4. Identifikace šifrovaného provozu

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

Šifrování síťového provozu – výhody a nevýhody

+ Ochrana dat proti neautorizovanému přístupu (odposlechy).
- Přenos malware v šifrovaných kanálech → problém detekce.
- Tunelování dat přes šifrované kanály → obcházení filtrování provozu.
- Omezená viditelnost dat → problém monitorování a správy sítě.

Analýza šifrovaného provozu

- na úrovni paketů (packet-level): payload size, inter-arrival time
- na úrovni toků (session-level): flow size, duration, fwd/bwd packets

Atributy pro analýzu šifrovaného provozu

- časové atributy: inter-arrival time, trvání toku (avg/min/max/std/var)
- statistické atributy: velikost paketu/toku, počet paketů v toku, velikost hlavičky IP, TCP, velikost plovoucího okna (avg/min/max/std/var)
- protokolově závislé atributy: verze TLS, certifikát, šifrovací sady, SNI, ALPN

4. Metoda otisků TLS

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

Identifikace aplikací pomocí otisků TLS

- Kombinace vybraných parametrů TLS se liší u různých aplikací.
- Tyto parametry z TLS Client Hello vytvářejí tzv. otisk JA3 (JA3 Fingerprint):
  - `Version, Cipher Suites, Extensions, Supported Groups, EC Format.`
  - Zachovává pořadí hodnot v atributech Cipher Suite, Extensions a Supported Groups.
  - Nutné eliminovat náhodné hodnoty GREASE, viz RFC 8701.
  - Seznam atributů je spojen do řetězce a zahešován pomocí MD5.
  - Výsledný řetězec tvoří *otisk JA3*, viz `https://github.com/salesforce/ja3`.

Version, Cipher Suites, Extensions, Supported Groups, EC format

0x00000303 - 49195,49196,52393,49199,49200,52392,158,159,49161,49162,49171,49172,51,57,156,157,47,53 - 65281,0,23,35,13,16,11,10 - 0x00000017,0x00000018,0x00000019 - 0

↓

771, 49195-49196-52393-49199-49200-52392-158-159-49161-49162-49171-49172-51-57-156-157-47-53, 65281-0-23-35-13-16-11-10, 23-24-25, 0

↓

n8bvbvyZuTPF4tj89PaJVQ

4. Metoda otisků TLS

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

Příklad: otisky webových prohlížečů [7]

	Firefox				Chrome				Opera			
JA3 hash	Ubuntu	Win	Kali	MacOS	Ubuntu	Win	Kali	MacOS	Ubuntu	Win	Kali	MacOS
0e6f3c8f2b18f3011f1d6cbbdcfcbd65						x				x		
1344ed2e9d7d8e3e84e6ab655047ba32	x	x	x	x								
1f3c530fc35e41300422550c3c980e85							x	x	x	x	x	x
4863015f73b8332cf91cfa3a14a4893d		x										
5a291b49748c50adf1da70f8142d4cc4					x				x			
756094f51da8214018fbfba93211d59f	x	x	x	x								
a839cfeed30d55439b09de5f1b47fa3a					x	x	x	x	x	x	x	x
d889531a0389787425d5638caf6d84b3					x	x	x	x	x	x	x	
d90d517f72e9b8af9a8c1e2fe1fb2da8	x			x								

Problémy při vytváření otisků JA3

- Problém stability: knihovny TLS, operační systém, verze aplikace.
- Odstranění šumu: spojení TLS pro analytické účely, reklamní servery apod.

Serverový otisk JA3S (JA3S Fingerprint)

- Získaný ze zpráv TLS Server Hello.
- Atributy: `Version, Cipher Suites, Extensions`.
- Otisk se vytváří podobným způsobem jako otisk JA3.

