Comparison of Anti-Virus Programs using Fuzzy Logic

Vaclav Bezdek

Thomas Bata University, Zlín, Czech Republic

bezdek@fai.utb.cz

Abstract: *This work follows the previous author´s paper: Possible use of Fuzzy Logic in Database. It tries to show application of Fuzzy Logic in selecting the best anti-virus software based on testing made by AV-Comparatives.*

Keywords: Fuzzy logic, anti-virus program

1. Introduction

AV-Comparatives test covers a broad spectrum of all potential anti-virus properties. In 2011, AV-Comparatives released a total of 9 tests of anti-virus programs in various fields. Tests were attended by 20 producers – both worldwide known and famous and, although worldwide known, less famous. On the grounds of these tests, the best anti-virus software for 2011 was then declared. This paper is based on results of these tests and selects the best anti-virus program using fuzzy logic.

However, to choose the right anti-virus program that will meet all of our requirements best, is difficult. To include all of our wishes, possibilities and needs in the selection process and to choose the best is possible when we use fuzzy logic. This paper omits the price-requirement and focuses primarily on the quality of the anti-virus programs. As input data we used results of tests by AV-Comparatives, which tests the detection rate of malware, heuristic detection, false detection, scanning speed and an impact on the system, protection from malware-infected sites and the ability to remove malware without falls, hangs or other errors.

In 2011, only 7 manufacturers participated on all tests and were also evaluated in these tests. These manufacturers were Kaspersky, BitDefender, Panda, Eset, F-Secure, Avira and G Data. Other manufacturers did not participate on some tests either voluntarily (for any reason), or did not permit evaluation of the tests (this decision was due to a total failure in tests, or other problem).

At the end of 2011, AV-Comparatives announced a partial order in seven categories which ultimately determined the overall ranking. According to a series of tests, Kaspersky became Product of the Year last year.

(Summary reports can be found at http://www.av-comparatives.org/comparativesreviews/summary-reports/137-summary-report-december-2011)

2. Fuzzy logic

The concept of fuzzy logic was first discovered in the work of Zadeh, LA: Fuzzy Sets. (Information & Control – Vol. 8, 1965, pp. 338-353). Fuzzy logic (unlike classical logic) admits partial membership to a set using membership functions. The simplest ones are shown below:

$$L(x,a,b) = \begin{cases} 1 & x < a \\ \dfrac{b-x}{b-a} & a \le x \le b \\ 0 & x > b \end{cases}$$

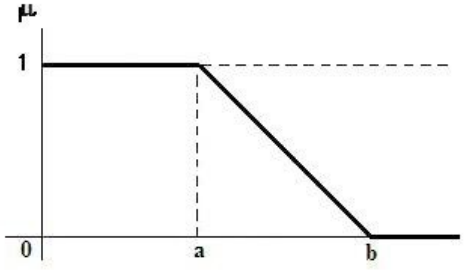

Figure 2.1 – **L-membership function**

$$\Gamma(x, a, b) = \begin{cases} 0 & x < a \\ \dfrac{x-a}{b-a} & a \le x \le b \\ 1 & x > b \end{cases}$$

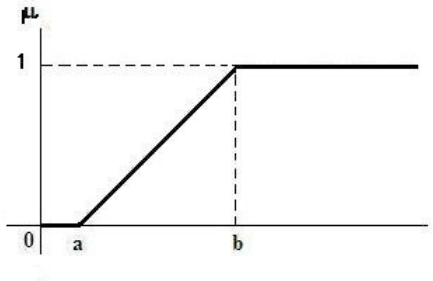

Figure 2.2 – Γ-membership function

The entire system then operates in following 3 steps:

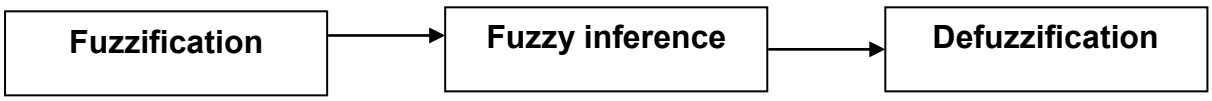

Figure 2.3 – Solving Problem Using Fuzzy Logic

Particular steps of problem solving using fuzzy logic (Fuzzification - transformation of the fair input values, Fuzzy inference – definition of system behavior using rules, Defuzzification - obtaining of resulting values) are explained in detail in the cited literature.

