Annals of Telecommunications
https://doi.org/10.1007/s12243-018-0672-1

A cooperative approach with improved performance for a global intrusion detection systems for internet service providers

Renato S. Silva[1] · **Luís F. M. de Moraes**[1]

Received: 4 May 2018 / Accepted: 16 October 2018

Abstract

Typical perimeter-based intrusion detection systems do not provide the user with the necessary preventive protection measures. In addition, many of the available solutions still need to improve their true-positive detection rates and reduce the proportion of false-positive alarms. Therefore, internet service providers, utilising this type of device to defend their assets and subscribers against malicious traffic, may be induced by them to make incorrect decisions. In this paper, we propose a global intrusion detection system, based upon the BGP protocol that establishes a cooperative federation whose members are distributed autonomous intrusion detection elements. These elements are able to propagate alarms of potential threatening flows traversing their respective autonomous systems. We present the architecture for the described approach and an analytical model based upon Dempster-Shafer's combination rule, in order to evaluate specific performance metrics. The results show significant improvements over the assessed metrics, highlighting the advantage of using the proposed solution as a frontline to prevent cyberattacks.

Keywords Cyberattacks · Federation · BGP · Intrusion detection systems · Dempster-Shafer · Fusion · Flow-spec

1 Introduction

The connectivity-based attribute on which the internet was designed and constructed has also been one of the main factors exploited by many cyberattackers [1]. Therefore, considering the continuous growth observed in the internet connectivity, it is expected that cyberattacks will also become more threatening and even more effective, particularly concerning internet service providers (ISPs), who are attractive targets, utilised to spread attacks to their subscribers. Regarding this compromising scenario, ISPs are indeed spending a lot of money on typical perimeter-based intrusion detection systems (IDSs) to defend themselves (and their clients) from cyberattacks threats [2]. Despite the ability of such confined systems to identify malicious flows, they still face performance challenges to improve the true-positive detection rate and to reduce the proportion of false-positive alarms. Therefore, even having their detection systems fully updated, ISPs are not safe against zero-day attacks [3]. In order to prevent incoming cyberattacks, ISP security teams often correlate information from several sources, such as private warning systems, Cyber Emergency Response Teams (CERT) [4] and internet forums. However, this is also a very time-consuming task.

Even though internet design helps cyberattacks to reach their targets wherever they are, the number of networks traversed by a malicious flow can also be used to detect them. As reported in [5], approximately 97% of Distributed denial of service (DDoS) attacks come from external autonomous systems (ASs). Therefore, assuming that each of these ASs has its own IDS able to identify an anomalous flow, the detection likelihood increases with the number of IDSs along the attack path.

Based on what prior distributed intrusion detection system (DIDS) approaches have lacked, we propose a global intrusion detection system composed of autonomous internet-distributed detection systems. In our approach, federated intrusion detection elements cooperate with each other by sending information about a potential dangerous flow that traverses their respective ASs. The proposed DIDS

✉ Renato S. Silva
renato@ravel.ufrj.br

Luís F. M. de Moraes
moraes@ravel.ufrj.br

[1] Ravel Laboratory – PESC / Coppe-UFRJ, Avenida Horácio Macedo, 2030 Cidade Universitária, 21941-914 Rio de Janeiro, RJ Brazil

Published online: 05 November 2018

architecture relies on the Border Gateway Protocol (BGP) capabilities, so as to carry normalised warning messages across internet routing domains. The purpose of which would be in notifying a potential attack destination.

The remainder of this paper is organised as follows: Section 2 comments on the state-of-the-art in distributed attacks detection systems. Sections 3 and 4 present background information concerning our approach. Section 5 outlines key elements that compose the proposed architecture. In Section 6, we present an analytic model to evaluate the system performance combining intrusion information provided by federated IDSs. Section 7 briefly describes how some of the BGP capabilities, in accordance with RFCs [6] and [7], can be used to advertise malicious traffic warnings. Conclusion and planned future work is presented in Section 8.