4. Metoda otisků TLS

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

Příklady otisků JA3 a JA3S pro vybrané mobilní aplikace

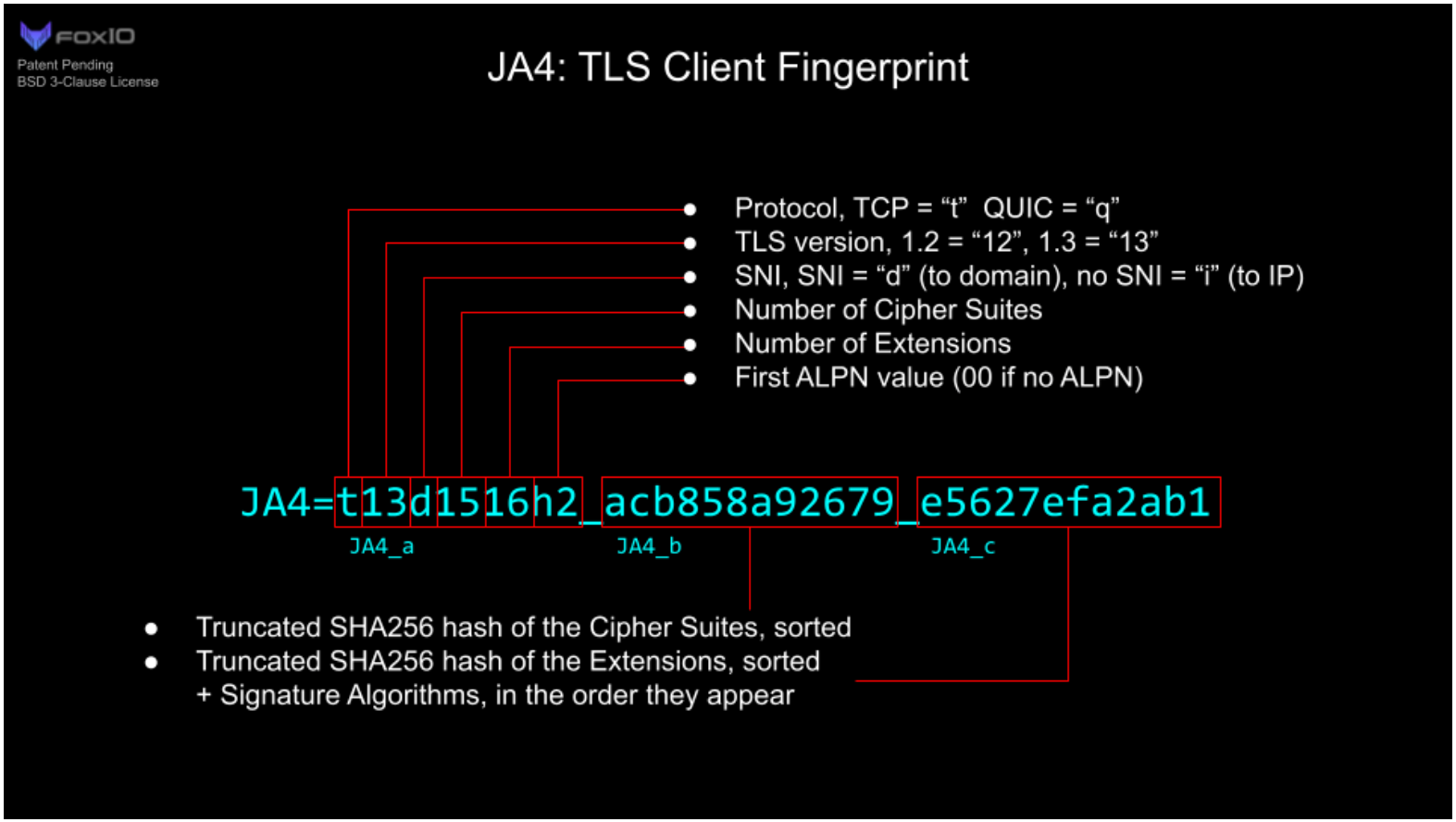
Otisk JA3	Otisk JA3S	Server Name Indication (SNI)	Aplikace
193c522402283ed9e84b8bb38137829f	0bcfa5ab48fd49e9b452fbea51bf9ff7	api.accuweather.com	Accuweather
193c522402283ed9e84b8bb38137829f	4e3362a4d6bdc0739bcf48fe32243a69	api.accuweather.com	Accuweather
0529055d554c9da011b745452211c296	0bcfa5ab48fd49e9b452fbea51bf9ff7	api.accuweather.com	Accuweather
1bff249589c418e6881e847dda91068a	896415616b22361262d7a961b6325cfd	content.cdn.viber.com	Viber
81d2604dcc31ff39cdddb6079692b0b0	9ab8f8c869ad234d4025e882270a547a	mail.google.com	Gmail
2e24fc360206a7620c6528c53f96f76f			Tor
1bff249589c418e6881e847dda91068a	331b5123a1eab3b045a3961e24e21553	best.discord.media	Discord
1bff249589c418e6881e847dda91068a	3e22c1e49e52f88fc45c8cbd6b8e1f37	discordapp.com	Discord
1bff249589c418e6881e847dda91068a	b413bf7202b1245fbcbd52913bce9865	ca.slack-edge.com	Slack
1bff249589c418e6881e847dda91068a	35b476bf06ae1c4b036bf7246dcf499c	slack.com	Slack
dc51fc24cb36ff806f272ee200f381c2	70745099b394fe3f42264227c098cc98	ma.equamobile.cz	EquaBank CZ
fd326947e94ed2d647823b8efe42ba34	70745099b394fe3f42264227c098cc98	ma.equamobile.cz	EquaBank CZ
dc51fc24cb36ff806f272ee200f381c2	a8e0da2f607d2a3c1956f56afc6da012	boomplaymusic.com	Boomplay Music
fd326947e94ed2d647823b8efe42ba34	69be2fcee93868ba03998266cb051021	boomplaymusic.com	Boomplay Music
fd326947e94ed2d647823b8efe42ba34	fd478200de5839a3178b3d0372295909	login.kb.cz	KB Klic
a839cfeed30d55439b09de5f1b47fa3a	0bcfa5ab48fd49e9b452fbea51bf9ff7	api.nextbike.net	Nextbike
a839cfeed30d55439b09de5f1b47fa3a	15af977ce25de452b96affa2addb1036	mon.tiktokv.com	TikTok
a839cfeed30d55439b09de5f1b47fa3a	15af977ce25de452b96affa2addb1036	abtest-va-tiktok.byteoversea.com	TikTok
fd326947e94ed2d647823b8efe42ba34	7b76ba926d8e1431f720be59188fa170	abtest-va-tiktok.byteoversea.com	TikTok
2b785fe0414ff99aa68c0c275ebfbc5c	545ffb1bd88f345709bd65c96be77da1	main.crws.cz	Cestovne Poriadky
2b785fe0414ff99aa68c0c275ebfbc5c	3a43b4ff95d6a19ed01b13623c0dcf82	resourcessk.crws.cz	Cestovne Poriadky
732f7c0b5b32a974a43fea990983351f	738f812c66d53a4e5bcf7c5bbc6e946	main.crws.cz	Cestovne Poriadky
732f7c0b5b32a974a43fea990983351f	c8bf8936cdcf0a17a270301428dfd5a6	resourcessk.crws.cz	Cestovne Poriadky
fada0859379fec2c87b490b8203dc520	7b76ba926d8e1431f720be59188fa170	ipws2.timetable.cz	Muj vlak
5055fa5299e55aa616459e823adb8613	7b76ba926d8e1431f720be59188fa170	ipws2.timetable.cz	Muj vlak

- Problém s překrývajícími se otisky → kombinace JA3, JA3S a SNI.

4. Metoda otisků TLS

Rozšířené otisky TLS: JA4, JA4S, JA4H, JARX, viz JA4+ Network Fingerprinting

- Kombinace různých hodnot z TLS Client Hello tvoří tři části otisku a_b_c.
- Příklad otisku JA4: t00d0307h2_55b375c5d22e_8f5d6a331b25 (Facebook)



4. Metoda otisků TLS

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

Příklady otisků JA4, JA4S, JA4H, JARX

Application	JA4+ Fingerprints
Chrome	JA4=t13d1518h2_8daaf6152771_e5627efa2ab1 (TCP) JA4=q13d0310h3_55b375c5d22e_cd85d2d88918 (QUIC)
IcedID Malware Dropper	JA4H=ge11cn020000_9ed1ff1f7b03_cd8dafe26982
IcedID Malware	JA4=t13d201100_2b729b4bf6f3_9e7b989ebec8 JA4S=t120300_c030_5e2616a54c73
Sliver Malware	JA4=t13d190900_9dc949149365_97f8aa674fd9 JA4S=t130200_1301_a56c5b993250 JA4X=000000000000_4f24da86fad6_bf0f0589fc03 JA4X=000000000000_7c32fa18c13e_bf0f0589fc03
Cobalt Strike	JA4H=ge11cn060000_4e59edc1297a_4da5efaf0cbd JA4X=2166164053c1_2166164053c1_30d204a01551
SoftEther VPN	JA4=t13d880900_fcb5b95cb75a_b0d3b4ac2a14 (client) JA4S=t130200_1302_a56c5b993250 JA4X=d55f458d5a6c_d55f458d5a6c_0fc8c171b6ae
Evilginx	JA4=t13d191000_9dc949149365_e7c285222651
Reverse SSH Shells	JA4SSH=c76s76_c71s59_c0s70

- Otisky JA3/S a JA4+ implementovány jako pluginy do Wiresharku.

Srovnání metod pro identifikaci sítového provozu

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

1. *Identifikace podle hodnot z hlaviček paketů*
   - Pro identifikaci využívá čísla portů a protokolů z hlaviček L3 a L4.
   - Jednoduché na implementaci, rychlé, nevyžaduje trénovací množinu.
   - Identifikace na základě přesné shody.
   - Omezená míra použitelnosti.
2. *Identifikace podle signatur*
   - Nespoléhá na hodnoty z hlaviček paketů.
   - Vyžaduje vytvoření databáze signatur a její pravidelnou aktualizaci.
   - Výpočetně náročné.
3. *Identifikace na základě pravděpodobnostního modelu protokolu*
   - Vhodné pro tunelovaná či šifrovaná data.
   - Využívá pravděpodobnostní rozložení různých atributů protokolu.
   - Vyžaduje vytvoření modelu protokolu na základě trénovací množiny.
   - Může chybně detekovat provoz (false positives).
4. *Metoda otisků TLS*
   - Detekce aplikací v šifrovaném provozu. Využívá data z navazování spojení.
   - Rychlý výpočet otisků z handshaku TLS: vyžaduje nešifrované TLS Hello.
   - Vyžaduje databázi otisků TLS.
   - Otisky bývají nestabilní, závisí na verzi knihoven TLS či OS.

