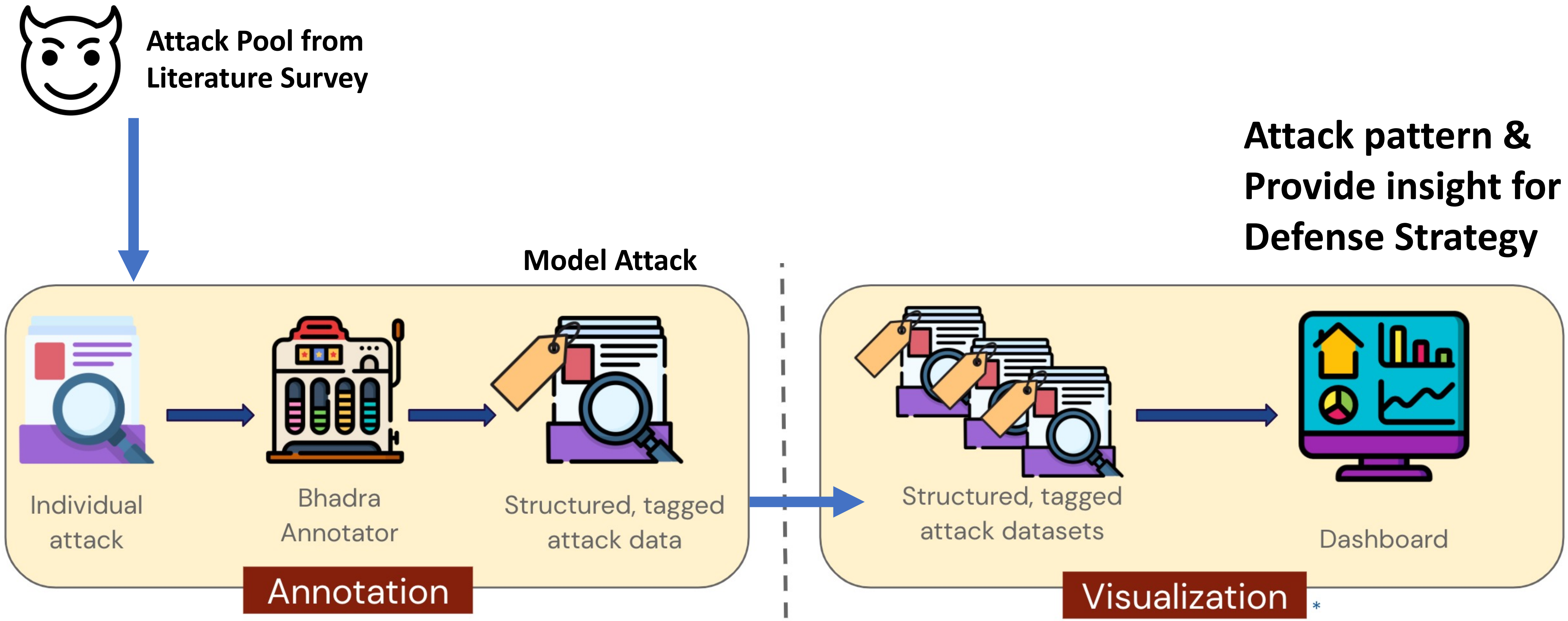


PSTN: Public Switched Telephone Network
PLMN: Public land mobile network

Bhadra Framework

	Attack Mounting				Attack Execution			Attack Results	
Tactic	**Reconnaissance**	**Initial Access**	**Persistence**	**Discovery**	**Lateral Movement**	**Standard Protocol Misuse**	**Defense Evasion**	**Collection**	**Impact**
Technique	Perimeter mapping of network infrastructure	Access from UE	Infecting UE hardware or software	Operator network mapping	Exploit roaming agreements	SS7-based techniques	Malware anti-detection techniques	Admin,node, and user credentials	Location tracking
	Perimeter mapping for mobiles	SIM-based compromised	Infecting network elements	CN-protocol scanning	Abusing interworking functionalities	Diameter-based techniques	Blacklist evasion	User-specific identifiers	Calls eavesdropping
	Target intelligence gathering	Access from radio access network	Hard-to-repair vulnerabilities	Target intelligence gathering	Core-network access from compromised base station	GTP-based techniques	Exploit misconfigurations & implementation errors	Communication metadata	SMS and IMS interception
		Access from partner mobile network	Command and control channels	Internal resource search	Exploit platform- & service-specific vulnerabilities	IP-based techniques	Bypass firewall	User data	Data interception
		Access from inside the operator network		UE knocking		Pre-AKA techniques	Bypass homerouting	Operator-specific identifiers	Billing frauds
		Access from operator's IP network infrastructure				SIP-based techniques	Downgrading	Operator data	DoS against the network
		Access from the public Internet					Redirection		DoS against a specific user
		Compromised Insiders and Human Errors					Stealth scanning		Identity-related attacks

Methodology



Attack Pool from Literature Survey

Attack pattern & Provide insight for Defense Strategy

Model Attack

Individual attack

Bhadra Annotator

Structured, tagged attack data

Annotation

Structured, tagged attack datasets

Dashboard

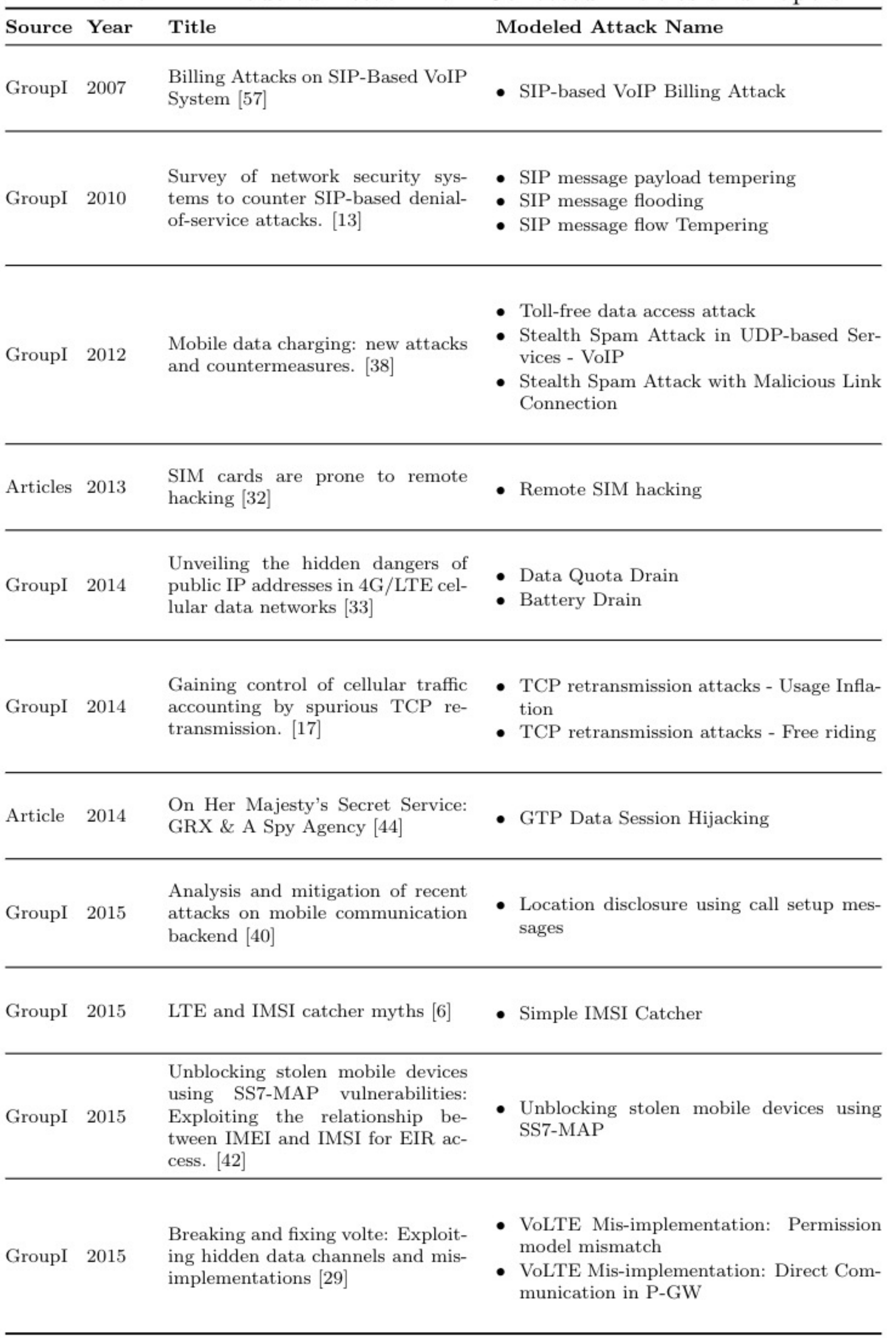
Visualization *

Graph Analysis

Attack Collection

- Literature Survey from Bhadra’s original paper
  - Group I: peer-reviewed papers that describe one or multiple attacks scenarios.
  - Group II: security reports from standardization bodies (e.g., 3GPP, GSMA),regulatory agencies (e.g. ENISA) and security companies
- Selection process
  - Multi-stage attack
  - Clear initial access and impact
  - Variety of attack vectors
- 60 attacks populated from 30 of the sources