3. Tested programs

List of advantages and disadvantages of the tested programs: (A comparison can be found at http://www.av-comparatives.org/images/docs/avc_cor_201109_en.pdf)

3.1 Avira

Overall – Avira is easy to use and suitable for both experts and non-experts.

Plus points – Large range of configuration and installation options offered by the setup wizard, including choice of components. Clear and simple interface design makes important information and functionality easily accessible. Comprehensive manual easily found from Help menu.

Minus points – No obvious way of turning off outgoing firewall queries, other than uninstalling Avira´s firewall and using Windows Firewall instead.

Conclusion – Amongst the conventional LAN-based security solutions, Avira stands out clearly for its ease and speed of installation. There are a number of reasons for this. Firstly, the simple, concise How to guides allows the administrator to find essential information quickly, and explain clearly what needs to be done. Any additional software components needed such as C++ libraries, are installed automatically by the Avira installer. The design of the MMC console means that the user does not feel overwhelmed by too many features, and the user interface is intuitive and consistent. Client preparation is minimal, and the installation programs runs quickly and reliably. Although the Avira software is suitable for use in enterprise networks, the fact that it installs so rapidly and easily makes it especially suitable for small business networks, where it does not make sense to spend a long time preparing the automated installation of just a few client PCs. We also feel that Avira would be ideal for less experienced administrators, as its installation is so simple and trouble-free.

3.2 Bitdefender

Overall – Bitdefender is easy to use and suitable for both experts and non-experts.

Plus points – Installation is very easy, with almost no questions to answer.

Minus point – Slightly confusing scan results dialog box.

Conclusion – Bitdefender protects small business network particularly quick, simple and unproblematic. The manual explains clearly how to install and deploy the software, and the procedure is simple in practice. The management console gives the administrator the ability to carry out a wide

range of tasks and audits, not only for the antivirus software, but also for the entire Windows system. There is very little to criticize, and the management features make the software very suitable for medium-sized business networks.

3.3 ESET

Overall – ESET is a well-designed and easy-to-use suite offering sensible default setting for non-experts and wide range of easily accessible options for advanced users.

Plus points – Exceptionally clear, simple and elegant user interface, excellent manuals and online help.

Minus points – Confusing labeling of context-menu scans, parental control shown as active when effectively it is not.

Conclusion – Using ESET software for small business network protection is very straightforward. By a large the website makes clear which product does what, although an extra word of explanation on the server products would not go amiss. The manuals are well written and clearly laid out, making it easy to find what you need to complete the installation and configuration. In general, ESET´S business software is simple, well designed and easy to use, and can be recommended for large or small networks.

3.4 F-Secure

Overall – Despite some irritations, F-secure is largely simple to use and could be used by non-experts as well as experts.

Plus points – Interface is largely clear and simple. Excellent notification/choices when malware is discovered.

Minus points – No „FIX ALL“ button. Completely non-functional in Safe Mode. Program has to be started via irritating Launch Pad.

3.5 G DATA

Overall – G Data is very well thought-out site, suitable for use by both non-experts and advanced users.

Plus points – Interface allows clear overview of the components of the suite and their status, with easy access to configuration setting. There is a choice of components in both the installer and the uninstaller.

Minus points – Leaving OKB files after „cleaning“ malware, inability to function in Safe Mode.

Conclusion – G Data´s software stands out as being extremely quick and easy to install and configure. The management console used for both Anti-Virus and Mail-Security elements is very clear, simple, intuitive and consistent. We feel that the package would be particularly suitable for less experienced administrators, due to its simplicity and ease for use. Unfortunately, the manual is extremely frustrating to use, despite being essentially well written, because of its poor production. However, it could be very easily improved with some screenshots, and proper indexing and bookmarks, and we would urge G Data to do this. The minimalist client software is unique in its simplicity, and allows the administrator a high degree of control over the interface the user sees.