Detekce anomálií

Co je to anomálie?

→ Anomálie je odchylka od očekávaného (normálního, běžného) stavu či chování.

→ Co je normální chování (v síťovém provozu)?

Detekce anomálií v síťovém provozu

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

Detekce anomálií v síťovém provozu

- Sledujeme odchylky komunikace od očekávaného (typického) provozu.

Co způsobuje odchylky v síťovém provozu?

- Změna struktury provozu, např. neočekávaná komunikace, jiné protokoly.
- Odlišná struktura a četnost vzájemné komunikace uzlů.
- Neobvyklý počet přenesených dat, paketů, časové odchylky mezi pakety.
- Neobvyklý výskytu určitých hodnot v hlavičkách paketů (typ požadavku).
- Výpadky v komunikaci (keep-alive), neúplná komunikace.

...

$\rightarrow$ Odchylka může vzniknout také novým chováním systému.

Systém pro detekci anomálií (Anomaly Detection System)

- Vytváří model normálního chování komunikace $\rightarrow$ model se může v čase měnit.
- Umožňuje rozpoznat i útoky, které dosud nebyly zachyceny a popsány.
- Měl by korektně zpracovat malé výchylky oproti normálnímu chování.

Detekce anomálií v síťovém provozu

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

Vytvoření modelu síťové komunikace

1. Potřebujeme znát typické chování komunikace → trénovací data.
2. Potřebujeme vytvořit dostatečně přesný model na základě trénovacích dat.
3. Potřebujeme metriku pro hledání odchylky testovacího provozu od modelu.
4. Potřebujeme stanovit práh odlišující obvyklý a anomální provoz.

Jak reprezentovat (modelovat) síťovou komunikaci?

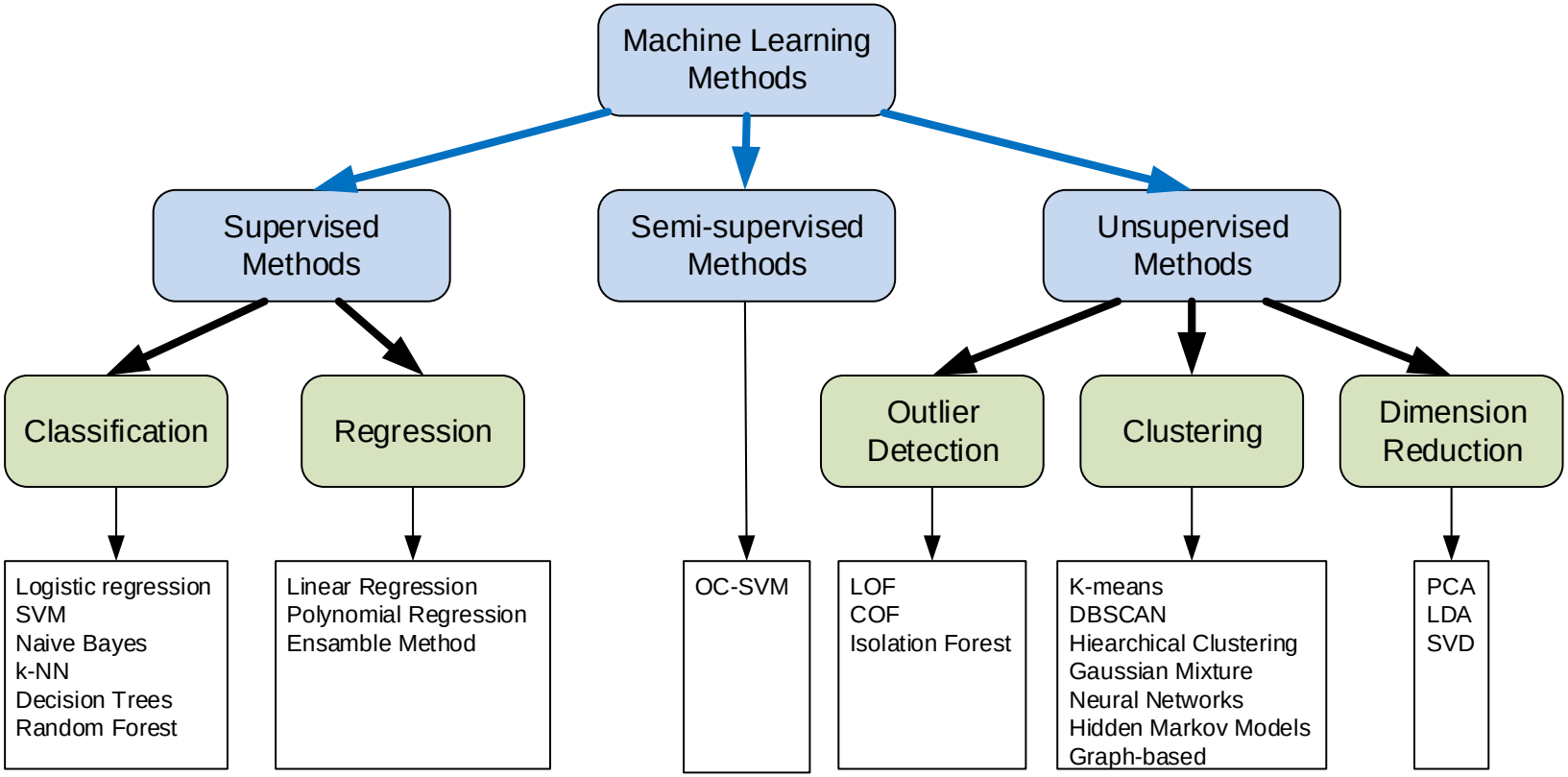
- Pravděpodobnostní modely.
- Modely shluků (clustering): K-means, k-NN clusters, subspace clustering.
- Popis chování a komunikace pomocí konečných automatů.
- Klasifikační modely: naivní bayesovský model, SVM, neuronové sítě.
- a další ...

Jaká vstupní data můžeme použít pro modelování a detekci?

- Plný záchyt data paketů (packet capturing).
- Síťové statistiky o tocích (Netflow, IPFIX).
- Statistiky provozu (SNMP).
- Logovací záznamy.

Detekce anomálií v síťovém provozu

Jakou metodu použít pro modelování síťového provozu?



- Anotovaná vs. neanotovaná data
- Časové sekvence (řady) vs. diskrétní data
- Klasifikace vs. predikce
- Výběr (redukce) atributů

Detekce anomálií v síťovém provozu

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

Co obsahuje systém pro detekci anomálií

1. Definici vstupních dat: extrakce dat z provozu, výběr atributů, abstrakce.
2. Trénování: dostatečně reprezentativní množina (normální i anomální data).
3. Vytvoření klasifikačního modelu: výběr metody, parametrů, validace modelu.
4. Detekce anomálií: metrika pro měření anomálií, určení prahové hodnoty, přeučení.

→ Systém funguje pouze tehdy, pokud jsme schopni sestavit model běžného chování.

