


# Journal of Financial and Actuarial Mathematics and Management

A joint edition of the Institute of Information Sciences and Institute of Social Sciences of Perun Academy
Publishing Company: PSP Publishing
ISSN: 2367-5810
Issue 7, Year VII (2019)
Founding Editor and Editor-in-Chief: Pavel Stoynov

Editorial Board: Hiroyuki Ono (Japan), Yasukazu Yoshizawa (Japan), Naoyuki Ishimura (Japan), Boris Melnikov (Russia), Elena Melnikova (Russia), Goran Karanovic (Croatia), James Osondu (Nigeria)

# Contents

P. Stoynov. Databases of anomalous traffic for estimation of
Intrusion detection based on network transactions…….....…….3
P. Stoynov. Evaluating Network Intrusion Detection Systems..…….…….....6
P. Stoynov, N. Kozlev. Classification of the IBNR Methods…….……10
M. Mali, M. Shams, A. Saeedi, M. Nejad. Explanation of the
Reduction of Consequences of the Behavioral Finance Biases on
the Banking System Recession…….……...16

# Databases of anomalous traffic for estimation of Intrusion detection based on network transactions

Pavel Todorov Stoynov
Perun R&D Academy, Sofia, Bulgaria

**Abstract.**

Intrusion Detection Systems (IDS) are IT security systems for detecting hostile activity in IT networks with different use (financial, trade, administration, scientific etc.). When these systems also prevent the hostile activity, they are called Intrusion Detection and Prevention Systems (IDPS). The models for intrusion detection can be divided into two groups:

1. Signature verification. In this case, the system detects previously registered intrusion signature.

2. Anomaly detection. In this case, The system looks for abnormal behavior.

Contemporary IDS usually include both signature verification and anomaly detection realized by rule-based expert system and statistical module correspondingly.

Anomaly detection IDS are mainly in research stage today.

This paper aims at presenting some popular databases of anomalous traffic for estimation of Intrusion Dtection Systems (IDS). KDD'99, MetroSec and ADFA-IDS are presented.

**Key words:** Intrusion Dtection Systems (IDS), statistical evaluation of IDS, KDD'99, MetroSec, and ADFA-IDS

## Introduction

Intrusion Detection Systems (IDS) are IT security systems for detecting hostile activity in IT networks with different use (financial, trade, administration, scientific etc.). When these systems also prevent the hostile activity, they are called Intrusion Detection and Prevention Systems (IDPS). They can be divided into two groups:

1. Host-based – for detecting hostile activity on host systems. They analyze information from operation systems and application files captured by software agents.

2. Network based – for detecting hostile activity on networks. They evaluate information from network communication, analyzing the stream of packets captured by sensors.

The models for intrusion detection can be divided into two groups (Gotseva, Trifonov and Stoynov, 2019):

1. Signature verification. In this case, the system detects previously registered intrusion signature.

2. Anomaly detection. In this case, The system looks for abnormal behavior.

Most IDS commercial tools follow the signature verification detection system. However, they have some drawbacks (false alarms, signature of the attack can't be easily discovered, IDS should be periodically updated with new signatures).

Contemporary IDS usually include both signature verification and anomaly detection modules.

For statistically evaluating Intrusion Dtection Systems IDS in network information security, researchers need a documented attack database which database generally represents the ground truth (Rindberg et al., 2008). The evaluation itself counts the number of true positives, true negatives, false positives, and false negatives.

This paper aims at presenting some popular databases of anomalous traffic for estimation of Intrusion Dtection Systems (IDS). The databases KDD'99, MetroSec and ADFA-IDS are presented.

## Database KDD'99

Up to now, the most used database is KDD'99 originating from DARPA project on the off-line analysis of intrusion detection systems, at the MIT' Lincoln laboratory MIT (2008). A small network was set-up for this purpose, the aim being to emulate a US Air Force base connected to the Internet. The background traffic was generated by injecting attacks in well defined points of the network, and collected with TCPDUMP. Traffic was grabbed and recorded for 7 weeks, and served for IDS calibration. Once calibration was performed, 2 weeks of traces containing attacks were used to evaluate the performance of IDS under study. This DARPA work in 1998 used a wide range of intrusion attempts, tried to simulate a realistic normal activity, and produced results that could be shared between all researchers interested in such topic. After some changes, mainly dealt with the use of more furtive attacks, the use of target machines running Windows NT, the definition of a security policy for

the attacked network, and tests with more recent attacks, this database is used nowadays under the name KDD'99.

McHugh (2001) published a strong criticism on the procedures used when creating the KDD'99 database, especially on the lack of verification of the network realism compared to an actual one. Mahoney et Chan (2003) reviewed into detail the database and showed that the traces were far from simulating realistic conditions, and therefore, that even a very simple IDS can exhibit very high performance results, performances that it could never reach in a real environment.

Despite all the disclaimers about this KDD'99 database for IDS evaluation, it is still massively used. This is mainly due to the lack of other choices and efforts for providing new attack databases.

**MetroSec project Data**

The limitations of the KDD'99 database motivated MetroSec project from the French ACI program on Security & Computer science, 2004-2007 (MetroSec, 2008) to produce controlled and documented traffic traces, with or without anomalies, for testing and validating intrusion detection methods Owezarski (2007).

The experimental platform for creating the MetroSec trace database uses the Renater network, the French network for education and research. Renater is an operational network which is used by a significantly large community in its professional activity. The laboratories involved in the generation of traces are ENS in Lyon, LIP6 in Paris, IUT of Mont-de-Marsan, ESSI in Nice, and LAAS in Toulouse. Traffic is captured at these different locations by workstations equipped with DAG cards Owezarski (2007).