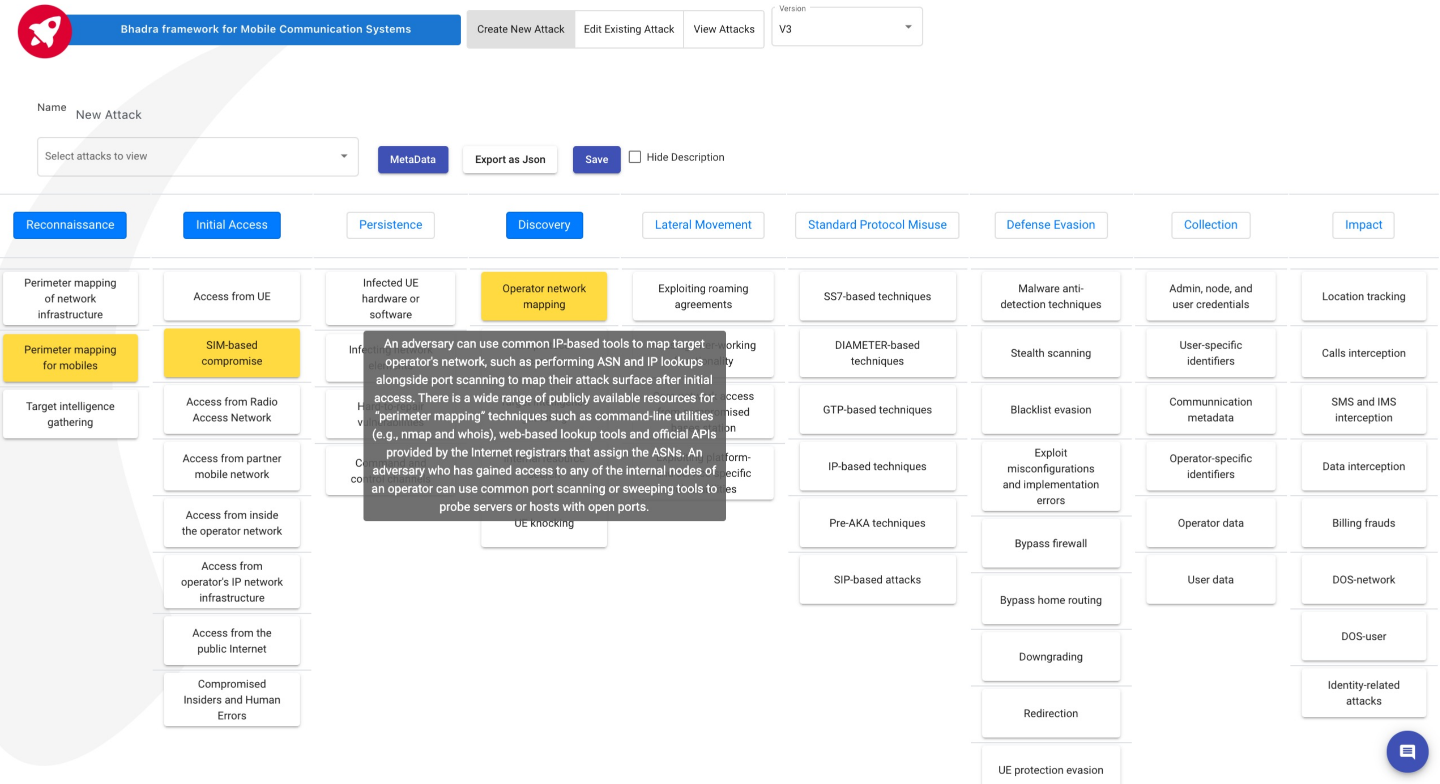
Table A.1: Modeled Attack from Collected Articles and Papers



Source	Year	Title	Modeled Attack Name
GroupI	2007	Billing Attacks on SIP-Based VoIP System [57]	• SIP-based VoIP Billing Attack
GroupI	2010	Survey of network security systems to counter SIP-based denial-of-service attacks. [13]	• SIP message payload tempering • SIP message flooding • SIP message flow Tempering
GroupI	2012	Mobile data charging: new attacks and countermeasures. [38]	• Toll-free data access attack • Stealth Spam Attack in UDP-based Services - VoIP • Stealth Spam Attack with Malicious Link Connection
Articles	2013	SIM cards are prone to remote hacking [32]	• Remote SIM hacking
GroupI	2014	Unveiling the hidden dangers of public IP addresses in 4G/LTE cellular data networks [33]	• Data Quota Drain • Battery Drain
GroupI	2014	Gaining control of cellular traffic accounting by spurious TCP retransmission. [17]	• TCP retransmission attacks - Usage Inflation • TCP retransmission attacks - Free riding
Article	2014	On Her Majesty’s Secret Service: GRX & A Spy Agency [44]	• GTP Data Session Hijacking
GroupI	2015	Analysis and mitigation of recent attacks on mobile communication backend [40]	• Location disclosure using call setup messages
GroupI	2015	LTE and IMSI catcher myths [6]	• Simple IMSI Catcher
GroupI	2015	Unblocking stolen mobile devices using SS7-MAP vulnerabilities: Exploiting the relationship between IMEI and IMSI for EIR access. [42]	• Unblocking stolen mobile devices using SS7-MAP
GroupI	2015	Breaking and fixing volte: Exploiting hidden data channels and mis-implementations [29]	• VoLTE Mis-implementation: Permission model mismatch • VoLTE Mis-implementation: Direct Communication in P-GW

