Moscow Technical University of Communications and Informatics (MTUCI)

SpacSec 2026 International Conference on Cyber Warfare, Security & Space Computing

Cascade model of rare multi-label anomalous events in a computer network

Dmitriy Igorevich Rakovskiy
Cand. Sci. (Eng.), Associate Professor, Information Security Department

Oleg Ivanovich Sheluhin
Dr. Sci. (Eng.), Professor, Head of the Information Security Department

Saint Petersburg, Russia, 2026

Events in a shared computer network

Event — an observed manifestation of computer network operation, defined for a given object and observation window.

Three properties of one observed event

RARITY

An event is rare if its occurrence probability in the chosen context does not exceed threshold ε.

MULTI-LABEL NATURE

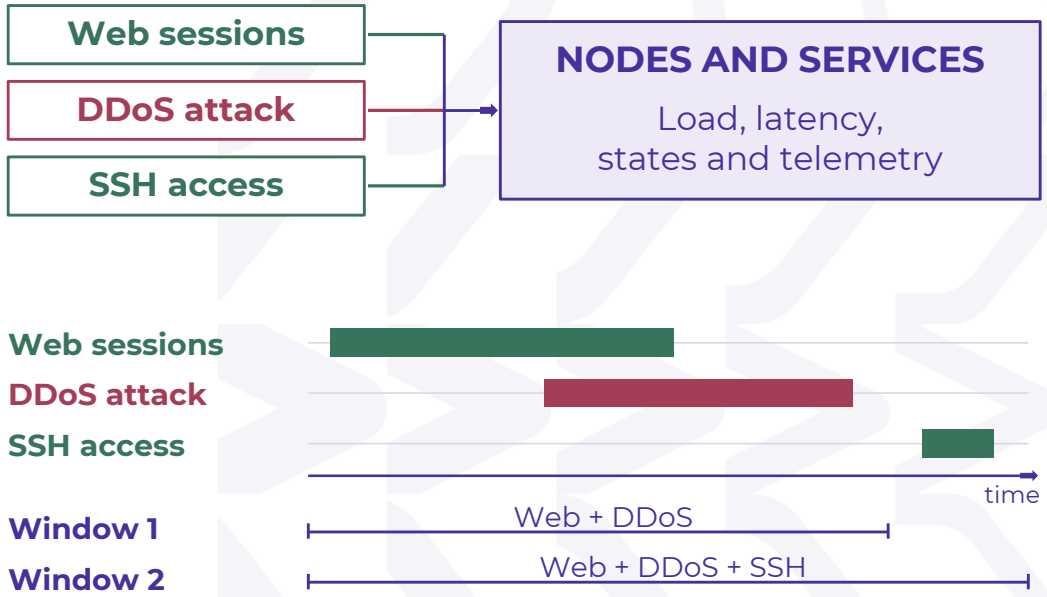
An event is associated with two or more distinct class labels.

ANOMALOUSNESS / DESTRUCTIVENESS

Confidentiality, availability or integrity is violated.

Both legitimate events and attacks can be rare.

Impact on shared nodes and resources



Objective: develop a model of rare multi-label anomalous events based on the composition of subsets of anomalous (destructive), multi-label and rare events.

An event and three criteria: what must be defined

D — set of events; *d* — one event; *F* — set of flows; *f* — one flow.
u — sending host; *h* — receiving host; $L(d)$— the event's set of class labels.

Full observation period: a directed host pair

$$d = (u, h) \qquad d \in D$$

F: all source records; f ∈ F: one flow.
u and h: source and destination IP addresses.

$$F_{u,h} = \{f \in F : src(f) = u, dst(f) = h\}$$

$$L(d) = \{\ell : \exists f \in F_{u,h}, \ell \in L(f)\}$$

L(f): one attack label, or ⌀ for Normal.

Window: a node's flows over an interval

$$I = [t_0, t_0 + \Delta), d = (h, I)$$

s(f), e(f): flow start and end.
t_0: window start; Δ > 0: window duration.

$$F_h(I) = \{f \in F : dst(f) = h, [s(f), e(f)] \cap I \neq \emptyset\}$$

$$L(d) = \{\ell : \exists f \in F_h(I), \ell \in L(f)\}$$

A label set contains the event's distinct labels.