Anomalies studied and generated in the framework of the MetroSec project consist of more or less significant increases of traffic in terms of volume. Two kinds of anomalies are considered: anomalies due to legitimate traffic (like flash crowds- FC) and anomalies due to illegitimate traffic, as flooding attacks, generated by several classical attacking tools.

The anomalies due to illegitimate traffic were DDoS attacks, launched by using flooding attacking tools (IPERF, HPING2, TRIN00 et TFN2K), with changes frequently the attack characteristics and parameters (duration, DoS flow intensity, size and rate of packets) in order to create different profiles for attacks to be detected afterwards Owezarski (2007).

**Database ADFA-IDS**

Another recent dataset is the Intrusion Dataset (IDS) of Australian Defence Force Academy (ADFA) - ADFA-IDS (Creech and Hu, 2017). It is provided by the University of Arizona Artificial Intelligence Lab and intended as representative of modern attack structure and methodology to replace the older datasets KDD and UNM (Creech and Hu, 2013; Tran et al., 2012).

The version of ADFA-IDS used is released on March 27th, 2017 (Haider et al., 2017) as an update to the original ADFA-IDS made publicly available in 2013 (Creech and Hu, 2013; Creech and Hu, 2014; Haider et al., 2015). ADFA IDS includes independent datasets for Linux and Windows environments.

ADFA-LD (Linux dataset) was generated on a Ubuntu Linux 11.04 host OS with Apache 2.2.17 running PHP 5.3.5. FTP, SSH, MySQL 14.14, and TikiWiki were started (Xie and Hu, 2013; Xie et al., 2014).

Table 1 below shows the payloads and vectors used to attack the Ubuntu OS and generate the dataset.

Table 1. The payloads and vectors used to attack the Ubuntu OS and generate the dataset

| PAYLOAD/EFFECT | VECTOR |
|---|---|
| password bruteforce | FTP by Hydra |
| password bruteforce | SSH by Hydra |
| add new superuser | Client side poisoned executable |
| Java based meterpreter | Tiki Wiki vulnerability exploit |
| Linux meterpreter payload | Client side poisoned executable |
| C100 Webshell | PHP remote file inclusion vulnerability |

ADFA-WD (Windows dataset) was genearted on a Windows XP Service Pack 2 host OS with the XP default firewall enabled for all attacks, and file sharing enabled, a network printer configured, wireless and Ethernet networking (Haider et al., 2016a; Haider et al., 2016b). Norton AV 2013 was used to scan certain

payloads. FTP server, web server and management tool, and streaming audio digital radio package were activated.

A target ratio of 1:10:1=normal:validation:attack data was used to guide collection and structuring activities.

The vectors used here are: TCP ports, web based vectors, browser attacks, and malware attachments

The effects are: Bind shell, reverse shell, exploitation payload, remote operation, staging, system manipulation, privilege escalation, data exfiltration, and back-door insertion.

**References**

Creech, G. and J. Hu (2013) Generation of a new IDS test dataset: Time to retire the KDD collection, 2013 IEEE Wireless Communications and Networking Conference, WCNC 2013, pp.4487-4492.

Creech, G. and J. Hu (2014) A semantic approach to host-based intrusion detection systems using contiguous and discontiguous system call patterns, IEEE Transactions on Computers, vol. 63, issue 4, April 2014, pp. 807-819.

Creech, G. and J. Hu (2017) ADFA IDS Dataset, University of Arizona Artificial Intelligence Lab, AZSecure-data, Director Hsinchun Chen.

Gotseva, D., R. Trifonov, P. Stoynov (2019) Neural Networks for Intrusion Detection – Proceedings of the International conference HiTtech-2019, 10-12 October, Sofia, Bulgaria.

Haider, W., J. Hu, and M. Xie (2015) Towards reliable data feature retrieval and decision engine in hostbased anomaly detection systems, Proc. Of the 2015 10th IEEE Conference on Industrial Electronics and Applications, ICIEA 2015, pp. 513-517.

Haider, W., J. Hu, X. Yu, and Y. Xie (2016a) Integer data zero-watermark assisted system calls abstraction and normalization for host based anomaly detection systems, Proc. Of the 2nd IEEE International Conference on Cyber Security and Cloud Computing, 2016, pp. 349-355.

Haider, W., G. Creech, Y. Xie, and J. Hu (2016b) Windows Based Data Sets for Evaluation of Robustness of Host Based Intrusion Detection Systems (IDS) to Zero-Day and Stealth Attacks. Future Internet 8.3 (2016): 29.

Haider, W., J. Hu, S. Slay, B. P. Turnbull and Y. Xie (2017) Generating Realistic Intrusion Detection System Dataset based on Fuzzy Qualitative Modeling," Journal of Network and Computer Applications (JNCA), 2017, DOI: 10.1016/j.jnca.2017.03.018.

Mahoney, M., P. Chan (2003) An analysis of the 1999 darpa/lincoln laboratory evaluation data for network anomaly detection. In Recent Advances in Intrusion Detection (RAID 20003), pages 220–237, September 2003.

McHugh, J. (2001) Testing intrusion detection systems: A critique of the 1998 and 1999 darpa intrusion detection system evaluations as performed by lincoln laboratory. ACM Transactions on Information and System Security, 3(4):262–294, 2001.

Metrosec (2008) http://www.laas.fr/METROSEC.

MIT (2008) Lincoln Laboratory. http://www.ll.mit.edu/mission/communications /ist/corpora/ideval, 2008.

Rindberg, H., M. Roughan and J. Rexford (2008) The need for simulation in evaluating anomaly detectors. Computer Communication Review, 38(1):55–59, January 2008.

Owezarski, P. (2007) Contribution of the French METROSEC project to traffic anomalies detection, Colloque STIC, Paris, France, 5-7 November 2007.