3.6 Kaspersky

Overall – Kaspersky is very easy to install and use. It is suitable for both non-experts and advanced users.

Plus points – Full installer that checks for updates if online, new interface is simple, clean and user-friendly, updating and scanning functions are fully operational is Safe mode, online support for the suite is superb once you find it, comprehensive manual available.

Minus point – Warning message about malware download could be clearer, Support link in the program doesn´t link to the optimal page of Kaspersky´s website.

Conclusion – Kaspersky retains all the strengths of the previous version, i.e. easy navigation through the Microsoft Management Console Interface, quick access to important features, and excellent real-time reporting on deployment. The design of the client software, Kaspersky Endpoint Security 8.0, is innovative and rational, though it is aimed at administrators rather than end user. Manuals for the new software have not yet been produced, and so we are unable to comment on them. Kaspersky Security 8.0 for Microsoft Exchange Servers is straightforward to install, and has a very simple, clear console, making it easy to use.

3.7 Panda

Overall – Panda is very easy to install and use, but has a number of easily accessible advanced configuration options, making it user-friendly for both expert and non-expert users.

Plus point – Setup wizard gives choice of components to install, choice of using Panda or Windows firewall, choice of allowing outgoing program access without querying.

Minus point – Inability to run at all in Safe Mode. Parental Control shown as active before user accounts have been configured.

4. Tests carried out

AV-Comparatives tested anti-virus programs nine times and rated them as ADVANCED + award, ADVANCED, STANDARD or just TESTED. After evaluation, the best product was determined. To be rated as "Product of the Year" by AV-Comparatives, an anti-virus program must have very high detection rate of malware (with internet access and latest signatures), good heuristic detection, produce very few false positives, scan fast and reliably with a low system impact, protect the system against malware/websites with malicious software without relying significantly on user decision/interactions, have good malware removal capabilities, cause no crashes or hangs, and have no annoying bugs (all results can be found at http://www.av-comparatives.org/comparativesreviews/summary-reports/137-summary-report-december-2011).

4.1 On-Demand Detection of Malicious Software – February 2011

A high detection rate of malware – without causing too many false alarms – is still one of most important, deterministic and reliable features of anti-virus product (as e.g. is not heavily dependent of vectors and other factors).

This test works on the following principle. An anti-virus software is chosen and few infected files are sent whose virus-definitions are well-known and so the anti-virus should recognize them. Then, the success rate of detected files, the number of viruses that anti-virus missed and also false positives or scanning speed is evaluated. The following table shows the ratio of captured viruses (out of total 403543), the number of false detection (≤2 is evaluated as very few, ≤15 as few, ≤100 as many and ≥100 a very many) and scan speed (if scan speed is ≥12 MB/sec, it is evaluated as fast, between 7 and 12 MB/sec. it is average and if less than 7 MB/sec., it is slow).

Best results :	G Data 99,8 %,	False detection – McAfee 0,	Scan speed – Avast 16,3.
Worst results :	K7 TotalSecurity 84,4 %,	False detection – TrendMicro 290,	Scan speed – Microsoft 6,6

Tab. 4.1 – Test 1

		False detection	Scan speed
Avira	97,5	9	10,2
Bitdefender	97,6	3	9,7
ESET	97,5	20	8,3
F Secure	98,1	3	9,4
G Data	99,8	18	8,5
Kaspersky	97,0	12	10,3
Panda	98,1	18	13,2

4.2 Retrospective Test – February 2011

This test examined the effectiveness of anti-virus software against unknown threats. Anti-virus database of programs is "conserved" for a few weeks and then viruses are sent that emerged after the date of preservation. These threats therefore behave as completely unknown viruses, because the anti-virus does not have their samples in the database. Thus, the ability of anti-virus to detect an unknown problem comes into play.

Overall rating by AV-Comparatives consisted of number of successful detections of unknown viruses, but also the number of false detections. The best program in detection, but with a high number of false positives cannot turn out the best in general. The following table shows the success ratio of anti-virus programs on a sample of 9177 unknown viruses, including the number of false alarms (0-3 means very few false alarms, 4-15 means few alarms, 15-100 means many false alarms and over 100 means a very many false alarms).

