Detekcja spamu na podstawie cech niskiego poziomu

Marcin Luckner
Politechnika Warszawska
Wydział Matematyki i Nauk Informacyjnych
mluckner@mini.pw.edu.pl
http://www.mini.pw.edu.pl/~lucknerm

Cechy niskiego poziomu

- Moore 2005
  - Zbiór danych opisujących pojedyncze przepływy pakietów TCP pomiędzy klientem i serwerem
  - Każdy rekord zawiera 248 cech
  - Rekordy podzielone są na klasy (w tym mail)

Number	Short	Long
33	ack_pkts_sent_*a b*	The total number of ack packets seen (TCP segments seen with the ACK bit set) (client→server).
34	ack_pkts_sent_*b a*	" (server→client)
35	pure_acks_sent_*a b*	The total number of ack packets seen that were not piggy-backed with data (just the TCP header and no TCP data payload) and did not have any of the SYN/FIN/RST flags set (client→server)
36	pure_acks_sent_*b a*	" (server→client)
37	sack_pkts_sent_*a b*	The total number of ack packets seen carrying TCP SACK [6] blocks (client→server)
38	sack_pkts_sent_*b a*	" (server→client)
39	dsack_pkts_sent_*a b*	The total number of sack packets seen that carried duplicate SACK (D-SACK) [7] blocks. (client→server)
40	dsack_pkts_sent_*b a*	" (server→client)
41	max_sack_blks/ack_*a b*	The maximum number of sack blocks seen in any sack packet. (client→server)
42	max_sack_blks/ack_*b a*	" (server→client)
43	unique_bytes_sent_*a b*	The number of unique bytes sent, i.e., the total bytes of data sent excluding retransmitted bytes and any bytes sent doing window probing. (client→server)
44	unique_bytes_sent_*b a*	" (server→client)
45	actual_data_pkts_*a b*	The count of all the packets with at least a byte of TCP data payload. (client→server)
46	actual_data_pkts_*b a*	" (server→client)
47	actual_data_bytes_*a b*	The total bytes of data seen. Note that this includes bytes from retransmissions / window probe packets if any. (client→server)
48	actual_data_bytes_*b a*	" (server→client)
49	rexmt_data_pkts_*a b*	The count of all the packets found to be retransmissions. (client→server)
50	rexmt_data_pkts_*b a*	" (server→client)
51	rexmt_data_bytes_*a b*	The total bytes of data found in the retransmitted packets. (client→server)
52	rexmt_data_bytes_*b a*	" (server→client)
53	zwnd_probe_pkts_*a b*	The count of all the window probe packets seen. (Window probe packets are typically sent by a sender when the receiver last advertised a zero receive window, to see if the window has opened up now). (client→server)
54	zwnd_probe_pkts_*b a*	" (server→client)
55	zwnd_probe_bytes_*a b*	The total bytes of data sent in the window probe packets. (client→server)
56	zwnd_probe_bytes_*b a*	" (server→client)
57	outoforder_pkts_*a b*	The count of all the packets that were seen to arrive out of order. (client→server)

Continued on next page

Nagłówek IP

0 - 3	4 - 7	8 - 11	12 - 15	16 - 19	20 - 23	24 - 27	28 - 31
Version	IHL	ToS/DSCP/ECN		Total Length			
Identification				Fragment Flags (3) and Offset (13)			
Time To Live		Protocol		Header Checksum			
Source Address							
Destination Adress							
Options							