Attack Modeling

- Independent Modeling
- Discussion



Bhadra framework for Mobile Communication Systems

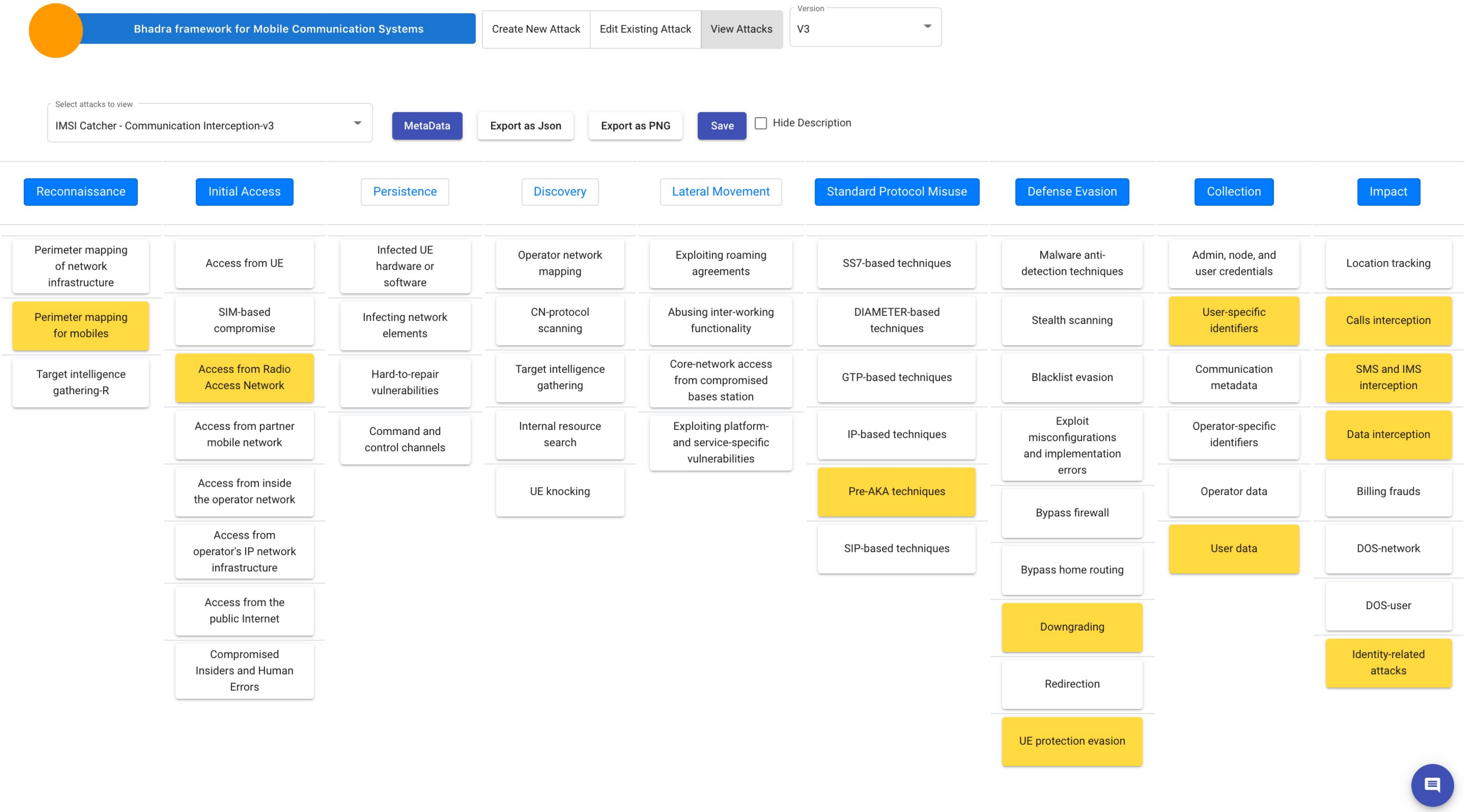
Name: New Attack

Select attacks to view

Reconnaissance	Initial Access	Persistence	Discovery	Lateral Movement	Standard Protocol Misuse	Defense Evasion	Collection	Impact
Perimeter mapping of network infrastructure	Access from UE	Infected UE hardware or software	Operator network mapping	Exploiting roaming agreements	SS7-based techniques	Malware anti-detection techniques	Admin, node, and user credentials	Location tracking
Perimeter mapping for mobiles	SIM-based compromise	Inf		orking ty	DIAMETER-based techniques	Stealth scanning	User-specific identifiers	Calls interception
Target intelligence gathering	Access from Radio Access Network	H v		ccess ised on	GTP-based techniques	Blacklist evasion	Communication metadata	SMS and IMS interception
	Access from partner mobile network	C co		form- ecific es	IP-based techniques	Exploit misconfigurations and implementation errors	Operator-specific identifiers	Data interception
	Access from inside the operator network		UE knocking		Pre-AKA techniques	Bypass firewall	Operator data	Billing frauds
	Access from operator's IP network infrastructure				SIP-based attacks	Bypass home routing	User data	DOS-network
	Access from the public Internet					Downgrading		DOS-user
	Compromised Insiders and Human Errors					Redirection		Identity-related attacks
						UE protection evasion		

An adversary can use common IP-based tools to map target operator's network, such as performing ASN and IP lookups alongside port scanning to map their attack surface after initial access. There is a wide range of publicly available resources for "perimeter mapping" techniques such as command-line utilities (e.g., nmap and whois), web-based lookup tools and official APIs provided by the Internet registrars that assign the ASNs. An adversary who has gained access to any of the internal nodes of an operator can use common port scanning or sweeping tools to probe servers or hosts with open ports.

Model Individual Attack – IMSI Catcher Communication Interception



Version: V3

Select attacks to view: IMSI Catcher - Communication Interception-v3

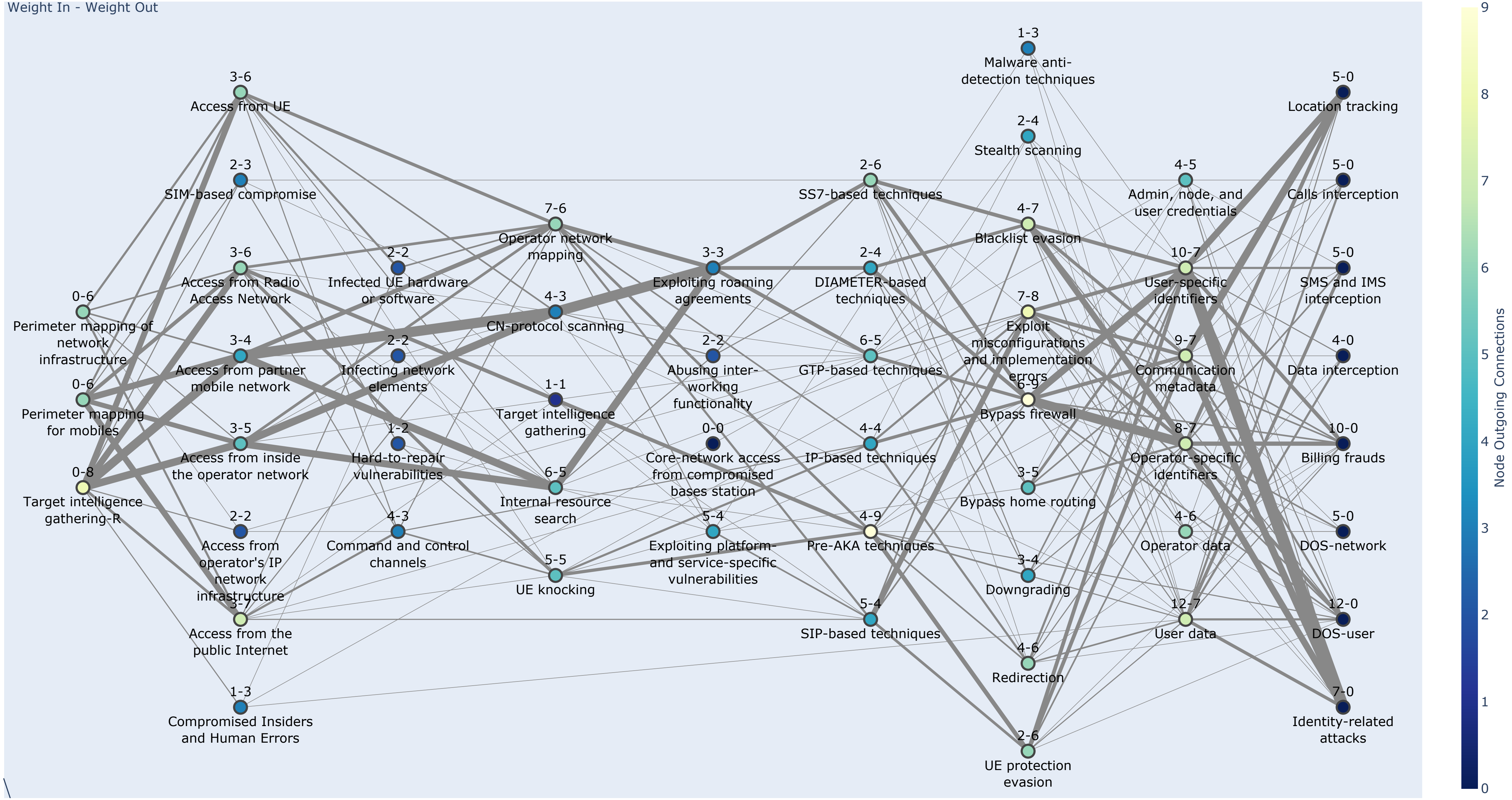
□ Hide Description

Reconnaissance	Initial Access	Persistence	Discovery	Lateral Movement	Standard Protocol Misuse	Defense Evasion	Collection	Impact
Perimeter mapping of network infrastructure	Access from UE	Infected UE hardware or software	Operator network mapping	Exploiting roaming agreements	SS7-based techniques	Malware anti-detection techniques	Admin, node, and user credentials	Location tracking
Perimeter mapping for mobiles	SIM-based compromise	Infecting network elements	CN-protocol scanning	Abusing inter-working functionality	DIAMETER-based techniques	Stealth scanning	**User-specific identifiers**	**Calls interception**
Target intelligence gathering-R	**Access from Radio Access Network**	Hard-to-repair vulnerabilities	Target intelligence gathering	Core-network access from compromised bases station	GTP-based techniques	Blacklist evasion	Communication metadata	**SMS and IMS interception**
	Access from partner mobile network	Command and control channels	Internal resource search	Exploiting platform- and service-specific vulnerabilities	IP-based techniques	Exploit misconfigurations and implementation errors	Operator-specific identifiers	**Data interception**
	Access from inside the operator network		UE knocking		**Pre-AKA techniques**	Bypass firewall	Operator data	Billing frauds
	Access from operator's IP network infrastructure				SIP-based techniques	Bypass home routing	**User data**	DOS-network
	Access from the public Internet					**Downgrading**		DOS-user
	Compromised Insiders and Human Errors					Redirection		**Identity-related attacks**
						UE protection evasion		