RARITY

What is the probability of this event type?

$$D_R = \{d \in D : P(d) \leq \varepsilon\}$$

Threshold ε = 1%.
Both recording sessions, all nodes.

MULTI-LABEL NATURE

How many distinct labels are associated with the event?

$$D_M = \{d \in D : |L(d)| \geq 2\}$$

DESTRUCTIVENESS

Is confidentiality, availability or integrity violated?

$$D_A = \{d \in D : A(d) = 1\}$$

In UNSW: A = 1 if a labelled attack is present.

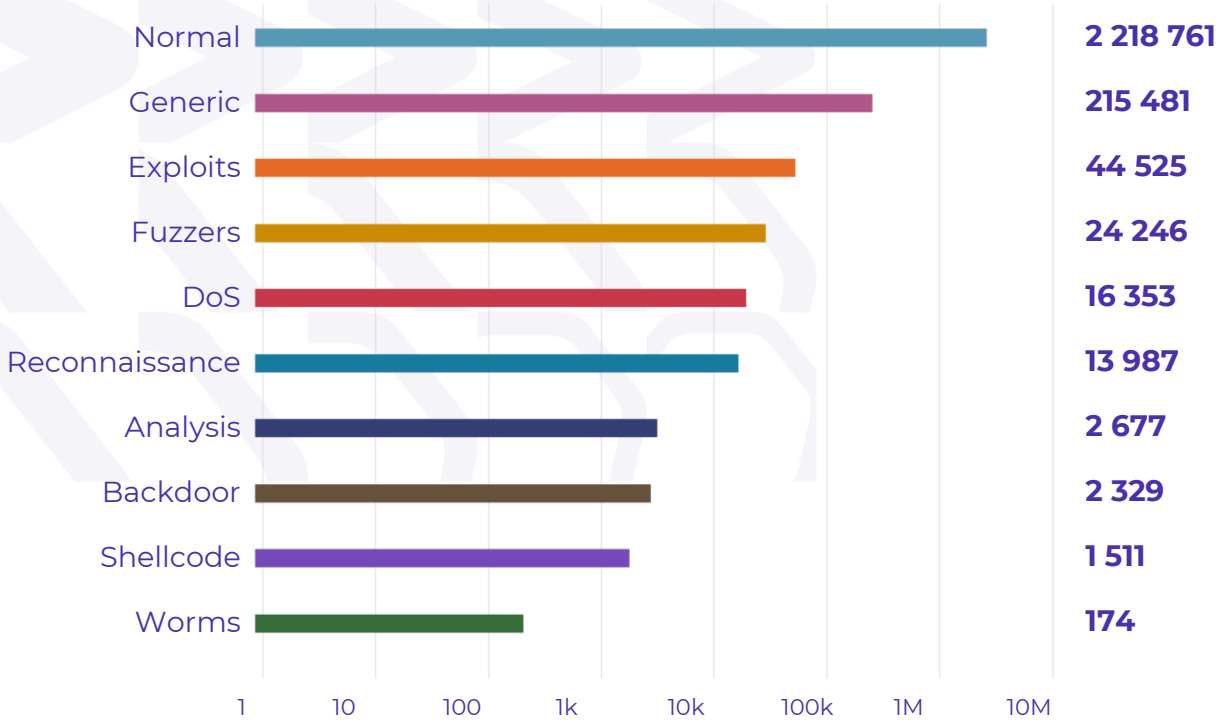
In data analysis, rarity is assessed by the relative frequency of the event's label set: the proportion of all events with exactly that set. An event is rare if this proportion does not exceed ε. Here ε is one percent.