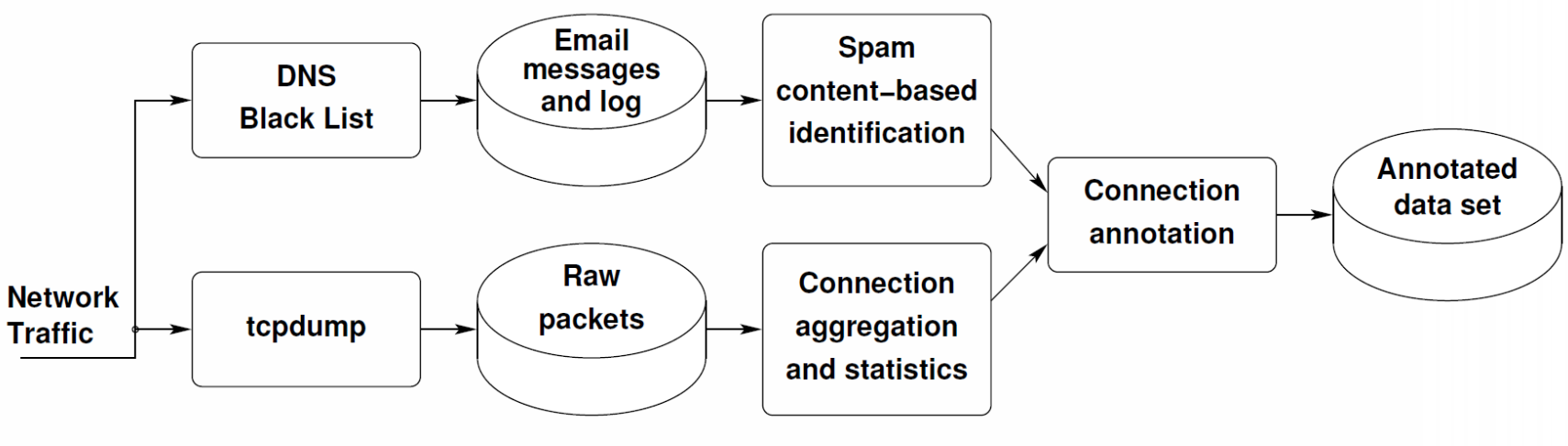
Przykładowe cechy

- Minimalny, średni i maksymalny
  - Rozmiar pakietu
  - Interwał między pakietami
  - Rozmiar pakietu z daną flagą
  - Rozmiar okna TCP
- Liczba
  - Pakietów
  - Pakietów z daną flagą

Wykrywanie spamu

- Žádník 2008
  - Analiza ruchu mailowego
    - 9 tygodni
  - 60 cech niskiego poziomu
    - 2* 30 w obu kierunkach
  - Podział ruchu na 5 klas

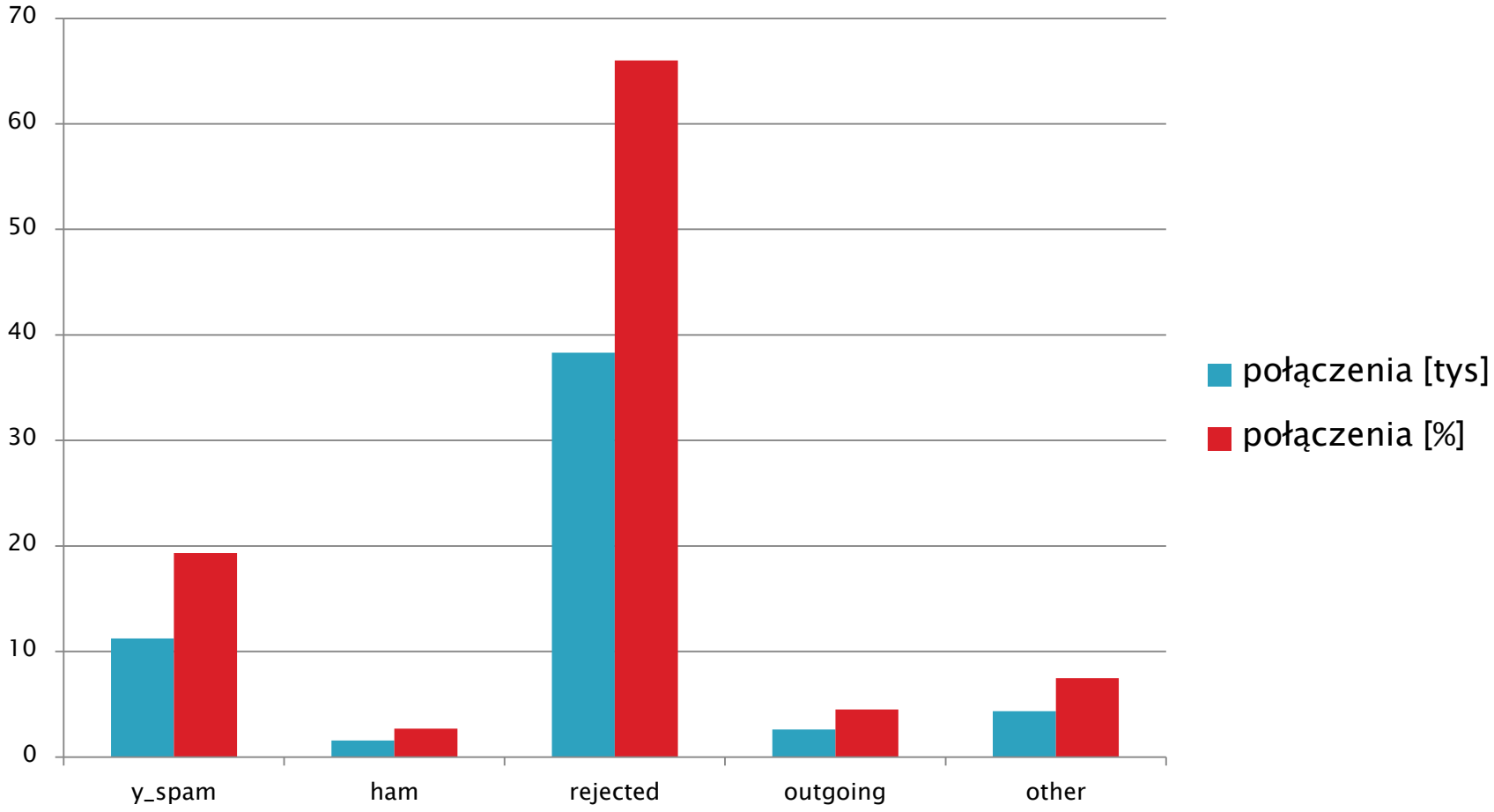
Tworzenie zbioru danych



Klasyfikacja ruchu

- *Ham* połączenia zaznaczone jako nie spam przez SpamAssasin
- *Y_spam* połączenia zaznaczone jako nie spam przez SpamAssasin
- *Rejected* połączenia z DNS będących na czarnej liście
- *Outgoing* połączenia wychodzące
- *Other* skanowanie portów, DoS, inne