2 Related works

The authors in [8] assess how the human immunisation system (HIS) mechanism can be used to distinguish normal from abnormal network activities. The analysis proposed in [9] defines three design goals for an efficient network-based IDS: being distributed, self-organising and lightweight. Having a distributed architecture suggests that a zero-day attack experienced by an IDS may no longer be undetectable for other remote IDS. Self-organising means that IDS agents can reconfigure themselves. Agents can be added or removed from the system without noticeable loss. Being lightweight means easy to deploy without requiring a complex structure to operate. In other words, lightweight platforms encourage attracting new agents. According to [10], the larger the federation size, the better the DIDS performs.

Although the distributed concept of DIDS has been accepted as a potential solution to improve detection performance, network infrastructure to support its communication requirements remains an issue. To overcome the availability problems resulting in a single central processing, Igbe et al. [11] propose a fully distributed network intrusion detection system (NIDS) approach where no central controller is needed. The detection system is based on an adaptive artificial immune mechanism, whose classifying method uses unsupervised machine learning to distinguish normal (self) from the abnormal traffic (non-self). The authors advocate that zero-day attacks can be detected through interactions between distant IDSs.

Besides problems related to network infrastructure, collecting information from multiple heterogeneous sources and combining them to derive more meaningful results has been investigated in numerous works. While some works propose building an entire communication architecture among their agents [12–17], other approaches concern improving detection performance by using different strategies for combining data from distributed agents [18–23].

There are various security database services assembled with invasion data collected from volunteer agents scattered over the internet. The technical report in [24] classifies some of these services and compares them according to their design, objective, sources of data, the ability to perform anonymous uploads, and availability of attacker notification and tracking tools. Although some of these services are free, they do not offer specific analysis regarding threats to an individual network.

The concept of distributing sensor elements and making them cooperate with each other is not new. There are several different approaches aiming to defend ISPs from cyberattacks. Yet, even with a number of approaches, an open global detection system still does not exist. In our previous work [25], we suggest the complexity for rapidly extending the federation and the heterogeneity of its members are the main reasons for this lacking. In this paper, we properly address these two issues to propose a feasible security framework as a frontline to prevent cyberattacks. Instead of facing heterogeneity as a problem, we take advantage of BGP ubiquity and ASs autonomy to broaden the detection surface and to improve its performance.

3 Intrusion detection systems—IDS

An intrusion is a kind of cyberattack where the attacker tries to overcome security mechanisms in order to violate the integrity, availability or confidentiality of network services [26]. An IDS can identify and report intrusions by monitoring traffic, inspecting and scanning packets for suspicious data.

Regarding the source of auditing data, there are two different approaches, namely, network-based and host-based detection. The host-based intrusion detection system (HIDS) monitors suspicious activities directly on the operating system such as read/write attempts and network connection attempts. The network-based intrusion detection system (NIDS) relies upon online network connection to inspect all the elements attached to the same network. IDSs may also be classified according to their detection methodology as statistical anomaly detection and signature-based detection [27]. Whatever the approach or methodology, the main drawback of any detection system is given by the false-positives (FP) and false-negatives (FN) reports.

The DIDS concept has emerged as a solution to improve detection performance and overcome problems related to the monolithic architecture of traditional detection systems. A DIDS can be defined as a group of network-distributed IDSs that communicate with each other, or with a central

Table 1 Flow attributes in NRLI-type field defined at RFC 5575

Type	Description	Type	Description	Type	Description
1	Destination prefix	5	Destination port	9	TCP flags
2	Source prefix	6	Source port	10	Packet length
3	IP protocol	7	ICMP type	11	DSCP
4	Port	8	ICMP code	12	Fragment

point, to extend network monitoring borders [28]. DIDS architecture can be seen as part of the artificial immune system (AIS) where several distributed autonomous systems cooperate with each other to detect intrusions. The main challenge of deploying a DIDS refers to the network infrastructure to support its distributed arrangement.

4 Dissemination of flow specification rules

The BGP flow-spec protocol is defined at RFC 5575 [6]. It allows BGP speakers to automatically filter a pre-defined flow advertised to upstream neighbours via BGP. The prior motivation of flow-spec is traffic filtering to prevent denial of service (DoS) attacks. However, it can be used for a wide variety of applications in which filtering information must be dynamically distributed throughout a network.