Best results : G Data – 61 %, False detection - Microsoft 1,

Worst results : Sophos 23 %, False detection - Qihoo – 104

Tab. 4.2 – Test 2

	%	False detection
Avira	59	9
Bitdefender	35	3
ESET	59	20
F Secure	35	3
G Data	61	18
Kaspersky	55	12
Panda	52	18

4.3 Performance Test – July 2011

This specific test examines, how various anti-virus programs burden system activity, i.e. what impact they have on slowing computer functioning. The slowdown in the computer functioning was examined on 5 different activities, namely: file copying, archiving and extracting, encoding/transcoding, install/uninstall programs, launch applications. Furthermore, the PC Mark test was performed. Summary of results is in the Tab. 4.3 (maximum AV-Score is 90, maximum PC Mark Score is 1640):

Best results: AV Score - Eset – 90, PC Score - K7 – 99,6

Worst results: AV Score - PC Tools 57,5 PC Score - PCTools – 96,1

Tab. 4.3 – Test 3

	AV- Score	PC Mark Score
Avira	87,5	1601
Bitdefender	82,5	1593
ESET	90	1611
F Secure	85	1622
G Data	75	1582
Kaspersky	85	1600
Panda	85	1599

4.4 Whole Product "Real-World" Dynamic Test – March-June 2011

This long-term test was conducted from March to June of 2011. The task was to find out how the tested software works when browsing on websites infected with malicious code. In addition, there has

been installed other potentially "malicious software" in the computer, which maintained "in the factory settings" and was not configured so as to enhance detection capabilities. 2480 examines was carried out during the whole test.

Thus, there was examined how many viruses each product successfully captures and of course what is the number of badly evaluated domains and download files – i.e. the rate of false positives. The results are shown in the Tab. 4.4 (average value of wrongly blocked score is 27):

Best results: Protection rate – Symantec – 99,3 %

Worst results: Protection rate – K7 – 92,1 %

Tab. 4.4 – Test 4

	Blocked	User dependent	Compromised	Protection rate	Wrongly blocked score
Avira	2402	0	78	96,9	16
Bitdefender	2457	0	23	99,1	7
ESET	2436	0	44	98,2	7,5
F Secure	2459	4	17	99,2	17
G Data	2453	0	27	98,9	12
Kaspersky	2424	23	33	98,2	8,5
Panda	2445	0	35	98,6	16

4.5 On-Demand Detection of Malicious Software – August 2011

The same test as Test 1, except that the total number of viruses, which was 206043. The number of false detection ≤3 is evaluated as very few, ≤15 as few, ≤100 as many and ≥100 a very many. Scan speed ≥12 MB/sec. is evaluated as fast, between 8 and 12 MB/sec. it is average and if less than 8 MB/sec., it is slow.

Best results : G Data - 99,7 %, False detection – McAfee - 0, Scan speed – Avast - 16,4.

Worst results : K7 TotalSecurity-85,6 %, False detection – TrustPort - 59, Scan speed – Microsoft - 7,1

Tab. 4.5 – Test 5

	%	False detection	Scan speed
Avira	99,5	11	12,3
Bitdefender	98,4	8	10,5
ESET	97,3	3	9,8
F Secure	98,5	6	10,3
G Data	99,7	14	10,1
Kaspersky	98,3	1	9,9
Panda	99,3	1	9,6

4.6 Retrospective Test – August 2011

The same test as Test 2. This time, the number of unknown viruses was 9003. The number of false alarms between 0-3 is evaluated as very few false alarms, 4-15 few false alarms, 15-100 means many false alarms and over 100 means a very many false alarms.

Best results: Qihoo – 67,6 %, False detection – Kaspersky, Panda 1,

Worst results: Panda – 41,4 %, False detection - Trustport – 59

Tab. 4.6 – Test 6

	%	False detection
Avira	62,4	11
Bitdefender	57,2	8
ESET	61,6	3
F Secure	57,5	6
G Data	64,0	14
Kaspersky	60,1	1
Panda	41,4	1

4.7 Performance Test – November 2011

Test (alike Test 3) which is intended to identify and compare the performance of anti-virus programs during "regular work". Maximum AV-Score is 90, maximum PC Mark Score is 2024.