$$\hat{p}\big(L(d)\big) = \frac{|\{d' \in D : L(d') = L(d)\}|}{|D|}$$

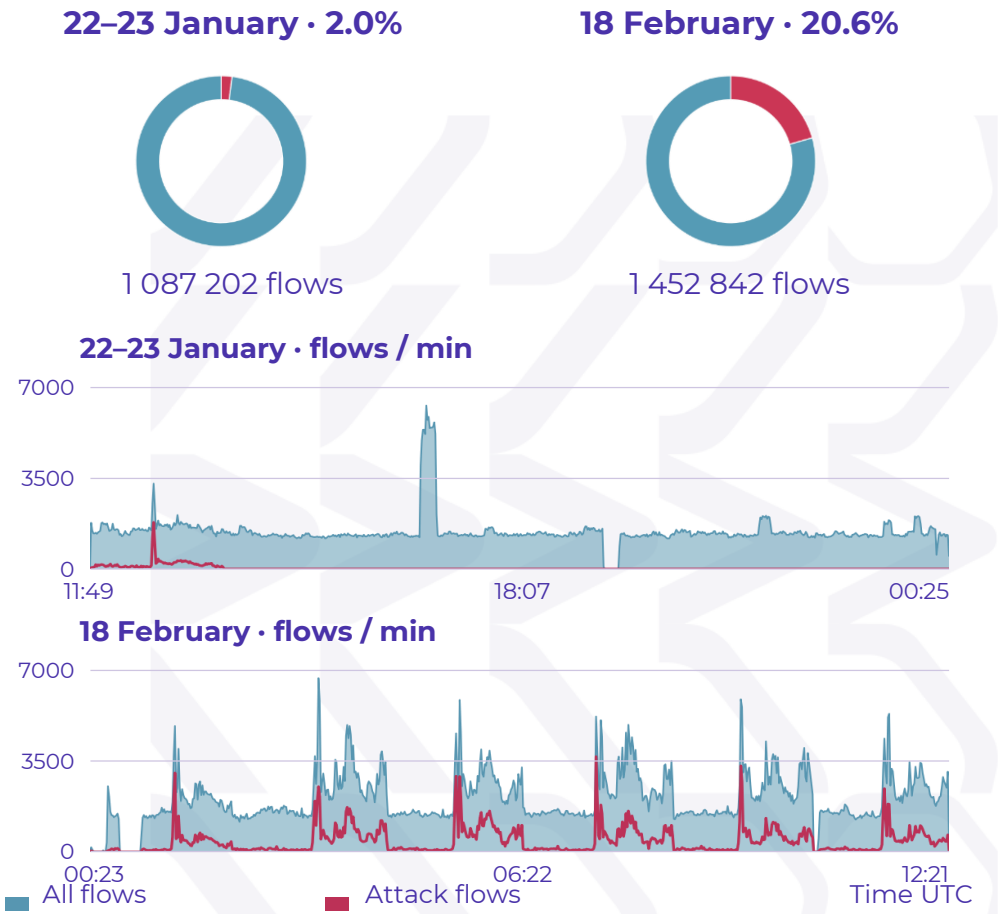
UNSW-NB15: data composition and temporal dynamics