Požadavky na chování systému:

- Možnost natrénovat systém v konkrétním prostředí.
- Automatizované nastavení parametrů systémů s možností úprav prahových hodnot.
- Přeučení systému detekce.
- Velký počet falešných detekcí (FP) způsobí, že systém se nebude používat.
- Vyladění okrajových hodnot a netypických stavů (aktualizace sw, apod.).

Příklad 1: pravděpodobnostní automaty

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

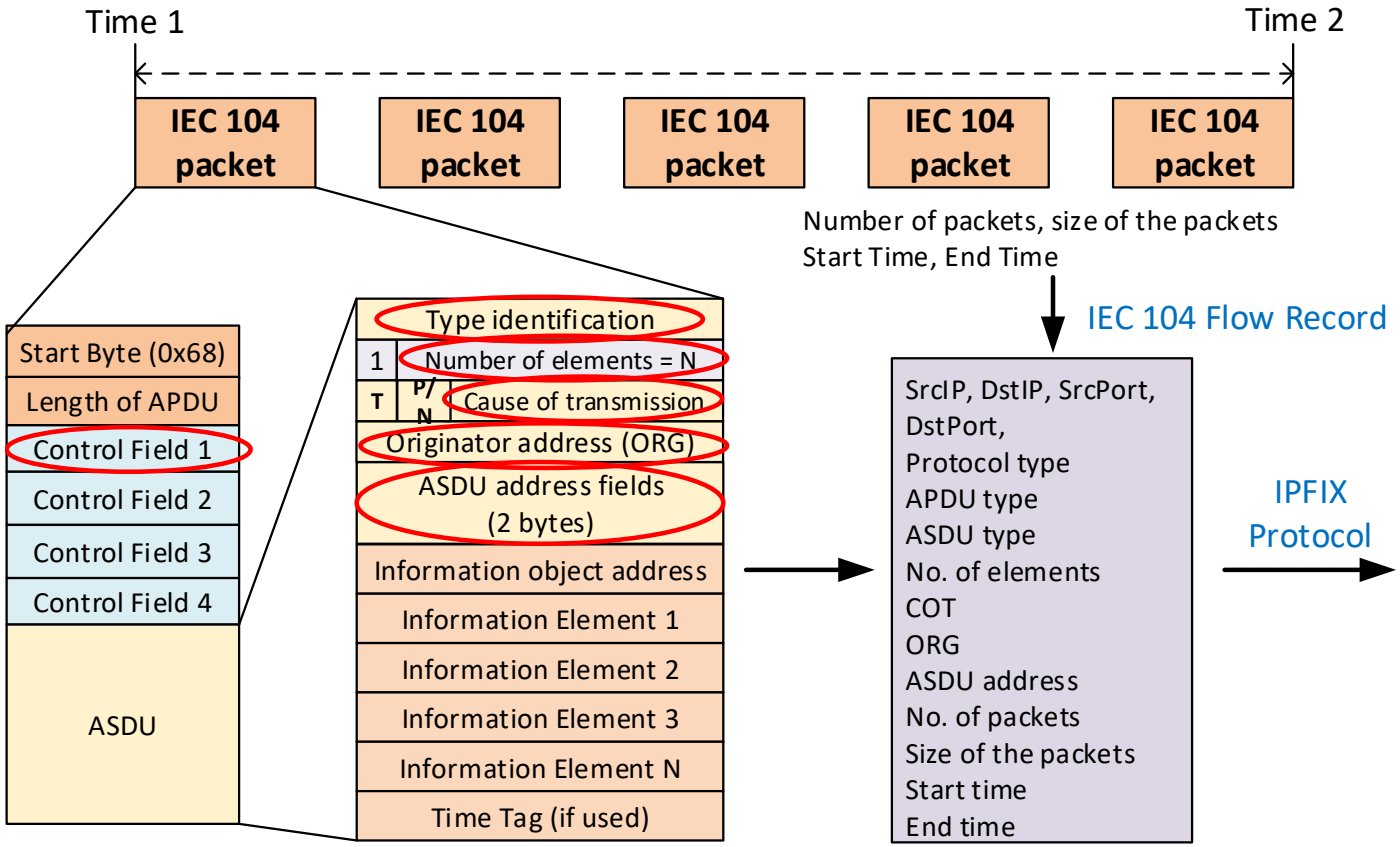
Průmyslový protokol IEC 60870-5-104 (IEC 104) [8]

- Aplikační protokol typu master-slave pro komunikaci zařízení v energetické síti

Master (10.20.102.1) < --- > Slave (10.20.100.108) communication				
No.	**Direction**	**object**	**Cause of transmission (COT)**	**Setting values of the information element**
2	---->	IOA=13	activation	single command ON
	<----	IOA=13	activation confirmation	single command ON
		IOA=13	activation termination	single command ON
		IOA=13	spontaneous	SIQ=0x01 (SPI=ON) with time tag
6	---->	IOA=1	activation	regulating step cmd: UP
	<----	IOA=1	activation confirmation	regulating step cmd: UP
		IOA=1	activation termination	regulating step cmd: UP
		IOA=1	spontaneous	step position = 1
8	---->	IOA=3	activation	bitstring = 0x 02 00 00 00
	<----	IOA=3	activation confirmation	bitstring = 0x 02 00 00 00
	<----	IOA=3	activation termination	bitstring = 0x 02 00 00 00
		IOA=3	spontaneous	bitstring = 0x 02 00 00 00
10	---->	IOA=1	activation	set point, normalized value = 0.03125
	<----	IOA=1	activation confirmation	set point, normalized value = 0.03125
	<----	IOA=1	activation termination	set point, normalized value = 0.03125
		IOA=1	spontaneous	measured valued, normalized value = 0.03125
14	---->	IOA=1	activation	set point, short float = 3.14
	<----	IOA=1	activation confirmation	set point, short float = 3.14
		IOA=1	activation termination	set point, short float = 3.14
		IOA=1	spontaneous	measured value, short float= 3.14

Příklad 1: pravděpodobnostní automaty

1. Získání monitorovacích dat z protokolu IEC 104 pomocí IPFIX [9]

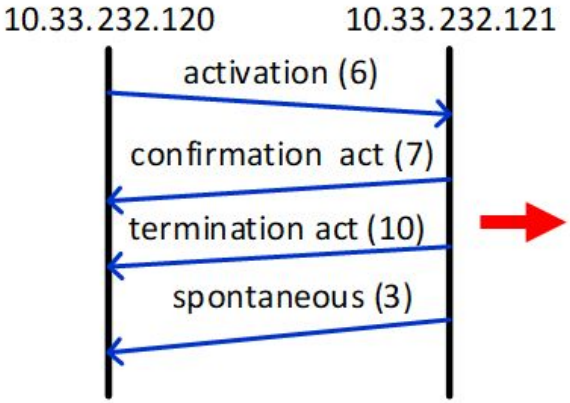


- APDU frame: i-frame, s-frame, u-frame.
- ASDU type: interrogation, end of initialization, single point of info, measured value.
- Cause of transmission: activation, initialized, confirmation, interrogate, spontaneous.