Best results: AV Score – more programs – 90, PC Score – ESET, K7 – 99,8
Worst results: AV Score - Trustport – 60 PC Score - PCTools – 94,3

Tab. 4.7 – Test 7

	AV-C Score	PC Mark Score
Avira	90	2006
Bitdefender	70	1982
ESET	90	2019
F Secure	90	2015
G Data	70	1984
Kaspersky	90	2001
Panda	88	1993

4.8 Malware removal test – autumn 2011

In autumn of 2011, AV-Comparatives tested anti-virus ability to fight an infection and remove all its manifestations. Thus, there was not tested the defensive capability of anti-virus programs, but the ability to remove infection from an already infected computer. Older viruses, that anti-virus should know and have these samples in their virus databases, were utilized. In addition, used samples had not destructive capabilities and were not a kind of malware that can totally destroy a computer. A total of 10 groups of malware samples were selected, that contained the most common Trojans, worms and fake anti-viruses.

As for the rating, anti-virus capabilities were divided into a total of ten groups from AA to DD (AA = 100, DD = 0) which represent the level of ability to remove anti-virus infection and the complexity of "cleansing process" for the user. Average score gives the final result that is shown in the following table. Of course, the maximum value is 100 points.

Best results: Bitdefender – 90 points,
Worst results: Avast – 52 points

Tab. 4.8 – Test 8

Avira	80
Bitdefender	90
ESET	58
F Secure	67
G Data	55
Kaspersky	86
Panda	63

4.9 Whole Product "Real-World" Dynamic Test – August-November 2011

The same test as Test 4 – this time running from August to November. Each testing day, all available security updates for installed applications were installed on each computer prior to start of testing and of course the anti-virus virus database had been continuously updated. Subsequently, computers began to penetrate the website containing (or potentially containing) malicious code. 4 series of tests were performed that included a total of 1898 "test cases". The number of successfully and unsuccessfully blocked sites and of course the number of false positives – that means blocking of legitimate sites and files – was evaluated. Average value of wrongly blocked score is 12.

Best results : Protection rate – Symantec – 99,5 %
Worst results : Protection rate – Webroost – 93,6 %

Tab. 4.9 – Test 9

	Blocked	User dependent	Compromised	Protection rate	Wrongly blocked score
Avira	1864	0	34	98,2	17
Bitdefender	1886	0	12	99,4	4
ESET	1844	7	47	97,3	1
F Secure	1872	5	21	98,8	7
G Data	1874	0	24	98,8	3
Kaspersky	1877	8	13	99,1	0,5
Panda	1849	0	49	98,2	1

5. Comparison of anti-virus software using fuzzy logic

5.1 Fuzzification

Only results of those 7 programs that attended all nine tests are compared using fuzzy logic. First, the user can select the preferences of particular tests (any amount so that it clearly shows his attitude to specific tests) –that will be omitted in this paper. Then the results will be compared with each other and evaluated using the following procedure:

- Test number 1 – On-Demand Detection of Malicious Software – February 2011
  - The success rate will be recalculated using percent expressed in decimal number.
  - False detection will be recalculated using L-membership function, where parameter *a* will be equal 2 and parameter *b* is equal 100
  - Scan Speed will be recalculated using the Γ-membership function, where parameter *a* is equal 7 and parameter *b* is equal 12.
- Test number 2 – Retrospective Test – February 2011
  - The success rate will be recalculated using percent expressed in decimal number.
  - False detection – L(x,3,100).
- Test number 3 – Performance Test – July 2011
  - AV-Score and PC Mark Score will be recalculated using percent expressed in decimal number.
- Test number 4 – Whole Product "Real-World" Dynamic Test – March-June 2011
  - Score in Protection rate will be recalculated using percent expressed in decimal number.
  - Wrongly blocked score L(x,0,54).
- Test number 5 – On-Demand Detection of Malicious Software – August 2011
  - The success rate will be recalculated using percent expressed in decimal number.
  - False detection – L(x,3,100)
  - Scan Speed – Γ(x,8,12)
- Test number 6 – Retrospective Test – August 2011
  - The success rate will be recalculated using percent expressed in decimal number.
  - False detection – L(x,3,100).
- Test number 7 – Performance Test – November 2011
  - AV-Score and PC Mark Score will be recalculated using percent expressed in decimal number.