Full corpus: 2 540 044 flows

49 IP addresses · 311 directed pairs · 9 attack categories



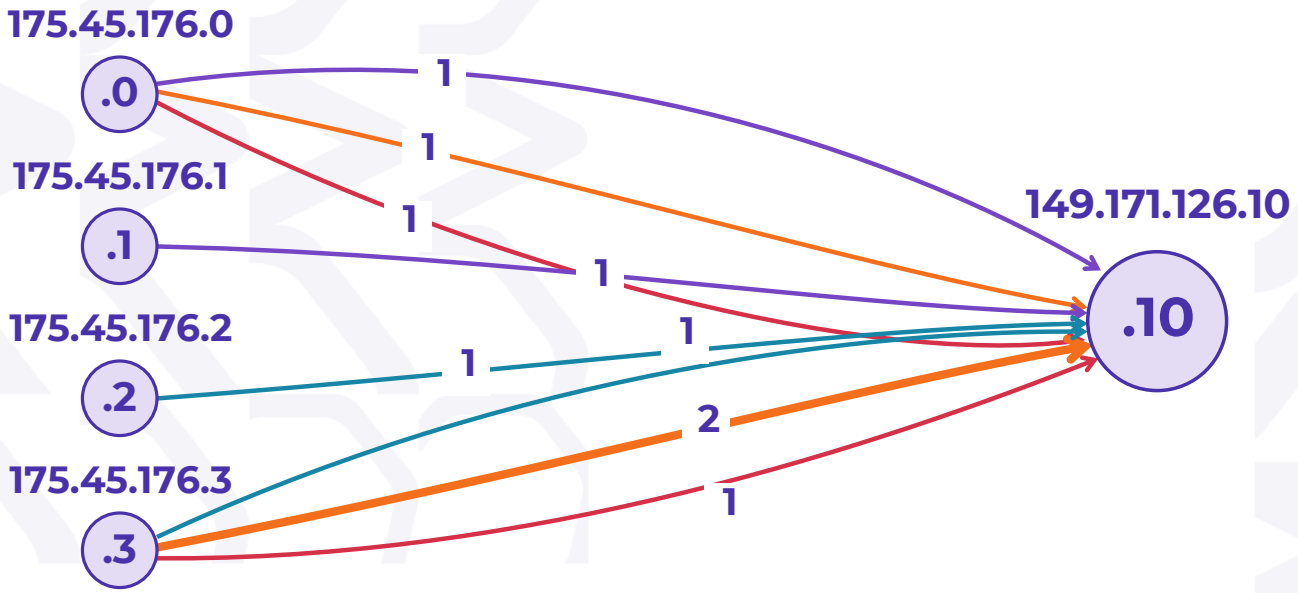
Two recording sessions · attack share



In this experiment, an event is the set of a node's incoming flows within an observation window.

Node activity over 1 minute of observation

149.171.126.10 (22 January 2015)