The flow-spec protocol uses MP-BGP [7] interworking capabilities to distribute traffic flow specifications through a new BGP network layer reachability information (NLRI). For each matched flow, RFC 5575 also defines a minimum set of filtering actions so as to specify its related processing at remote routers. The NRLI-type field comprises several matching options, according to Table 1. A packet is considered to match flow specification when it matches the intersection of all the components present at the NRLI-type field.

5 Proposed architecture

Inspired by the HIS, the proposed architecture creates a front-line to protect ISPs from cyberattacks by extending their detection surface. Our detection approach relies on using BGP to build a ubiquitous, lightweight and self-organised communication platform to interconnect all geographically distributed members forming as one detection federation. The three pillars of our approach are as follows:

- Using the intrusion AS-path to increase its detection likelihood.
- Taking advantage of the federation's autonomy to extend the range of detection.
- Normalizing heterogeneous warnings to make them cooperate with each other.

Our DIDS proposal meets these three pillars on (i) using federated IDSs in the intrusion AS-path to increase the likelihood of detecting a malicious flow. Once detecting the intrusion, the IDS of the traversed AS advertises an update message to the destination target to warn it about a potential threat. Each autonomous system is capable of deploying its own IDS according to its own traffic premises (ii). The distributed location of the autonomous IDSs creates a heterogeneous intrusion dataset from different agents, geographically spread across the internet. We argue that the more heterogeneous the elements, the better the chance of detecting a potential intrusion, including a zero-day one. Further, instead of triggering an immediate action for a specific kind of attack, we propose let security teams at the target AS assess the information inside the combined message as well as its reliability (iii). The greater the number of combinable messages, the more reliable is the combined information. Figure 1 shows the proposed scenario.

6 Modeling and performance analysis

Rather than improving the combination method of intrusion messages as proposed in [18], we use Dempster-Shafer's combination rule to evaluate how performance metrics behave in case of combining a number of intrusion warnings from different IDS members at a destination target.

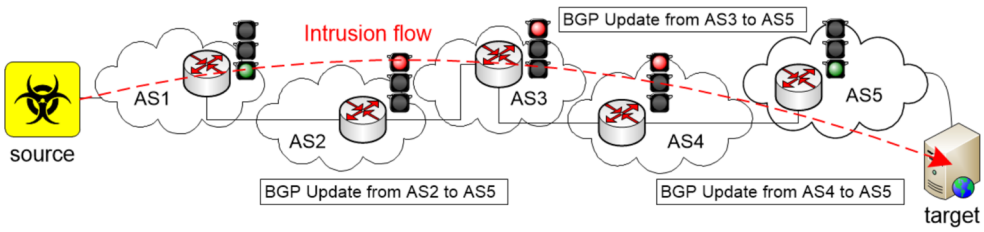


Fig. 1 One attacker from $AS1$ performing an attack against a target in $AS5$. IDSs in ASs 2, 3 and 4 detect the anomalous flow and advertise a BGP update to warn $AS5$ about the threat

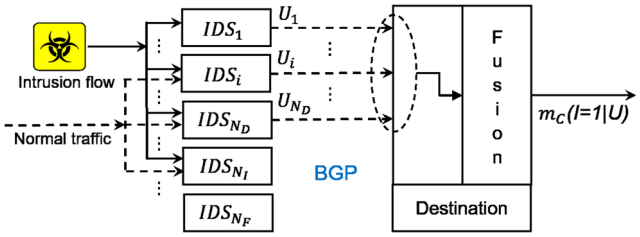


Fig. 2 Parallel intrusion evidence being fused at the destination target according to flow attribute

Figure 2 outlines a schematic model composed by N_F weight-equivalent and mutually independent IDS members. It also shows normal traffic and an intrusion flow passing through a number N_I ($N_I \leq N_F$) of IDSs towards its destination. Each IDS in the path flow may or may not detect this intrusion, according to its own detection performance. An IDS_i that detects such an intrusion advertises a BGP update message related to the intrusion flow. Once arriving at the destination, these N_D ($N_D \leq N_I$) BGP messages are correlated and combined according to their flow information.