Příklad 1: pravděpodobnostní automaty

2. Vytvoření modelu komunikace IEC 104

- Hypotéza: komunikační vzory mezi dvěma IEC 104 zařízeními jsou stabilní a obsahují konečnou množinu posloupností příkazů.
- Úkol: vytvořit model pro tyto konverzace → jakou metodu popisu zvolit?



timestamp	SrcIP	srcPort	dstIP	dstPort	ASDU type	COT	COA
08:24:42.18	10.33.232.120	44216	10.33.232.121	2404	45	6	83
08:24:52.336	10.33.232.121	2404	10.33.232.120	44216	45	7	83
08:24:52.416	10.33.232.121	2404	10.33.232.120	44216	45	10	83
08:24:52.416	10.33.232.121	2404	10.33.232.120	44216	1	3	83
08:24:52.416	10.33.232.121	2404	10.33.232.120	44216	1	3	83

```
S = { [<45,6>,<45,7><45,10>], [<1,3>], [<1,3>],  ...  }
```

Způsob reprezentace komunikace IEC 104

- Komunikaci lze popsat jako množinu S vzorků komunikace (tzv. konverzací).
- Jednotlivé příkazy vyjádřeny abstraktně jako dvojice $\langle \text{AsduType}, \text{CoT} \rangle$.
- Konverzace je logická sekvence příkazů popisující určitou výměnu dat.

Příklad 1: pravděpodobnostní automaty

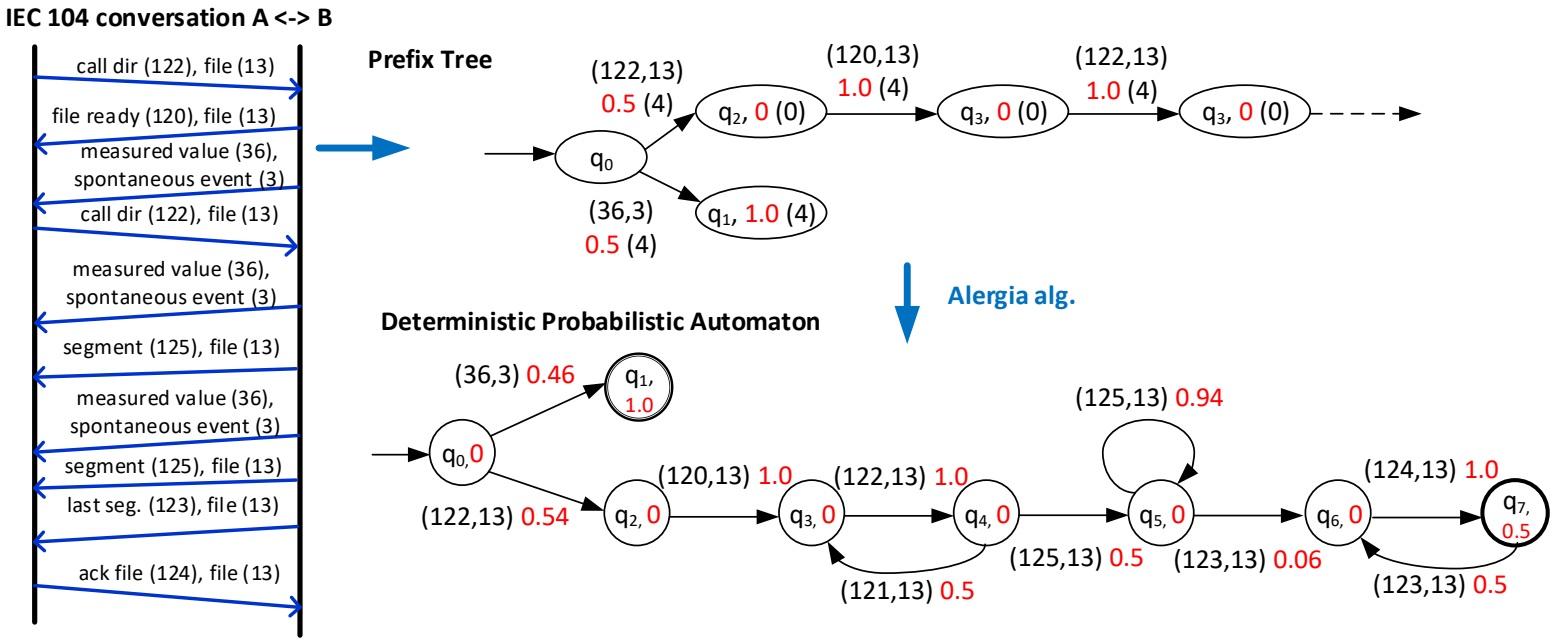
2. Vytvoření modelu komunikace IEC 104

- Na základě vzorků komunikace hledáme regulární jazyk, který ji popisuje.
- Máme pouze vzorky → hledáme pravděpodobností jazyk.

→ Využití pravděpodobnostních automatů.

Co jsou pravděpodobnostní automaty? [10]

- Přechody a koncové stavy obsahují pravděpodobnost přechodu či přijetí řetězce.
- Reprezentace: prefixový strom (PT) či pravděpodobnostní automat (DPA).



Příklad 1: pravděpodobnostní automaty

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

2. Validace vytvořeného modelu

- Jak velké budou automaty?
- Jak přesná bude detekce?

Dataset	Prefix Tree			DPA		
	States	Accuracy	(Detected/All)	States	Accuracy	(Detected/All)
iec104	44	0%	(0/31)	44	0%	(0/31)
10122018-104Mega	49	99.8%	(4636/4642)	8	100%	(4642/4642)
10122018-104Mega_0	48	99.7%	(337/338)	8	99.7%	(337/338)
13122018-mega104	38	99.9%	(61606/61612)	8	99.9%	(61606/61612)
13122018-mega104_1	28	99.8%	(2412/2415)	8	99.9%	(2414/2415)
mega104-14-12-18	39	100%	(6114/6114)	8	100%	(6114/6114)
mega104-17-12-18	3	100%	(25233/25233)	3	100%	(25233/25233)
KTH-RTU1	12	100%	(2088540/2088540)	12	100%	(2088540/2088540)
KTH-RTU1_1	9	98.3%	(58/59)	9	98.3%	(58/59)
KTH-RTU1_2	9	100%	(55/55)	9	100%	(55/55)
KTH-RTU4	10	100%	(1107537/1107537)	10	100%	(1107537/1107537)
RICS	2	100%	(519352/519352)	2	100%	(519352/519352)

2/3 of samples used for training, 1/3 used for testing

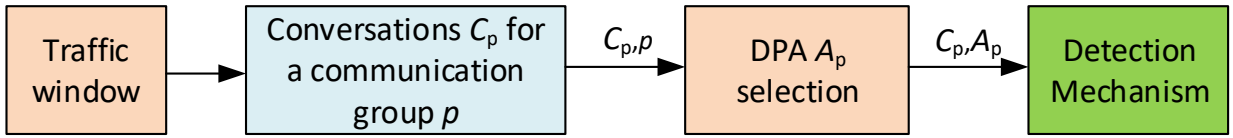
Příklad 1: pravděpodobnostní automaty

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

3. Detekce anomálií [11]

- Hledáme, zda daná konverzace c_i patří do naučeného modelu systému.