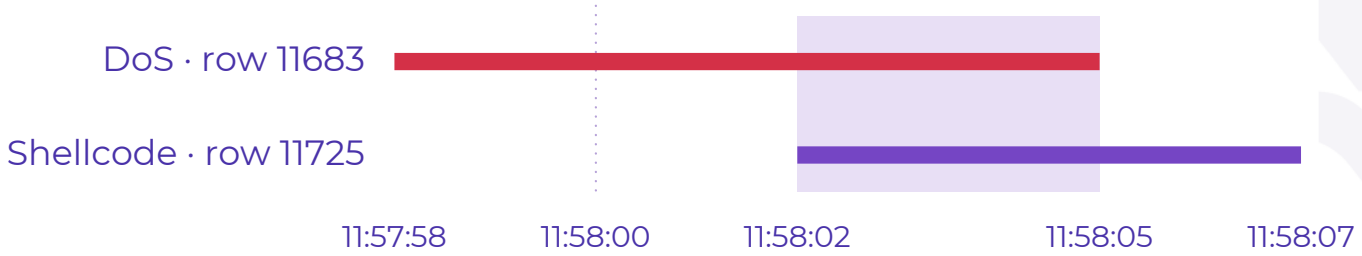
11:58–11:59

9 incoming flows

- Exploits
- Reconnaissance
- DoS
- Shellcode

Edges show the number of flow starts per minute

Two source records: UNSW-NB15_1.csv



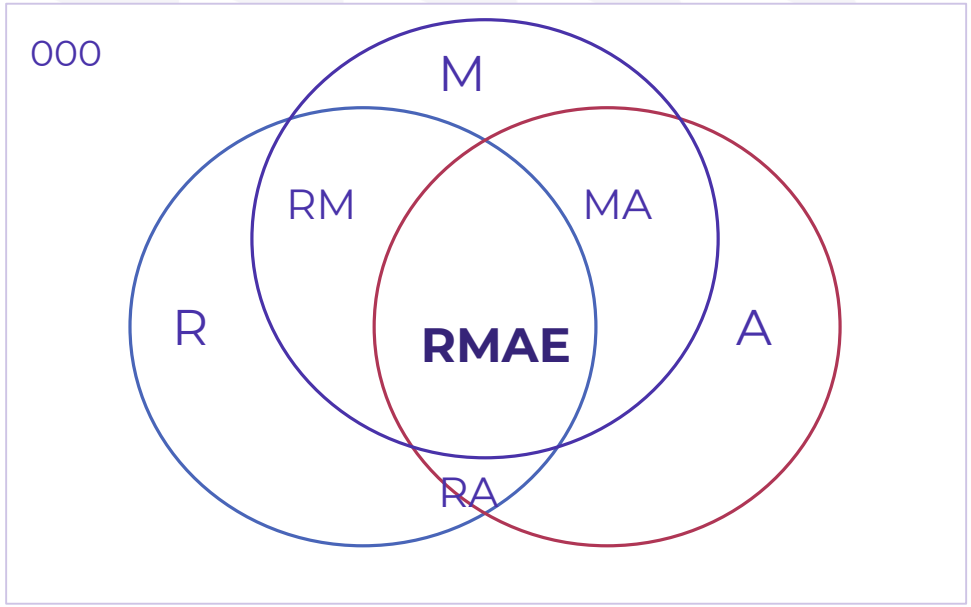
3 seconds

of interval overlap at one-second resolution

Cascade model: eight regions

$$D_{\mathrm{RMAE}} = D_R \cap D_M \cap D_A$$

Universe of observed events D



R: rarity; M: multi-label nature;
A: destructiveness

Property order: R / M / A

Disjoint regions for all property combinations

$$D_{000} = (D \setminus D_R) \cap (D \setminus D_M) \cap (D \setminus D_A)$$

$$D_{001} = (D \setminus D_R) \cap (D \setminus D_M) \cap D_A$$

$$D_{010} = (D \setminus D_R) \cap D_M \cap (D \setminus D_A)$$

$$D_{011} = (D \setminus D_R) \cap D_M \cap D_A$$

$$D_{100} = D_R \cap (D \setminus D_M) \cap (D \setminus D_A)$$

$$D_{101} = D_R \cap (D \setminus D_M) \cap D_A$$

$$D_{110} = D_R \cap D_M \cap (D \setminus D_A)$$

$$D_{111} = D_R \cap D_M \cap D_A$$

ρ — analysis route; υ — update route after verification

(1) $\rho(d) = M_1 \Leftrightarrow d \in D_{110} \cup D_{111}$

(2) $\rho(d) = M_2 \Leftrightarrow d \in D_{010} \cup D_{011}$

(3) $\rho(d) = M_3 \Leftrightarrow d \in D_{100} \cup D_{101}$

(4) $\rho(d) = M_4 \Leftrightarrow d \in D_{000} \cup D_{001}$

(5) $\upsilon(d) = \mathrm{ACoUM} \Leftrightarrow d \in D_A$

(6) $\upsilon(d) = \mathrm{LCoUM} \Leftrightarrow d \in D \setminus D_A$

Cascade processing: event description → R/M/A assessment → selection of a specialized module.
Verified results refine the context for subsequent events.

Cascade model: event routing

ρ Eight regions feed into four modules

A = 0	A = 1	Module	Routing rule
D_{110}	D_{111}	M_1	$\rho(d) = M_1 \Leftrightarrow d \in D_{110} \cup D_{111}$
D_{010}	D_{011}	M_2	$\rho(d) = M_2 \Leftrightarrow d \in D_{010} \cup D_{011}$
D_{100}	D_{101}	M_3	$\rho(d) = M_3 \Leftrightarrow d \in D_{100} \cup D_{101}$
D_{000}	D_{001}	M_4	$\rho(d) = M_4 \Leftrightarrow d \in D_{000} \cup D_{001}$

υ Update destination after verification

A = 1 ⟶ ACoUM

$$\upsilon(d) = \text{ACoUM} \Leftrightarrow d \in D_A$$

A = 0 ⟶ LCoUM

$$\upsilon(d) = \text{LCoUM} \Leftrightarrow d \in D \setminus D_A$$

Bit order in regions: R/M/A
1: property present; 0: absent

Cascade processing: event description → R/M/A assessment → selection of a specialized module.
Verified results refine the context for subsequent events.