Assuming I is a Bernoulli random variable which indicates that an intrusion is taking place ($I = 1$) or not ($I = 0$) at a given instant of time, and U_i, for $i = 1, 2, \cdots, N_F$, be independent and identically distributed Bernoulli random variables indicating the statement generated by the federated IDS_i (i.e. $U_i = 1$ if IDS_i detects an attack or $U_i = 0$ if IDS_i otherwise), respectively. The probability of an intrusion taking place is $\Pr(I = 1) = 1 - \Pr(I = 0)$. Likewise, the probability of a positive warning being generated by IDS_i is $\Pr(U_i = 1) = 1 - \Pr(U_i = 0)$; for each $i = 1, 2, \cdots, N_F$.

The positive prediction value (PPV_i) and positive rate (PR_i) represent performance metrics of IDS_i, which can be computed from its pre-evaluated confusion matrix, as presented in Table 2.

Positive prediction value (PPV_i) of an IDS_i defines the fraction of data predicted as genuine intrusions. For a sufficiently large and diversified dataset, we can approximate the PPV_i definition from the confusion matrix

Table 2 TP_i is the number of intrusions correctly predicted as intrusions by IDS_i

	$I = 1$	$I = 0$
$U_i = 1$	TP_i	FP_i
$U_i = 0$	FN_i	TN_i

FN_i refers to the number of intrusions incorrectly predicted as normal. Normal traffic correctly predicted as normal is TN_i. FP_i is the number of normal flows predicted as intrusive ones

to the conditional probability of being an intrusion, given that IDS_i has detected it.

$$\text{PPV}_i \triangleq \frac{TP_i}{TP_i + FP_i} \sim \Pr(I = 1|U_i = 1) \tag{1}$$

Positive rate (PR_i) refers to the rate of intrusion alarms (true or false) emitted by an IDS_i. Similarly, we approximate the PR_i definition to the conditional probability of IDS_i to emit a positive warning.

$$\text{PR}_i \triangleq \frac{TP_i + FP_i}{TP_i + FP_i + TN_i + FN_i} \sim \Pr(U_i = 1) \tag{2}$$

In order to evaluate additional performance metrics of our DIDS approach as a whole, we rely on Fig. 2, which proposes a typical scenario where an intrusion traverses a number N_I of different IDSs towards its target. However, although the intrusion flow traverses N_I-independent IDSs, it is supposed that just a number N_D of them have detected it and advertised a warning message.

True-positive rate (TPR) is a typical metric to infer about performance detection of IDSs in general. It measures the IDS sensitivity to detect real intrusions. Using the probabilistic term, we employ Bayes' rule to infer about true-positive rate of our DIDS approach as a whole (TPR_{DIDS}).

$$\text{TPR}_{\text{DIDS}} \sim \Pr(U=1|I=1) = \frac{\Pr(I=1|U=1) \times \Pr(U=1)}{\Pr(I=1)} \tag{3}$$

where $0 \leq \Pr(I = 1) \leq 1$ is the prior probability that normalizes Eq. 3 due to its mutually exclusive behaviour. $\Pr(U = 1)$ can be thought of as the probability of at least one of N_I IDSs conveys a positive warning (2).

$$\Pr(U = 1) = 1 - \prod_{i=1}^{N_I}(1 - PR_i) \tag{4}$$

$\Pr(I = 1|U = 1)$ in the right side of Eq. 3 refers to the PPV of throughout DIDS, which can be approximated to the belief degree of having a real intrusion, given that just N_D combinable warnings are received at the destination.

Dempster-Shafer's theory [29] has been used to model uncertainty, particularly in diagnostic domains for decisions. In our case, a number of federated IDSs that detect an intrusion play a role of multiple sources of evidence, whose warnings shall be fused at the destination.

Our exhaustive and mutually exclusive frame of discernment from the sources of evidence $\Omega = \{I = 1|U, I = 0|U\}$ is composed by only two elements representing the existence or not of an intrusion, given that a number N_D ($N_D \leq N_I \leq N_F$) of federated IDSs have detected it. The set of all hypothesis subsets of Ω is named as the power-set of Ω and is denoted by $2^{\Omega} = \{\{I = 1|U\}, \{I = 0|U\}, \{I = 1|U\} \cup \{I = 0|U\}, \{\emptyset\}\}$.