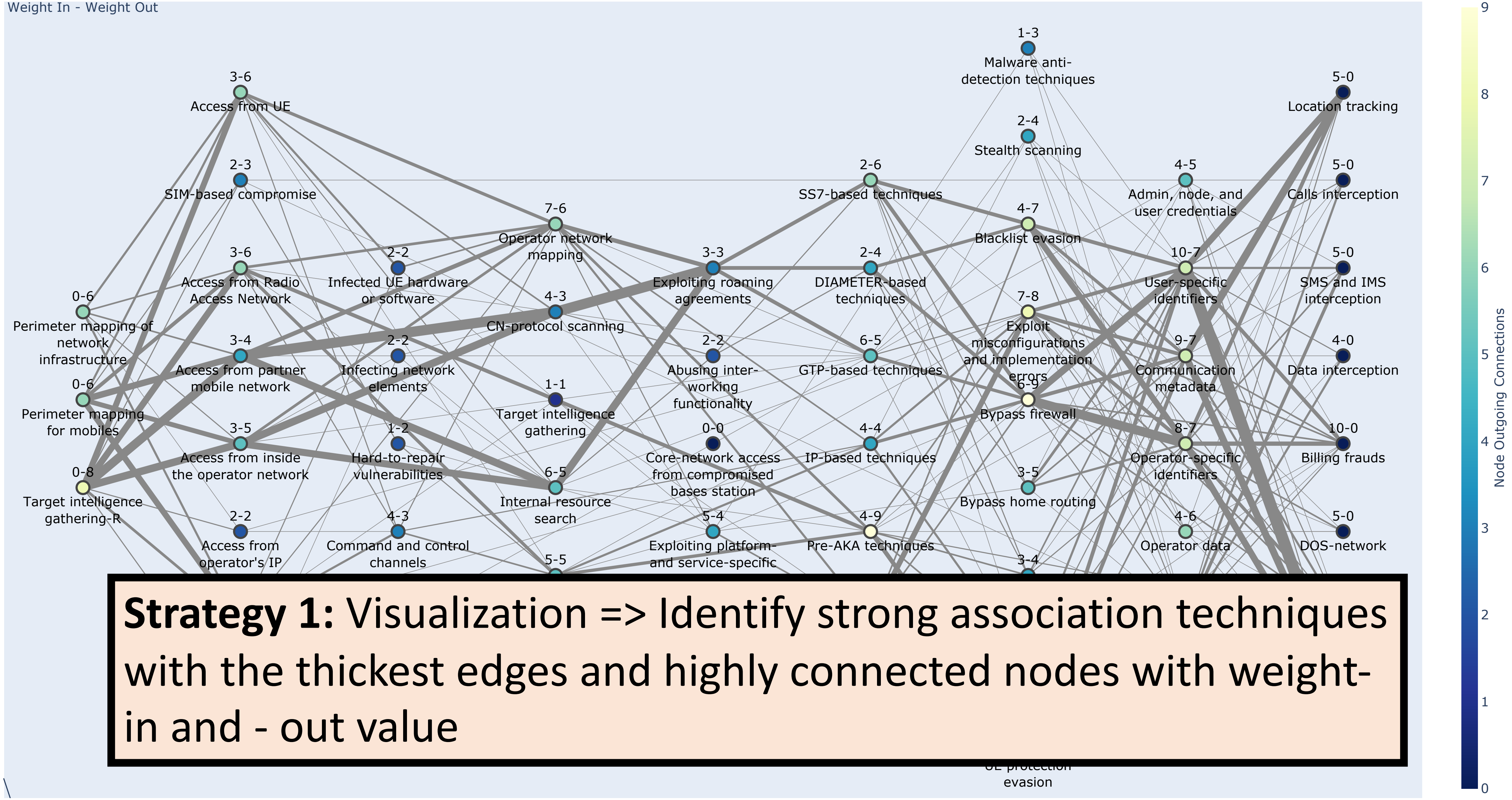
Graph Analysis

Common Subpaths – Association of Techniques
Connectivity – Importance of Techniques
Unique Paths – Diversity of Attack Techniques

Attack graphs


Weight In - Weight Out
0-6
Perimeter mapping of network infrastructure
0-6
Perimeter mapping for mobiles
0-8
Target intelligence gathering-R
3-6
Access from UE
2-3
SIM-based compromise
3-6
Access from Radio Access Network
3-4
Access from partner mobile network
3-5
Access from inside the operator network
2-2
Access from operator's IP network infrastructure
3-7
Access from the public Internet
1-3
Compromised Insiders and Human Errors
2-2
Infected UE hardware or software
2-2
Infecting network elements
1-2
Hard-to-repair vulnerabilities
4-3
Command and control channels
7-6
Operator network mapping
4-3
CN-protocol scanning
1-1
Target intelligence gathering
6-5
Internal resource search
5-5
UE knocking
3-3
Exploiting roaming agreements
2-2
Abusing inter-working functionality
0-0
Core-network access from compromised bases station
5-4
Exploiting platform- and service-specific vulnerabilities
2-6
SS7-based techniques
2-4
DIAMETER-based techniques
6-5
GTP-based techniques
4-4
IP-based techniques
4-9
Pre-AKA techniques
5-4
SIP-based techniques
1-3
Malware anti-detection techniques
2-4
Stealth scanning
4-7
Blacklist evasion
7-8
Exploit misconfigurations and implementation errors
6-9
Bypass firewall
3-5
Bypass home routing
3-4
Downgrading
4-6
Redirection
2-6
UE protection evasion
4-5
Admin, node, and user credentials
10-7
User-specific identifiers
9-7
Communication metadata
8-7
Operator-specific identifiers
4-6
Operator data
12-7
User data
5-0
Location tracking
5-0
Calls interception
5-0
SMS and IMS interception
4-0
Data interception
10-0
Billing frauds
5-0
DOS-network
12-0
DOS-user
7-0
Identity-related attacks
9
8
7
6
5
4
3
2
1
0
Node Outgoing Connections

Attack graphs


Weight In - Weight Out
0-6
Perimeter mapping of network infrastructure
0-6
Perimeter mapping for mobiles
0-8
Target intelligence gathering-R
3-6
Access from UE
2-3
SIM-based compromise
3-6
Access from Radio Access Network
3-4
Access from partner mobile network
3-5
Access from inside the operator network
2-2
Access from operator's IP
2-2
Infected UE hardware or software
2-2
Infecting network elements
1-2
Hard-to-repair vulnerabilities
4-3
Command and control channels
7-6
Operator network mapping
4-3
CN-protocol scanning
1-1
Target intelligence gathering
6-5
Internal resource search
5-5
3-3
Exploiting roaming agreements
2-2
Abusing inter-working functionality
0-0
Core-network access from compromised bases station
5-4
Exploiting platform- and service-specific
2-6
SS7-based techniques
2-4
DIAMETER-based techniques
6-5
GTP-based techniques
4-4
IP-based techniques
4-9
Pre-AKA techniques
1-3
Malware anti-detection techniques
2-4
Stealth scanning
4-7
Blacklist evasion
7-8
Exploit misconfigurations and implementation errors
6-9
Bypass firewall
3-5
Bypass home routing
3-4
UE protection evasion
4-5
Admin, node, and user credentials
10-7
User-specific identifiers
9-7
Communication metadata
8-7
Operator-specific identifiers
4-6
Operator data
5-0
Location tracking
5-0
Calls interception
5-0
SMS and IMS interception
4-0
Data interception
10-0
Billing frauds
5-0
DOS-network
Node Outgoing Connections
0
1
2
3
4
5
6
7
8
9

Strategy 1: Visualization => Identify strong association techniques with the thickest edges and highly connected nodes with weight-in and - out value