Rozkład w grupach



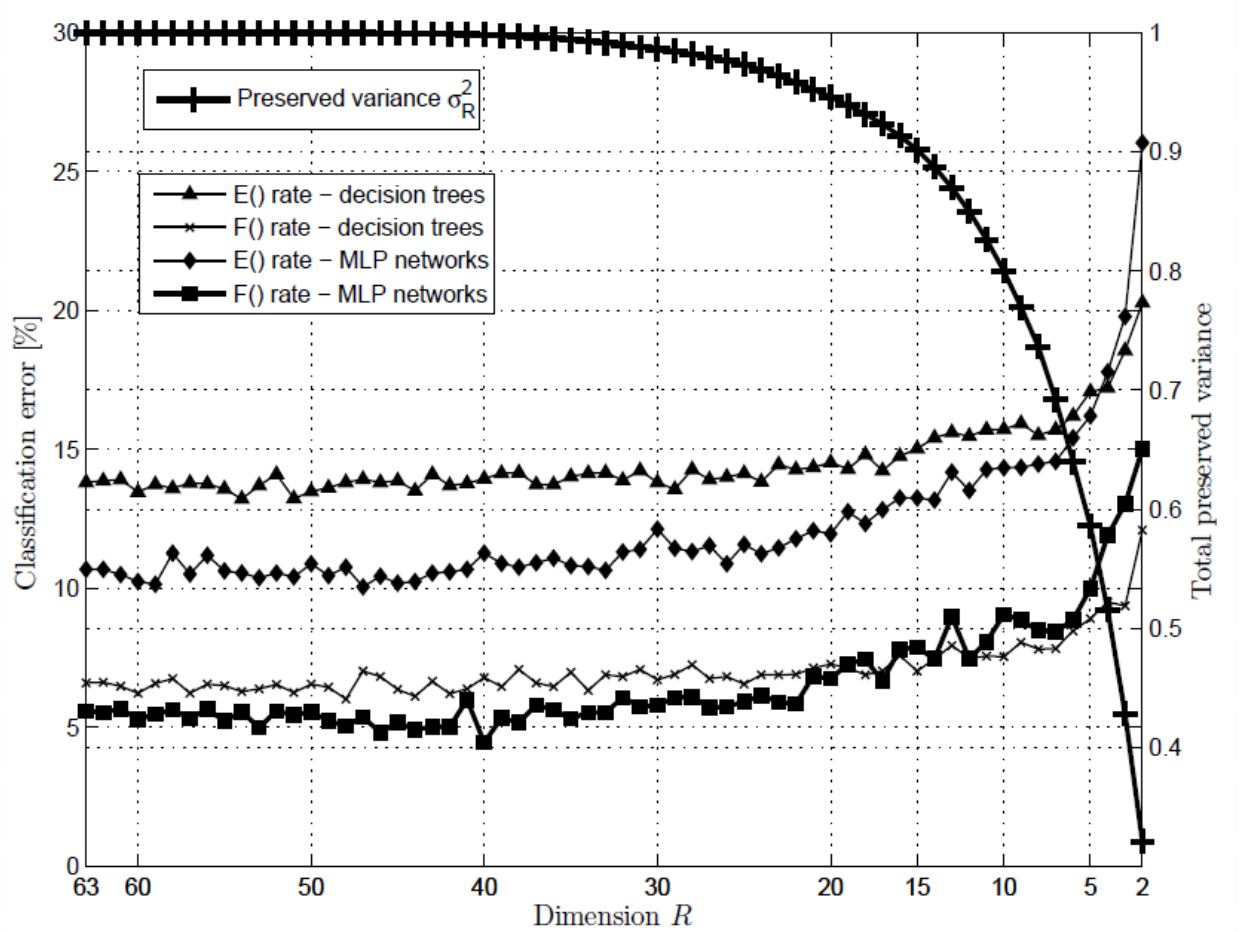
Wyniki klasyfikacji

Rozpoznana:	y_spam	ham	rejected	outgoing	other
y_spam	3546	28	138	0	48
ham	189	531	4	0	5
rejected	7	0	12986	0	78
outgoing	0	0	0	896	0
other	60	4	181	0	1214
Skuteczność	93.3%	90.3%	97.6%	100%	90.3%

Redukcja cech

- Grzenda 2012
  - Powtórzenie testów Žádníka
  - Redukcja wymiaru danych

Wpływ redukcji wymiaru cech na skuteczność klasyfikacji



Bibliografia

- **Discriminators for use in flow-based classification (2005)** Andrew Moore , Michael Crogan , Andrew W. Moore , Queen Mary , Denis Zuev , Denis Zuev , Michael L. Crogan
- **Is Spam Visible in Flow-level Statistics? (2008)** Martin Žádník, Zbyněk Michlovský
- **Towards the Reduction of Data Used for the Classification of Network Flows (2012)** Maciej Grzenda