Tran, Q., F. Jiang, and J. Hu (2012) A real-time NetFlow-based intrusion detection system with improved BBNN and high-frequency field programmable gate arrays, Proc. Of the 11th IEEE International Conference on trust, Security and Privacy in Computing and Communications, TurstCom 2012, 2012, pp. 201-208.

Trifonov, R., G. Tsochev, R. Yoshinov, S. Manolov, G. Pavlova (2017) Conceptual model for cyber intelligence network security system. International Journal of Computers. Vol. 11, 2017.

Xie, M. and J. Hu (2013) Evaluating host-based anomaly detection systems: A preliminary analysis of ADFA-LD, Proc. Of the 6th International Congress on Image and Signal Processing, CISP 2013, pp. 1711-1716.

Xie, M., J. Hu, X. Yu, and E. Chang (2014) Evaluating host-based anomaly detection systems: Applications of the frequency-based algorithms to ADFA-LD," LNCS, vol. 8792, 2014, pp.542-549.

# Evaluating
# Network Intrusion Detection Systems

Pavel Todorov Stoynov
Perun R&D Academy, Sofia, Bulgaria

**Abstract.**
This paper considers some approaches for detection of intrusions in on-line transaction systems and some ways for evaluation of the efficiency of the Intrusion Detection Systems (IDS) based on different attack datasets. By confronting IDS to the attack traces in the datasets, it is possible to get a statistical evaluation of IDS, and to rank them according to their detection capabilities.

**Key words:** Intrusion Detection Systems (IDS), Intrusion Detection methods, Statistical evaluation of IDS, attack traces, attack tools

## Introduction

Intrusion Detection Systems (IDS) are IT security systems for detecting hostile activity in IT networks with different use (financial, trade, administration, scientific etc.). When these systems also prevent the hostile activity, they are called Intrusion Detection and Prevention Systems (IDPS). They can be divided into two groups:

1. Host-based – for detecting hostile activity on host systems. They analyze information from operation systems and application files captured by software agents.

2. Network based – for detecting hostile activity on networks. They evaluate information from network communication, analyzing the stream of packets captured by sensors.

The models for intrusion detection can be divided into two groups (Gotseva, Trifonov and Stoynov, 2019):

1. Signature verification. In this case, the system detects previously registered intrusion signature.

2. Anomaly detection. In this case, The system looks for abnormal behavior.

Most IDS commercial tools follow the signature verification detection system. However, they have some drawbacks (false alarms, signature of the attack can't be easily discovered, IDS should be periodically updated with new signatures).

Contemporary IDS usually include both signature verification and anomaly detection modules.

For statistically evaluating Intrusion Dtection Systems IDS in network information security, researchers need a documented attack database which database generally represents the ground truth (Rindberg et al., 2008).

This paper aims at presenting some methods for evaluating anomaly-based Intrusion Detection Systems

## Evaluating IDS and Anomaly Detection Algorithms

The statistical IDS evaluation itself counts the number of true positives, true negatives, false positives, and false negatives. The relations between these values can then be exhibited by mean of a ROC curve (Receiver Operating Characteristic). The ROC technique has been used in 1998 for the first time for evaluating IDS in the framework of the DARPA project on the off-line analysis of intrusion detection systems, at the MIT' Lincoln laboratory MIT (2008). Several papers describe this experience as Durst et al. (1999), Lippmann et al. (2000) and Lee et al. (1999).

ROC technique consists in combining detection results with the number of testing sessions to issue two values which summarize IDS performance: the detection ratio (number of detected intrusions divided by the number of intrusion attempts) and the false alarm rate (number of false alarms divided by the total number of network sessions). These summaries of detection results then represent one point on the ROC curve for a given IDS. The ROC space is defined by the false alarms and true positive rates on $X$ and $Y$ axis respectively, what in fact represents the balance between efficiency and cost. The best possible IDS would then theoretically be represented by a single point curve of coordinates $(0,1)$ in the ROC space. Such a point means that all attacks were detected and no false alarm raised. A random detection process would be represented in the ROC space by a strait line going from the bottom left corner $(0,0)$ to the upper right corner $(1,1)$ (the line with equation $y = x$). Points over this line mean that the detection performance is better than the one of a random process. Under the line, it is worse, and then of no real meaning (Owezarski, 2007).

NADA (Network Anomaly Detection Algorithm) is an anomaly detection tool relying on the use of deltoids for detecting significantly anomalous variations on traffic characteristics. This tool also includes a classification mechanism of anomalies aiming at determining whether detected anomalies are legitimate and their

characteristics (Farraposo et al., 2007). NADA has been issued in the framework of the Metrosec project (Metrosec, 2008). NADA uses a threshold $k$ which aims at determining whether a deltoid corresponds to an anomalous variation. Setting the $k$ threshold allows the configuration of the detection tool sensitivity, in particular related to the natural variability of normal traffic.

The Gamma-FARIMA approach (Scherrer et al., 2007) is also one of the achievements of the MetroSec projects.

Packet Header Anomaly Detection (PHAD) tool, funded by the American NSF, is said to be the ultimate intrusion and anomaly detection tool (Mahoney et al., 2001). The argumentation of its authors mainly relies on tests lead with KDD'99 traces: on these traces, PHAD gives perfect results.

## Attacking tools

There are different attacking tools used to perform attacks which are registered in anomalies databases and used for evaluation of IDS.

The IPERF tool under Linux (IPERF, 1999) aims at generating UDP flows at variable rates, with variable packets rates and payloads.

The HPING2 tool (HPING2, 2019) aims at generating UDP, ICMP and TCP flows, with variable rates (same throughput control parameters as IPERF). With this tool, it is also possible to set TCP flags, and then to generate specific signatures in TCP flows.

TRINOO (Trinoo, 2019) and TFN2K (TFN2K, 2019) are two well known distributed attacking tools. They allow the installation on different machines of a program called zombie, daemon, or bot. This program is in charge of generating the attack towards the target. It is remotely controlled by a master program which commands all the bots. It is possible to constitute an attacking army (or botnet) commanded by one or several masters.