Cascade model application scenario for UNSW-NB15

Descriptive analysis of the full corpus

1. Source data

↓

2. Observation rules

Node, 10 s window, label set and its frequency

↓

3. Rarity, multi-label nature, destructiveness

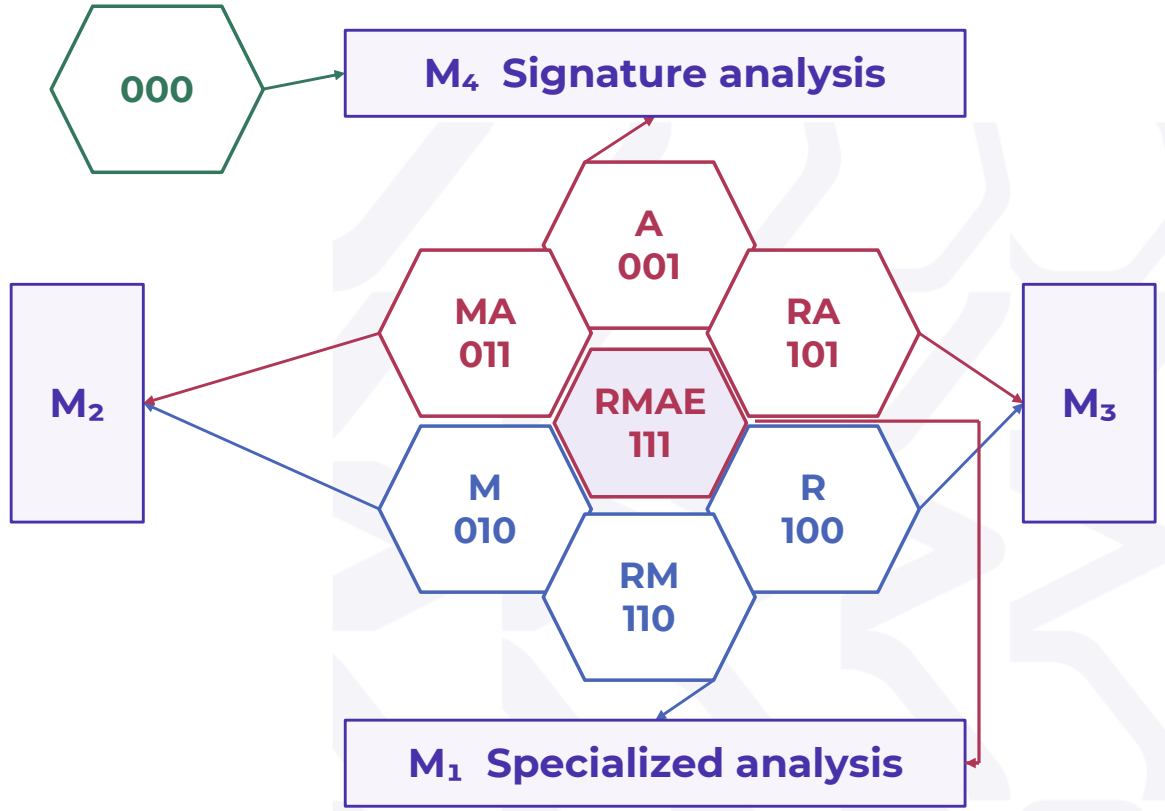
→

Verified results refine the context

Destructive event update module

Legitimate context update module

Cascade regions and modules



M_2: multi-label analysis; M_3: rare-event analysis

Eight regions illustrated by 10-second windows

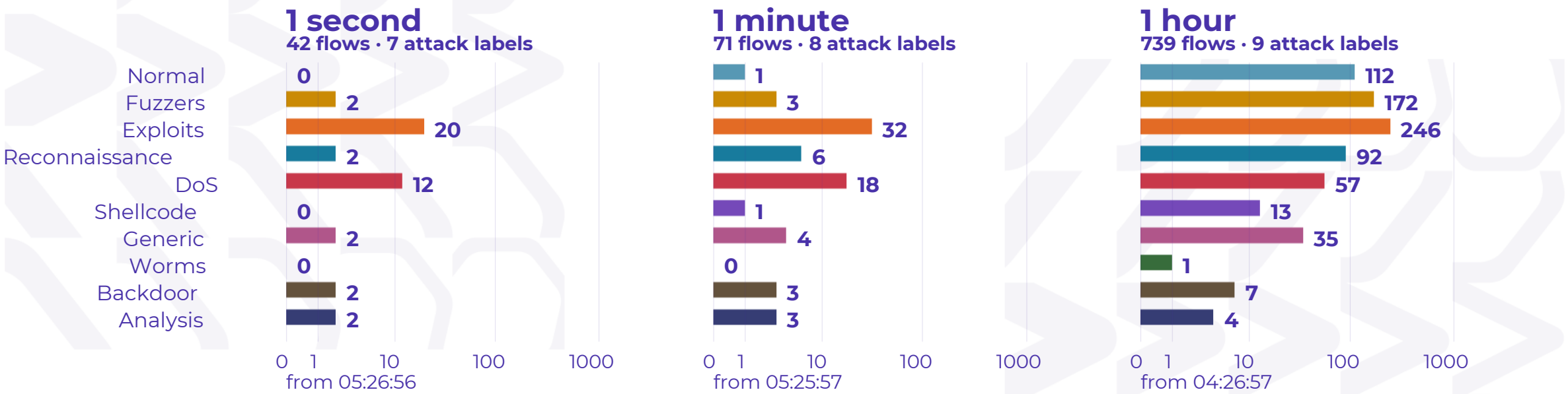
An event is one window at one node, **Δ = 10 s**