Common Subpaths

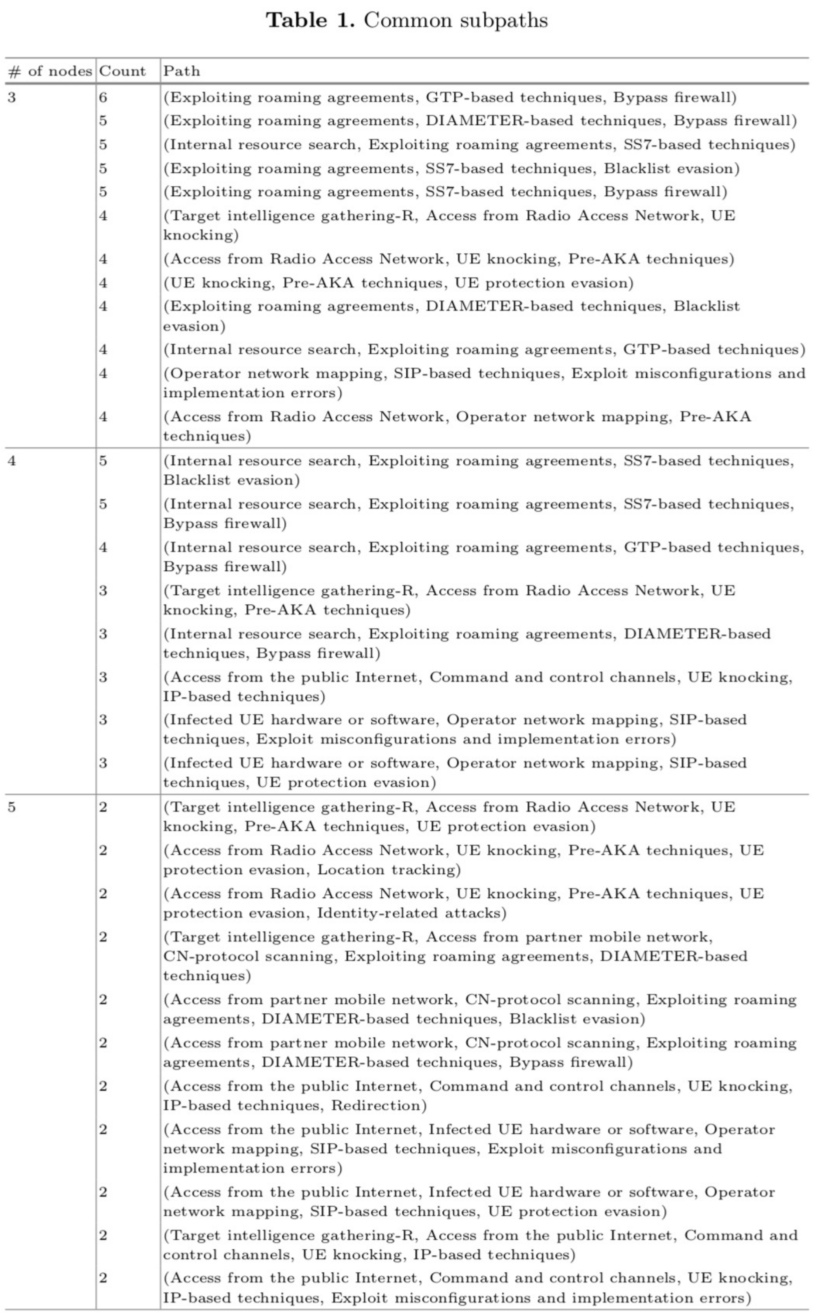


Table 1. Common subpaths

# of nodes	Count	Path
3	6	(Exploiting roaming agreements, GTP-based techniques, Bypass firewall)
	5	(Exploiting roaming agreements, DIAMETER-based techniques, Bypass firewall)
	5	(Internal resource search, Exploiting roaming agreements, SS7-based techniques)
	5	(Exploiting roaming agreements, SS7-based techniques, Blacklist evasion)
	5	(Exploiting roaming agreements, SS7-based techniques, Bypass firewall)
	4	(Target intelligence gathering-R, Access from Radio Access Network, UE knocking)
	4	(Access from Radio Access Network, UE knocking, Pre-AKA techniques)
	4	(UE knocking, Pre-AKA techniques, UE protection evasion)
	4	(Exploiting roaming agreements, DIAMETER-based techniques, Blacklist evasion)
	4	(Internal resource search, Exploiting roaming agreements, GTP-based techniques)
	4	(Operator network mapping, SIP-based techniques, Exploit misconfigurations and implementation errors)
	4	(Access from Radio Access Network, Operator network mapping, Pre-AKA techniques)
4	5	(Internal resource search, Exploiting roaming agreements, SS7-based techniques, Blacklist evasion)
	5	(Internal resource search, Exploiting roaming agreements, SS7-based techniques, Bypass firewall)
	4	(Internal resource search, Exploiting roaming agreements, GTP-based techniques, Bypass firewall)
	3	(Target intelligence gathering-R, Access from Radio Access Network, UE knocking, Pre-AKA techniques)
	3	(Internal resource search, Exploiting roaming agreements, DIAMETER-based techniques, Bypass firewall)
	3	(Access from the public Internet, Command and control channels, UE knocking, IP-based techniques)
	3	(Infected UE hardware or software, Operator network mapping, SIP-based techniques, Exploit misconfigurations and implementation errors)
	3	(Infected UE hardware or software, Operator network mapping, SIP-based techniques, UE protection evasion)
5	2	(Target intelligence gathering-R, Access from Radio Access Network, UE knocking, Pre-AKA techniques, UE protection evasion)
	2	(Access from Radio Access Network, UE knocking, Pre-AKA techniques, UE protection evasion, Location tracking)
	2	(Access from Radio Access Network, UE knocking, Pre-AKA techniques, UE protection evasion, Identity-related attacks)
	2	(Target intelligence gathering-R, Access from partner mobile network, CN-protocol scanning, Exploiting roaming agreements, DIAMETER-based techniques)
	2	(Access from partner mobile network, CN-protocol scanning, Exploiting roaming agreements, DIAMETER-based techniques, Blacklist evasion)
	2	(Access from partner mobile network, CN-protocol scanning, Exploiting roaming agreements, DIAMETER-based techniques, Bypass firewall)
	2	(Access from the public Internet, Command and control channels, UE knocking, IP-based techniques, Redirection)
	2	(Access from the public Internet, Infected UE hardware or software, Operator network mapping, SIP-based techniques, Exploit misconfigurations and implementation errors)
	2	(Access from the public Internet, Infected UE hardware or software, Operator network mapping, SIP-based techniques, UE protection evasion)
	2	(Target intelligence gathering-R, Access from the public Internet, Command and control channels, UE knocking, IP-based techniques)
	2	(Access from the public Internet, Command and control channels, UE knocking, IP-based techniques, Exploit misconfigurations and implementation errors)

Common Subpaths

- Exploit roaming agreement

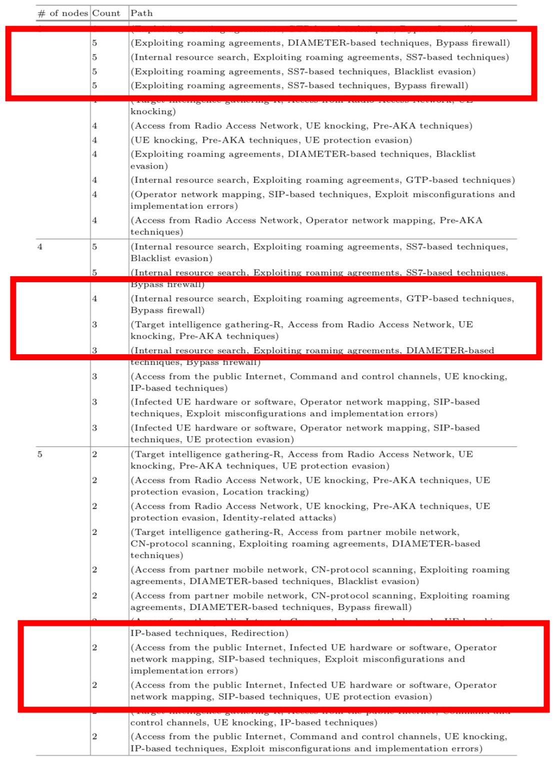
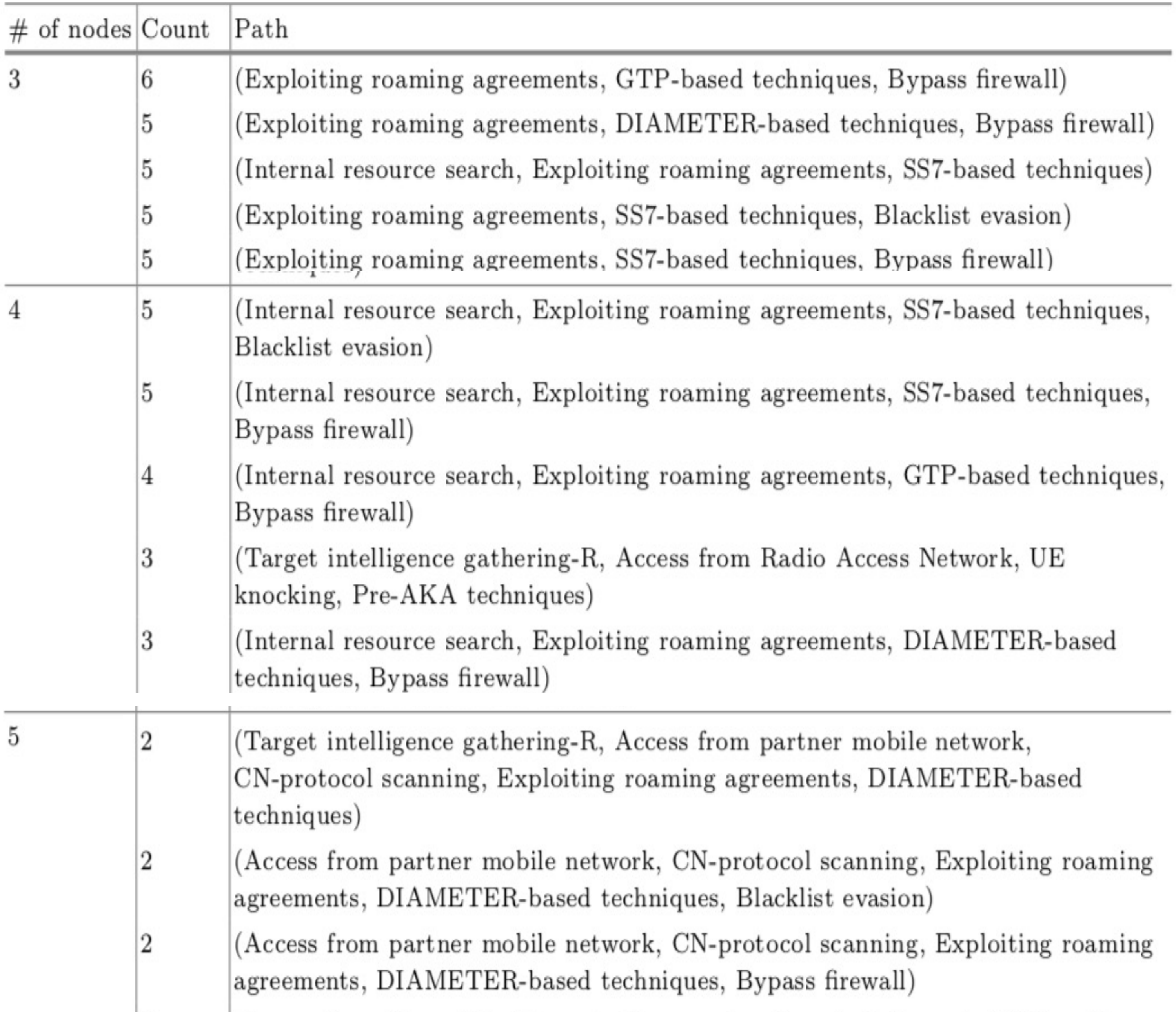