A) Testování jednotlivých konverzací



- Pro každou konverzaci $c \in \mathcal{C}_p$ spočítáme $\mathcal{P}_{\mathcal{A}_P}(c)$.
- Pravděpodobnost cesty π: $\mathcal{P}_{\mathcal{A}}(\pi) = \mathbb{I}(q_0).\delta(q_0, a_1, q_1), \ldots, \delta(q_{n-1}, a_n, q_n).\mathbb{F}(q_n)$.
- Anomálie nastane, pokud platí $\mathcal{P}_{\mathcal{A}_P}(c) \leq \mu$, v našem případě je práh $\mu = 0$.

B) Testování konverzací v daném časové okně

- Vytvoříme DPA $\mathcal{A}'_P$ pro komunikace v časovém okně a porovnáme s modelem $\mathcal{A}_P$.
- Podobnost automatů měříme euklidovskou vzdáleností:

$$L_2(\mathcal{A}_p, \mathcal{A}'_p) = \sqrt{\sum_{w \in \Sigma^*} \left(\mathcal{P}_{\mathcal{A}_p}(w) - \mathcal{P}_{\mathcal{A}'_p}(w)\right)^2}$$

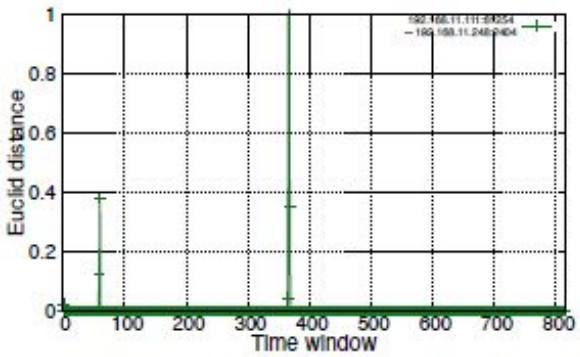
- Anomálie nastane, pokud $L_2(\mathcal{A}_p, \mathcal{A}'_p) > \theta$, kde $\theta \in [0, 1]$.

Příklad 1: pravděpodobnostní automaty

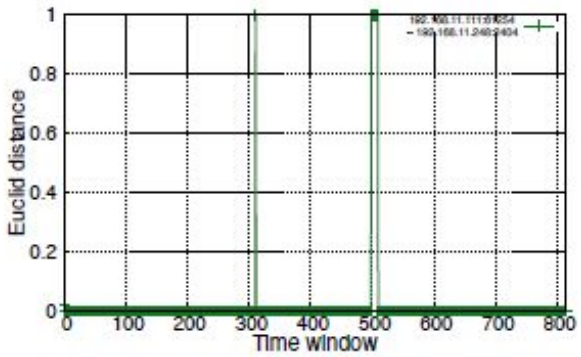
FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

3. Detekce anomálií [11]

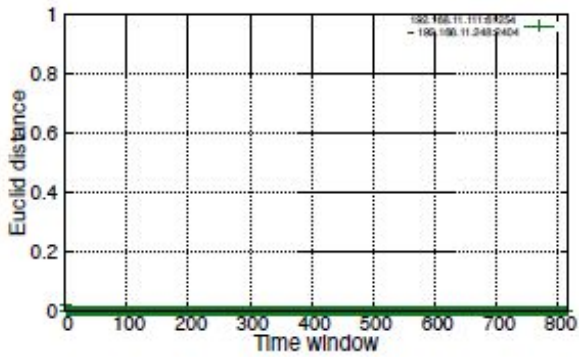
- Ověření úspěšnosti detekce na běžných anomáliích.