- Test number 8 – Malware removal test – autumn 2011
  - Score will be recalculated using percent expressed in decimal number.
- Test number 9 – Whole Product "Real-World" Dynamic Test – August-November 2011
  - Score in Protection rate will be recalculated using percent expressed in decimal number.
  - Wrongly blocked score L(x,0,24).

The results (2 decimal places) are presented in the following table:

Tab. 5.1 – Tests results when using fuzzy logic

	1			2		3		4		5			6		7		8	9	
		false	speed		false	Av	Pc		wrongly		false	speed		false	Av	Pc			wrongly
A	0,98	0,93	0,64	0,59	0,94	0,97	0,98	0,97	0,70	1,00	0,92	1,00	0,62	0,92	1,00	0,99	0,80	0,98	0,29
B	0,98	0,99	0,54	0,35	1,00	0,92	0,97	0,99	0,87	0,98	0,95	0,63	0,57	0,95	0,78	0,98	0,90	0,99	0,83
E	0,98	0,82	0,26	0,59	0,82	1,00	0,98	0,98	0,86	0,97	1,00	0,45	0,62	1,00	1,00	1,00	0,58	0,97	0,96
F	0,98	0,99	0,48	0,35	1,00	0,94	0,99	0,99	0,69	0,99	0,97	0,58	0,57	0,97	1,00	1,00	0,67	0,99	0,71
G	1,00	0,84	0,30	0,61	0,85	0,83	0,96	0,99	0,78	1,00	0,89	0,53	0,64	0,89	0,78	0,98	0,55	0,99	0,88
K	0,97	0,90	0,66	0,55	0,91	0,94	0,98	0,98	0,84	0,98	1,00	0,48	0,60	1,00	1,00	0,99	0,86	0,99	0,98
P	0,98	0,84	1,00	0,52	0,85	0,94	0,98	0,99	0,70	0,99	1,00	0,40	0,41	1,00	0,98	0,98	0,63	0,97	0,96

5.2 Fuzzy Inference

We evaluate every anti-virus program with one fuzzy number in each test. Test number 8 is rated the same, but the tests 2,3,4,6,7,9 are rated with two values and tests 1 and 5 with three. Thus, we use the appropriate logic operation for evaluation of the test. Operation of conjunction seems to be appropriate for this purpose.

As fuzzy conjunctions we call binary operations $\otimes$ in real interval <0,1>, which meet the following axioms for all a, b, c $\in$ <0.1>:

$a \otimes b = b \otimes a$	commutativity
$(a \otimes b) \otimes c = a \otimes (b \otimes c)$	associativity
$a \leq b$ implicates $a \otimes c \leq b \otimes c$	monotony
$a \otimes 1 = a$	neutral element

The most suitable for our fuzzy inference from all known fuzzy conjunctions, seems to be following fuzzy conjunction:

$a \otimes b = \min(a, b)$ fuzzy conjunctions based on minimum

$a \otimes b = a \cdot b$ fuzzy conjunctions based on product

$a \otimes b = \max(a+b-1;0)$ Lukasiewicz conjunction

The resulting values (4 decimal places) for each fuzzy conjunction are presented in the following table:

Tab. 5.2 – Tests results when using fuzzy conjunctions based on minimum

	1	2	3	4	5	6	7	8	9
Avira	0,6400	0,5900	0,9722	0,7037	0,9175	0,6240	0,9911	0,8000	0,2917
Bitdefender	0,5400	0,3500	0,9167	0,8704	0,6250	0,5720	0,7778	0,9000	0,8333
ESET	0,2600	0,5900	0,9823	0,8611	0,4500	0,6160	0,9975	0,5800	0,9583
F-Secure	0,4800	0,3500	0,9444	0,6852	0,5750	0,5720	0,9956	0,6700	0,7083
G Data	0,3000	0,6100	0,8333	0,7778	0,5250	0,6400	0,7778	0,5500	0,8750
Kaspersky	0,6600	0,5500	0,9444	0,8426	0,4750	0,6010	0,9886	0,8600	0,9792
Panda	0,8367	0,5200	0,9444	0,7037	0,4000	0,4140	0,9778	0,6300	0,9583

Tab. 5.3 – Tests results when using fuzzy conjunctions based on product

	1	2	3	4	5	6	7	8	9
Avira	0,5794	0,5535	0,9491	0,6816	0,9129	0,5725	0,9911	0,8000	0,2864
Bitdefender	0,5217	0,3500	0,8904	0,8623	0,5833	0,5425	0,7616	0,9000	0,8281
ESET	0,2069	0,4866	0,9823	0,8458	0,4379	0,6160	0,9975	0,5800	0,9311
F-Secure	0,4661	0,3500	0,9341	0,6799	0,5489	0,5543	0,9956	0,6700	0,6996
G Data	0,2505	0,5157	0,8039	0,7693	0,4641	0,5674	0,7624	0,5500	0,8639
Kaspersky	0,5749	0,4990	0,9214	0,8275	0,4669	0,6010	0,9886	0,8600	0,9704
Panda	0,8208	0,4396	0,9208	0,6938	0,3972	0,4140	0,9628	0,6300	0,9336

Tab. 5.4 – Tests results when using Lukasiewicz fuzzy conjunctions

	1	2	3	4	5	6	7	8	9
Avira	0,5436	0,5281	0,9484	0,6723	0,9125	0,5415	0,9911	0,8000	0,2738
Bitdefender	0,5058	0,3500	0,8880	0,8611	0,5575	0,5205	0,7570	0,9000	0,8270
ESET	0,0513	0,4147	0,9823	0,8434	0,4230	0,6160	0,9975	0,5800	0,9299
F-Secure	0,4508	0,3500	0,9335	0,6775	0,5291	0,5411	0,9956	0,6700	0,6960
G Data	0,1347	0,4554	0,7980	0,7669	0,4086	0,5266	0,7580	0,5500	0,8624
Kaspersky	0,5280	0,4572	0,9201	0,8246	0,4580	0,6010	0,9886	0,8600	0,9702
Panda	0,8177	0,3654	0,9194	0,6896	0,3930	0,4140	0,9625	0,6300	0,9325

5.3 Aggregation of test scores

Results of particular individual tests in the tables 5.2 to 5.4 will now be aggregated with an appropriate function. There will be used fuzzy conjunctions based on minimum nad fuzzy conjunctions based on product (Lukasiewicz conjunction is omitted, all the results are at 0). For comparison, method based on arithmetic mean and median will be used.

Tab. 5.5 – Tests results when using different aggregation methods

Fuzzy inference	Minimum				Product				Lukasiewicz			
Aggregation by	Min	Product	Mean	Median	Min	Product	Mean	Median	Min	Product	Mean	Median
Avira	0,291	0,035	0,726	0,704	0,286	0,025	0,703	0,682	0,274	0,020	0,690	0,672
Bitdefender	0,350	0,040	0,709	0,778	0,350	0,025	0,693	0,762	0,350	0,029	0,685	0,757
Kaspersky	0,260	0,020	0,699	0,616	0,207	0,012	0,676	0,616	0,051	0,002	0,649	0,616
F-Secure	0,350	0,017	0,665	0,670	0,350	0,015	0,655	0,670	0,350	0,013	0,649	0,670
ESET	0,300	0,019	0,654	0,640	0,251	0,008	0,616	0,567	0,135	0,004	0,585	0,550
G Data	0,475	0,069	0,767	0,843	0,467	0,051	0,746	0,827	0,457	0,042	0,734	0,825
Panda	0,400	0,029	0,709	0,704	0,397	0,021	0,690	0,694	0,365	0,018	0,680	0,690