Table 1. Common subpaths

# of nodes	Count	Path
3	6	(Exploiting roaming agreements, GTP-based techniques, Bypass firewall)
	5	(Exploiting roaming agreements, DIAMETER-based techniques, Bypass firewall)
	5	(Internal resource search, Exploiting roaming agreements, SS7-based techniques)
	5	(Exploiting roaming agreements, SS7-based techniques, Blacklist evasion)
	5	(Exploiting roaming agreements, SS7-based techniques, Bypass firewall)
	4	(Target intelligence gathering-R, Access from Radio Access Network, UE knocking)
	4	(Access from Radio Access Network, UE knocking, Pre-AKA techniques)
	4	(UE knocking, Pre-AKA techniques, UE protection evasion)
	4	(Exploiting roaming agreements, DIAMETER-based techniques, Blacklist evasion)
	4	(Internal resource search, Exploiting roaming agreements, GTP-based techniques)
	4	(Operator network mapping, SIP-based techniques, Exploit misconfigurations and implementation errors)
	4	(Access from Radio Access Network, Operator network mapping, Pre-AKA techniques)
4	5	(Internal resource search, Exploiting roaming agreements, SS7-based techniques, Blacklist evasion)
	5	(Internal resource search, Exploiting roaming agreements, SS7-based techniques, Bypass firewall)
	4	(Internal resource search, Exploiting roaming agreements, GTP-based techniques, Bypass firewall)
	3	(Target intelligence gathering-R, Access from Radio Access Network, UE knocking, Pre-AKA techniques)
	3	(Internal resource search, Exploiting roaming agreements, DIAMETER-based techniques, Bypass firewall)
	3	(Access from the public Internet, Command and control channels, UE knocking, IP-based techniques)
	3	(Infected UE hardware or software, Operator network mapping, SIP-based techniques, Exploit misconfigurations and implementation errors)
	3	(Infected UE hardware or software, Operator network mapping, SIP-based techniques, UE protection evasion)
5	2	(Target intelligence gathering-R, Access from Radio Access Network, UE knocking, Pre-AKA techniques, UE protection evasion)
	2	(Access from Radio Access Network, UE knocking, Pre-AKA techniques, UE protection evasion, Location tracking)
	2	(Access from Radio Access Network, UE knocking, Pre-AKA techniques, UE protection evasion, Identity-related attacks)
	2	(Target intelligence gathering-R, Access from partner mobile network, CN-protocol scanning, Exploiting roaming agreements, DIAMETER-based techniques)
	2	(Access from partner mobile network, CN-protocol scanning, Exploiting roaming agreements, DIAMETER-based techniques, Blacklist evasion)
	2	(Access from partner mobile network, CN-protocol scanning, Exploiting roaming agreements, DIAMETER-based techniques, Bypass firewall)
	2	(Access from the public Internet, Command and control channels, UE knocking, IP-based techniques, Redirection)
	2	(Access from the public Internet, Infected UE hardware or software, Operator network mapping, SIP-based techniques, Exploit misconfigurations and implementation errors)
	2	(Access from the public Internet, Infected UE hardware or software, Operator network mapping, SIP-based techniques, UE protection evasion)
	2	(Target intelligence gathering-R, Access from the public Internet, Command and control channels, UE knocking, IP-based techniques)
	2	(Access from the public Internet, Command and control channels, UE knocking, IP-based techniques, Exploit misconfigurations and implementation errors)



# of nodes	Count	Path
3	6	(Exploiting roaming agreements, GTP-based techniques, Bypass firewall)
	5	(Exploiting roaming agreements, DIAMETER-based techniques, Bypass firewall)
	5	(Internal resource search, Exploiting roaming agreements, SS7-based techniques)
	5	(Exploiting roaming agreements, SS7-based techniques, Blacklist evasion)
	5	(Exploiting roaming agreements, SS7-based techniques, Bypass firewall)
4	5	(Internal resource search, Exploiting roaming agreements, SS7-based techniques, Blacklist evasion)
	5	(Internal resource search, Exploiting roaming agreements, SS7-based techniques, Bypass firewall)
	4	(Internal resource search, Exploiting roaming agreements, GTP-based techniques, Bypass firewall)
	3	(Target intelligence gathering-R, Access from Radio Access Network, UE knocking, Pre-AKA techniques)
	3	(Internal resource search, Exploiting roaming agreements, DIAMETER-based techniques, Bypass firewall)
5	2	(Target intelligence gathering-R, Access from partner mobile network, CN-protocol scanning, Exploiting roaming agreements, DIAMETER-based techniques)
	2	(Access from partner mobile network, CN-protocol scanning, Exploiting roaming agreements, DIAMETER-based techniques, Blacklist evasion)
	2	(Access from partner mobile network, CN-protocol scanning, Exploiting roaming agreements, DIAMETER-based techniques, Bypass firewall)

Common Subpaths

- Exploit roaming agreement

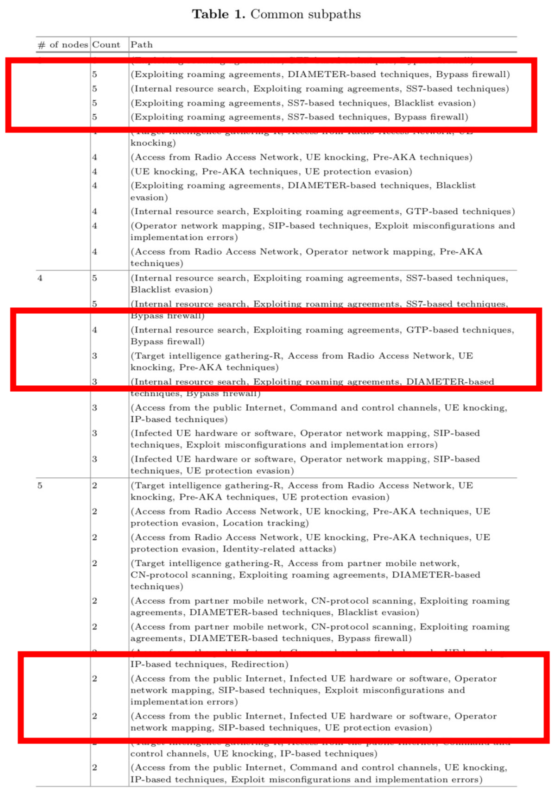
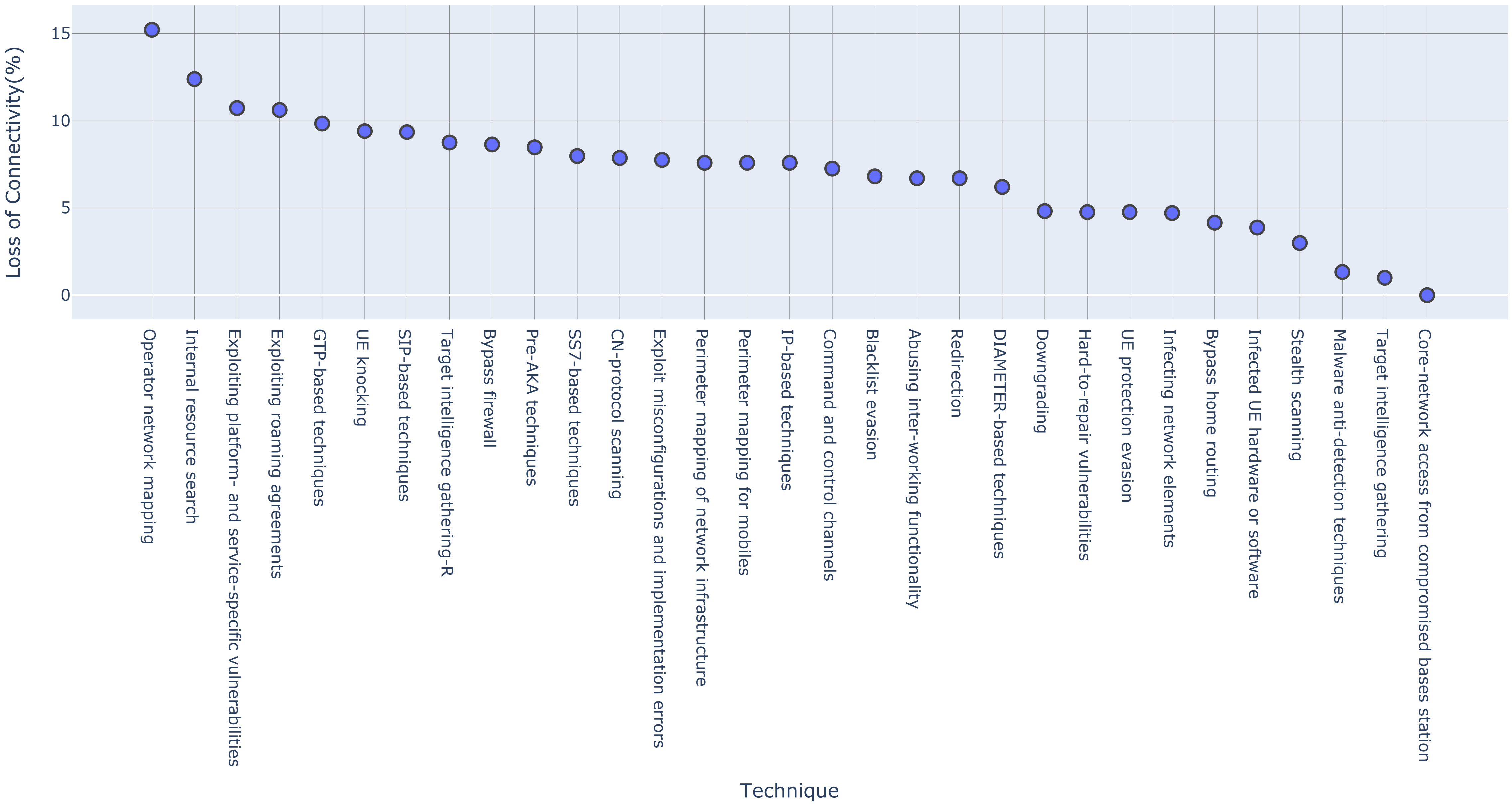