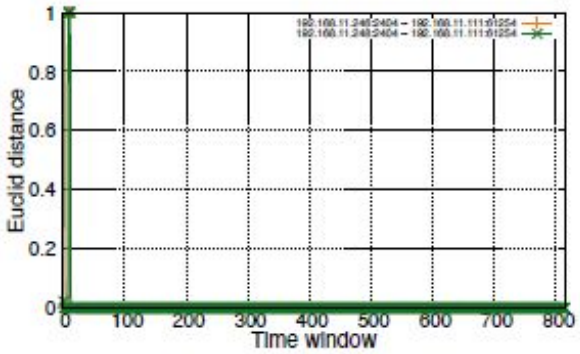
(a) Injection attack



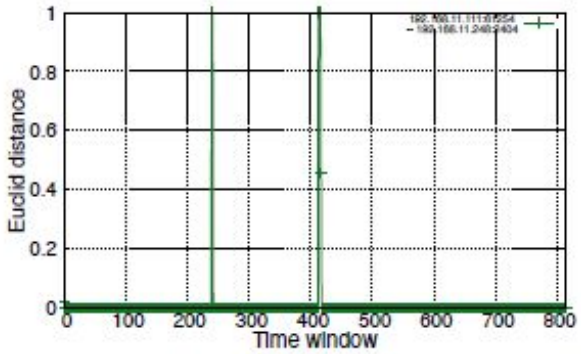
(b) Connection loss



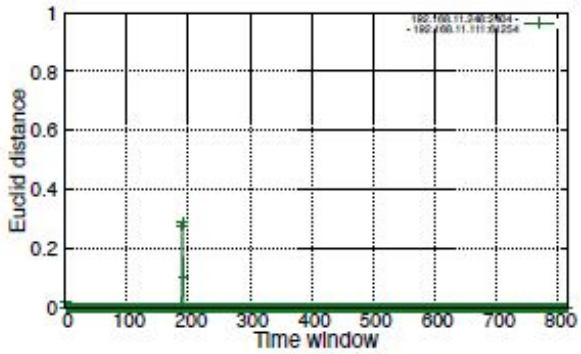
(c) DoS attack



(d) Rogue devices



(e) Scanning attack

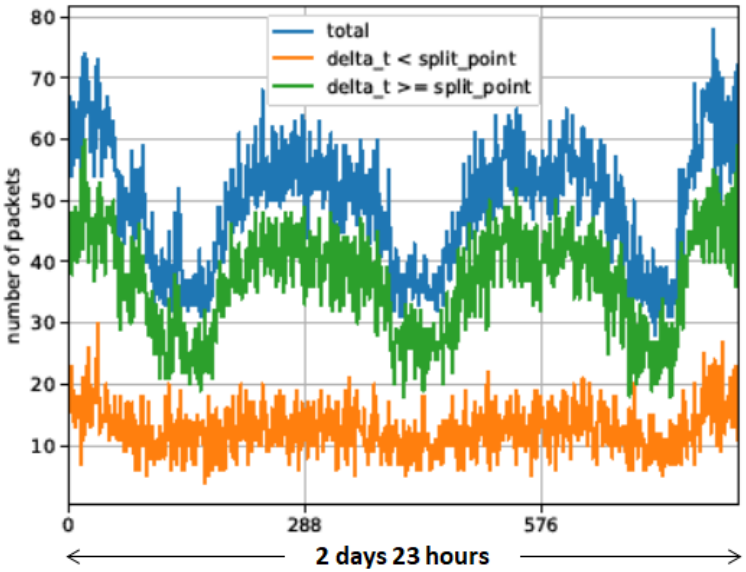


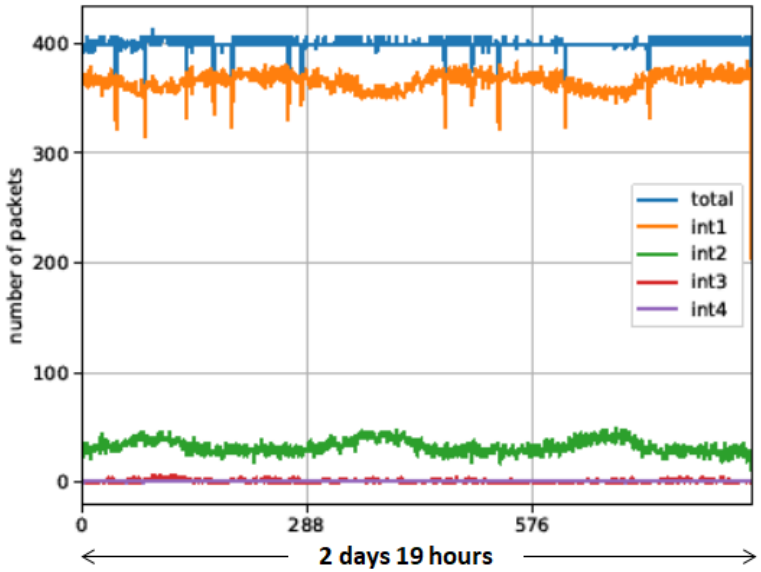
(f) Switching attack

Příklad 2: pravděpodobnostní modelování

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

Vzory chování v průmyslové komunikaci ICS





- Stabilní komunikační vzory: zpoždění, velikost paketů, počty paketů.
- Vytváříme pravděpodobností model vybraných atributů průmyslové komunikace.
- Pravděpodobnostní model popisuje chování komunikace ICS mezi zařízeními.

Statistické atributy

- Základní: počet přenesených paketů N, směr komunikace: $M \rightarrow S, S \rightarrow M$.
- Doplňkové: mezipaketové mezery Δt.

Příklad 2: pravděpodobnostní modelování

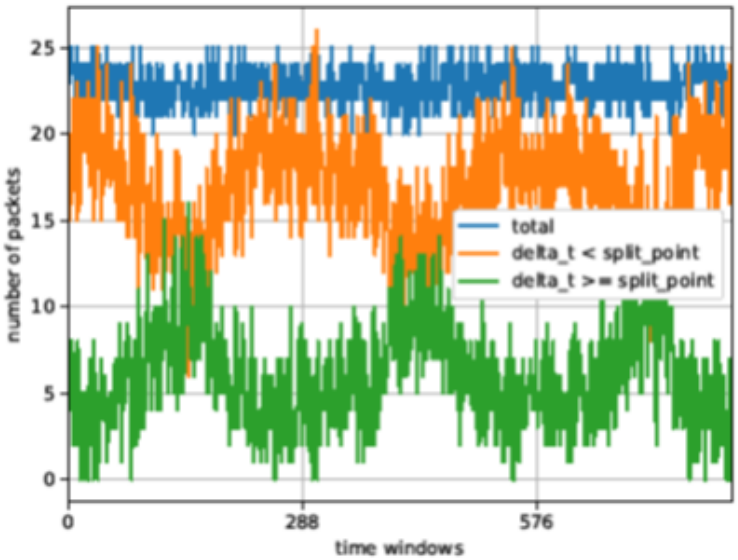
FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

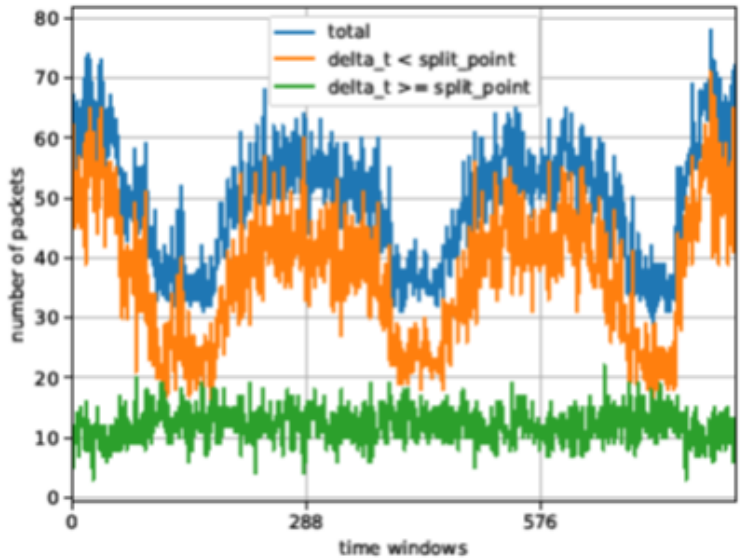
Rozdělení komunikace pomocí bodů rozdělení (split points)

- Rozdělíme množinu dat do několika regionů podle doplňkového atributu Δt .
- Regiony pak obsahují komunikaci se stabilními vzory chování.

→ Rozdělení je vhodné pro datové sady s periodickými vzory.

→ Regiony lépe zvýrazní anomálie, které by jinak zůstaly skryté v celkovém provozu.





Vytvoření pravděpodobnostního profilu komunikace v daném směru:

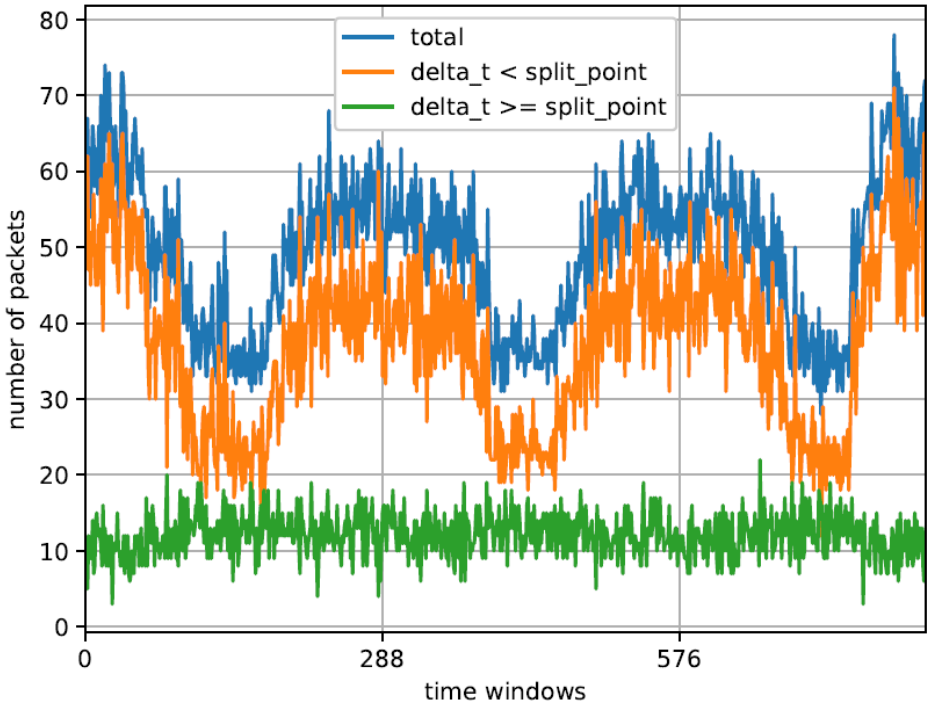
- Formát profilu: $P = (sp, \langle a_1, a_2 \rangle, \langle l_1, l_2 \rangle, \langle u_1, u_2 \rangle)$

  kde a, l, u jsou minimální a maximální počty přenesených paketů v daném směru.