The belief mass $m_i(I|U)$ represents the part of belief from IDS_i that supports the intrusion hypothesis in subset $A_s = \{\{I = 1|U\} \cap \{\{I = 1|U\} \cup \{I = 0|U\}\}$. Thus, $m_C(I = 1|U)$ is the combined belief mass of N_D independent sources of evidence.

$$m_C(I=1|U) = \frac{\sum_{\cap A_s=(I=1|U)} \prod_{1\le i\le N_D} m_i(A_s)}{1-K} \quad \text{where}$$
$$K = \sum_{\cap A_s=\emptyset} \prod_{1\le i\le N_D} m_i(A_s) \tag{5}$$

K evaluates the amount of conflict among the evidence.

As proposed in [18], we adopt the same binomial mapping framework of Jøsang [30] to convert combinable alarms to their respective belief masses $m_i(I = 1|U)$.

$$m_i(I = 1|U) = \frac{TP_i}{TP_i + FP_i + 2} \sim \text{PPV}_i \tag{6}$$

For a sufficiently large and diversified dataset, we suppose $TP_i + FP_i \gg 2$. Thus, the belief mass $m_i(I = 1|U)$ of each advertised message U_i (for $i = 1, 2, \cdots, N_D$) that arrives at the destination is represented by the PPV_i, previously defined in Eq. 1.

As the N_D intrusion messages to be fused do not conflict with each other ($K = 0$), positive prediction value of DIDS platform as a whole (PPV_{DIDS}) can be evaluated by using Eqs. 5 and 6.

$$\text{PPV}_{\text{DIDS}} = m_C(I = 1|U) = 1 - \prod_{i=1}^{N_D}(1 - \text{PPV}_i) \tag{7}$$

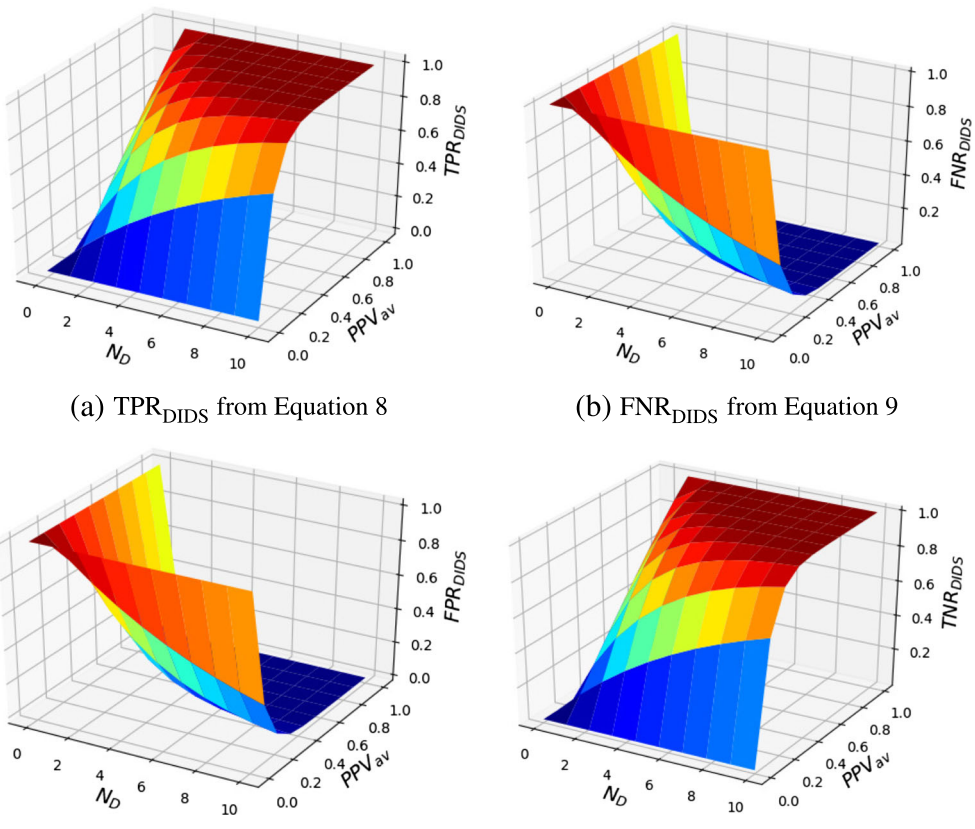
Taking average values for the performance metrics of all N_F-federated IDS as PPV_{av} and PR_{av}, we use Eqs. 7 and 4 to rewrite Eq. 3; and thereby evaluating the true-positive rate lower bound of our DIDS approach as a whole.