TFN2Kbots can launch several kinds of attacks. In addition of classical flooding attacks using UDP, ICMP and TCP protocols (sending of a large number of UDP, ICMP or TCP packet to the victim), many other attacks are possible. The mixed flooding attack is a mix of UDP flooding, ICMP flooding and TCP SYN flooding. Smurf is an attacking technique based on the concept of amplification: bots use the broadcast address for artificially multiplying the number of attacking packets sent to the target, and then multiplying the power of this attack. TRIN00 bots, on their side, can only perform UDP flooding (Owezarski, 2007).

## Comparative evaluation of IDS with different anomalies databases

The statistical evaluation of an IDS based on some Intrusion Dataset is usually performed using the traces with documented anomalies registered in the dataset. Each of the attack traces contain several attacks. In addition, the documented traces can be grouped according to the attacking tools used for generating the attacks/anomalies, and in each group differentiate them according to attack intensities, durations, etc.

The intensity and duration of anomalies are two characteristics which have a significant impact on the capability of anomaly based IDS to detect them. Whereas the detection of strong intensity anomalies is well done by most of detection tools, it is in general not the case when small intensity attacks are considered. Therefore, a suited method for evaluating anomaly detection tools performance must be able to count how many times it succeeds or failed in detecting anomalies contained in the traces, and among which some are of low intensity.

Usualy ROC curve is presented and curve analysis is performed.

**An Example.** NADA evaluation on KDD'99 database (Owezarski, 2007) uses the 10% KDD database, i.e. only one of the KDD'99 datasets.

During the International Knowledge Discovery and Data Mining Tools contest (UCI KDD Archive, 1999), 10% of the KDD database were used for the learning phase (Hettich and Bay, 1999). This part of the database contains 22 types of attacks and is a concise version of the full KDD database. This later contains a greater number of attack examples than normal connections, and the types of attacks do not appear in a similar way. Because of their nature, DoS attacks represent the huge majority of the database. On the other hand, the corrected KDD database provides a database with different statistical distributions compared to the databases "10% KDD" or "Full KDD". In addition, it contains 14 new types of attacks.

NADA performance ROC curve obtained with the 10% KDD database shows that NADA got very good results. Applied to the KDD'99 database, NADA exhibits a detection probability close to 90%, and a probability of false alarms around 2%.

**Dataset ADFA-IDS**

A possible dataset for statistical evaluation of IDS is the Intrusion Dataset (IDS) of Australian Defence Force Academy (ADFA) - ADFA-IDS (Creech and Hu, 2017). It is provided by the University of Arizona Artificial Intelligence Lab and intended as representative of modern attack structure and methodology to replace the older datasets KDD and UNM (Creech and Hu, 2013; Tran et al., 2012).

The version of ADFA-IDS used is released on March 27th, 2017 (Haider et al., 2017) as an update to the original ADFA-IDS made publicly available in 2013 (Creech and Hu, 2013; Creech and Hu, 2014; Haider et al., 2015). ADFA IDS includes independent datasets for Linux and Windows environments.

ADFA-LD (Linux dataset) was generated on a Ubuntu Linux 11.04 host OS with Apache 2.2.17 running PHP 5.3.5. FTP, SSH, MySQL 14.14, and TikiWiki were started (Xie and Hu, 2013; Xie et al., 2014).

Table 1 below shows the payloads and vectors used to attack the Ubuntu OS and generate the dataset.

Table 1. The payloads and vectors used to attack the Ubuntu OS and generate the dataset

| PAYLOAD/EFFECT | VECTOR |
|---|---|
| password bruteforce | FTP by Hydra |
| password bruteforce | SSH by Hydra |
| add new superuser | Client side poisoned executable |
| Java based meterpreter | Tiki Wiki vulnerability exploit |
| Linux meterpreter payload | Client side poisoned executable |
| C100 Webshell | PHP remote file inclusion vulnerability |

ADFA-WD (Windows dataset) was genearted on a Windows XP Service Pack 2 host OS with the XP default firewall enabled for all attacks, and file sharing enabled, a network printer configured, wireless and Ethernet networking (Haider et al., 2016a; Haider et al., 2016b). Norton AV 2013 was used to scan certain payloads. FTP server, web server and management tool, and streaming audio digital radio package were activated.

A target ratio of 1:10:1=normal:validation:attack data was used to guide collection and structuring activities.

The vectors used here are: TCP ports, web based vectors, browser attacks, and malware attachments

The effects are: Bind shell, reverse shell, exploitation payload, remote operation, staging, system manipulation, privilege escalation, data exfiltration, and back-door insertion.

**Conclusion**

The statistical evaluation of IDS and Anomaly Detection Algorithm is based on the number of true positives, true negatives, false positives, and false negatives. It is presented by ROC curves based on specified Intrusion Datasets where specific attacking tools generate intrusion attacks.

**References**

Creech, G. and J. Hu (2013) Generation of a new IDS test dataset: Time to retire the KDD collection, 2013 IEEE Wireless Communications and Networking Conference, WCNC 2013, pp.4487-4492.

Creech, G. and J. Hu (2014) A semantic approach to host-based intrusion detection systems using contiguous and discontiguous system call patterns, IEEE Transactions on Computers, vol. 63, issue 4, April 2014, pp. 807-819.

Creech, G. and J. Hu (2017) ADFA IDS Dataset, University of Arizona Artificial Intelligence Lab, AZSecure-data, Director Hsinchun Chen.

Available: http://www.azsecure-data.org/ [November 2016]

Durst, R., T. Champion, B. Witten, E. Miller anf L. Spagnuolo (1999) Testing and evaluating computer intrusion detection system. Communications of the ACM, 42(7), 1999.