Table 1. Common subpaths

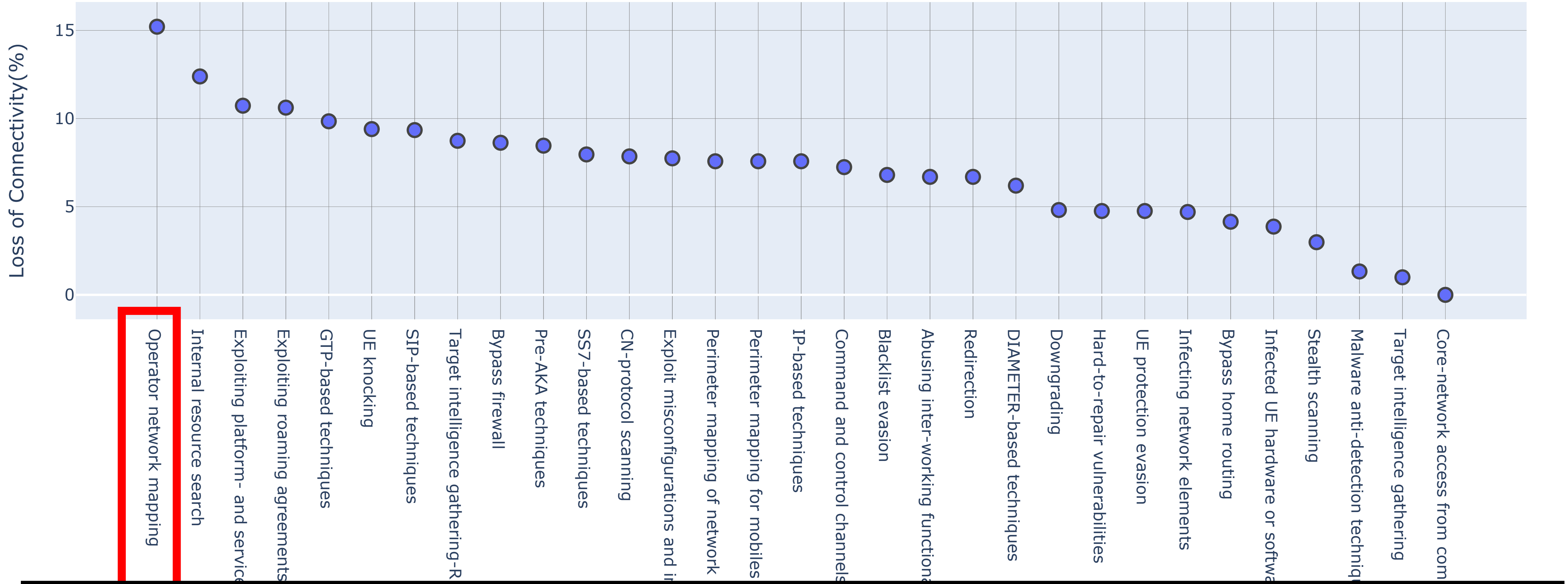
# of nodes	Count	Path
3	[illegible]	(Exploiting roaming agreements, GTP-based techniques, Bypass firewall)
	5	(Exploiting roaming agreements, DIAMETER-based techniques, Bypass firewall)
	5	(Internal resource search, Exploiting roaming agreements, SS7-based techniques)
	5	(Exploiting roaming agreements, SS7-based techniques, Blacklist evasion)
	5	(Exploiting roaming agreements, SS7-based techniques, Bypass firewall)
	4	(Target intelligence gathering-R, Access from Radio Access Network, UE knocking)
	4	(Access from Radio Access Network, UE knocking, Pre-AKA techniques)
	4	(UE knocking, Pre-AKA techniques, UE protection evasion)
	4	(Exploiting roaming agreements, DIAMETER-based techniques, Blacklist evasion)
	4	(Internal resource search, Exploiting roaming agreements, GTP-based techniques)
	4	(Operator network mapping, SIP-based techniques, Exploit misconfigurations and implementation errors)
	4	(Access from Radio Access Network, Operator network mapping, Pre-AKA techniques)
4	5	(Internal resource search, Exploiting roaming agreements, SS7-based techniques, Blacklist evasion)
	5	(Internal resource search, Exploiting roaming agreements, SS7-based techniques, Bypass firewall)
	4	(Internal resource search, Exploiting roaming agreements, GTP-based techniques, Bypass firewall)
	3	(Target intelligence gathering-R, Access from Radio Access Network, UE knocking, Pre-AKA techniques)
	3	(Internal resource search, Exploiting roaming agreements, DIAMETER-based techniques, Bypass firewall)
	3	(Access from the public Internet, Command and control channels, UE knocking, IP-based techniques)
	3	(Infected UE hardware or software, Operator network mapping, SIP-based techniques, Exploit misconfigurations and implementation errors)
	3	(Infected UE hardware or software, Operator network mapping, SIP-based techniques, UE protection evasion)
5	2	(Target intelligence gathering-R, Access from Radio Access Network, UE knocking, Pre-AKA techniques, UE protection evasion)
	2	(Access from Radio Access Network, UE knocking, Pre-AKA techniques, UE protection evasion, Location tracking)
	2	(Access from Radio Access Network, UE knocking, Pre-AKA techniques, UE protection evasion, Identity-related attacks)
	2	(Target intelligence gathering-R, Access from partner mobile network, CN-protocol scanning, Exploiting roaming agreements, DIAMETER-based techniques)
	2	(Access from partner mobile network, CN-protocol scanning, Exploiting roaming agreements, DIAMETER-based techniques, Blacklist evasion)
	2	(Access from partner mobile network, CN-protocol scanning, Exploiting roaming agreements, DIAMETER-based techniques, Bypass firewall)
	2	(Access from the public Internet, Command and control channels, UE knocking, IP-based techniques, Redirection)
	2	(Access from the public Internet, Infected UE hardware or software, Operator network mapping, SIP-based techniques, Exploit misconfigurations and implementation errors)
	2	(Access from the public Internet, Infected UE hardware or software, Operator network mapping, SIP-based techniques, UE protection evasion)
	2	(Target intelligence gathering-R, Access from the public Internet, Command and control channels, UE knocking, IP-based techniques)
	2	(Access from the public Internet, Command and control channels, UE knocking, IP-based techniques, Exploit misconfigurations and implementation errors)

Strategy 2: Identify bottleneck, in this case **exploit roaming agreement** => Deploy edge agents if not deployed, impose policies to filter incoming traffic and authentication between roaming partners