R	M	A	Event category	149.171.126.13 Label sets: 80 Windows: 3 546		149.171.126.18 Label sets: 74 Windows: 3 640		10.40.182.3 Label sets: 1 Windows: 6 526	
				Window labels	Corpus / node	Window labels	Corpus / node	Window labels	Corpus / node
1	**1**	**1**	Rare, multi-label, destructive	Exploits + Worms	**0.027%** **0.141%**	Generic + Shellcode	**0.049%** **0.440%**	Not observed	
1	1	0	Rare, multi-label, legitimate	Excluded with these labels: M = 1 ⇒ A = 1					
1	0	1	Rare, not multi-label, destructive	Worms	**0.038%** **0.254%**	Shellcode	**0.314%** **1.016%**	Not observed	
1	0	0	Rare, not multi-label, legitimate	Not observed: Normal is frequent across the corpus					
0	1	1	Frequent, multi-label, destructive	Exploits + Reconnaissance	**2.010%** **9.842%**	Exploits + Generic	**1.014%** **10.165%**	Not observed	
0	1	0	Frequent, multi-label, legitimate	Excluded with these labels: M = 1 ⇒ A = 1					
0	0	1	Frequent, not multi-label, destructive	Exploits	**7.092%** **33.136%**	Generic	**1.262%** **12.170%**	Not observed	
0	0	0	Frequent, not multi-label, legitimate	Normal	**78.067%** **3.582%**	Normal	**78.067%** **2.115%**	Normal	**78.067%** **100.000%**

R is determined across the full corpus at ε = 1%. Node frequency is shown for comparison.

Window size: observation and mathematical condition

Node 149.171.126.10, shared window end: 18.02.2015 05:26:57 UTC



In this example, the label set expands as the window grows

7 attack labels → **+ Shellcode** → **+ Worms**

8 attack labels

9 attack labels

L(Δ, t): union of labels of all flow arrivals in (t − Δ, t]. With fixed labels:

$$\Delta_1 \leq \Delta_2 \Rightarrow L(\Delta_1, t) \subseteq L(\Delta_2, t)$$

Multi-label representation preserves the given labels

13 422 windows (10 s) contain several distinct attack labels

Observed set

$$L(d) = \{\text{Exploits}, \text{Worms}\}$$

One atomic label

Exploits / Worms

Full label set

Exploits + Worms

Across the full corpus: 54 121 attack-label occurrences

34 336 retained with one label	19 785 lost — 36.56%

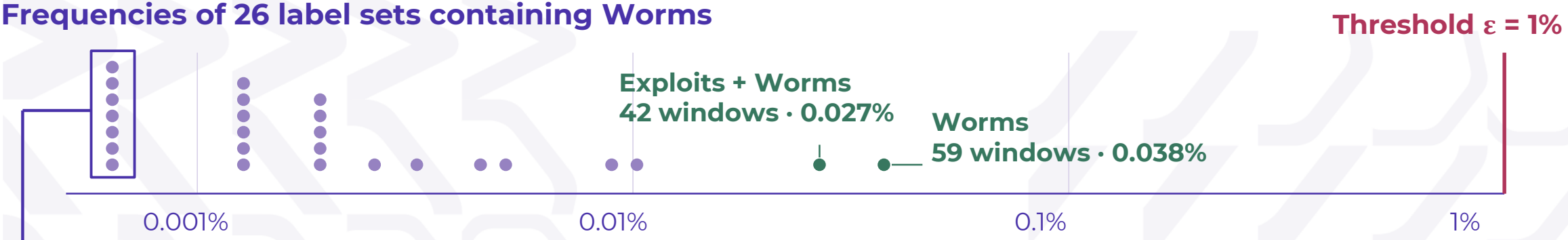
$$\text{Recall}(d) = \frac{|L(d) \cap \hat{L}(d)|}{|L(d)|} \leq \frac{1}{|L(d)|}, |L(d)| \geq 2$$