Gotseva, D., R. Trifonov, P. Stoynov (2019) Neural Networks for Intrusion Detection – Proceedings of the International conference HiTtech-2019, 10-12 October, Sofia, Bulgaria.

Farraposo, S., P. Owezarski, E. Monteiro (2007) Nada - network anomaly detection algorithm. In Proceedings of the 18th IFIP/IEEE Distributed Systems: Operations and Management (DSOM'2007), October 2007.

Haider, W., J. Hu, and M. Xie (2015) Towards reliable data feature retrieval and decision engine in hostbased anomaly detection systems, Proc. Of the 2015 10th IEEE Conference on Industrial Electronics and Applications, ICIEA 2015, pp. 513-517.

Haider, W., J. Hu, X. Yu, and Y. Xie (2016a) Integer data zero-watermark assisted system calls abstraction and normalization for host based anomaly detection systems, Proc. Of the 2nd IEEE International Conference on Cyber Security and Cloud Computing, 2016, pp. 349-355.

Haider, W., G. Creech, Y. Xie, and J. Hu (2016b) Windows Based Data Sets for Evaluation of Robustness of Host Based Intrusion Detection Systems (IDS) to Zero-Day and Stealth Attacks. Future Internet 8.3 (2016): 29.

Haider, W., J. Hu, S. Slay, B. P. Turnbull and Y. Xie (2017) Generating Realistic Intrusion Detection System Dataset based on Fuzzy Qualitative Modeling," Journal of Network and Computer Applications (JNCA), 2017, DOI: 10.1016/j.jnca.2017.03.018.

Hettich, S. and S. Bay (1999) The uci kdd archive, Irvine - University of California, Department of Information and Computer science. http://kdd.ics.uci.edu, 1999.

HPING2 (2019) http://sourceforge.net/projects/hping2.

IPERF (1999) The TCP/UDP bandwith Measurement Tool. http://dast.nlanr .net/Projects/Iperf/.

Lee, W., K. Stolfo, K. Mok (1999) Mining in a data-flow environment: Experience in network intrusion detection. In Proceedings of the ACM International Conference on Knowledge Discovery & Data Mining (KDD'99), pages 114–124, 1999.

Lippman, R., D. Fried, I. Graf, J. Haines, K. Kendal, D. McClung, D. Weber, S. Webster, D. Wyschogrod, R. Cunningham, Y. Zissman (2000) Evaluating intrusion detection systems: The 1998 darpa off-line intrusion detection evaluation. In DARPA Information Survivability Conference and Exposition, pages 12–26, 2000.

Mahoney, M., P. Chan (2001) Phad: Packet header anomaly detection for identifying hostile network traffic. In Technical Report CS-2001-04. Department of Computer Sciences - Florida Institute of Technology, 2001.

Mahoney, M., P. Chan (2003) An analysis of the 1999 darpa/lincoln laboratory evaluation data for network anomaly detection. In Recent Advances in Intrusion Detection (RAID 20003), pages 220–237, September 2003.

McHugh, J. (2001) Testing intrusion detection systems: A critique of the 1998 and 1999 darpa intrusion detection system evaluations as performed by lincoln laboratory. ACM Transactions on Information and System Security, 3(4):262–294, 2001.

Metrosec (2008) http://www.laas.fr/METROSEC.

MIT (2008) Lincoln Laboratory. http://www.ll.mit.edu/mission/communications /ist/corpora/ideval, 2008.

Rindberg, H., M. Roughan and J. Rexford (2008) The need for simulation in evaluating anomaly detectors. Computer Communication Review, 38(1):55–59, January 2008.

Owezarski, P. (2007) Contribution of the French METROSEC project to traffic anomalies detection, Colloque STIC, Paris, France, 5-7 November 2007.

Scherrer, A., N. Larrieu, P. Owezarski, P. Borgnat, P. Abri (2007) Non-gaussian and long memory statistical characterisations for internet traffic with anomalies. IEEE Transaction on Dependable and Secure Computing, 4(1), January 2007.

TFN2K (2019) An analysis.
http://packetstormsecurity.org/distributed/TFN2k Analysis-1.3.txt.

Tran, Q., F. Jiang, and J. Hu (2012) A real-time NetFlow-based intrusion detection system with improved BBNN and high-frequency field programmable gate arrays, Proc. Of the 11th IEEE International Conference on trust, Security and Privacy in Computing and Communications, TurstCom 2012, 2012, pp. 201-208.

Trifonov, R., G. Tsochev, R. Yoshinov, S. Manolov, G. Pavlova (2017) Conceptual model for cyber intelligence network security system. International Journal of Computers. Vol. 11, 2017.

Trinoo (2019) The DoS Project's "trinoo" distributed denial of service attack tool http://staff.washington.edu/dittrich/misc/trinoo.analysis.

UCI KDD Archive (1999) KDD'99 datasets. http://kdd.ics.uci.edu/databases/ kddcup99/kddcup99.html.

Xie, M. and J. Hu (2013) Evaluating host-based anomaly detection systems: A preliminary analysis of ADFA-LD, Proc. Of the 6th International Congress on Image and Signal Processing, CISP 2013, pp. 1711-1716.

Xie, M., J. Hu, X. Yu, and E. Chang (2014) Evaluating host-based anomaly detection systems: Applications of the frequency-based algorithms to ADFA-LD," LNCS, vol. 8792, 2014, pp.542-549.

# Classification of the IBNR Methods

Pavel Todorov Stoynov.
Perun R&D Academy, Sofia, Bulgaria
Nikolay Kozlev,
Sofia University, Sofia, Bulgaria

**Abstract.**
The article considers a classification of the IBNR models in actuarial mathematics. .
**Key words:** insurance, actuarial mathematics, IBNR models.