$$\text{TPR}_{\text{DIDS}} \ge \left[1 - (1 - \text{PPV}_{\text{av}})^{N_D}\right]\left[1 - (1 - \text{PR}_{\text{av}})^{N_I}\right] \tag{8}$$

False-negative rate infers about the fraction of false warnings generated by our DIDS platform ($\text{FNR}_{\text{DIDS}} = 1 - \text{TPR}_{\text{DIDS}}$).

$$\text{FNR}_{\text{DIDS}} \le 1 - \left[1 - (1 - \text{PPV}_{\text{av}})^{N_D}\right]\left[1 - (1 - \text{PR}_{\text{av}})^{N_I}\right] \tag{9}$$

False-positive rate (FPR_{DIDS}) measures the proportion of normal flows that are incorrectly warned as intrusions. FPR_{DIDS} can be evaluated from the disbelief in all N_D combinable warnings received at the destination and the



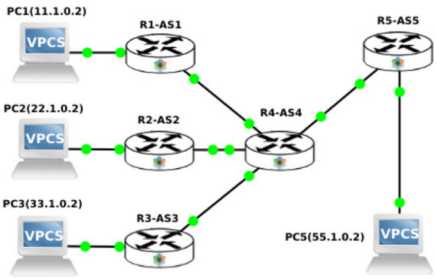
(a) TPR_{DIDS} from Equation 8

(b) FNR_{DIDS} from Equation 9

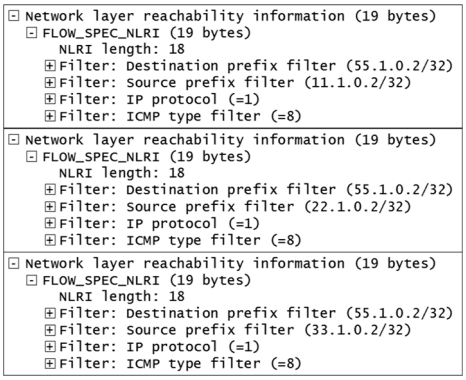
(c) FPR_{DIDS} from Equation 10

(d) TNR_{DIDS} from Equation 11

Fig. 3 Average positive rate (PR_{av}) and the number of involved IDS (N_I) have been fixed in 0.446 and 10 respectively [31]



(a) GNS3 view



(b) Wireshark logs collected at router 5

Fig. 4 Network topology comprising 4 border routers, with each router in its respective AS, emulating a coordinated ICMP attack against *PC5* from *PC1*, *PC2* and *PC3*

probability of one of N_I IDS member sends a warning (true or false).

$$\mathrm{FPR_{DIDS}} \leq (1 - \mathrm{PPV_{av}})^{N_D} \left[1 - (1 - \mathrm{PR_{av}})^{N_I}\right] \tag{10}$$

The true-negative rate ($\mathrm{TNR_{DIDS}}$) measures how specific the DIDS is by not warning in case of normal traffic. It is the proportion of normal traffic that is not warned as an intrusion. ($\mathrm{TNR_{DIDS}} = 1 - \mathrm{FPR_{DIDS}}$).

$$\mathrm{TNR_{DIDS}} \geq 1 - (1 - \mathrm{PPV_{av}})^{N_D} \left[1 - (1 - \mathrm{PR_{av}})^{N_I}\right] \tag{11}$$

Figure 3 shows how these performance metrics behave varying both $\mathrm{PPV_{av}}$ and the number of combinable warnings received at the destination.