Příklad 2: pravděpodobnostní modelování

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

Příklad modelování provozu IEC 104 [12]



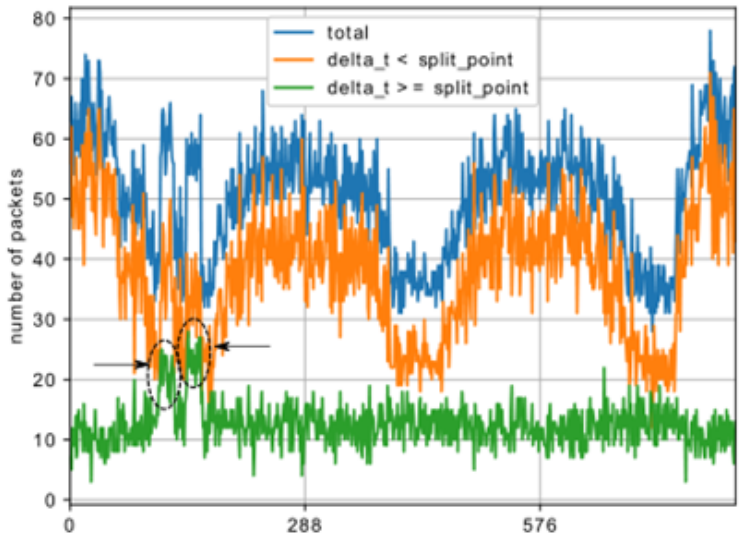
Pravděpodobnostní profil: $P = (5.66, \langle 20.30, 76.94 \rangle, \langle 4.7, 68.05 \rangle, \langle 3.9, 20.62 \rangle)$

- Bod rozdělení: kvartil Q3 $= 5.66$ (vybraná hodnota Δt)
- Dolní region: $\langle 4.7, 68.05 \rangle$ (počet paketů s vlastností $\Delta t < 5.66$)
- Horní region: $\langle 3.9, 20.62 \rangle$ (počet paketů s vlastnostní $\Delta t \geq 5.66$)
- Celková komunikace: $\langle 20.30, 76.94 \rangle$ (celkový počet přenesených paketů)

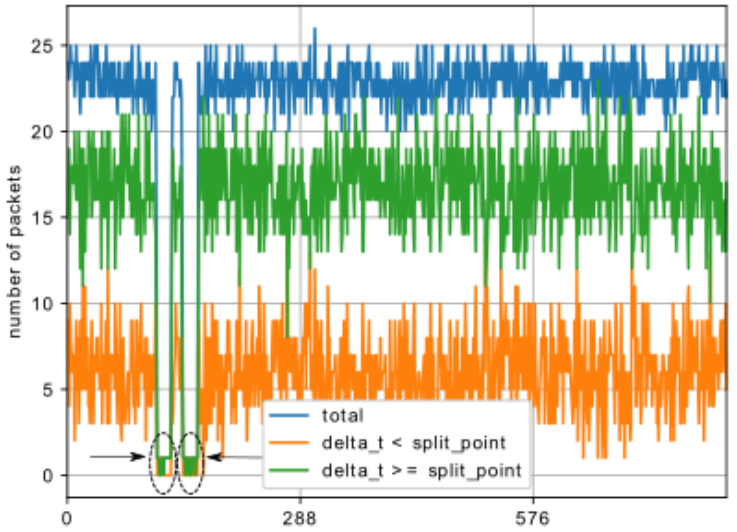
Příklad 2: pravděpodobnostní modelování

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

Příklad detekce útoku DoS



(a) from master direction



(a) to master direction

Směr komunikace	Profil	Časová okna obsahující anomálie 110-128	142-161
master to slave	celkem (a)	-	-
	$\Delta t < sp$ (l)	-	-
	$\Delta t \geq sp$ (u)	112-114, 117-121, 125-128 ↑	145-161 ↑
slave to master	celkem (a)	111-130 ↓	143-162 ↓
	$\Delta t < sp$ (l)	-	-
	$\Delta t \geq sp$ (u)	111-129 ↓	143-162 ↓

Použitá literatura I

[1] Byung-Chul Park, Young J Won, Myung-Sup Kim, and James W Hong. Towards automated application signature generation for traffic identification. In *Network Operations and Management Symposium, 2008*, pages 160–167. IEEE, 2008.

[2] Subhabrata Sen, Oliver Spatscheck, and Dongmei Wang. Accurate, Scalable In-network Identification of P2P Traffic Using Application Signatures. In *Proceedings of the 13th International Conference on World Wide Web*, WWW '04, pages 512–521, New York, NY, USA, 2004. ACM.

[3] Manuel Crotti, Maurizio Dusi, Francesco Gringoli, and Luca Salgarelli. Traffic Classification Through Simple Statistical Fingerprinting. *SIGCOMM Comput. Commun. Rev.*, 37(1):5–16, January 2007.

[4] Erik Hjelmvik and Wolfgang John. Statistical protocol identification with SPID: Preliminary results. In *Swedish National Computer Networking Workshop*, 2009.

[5] Eric Hjelmvik. The SPID Algorithm. Technical Report White paper, 2008.

[6] Christopher Köhnen, Christian Überall, Florian Adamsky, Veselin Rakocevic, Muttukrishnan Rajarajan, and Rudolf Jäger. Enhancements to Statistical Protocol IDentification (SPID) for Self-Organised QoS in LANs. In *Proceedings of the 19th Int. Conference on Computer Communications and Networks, IEEE ICCCN 2010, Zürich, Switzerland, 2010*, pages 1–6, 2010.

Použitá literatura II

[7] Petr Matoušek, Ivana Burgetová, Ondřej Ryšavý, and Malombe Victor. On Reliability of JA3 Hashes for Fingerprinting Mobile Applications. In *Digital Forensics and Cyber Crime, ICDF2C 2020*, volume 351 of *LNICST*, pages 1–22. Springer, 2021.

[8] Petr Matoušek. Description and analysis of IEC 104 Protocol. Technical Report FIT-TR-2017-12, Brno University of Technology, 2017.

[9] Petr Matoušek, Ondřej Ryšavý, Matěj Grégr, and Vojtěch Havlena. Flow based monitoring of ICS communication in the smart grid. *Journal of Information Security and Applications*, 54:102535, 2020.

[10] Colin de la Higuera. *Grammatical Inference: Learning Automata and Grammars*. Cambridge University Press, New York, NY, USA, 2010.

[11] Petr Matoušek, Vojtěch Havlena, and Lukáš Holík. Efficient Modelling of ICS Communication For Anomaly Detection Using Probabilistic Automata. In *IFIP/IEEE International Symposium on Integrated Network Management*, pages 1–9, 2021.

[12] Ivana Burgetová, Petr Matoušek, and Ondřej Ryšavý. Anomaly Detection of ICS Communication Using Statistical Models. In *Proceedings of the 17th International Conference on Network Service Management (CNSM 2021)*, page 7, 2021.