## Introduction

The IBNR models in insurance are a realistic way for determining the actuarial reserves taking into account the time. After the acceptance of the Solvency II directive in EU, they are widely used by the insurers acting at the territory of the union.

Apart from the abbreviation IBNR (Incurred but not Reported), other abbreviations are also used – RBNS (Reported but Not Settled), IBNFR (Incurred but not Fully Reported), IBNER (Incurred but Not Enough Reported), RBNFS (Reported but not Fully Settled). All they express the idea that there are time intervals between the occurrence of claims and their complete payment.

The basic IBNR model can be presented by a square table of random variables $X_{ij}, i=1,2,\ldots,t,\ j=1,2,\ldots t,$ where $X_{ij}$ are the paid claims occurred in year $i$ and paid after $j-1$ years, i. e. during the calendar year $i+j-1,$ and $i=1,2,\ldots,t$ is the year of occurrence of the actuarial event (year of origin, accident year), and $j=1,2,\ldots t$ is the year of payment of the claims (development year). In this way, $t^2$ independent random variables are obtained, indexed by two indecesq among which $\frac{t(t+1)}{2}$ variables are observations of historical values till the calendar year. The observed values have indeces $(i,j): i+j-1\le t.$ The explaining variables here are the row nimber $i$ and the column number $j.$ The observed variable in each cell can be really paid claims, loss ratios, average values on all $w_{ij}$ observations in the cell which play the role of natural weights or other variables.

Main point in this class of models is the so-called run-off triangle. It can be considered as a matrix $k\times k,$ in which the meaningful numbers are on and above the diagonal defined by the equation $k=i+j-1.$ The numbers in the run-off triangle can be cumulative or incremental losses of the insurer for the corresponding period of occurrence and development.

IBNR models can be divided into two large groups - standard (classical) models and contemporary (stochastic) models.

The standard IBNR models can be divided into models using historical data and models using historical data and apriori estimates.

IBNR models can be also divided to models which uses historical data only for claims and models which use historical data for the calims and for the premiums collected.

From the combination of these two classifications we obtain four groups standard IBNR models which will be considered below.

Among the models with historical data only about claims is the classical Chain Ladder модел.

The classical Chain Ladder model uses the so-called chain-ladder factors defined by the mean chain ratios

$$f_k^{CL}=\frac{\sum_{i=1}^{n-k}S_{i(k+1)}}{\sum_{i=1}^{n-k}S_{ik}},\quad k=1,2,\ldots,n-1,$$

$$S_{ik}=\sum_{j=1}^{k}X_{ij},\ i=1,2,\ldots,n;\quad k=1,2,\ldots,(n-i+1).$$

From hereq the final Loss Development Factors – LDF are defined.

$$F_k^{CL} = \prod_{j=k}^{n-1} f_j^{CL},. k = 1,2,\ldots,(n-1); \quad F_n^{CL} = 1.$$

They represent mean ratio of the Ultimate Aggregate Paid Claims – UAPC – to the aggregated registered claims for every period after $k$ years of development.

From the factors of development of the losses chain-ladder lag-factors can be determined:

$$p_i^{CL} = \frac{1}{F_{n-i+1}^{CL}}, i = 1,2,\ldots,n.$$

They represent the mean share of the UAPC from period of occurrence $i,$ revealed til the day of the analysis in development period $n-i+1.$

The chain-ladder IBNR factors are also obtained

$$q_i^{CL} = 1 - p_i^{CL}, i = 1,2,\ldots,n.$$

They are the mean share of UAPC from occurrence period $i,$ remained unknown till the day of the analysis in development period $n-i+1.$

Then we have

$$U_i^{CL} = \frac{S_{i(n-i+1)}}{p_i^{CL}}$$

for the final aggregate claims paid $U_i^{CL}, i = 1,2,\ldots,n.$ For the incurred but not reported claims IBNR the following equation holds:

$$IBNR_i^{CL} = q_i^{CL} U_i^{CL}, i = 1,2,\ldots,n.$$

The classical Chain Ladder model can be divided in the contxt of the multiplicative generalized regression model

$$X_{ij} \approx \alpha_i \beta_j \gamma_k.$$

Her $X_{ij}$ are independent exponentially distributed random variables. The year of the occurrence of the claim $i,$ the year of payment $j$ and the calendar year $k = i + j - 1$ are the explanatory independent variables and $X_{ij}$ are the explained dependent variables. Then $EX_{ij}$ is an exponent of the linear $\log\alpha_i + \log\beta_j + \log\gamma_k,$ i. e. the generalized regression model has a logarithmic function of the regression function. The variables $\alpha_i, \beta_j, \gamma_k$ are dummy, indicating the row, the column and the diagonal. For them an estimate can be found by the method of maximal likelihood at different assumptions about the distribution of $X_{ij}.$ Then the estimated values are

$$\hat{X}_{ij} = \hat{\alpha}_i \hat{\beta}_j \hat{\gamma}_k.$$

One common assumption about $\gamma_k,$ when $k > t,$ is that $\gamma_k = \gamma^k$ for some real number $\gamma.$

If we suppose that $X_{ij} \in Po(\alpha_i \beta_j), \gamma_k \equiv 1$ and we look for such estimates $\hat{\alpha}_i, \hat{\beta}_j, i, j = 1,\ldots,t,$ for which the summing by $i$ and $j$ of the products $\hat{\alpha}_i \hat{\beta}_j, i + j - 1 \le t,$ is equal to the corresponding sums of the observed variables, i. e.

$$\sum_i \hat{\alpha}_i \hat{\beta}_j = \sum_i X_{ij} = C_j,$$

$$\sum_j \hat{\alpha}_i \hat{\beta}_j = \sum_j X_{ij} = R_i,$$

which means the method of Marginal Totals is used, the future losses of the insurer for $(i, j) : i + j - 1 > t$ can be estimated by $\hat{\alpha}_i \hat{\beta}_j, i + j - 1 > t.$ Since the estimates by the method of Marginal Totals in case of $w_{ij} = 1$ are given by the equations

$$\alpha_i = \frac{\sum_j X_{ij}}{\sum_j \beta_j}$$

$$\beta_j = \frac{\sum_i X_{ij}}{\sum_i \alpha_i},$$

the Chain Ladder method leads to solving this system of dependencies for $(i, j) : i + j - 1 \le t.$ One of the approaches to solvethe systemis the method of Verbeek (1972).