The full set and its reversible code preserve all given labels.

Rarity identifies label sets containing Worms

174 flows → **189 windows (10 s)** → **26 label sets**

Frequencies of 26 label sets containing Worms



Label set	Win.
Backdoor + Worms	1
Generic + Worms	1
DoS + Fuzzers + Worms	1
DoS + Generic + Worms	1
Reconnaissance + Shellcode + Worms	1
DoS + Fuzzers + Reconnaissance + Worms	1
Analysis + Backdoor + DoS + Exploits + Fuzzers + Worms	1

One point = one distinct label set.
Frequency = the share of windows with exactly this set.

All 26 label sets with Worms meet the 1% rarity threshold

The model as a map of dataset properties

156 points: 156 observed label sets. Three properties are shown together.



The map shows shared properties while preserving differences between individual label sets.

Describing an event from flows: R/M/A properties for UNSW-NB15

Node 149.171.126.10, 18.02.2015, 00:42:20–00:42:30 UTC

5 source flows

- Worms
- Exploits
- Exploits
- Exploits
- Exploits

→ **.10** →

One window 10 seconds

Stored description

Attribute	Value
Label set	Exploits + Worms
Label-set frequency	42 / 156 547 ≈ 0.027%
R / M / A region	1 / 1 / 1
Basis for A	Labelled attacks present

Properties and route

R = 1: 0.027% ≤ 1% in the full corpus

M = 1: two distinct labels

A_{UNSW} = 1: labelled attacks present

↓

111 · RMAE → M_1

Specialized analysis

The description retains the properties, full label set and links to the source flows.

$$d_* = (h, I), \Delta = 10\ \text{s}, L(d_*) = \{\text{Exploits}, \text{Worms}\}$$

$$p_L(d_*) = \frac{42}{156547} \approx 0.027\% \leq 1\%, |L(d_*)| = 2, A_{\text{UNSW}}(d_*) = 1$$

$$(R, M, A_{\text{UNSW}})(d_*) = (1,1,1) \Rightarrow d_* \in D_{111} = D_{\text{RMAE}} \Rightarrow \rho(d_*) = M_1$$

What three properties add to the data description

Rarity

At ε = 1%, all **26 label sets with Worms** are rare.
They occur in **189 windows**.

Multi-label nature

Choosing one label loses **19 785** occurrences — **36.56%**.
The full set preserves all given labels.

RMAE in the sample

All three properties occur in **8 687** of 156 547 windows — **5.55%**.
Here anomalousness means an attack label is present.

Further research

Does a decision-making system have sufficient knowledge
to give a justified interpretation of a specific event?

THANK YOU FOR YOUR ATTENTION!

D. I. Rakovskiy · d.i.rakovskiy@mtuci.ru O. I. Sheluhin · sheluhin@mail.ru

Contacts

Federal State Budgetary Educational Institution of Higher Education
Moscow Technical University of Communications and Informatics, awarded the Order of the Red Banner of Labour

8A Aviamotornaya St., Moscow 111024, URL: https://mtuci.ru

Department: Information Security (IS),
URL: https://mtuci.ru/about_the_university/structure/769/
+7(495)957-77-99 (ext.136), **ib@mtuci.ru**

Oleg Ivanovich Sheluhin
Dr. Sci. (Eng.), Professor, Honoured Scientist of the Russian Federation, Head of the Information Security Department,
sheluhin@mail.ru

Dmitry Igorevich Rakovskiy
Cand. Sci. (Eng.), Associate Professor, Information Security Department,
d.i.rakovskiy@mtuci.ru