7 Emulation results

In order to test the RFC 5575 capabilities and to analyse the format of the extended BGP update messages received at the destination, we have developed an emulation model whose topology is depicted in Fig. 4a.

The model uses GNS3 [32] installed on Ubuntu 16.04 to emulate a test scenario with 5 virtual routers running Junos 12.1 [33]. After configuring flow advertisements on router *R1*, *R2*, and *R3*, we capture BGP update messages at the *WAN* interface of router 5. These three messages can be correlated according to their destination address (55.1.0.2/32). Wireshark logs in Fig. 4b summarize the NLRI field of the three BGP update messages.

Emulation results show the feasibility of using BGP as the communication platform to disseminate warning messages among federated ASs, preserving their autonomy to process information. BGP messages can also be easily monitored and combined at any federated AS using pre-existing resources. The number of combinable messages received at the destination target, their inter-arrival time interval as well as their BGP AS-path, may also be used to evaluate the threat severity according to the risk premises of each security team.

8 Conclusion and future works

The DIDS concept has emerged as a promising response to a number of issues involving architecture and performance of detection systems. However, despite a large number of proposed approaches, the DIDS evolution has not held. Issues related to network infrastructure and the complexity in processing heterogeneous information might have contributed for to the latter hypothesis. Leveraging BGP ubiquity opens further insights into building a security frontline against cyberattacks. Processing normalized information instead of classification details, mitigates the heterogeneity problem but still keeps useful data to take effective protective decisions.

The proposed analytical model combining the evidence theory with Bayes' rule in Section 6 shows significant improvements with respect to the typical detection performance metrics like true-positive rate and others.

The emulation results presented in Section 7 have demonstrated how BGP capabilities perform to advertise intrusion warnings as well as how to combine them at the destination. Therefore, assuming the BGP network as an already held resource, we also have demonstrated the feasibility of our approach.

For a future work, we intend to build a test bed to evaluate both performance and security aspects of the approach presented in this paper.

Acknowledgements The authors are profoundly grateful to Evandro L. Macedo for his assistance in helpful discussions, comments and suggestions to write this paper.

Funding information The authors thank FAPERJ—the official funding agency for supporting science & technology research in the State of Rio de Janeiro (Brazil) and Rede-Rio (the state academic backbone network)—for the support given in the course of this work.