Wuth the Verbeek method (1972), as one of the parameters is not needed, an assumption is made that $\sum_{j=1}^{t} \beta_j = 1.$ Also

$$\sum_i X_{ij} = C_j, \, i + j \le t$$

$$\sum_j X_{ij} = R_i, \, i + j \le t.$$

From summing of the first row we obtain

$$\hat{\alpha}_1(\hat{\beta}_1 + \hat{\beta}_2 + \cdots + \hat{\beta}_t) = R_1,$$

from where

$$\hat{\alpha}_1 = R_1.$$

After, from

$$\hat{\alpha}_1 \hat{\beta}_t = C_t,$$

is obtained

$$\hat{\beta}_t = \frac{C_t}{R_1}.$$

If we assume that for some $n < t$ the estimates $\hat{\beta}_{t-n+2}, \ldots, \hat{\beta}_t$ and $\hat{\alpha}_1, \ldots, \hat{\alpha}_{n-1}$ are found, the next estimates can be maid by using the equations

$$\hat{\alpha}_n(\hat{\beta}_1 + \hat{\beta}_2 + \cdots + \hat{\beta}_{t-n+1}) = R_n,$$

$$\hat{\alpha}_1(\hat{\alpha}_1 + \cdots + \hat{\alpha}_n)\hat{\beta}_{t-n+1} = C_{t-n+1}.$$

As $(\hat{\beta}_1 + \hat{\beta}_2 + \cdots + \hat{\beta}_t) = 1,$ the first equation gives an estimate for $\hat{\alpha}_n$, and from the second equation we may determine $\hat{\beta}_{t-n+1}.$ This procedure is repeating for $n = 2, \ldots, t.$

As examples of modification of Chain Ladder Double Chain Ladder ( DCL) and Munich Chain Ladder (MCL) can be shown.

Double Chain Ladder – DCL – uses two run-off triangles – triangle of payments and triangle of the number of claims. The classical Chain Ladder method is used for both run-off triangles.

When calculating reserves in the context of IBNR models separate run-off triangles are used for the paid losses and for the incurred losses, i. e. Paid losses and assigned reserves. The method Munich Chain Ladder (MCL) combines paid and incurred losses considering and projecting their ratio.

Among the models with curren data based only on claims and using apriori data, the model Bornhuetter-Ferguson (1972) and the model Cape Code can be cited.

At Cape Code model, the mean ratio of the losses (ratio of total losses to mean premiums) is used. More specifically, the ratio

$$L = \frac{\sum_{i=1}^{n} S_{i(n-i+1)}}{\sum_{i=1}^{n} p_i^{CL} P_i}$$

is defiend where $P_i$ are the premiums collected during the occurrence period $i.$ Then we have

$$IBNR_i^{CC} = q_i^{CL} LP_i,\ i = 1,2,\ldots,n.$$

The total claims are correspondingly

$$U_i^{CC} = S_{i(n-i+1)} + IBNR_i^{CC} = p_i^{CL} U_i^{CL} + (1 - p_i^{CL})LP,\ i = 1,2,\ldots,n.$$

At Bornhuetter-Ferguson model, instead of mean ratio of losses, an estimate of the loss ratio $L_i,\ i == 1,2,\ldots,n$ is used for every occurrence period $i.$ Then

$$IBNR_i^{BF} = q_i^{CL} L_i P_i,\ i = 1,2,\ldots,n.$$

For the aggregate claims we have

$$U_i^{BF} = S_{i(n-i+1)} + IBNR_i^{BF} = p_i^{CL} U_i^{CL} + (1 - p_i^{CL})L_i P,\ i = 1,2,\ldots,n.$$

One of the weeknesses of Chain Ladder is that the prognoses about the reserves can be unstable. A change by $p\%$ of the sum of the number of the claims in a given row leads to a change with the same percentage in all predicted values of the numbers of the claims in this row. The method of Bornhuetter-Ferguson (1972) is a trial to stabilize the claims prognoses.

At this method, it is supposed that there are preliminary estimates for the total amount of the claims which will appear for a given initial period $i.$ More precisely, it is supposed that

$$E(X_{i1} + X_{i2} + \cdots + X_{it}) = M_i$$

where $M_i$ are known and are also called schedule or budget ultimate losses. So, the estimates $\frac{M_i}{P_i}$ are given

where $P_i$ is the premium income for year $i.$

If we consider the case when the number of the insurance policies $n_i$ for every occurrence year is known, and $X_{ij}$ is the total number of claims and the loss ratio $\frac{M_i}{P_i} = const$ is constant, which means that

$$\frac{M_i}{P_i} = \frac{M_1}{P_1},$$

$$\frac{M_i}{n_i \overline{p}} = \frac{M_1}{n_1 \overline{p}},$$

wher $\overline{p}$ is the mean premium per policy, then

$$M_i = \frac{n_i}{n_1} M_1.$$

From other side,

$$E(X_{i1} + X_{i2} + \cdots + X_{it}) = M_i = \sum_j \hat{\alpha}_i \hat{\beta}_j \approx \hat{\alpha}_i$$

And it follows that $M_1 = \hat{\alpha}_1,$ from where

$$M_i = \frac{n_i}{n_1} \hat{\alpha}_1.$$

The last equation gives a preliminary estimate of the mean value of the total loss, corresponding to occurrence year $i.$

With the method Chain Ladder, the vectors $\hat{\alpha}$ are $\hat{\beta}$ constructed supposing that the sum of the coordinates of the vector $\beta$ is equal to, thus minimizing the devience between the future data and the historic data, i. e. The upper left triangle, of matrix $\hat{\alpha}\hat{\beta}'.$ After that the part of the future, i. e. the lower right triangle of the matrix $\hat{\alpha}\hat{\beta}'$ is used for determining of the reserves. The sum by rows of the future part of the matrix $\vec{M}\hat{\beta}'$ is determined by the methods of Bornhuetter-Ferguson.