5.4 Defuzzification

Defuzzification transfers the results of fuzzy inference into the output variables. The resulting order arises simply by comparing the calculated values for the selected fuzzy inference and aggregation methods. As the following table shows:

Tab. 5.6 – Tests results

Fuzzy inference	Minimum				Product				Lukasiewicz			
Aggregation by	Min	Product	Mean	Median	Min	Product	Mean	Median	Min	Product	Mean	Median
Avira	6	3	2	3	5	3	2	4	5	3	2	4
Bitdefender	3	2	3	2	3	2	3	2	3	2	3	2
Kaspersky	7	5	5	7	7	6	5	6	7	7	6	6
F-Secure	3	7	6	5	3	5	6	5	3	5	5	5
ESET	5	6	7	6	6	7	7	7	6	6	7	7
G Data	1	1	1	1	1	1	1	1	1	1	1	1
Panda	2	4	4	3	2	4	4	3	2	4	4	3

6. Summary

The measured data were compared using fuzzy logic. Only the data of 7 programs that attended all nine tests were taken into account. These data were compared one to each other using fuzzy logic. We established the order in which the first five ranks are occupied by selfsame programs that were rated by the group of AV-Comparatives.An evaluation using fuzzy logic is:

- Complex.

  Directly indicates the order of particular programs and not just the winners.

- Personal.

  Each user can adjust or edit rankings him/herself by adding some preferences in the beginning. (as mentioned at the beginning of chapter 5.1).

- More stable.

  If we add one or more investigational programs, the procedure does not change anyway.

- Variable.

  If we want to add one or more endpoints, the procedure will not change. Adding the points is achieved just by using membership functions and preferences.

7. Conclusion

AV-Comparatives, a professional anti-virus programs group for 2011, chose top 5 programs, without giving the order: Avira, Bitefender, ESET, F-Secure, Kaspersky. Of these, they chose the best program – Kaspersky. When using fuzzy logic for comparison of the programs, the best anti-virus program is the same: Kaspersky.

When comparing the results with regard to characteristics and use of fuzzy logic, this comparison has its substance and meaning.

Bibliography

ANTI-VIRUS COMPARATIVE, 2011: *Summary Report, Awards, winners, comments* [online] URL: http://www.av-comparatives.org/comparativesreviews/summary-reports/137-summary-report-december-2011

Bojadziev, G., Bojadziev, M., 2007: *Fuzzy Logic for Business, Finance and Management*. World Scientific Publishing, Singapore, 253 s. ISBN 13-978-981-270-649-2

Dostál, P. 2005: *Pokročilé metody manažerského rozhodování*. Grada Publishing, Praha, 166 s., ISBN 80-247-1338-1

Fuller, R., 1995: *Neural Fuzzy Systems*, Åbo, 253 s., ISBN 951-650-624-0

IT SECURITY PRODUCTS FOR CORPORATE USERS, *2011*: *Review of IT Security Suites for Corporate Users,* [online] URL: http://www.av-comparatives.org/images/docs/avc_cor_201109_en.pdf

Jura, J., 2003: *Základy fuzzy logiky pro řízení a modelování*. Nakladatelství VUITUM, Brno, 132 s., ISBN 80-214-2261-0

Novák, V., 2000: *Základy fuzzy modelování.* Nakladatelství BEN-technická literatura, Praha, 161 s., ISBN 80-7300-009-1

Vysoký, P., 1996: *Fuzzy řízení.* Vyd. 1. Praha, Vydavatelství ČVUT, 131 s. ISBN 80-01-01429-8

Zadeh, L.A., 1965: *Fuzzy Sets*. Information & Control - Vol. 8, pp. 338-353

Zadeh, L.A.,Klier, G.J., 1996: *Fuzzy sets, fuzzy logic, and fuzzy systems: selected papers*. River Edge, N.J., World Scientific, ISBN 978-981-02-2421-9

Zimmermann, H.J.,1996: *Fuzzy set theory – and its applications*. Kluwer Academic Publishers. Boston. ISBN 0-7923-9075-X

JEL Classification: C60, D80