Connectivity – Importance of a technique

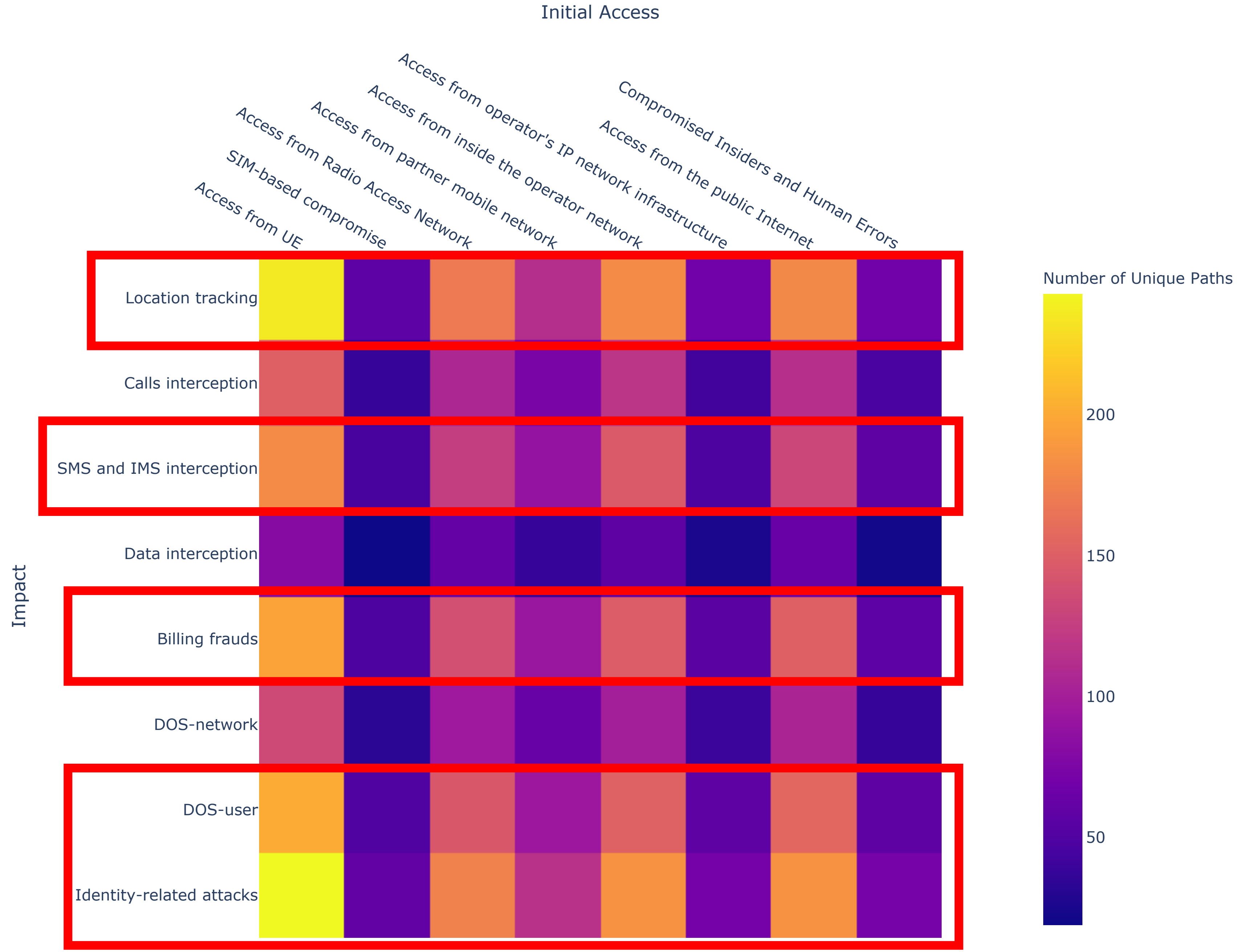


Connectivity – Importance of a technique



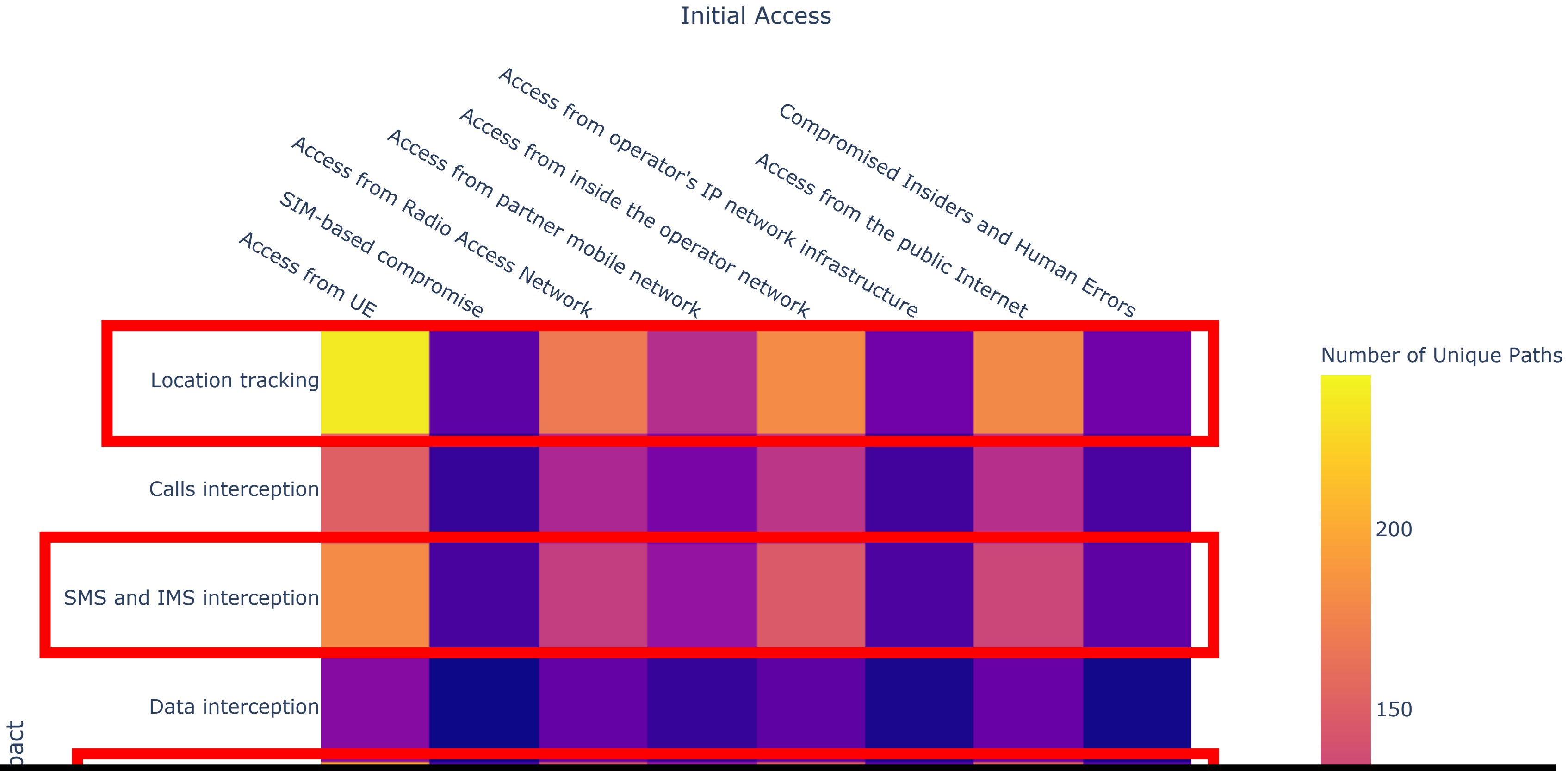
Strategy 3: Identify important techniques, in this case "**operator network mapping**" => deploy detection and defense mechanism on network mapping, close unnecessary open ports and public facing services

Number of Unique Path – Diversity of attacks



Number of Unique Path –

Diversity of attacks



Strategy 4:

a. Evaluate from attacker's point of view (capability and goal)

b. Evaluate from operator's point of view (weakest initial access point and least desired impact)

Investigate the unique paths between focused initial access and impact

Discussion

- Attacks collection from literature surveys indicate attacks observed in the wild?
- The techniques are too high-level?

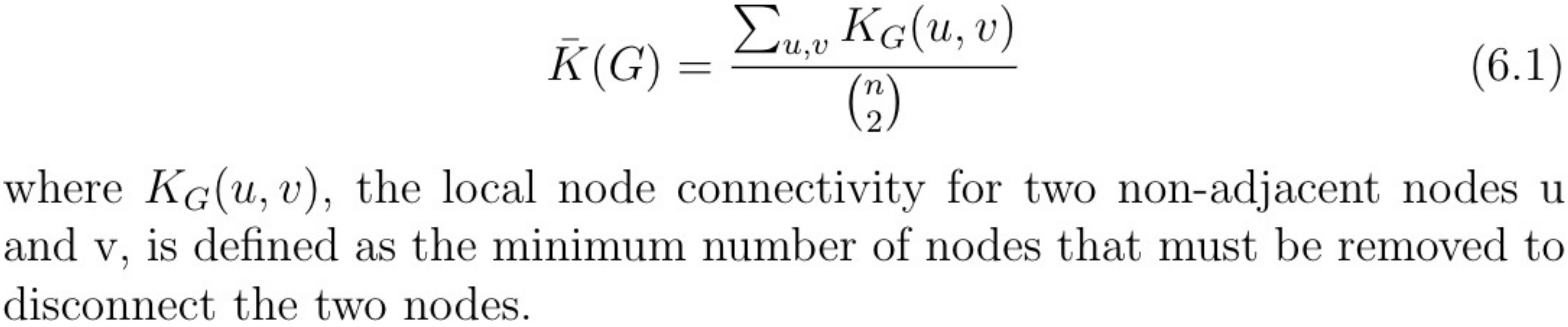
=> Demonstrate using graph analysis method with threat modelling framework to form defence strategies

Future Direction

- Include 5G / IoT attacks
- Open source and community driven
- Sub-techniques to be more specific and for automation
- Identify threat groups and attack patterns in the real-world

Thank you!
Questions or feedback?

Average connectivity - K



$$\bar{K}(G) = \frac{\sum_{u,v} K_G(u,v)}{\binom{n}{2}} \tag{6.1}$$

where $K_G(u,v)$, the local node connectivity for two non-adjacent nodes u and v, is defined as the minimum number of nodes that must be removed to disconnect the two nodes.