References

1. Leiner BM, Cerf VG, Clark DD, Kahn RE, Kleinrock L, Lynch DC, Postel J, Roberts LG, Wolff S (2009) A brief history of the internet. SIGCOMM Comput Commun Rev 39(5):22–31
2. Bass T (2000) Intrusion detection systems and multisensor data fusion. Commun ACM 43(4):99–105
3. Bilge L, Dumitras T (2012) Before we knew it: an empirical study of zero-day attacks in the real world. In: Proceedings of the 2012 ACM conference on computer and communications security, CCS'12. ACM, New York, pp 833–844
4. Stempfley RG (2017) Cert Coordination Center http://www.cert.org/. Accessed: 2018-04-12
5. Kupreev O, Strohschneider J, Khalimonenko A (2016) Kaspersky DDOS intelligence report for Q3 2016. https://securelist.com/kaspersky-ddos-intelligence-report-for-q3-2016/76464/. Accessed: 2018-04-30
6. Marques PR, Mauch J, Sheth N, Greene B, Raszuk R, Mcpherson DR (2009) Dissemination of flow specification rules
7. Bates T, Chandra R, Katz D, Rekhter Y (2007) Multiprotocol extensions for BGP-4
8. Kim J, Bentley P (1999) An artificial immune model for network intrusion detection. In: 7Th European congress on intelligent techniques and soft computing (EUFIT'99)
9. Kim J, Bentley P (2001) The human immune system and network intrusion detection. pp 1244–1252
10. Yegneswaran V, Barford P, Ullrich J (2003) Internet intrusions: Global characteristics and prevalence. SIGMETRICS Perform Eval Rev 31(1):138–147
11. Igbe O, Darwish I, Saadawi T (2016) Distributed network intrusion detection systems: an artificial immune system approach. In: 2016 IEEE First international conference on connected health: applications, systems and engineering technologies (CHASE), vol 00, pp 101–106
12. Balasubramaniyan JS, Garcia-Fernandez JO, Isacoff D, Spafford E, Zamboni D (1998) An architecture for Intrusion detection using autonomous agents. In: Proceedings 14th annual computer security applications conference (Cat. No.98EX217), pp 13–24
13. Cuppens F, Miege A (2002) Alert correlation in a cooperative intrusion detection framework. In: Proceedings 2002 IEEE symposium on security and privacy, pp 202–215
14. Kruegel C, Valeur F, Vigna G, Kemmerer R (2002) Stateful intrusion detection for high-speed networks. In: Proceedings of the 2002 IEEE symposium on security and privacy, SP'02. IEEE computer society, Washington, p 285
15. Janakiraman R, Waldvogel M, Zhang Q (2003) Indra: a peer-to-peer approach to network intrusion detection and prevention. In: 12Th IEEE international workshops on enabling technologies (WETICE 2003), infrastructure for collaborative enterprises, 9-11 June 2003. Linz, Austria, pp 226–231
16. Yegneswaran V, Barford P, Jha S (2004) Global intrusion detection in the DOMINO overlay system. In: Proceedings of network and distributed system security symposium (NDSS)
17. Snapp SR, Brentano J, Dias GV, Goan TL, Heberlein LT, Ho CL, Levitt KN, Mukherjee B, Smaha SE, Grance T, Teal DM, Mansur D (1998) Internet besieged. chap. DIDS (distributed intrusion detection system)-motivation, architecture, and an early prototype. New York, NY, USA, pp 211–227
18. Shah V, Aggarwal AK, Chaubey N (2017) Performance improvement of intrusion detection with fusion of multiple sensors. Complex & Intelligent Systems 3(1):33–39
19. Thomas C, Balakrishnan N (2009) Improvement in intrusion detection with advances in sensor fusion. IEEE Trans Inf Forensics Secur 4(3):542–551
20. Wang Y, Yang H, Wang X, Zhang R (2004) Distributed intrusion detection system based on data fusion method. In: Fifth world congress on intelligent control and automation, 2004. WCICA 2004, vol 5. IEEE, pp 4331–4334
21. Shah VM, Agarwal AK (2017) Reliable alert fusion of multiple intrusion detection systems. International Journal Network Security 19(2):182–192
22. Thomas C, Balakrishnan N (2008) Performance enhancement of intrusion detection systems using advances in sensor fusion. In: 2008 11th international conference on information fusion. IEEE, pp 1–7
23. Barford P, Jha S, Yegneswara V (2004) Fusion and filtering in distributed intrusion detection systems. In: Proceedings of the 42nd annual allerton conference on communication, control and computing
24. Robbins R (2002) Distributed intrusion detection systems: an introduction and review. Tech rep, InfoSec Reading Room - SANS Institute
25. Silva RS, Macedo ELC (2017) A cooperative approach for a global intrusion detection system for internet service providers. In: 2017 1st cyber security in networking conference (CSNet). pp 1–8
26. Simmons C, Ellis C, Shiva S, Dasgupta D, Wu Q (2009) AVOIDIT: a cyber attack taxonomy. In: Proceedings of 9th Annual Symposium on Information Assurance-ASIA, vol 14
27. Axelsson S (2000) Intrusion detection systems: a survey and taxonomy. Tech rep, Technical report
28. Varshney PK (1996) Distributed detection and data fusion. Springer, New York
29. Shafer G (1976) A mathematical theory of evidence. Princeton University Press, Princeton
30. Jøsang A (2016) Subjective logic: a formalism for reasoning under uncertainty. Springer, Berlin
31. Patil A, M, SY (2018) Performance analysis of anomaly detection of KDD cup dataset in R environment. Int J Appl Eng Res 13(6):4576–4582
32. Neumann JC (2014) The book of GNS3. No Starch Press, San Francisco
33. Thomas TM, Pavlichek DE, Dwyer III LH, Chowbay R, Downing WW (2003) Juniper networks reference guide: JUNOS routing, configuration, and architecture. Addison-Wesley Professional