Bornhuetter-Ferguson method combines internal development year factors $\beta_i$ with external a priori estimates of the loss ratio by occurrence years. At Chain Ladder method, the (development year factors, as well

as the accident year factors are estimated internally. It can be shown (Verrrall, 2004) that both methods are two border cases of the Bayesian estimates at generalized linear regression models with loose prior distribution at the method Chain ladder and tight prior distribution at the method of Bornhuetter-Ferguson.

By applying the method Chain Ladder, different actuaries would achieve similar results. By applying the method Bornhuetter-Ferguson different results are possible about the prior estimate of the total sum of claims $S.$ This sum can be manipulated – idf the aim is to receive estimate of the reserves $R,$ then it is possible to give an estimate of the total sum of claims $S = \frac{R}{q}.$

The method Cape Code (CC) can be considered as a modification of the method Bornhuetter-Ferguson. With this method, we assume that the premiums or other measures of the volume of the business are known for historical accident years and the final loss ratios are identical for all claims occurenc years. This method is sometimes called also Standart-Buhlman method.

The models Optimal Bornhuetter-Ferguson and Optimal Cape Code are modifications of Bornhuetter-Ferguson and Cape Code.

Among the models with current data based on claims and premiums without using prior data the method Individual Loss Ratiocan be considered.

Among the models with current data based on claims and premiums and using prior data the models Collective Loss Ratio and Credibility Models of total Loss Ratio – Benktander Credibility Loss Ratio, Neuhaus Credibility Loss Ratio, Optimal Credibility Loss Ratio can be mentioned.

The model of Gunar Benktander (1976) can be considered as a mixed model based on the models Chain Ladder and Bornhuetter-Ferguson. At this model, the reserves are estimated by the formula

$$\begin{aligned} R_k^{GB} &= p_k R_k^{CL} + (1-p_k) R_k^{BF} = \\ &= \frac{p_k q_k S_k}{p_k} + q_k R_k^{BF} = \\ &= q_k (S_k + R_k^{BF}) = q_k U_k^{BF}, \end{aligned}$$

where $p_k = p_{ik}$ are the parts of the total claim which occurred during period $i$, and were paid during period $k,$ $q_k = 1 - p_k,$ $S_k = S_{ik} = \sum_{j=1}^{k} X_{ij}$ are the total claims paid till period $k,$ $X_{ij}$ are the incremental claims for period of occurrence $i$ and development period $j,$ $R_k^{BF}$ are the reserves determined by the method of Bornhuetter-Ferguson for the period $k,$ $U_k^{BF} = S_k + R_k^{BF}$ are the posterior estimates of the total claims by the method of Bornhuetter-Ferguson. While at the method of Bornhuetter-Ferguson the reserves are determined from the equation $R_k^{BF} = q_k U,$ where $U$ are the prior estimates for the total claim and at the method Chain Ladder the reserves are determined from $R_k^{CL} = U_k^{CL} - S_k = \frac{S_k}{p_k} - S_k = q_k U_k^{CL},$ where $U$ are the prior estimate for the total sum of claims, at the model of Gunar Benktander the process of Bornhuetter-Ferguson continues iteratively and with the development of the claims, i. e. with increase of the index of the development year $j,$ the weight $p_k$ of the estimate of the total claims maid by the method Chain Ladder also inceases. The following relations hold:

$$\begin{gathered} R_k^{BF} = q_k U = q_k U_0, \\ U_1 = U_k^{BF} = U_k^{GB1} = S_k + q_k U_0 = (1-q_k) U_k^{CL} + q_k U_0, \\ R_1 = R_k^{GB1} = q_k U_1 = q_k U_k^{BF} = (1-q_k) R_k^{CL} + q_k R_k^{BF}, \\ U_2 = U_k^{GB2} = (1-q_k^2) U_k^{CL} + q_k^2 U_0, \\ \cdots \\ U_n = U_k^{BFn} = (1-q_k^n) U_k^{CL} + q_k^n U_0, \\ R_n = R_k^{GBn} = (1-q_k^n) R_k^{CL} + q_k^n R_k^{BF}, \\ U_{n+1} = U_k^{BF(n+1)} = (1-q_k^{n+1}) U_k^{CL} + q_k^{n+1} U_0, \\ \cdots \end{gathered}$$

$$U_{\infty} = U_k^{CL},$$
$$R_{\infty} = R_k^{CL}.$$

Thus the reserves determined by the method Gunar Benktander are obtained through mixed model (credibility mixture) of the reserves, determined by Chain Ladder and the reserves determined by Bornhuetter-Ferguson. The optimal mix of the two models is defined by the conditions

$$R_k^c = cR_k^{CL} + (1-c)R_k^{BF},$$
$$c \in [0,1],$$
$$\min E(R_k^c - ER_k^c)^2 \to c^*.$$

Thus, about the reserves corresponding to the optimal model $R_k^c$ it can be shown that they are always better than $R_k^{CL}$ and $R_k^{BF}$, ant the estimate of reserves $R_k^{GB1}$ is better than $R_k^{CL}$ и $R_k^{BF}$ in the most of the cases.