Feature Selection of Denial-of-Service Attacks Using Entropy and Granular Computing

Article · June 2017

DOI: 10.1007/s13369-017-2634-8

4 authors:

Suleman Khan
University of Malaya
32 PUBLICATIONS **207** CITATIONS
SEE PROFILE

Abdullah Gani
University of Malaya
187 PUBLICATIONS **2,511** CITATIONS
SEE PROFILE

Ainuddin Wahid
University of Malaya
75 PUBLICATIONS **338** CITATIONS
SEE PROFILE

Prem Kumar Singh
Amity University
23 PUBLICATIONS **212** CITATIONS
SEE PROFILE

Arab J Sci Eng
DOI 10.1007/s13369-017-2634-8

RESEARCH ARTICLE - COMPUTER ENGINEERING AND COMPUTER SCIENCE

Feature Selection of Denial-of-Service Attacks Using Entropy and Granular Computing

Suleman Khan[1] · **Abdullah Gani**[2] · **Ainuddin Wahid Abdul Wahab**[2] · **Prem Kumar Singh**[3]

Received: 20 December 2016 / Accepted: 7 June 2017

Abstract Recently, many researchers have paid attention toward denial of services (DoS) and its malicious handling. The Intrusion detection system is one of the most common detection techniques used to detect malicious attack which attempts to compromise the security goals. To deal with such an issue, some of the researchers have used entropy calculation recently to detect malicious attacks. However, it fails to identify the most potential feature for DoS attack which needs to be addressed on its early occurrence. Therefore, this paper focused on identifying some of the potential attributes of a DoS attack based on computed weight for each of the attributes using entropy calculation. In addition, the selection of potential attributes based on user-defined chosen granulation is also given using NSL KDD dataset.

Keywords Intrusion detection systems · DoS attack · Entropy

1 Introduction

In our extensive review of the literature, we found that most of the researchers have evaluated their IDS on a well-known dataset known as the NSL KDD, which is a refined and accurate form of the DARPA KDD'99 dataset without the redundant instances [1]. The NSL KDD dataset is considered as a benchmark dataset for anomaly detection, especially for intrusion detection. The dataset consists of 41 features representing different features of the network traffic. The network traffic is classified according to two main classes, the normal class and the anomaly class. The anomaly class represents intrusions or attacks found in the network at the time of recording the network traffic. Based on these attacks, the NSL KDD dataset is further classified into four main attack categories including DoS, probing, users to root (U2R), and remote to local (R2L). The DoS attack makes services unavailable to legitimate users by bombarding attack packets on computing or network resources. Examples of DoS attacks include backland, smurf, teardrop, and neptune attacks. Each DoS attack type and its affect is explained in Table 1. Probing attacks collect information from different resources in the network for suspicious purposes. Examples of probing attacks include ipsweep, nmap, saint, and portsweep attacks. In a U2R attack, the attacker uses the user's account and tries to exploit different vulnerabilities of the system by getting access to the root of the system. U2R attacks include access loadmodule, buffere_overflow, and rootkit attacks. In R2L attacks, the attacker finds vulnerabilities in the system in order to access it while not having legitimate access. R2L attacks include ftp_write, warezmaster, guess_password, and IMAP attacks.

This paper focused on DoS attacks due to its high rank among the various types of attack in terms of computer crime cost, as mentioned in the 2014 report [2]. A DoS attack is considered a major problem for legitimate users accessing services via the Internet. DoS attacks make services unavailable to users by draining network or system resources. Although a lot of research has been done by network security experts to overcome the DoS attack problem, DoS attacks are becoming more frequent and have a greater adverse impact with the passage of time. Many

✉ Suleman Khan
suleman.khan@monash.edu

[1] School of Information Technology, Monash University Malaysia, Subang Jaya, Selangor Darul Ehsan, Malaysia

[2] Center for Mobile Cloud Computing Research (C4MCCR), University of Malaya, Kuala Lumpur, Malaysia

[3] Amity Institute of Information Technology, Amity University, Noida, India

Published online: 17 June 2017

Table 1 Types and description of denial-of-services attacks

Attack class	Attack types	Descriptions	Affects
Denial-of-services (DoS)	Apache	Targets apache server through flood attack	Effect memory and CPU of the server
	Neptune	Generates SYN flood attack on network host by sending session establishment request	Victim host waits for session establishment
	Pod	Sends malformed and oversize packets to a victim by using simple ping command	Results in system crash
	Smurf	Targets misconfigure network device to send broadcast message to all hosts in the network	Exhausts network bandwidth and host resource
	Teardrop	It sends mixed IP fragments with overlapping and oversize payload to the victim	Loss of data
	Mailbomb	Sends huge amount of emails to a specific host	Used entire server working it properly
	Udpstorm	Floods UDP packets on random ports of specific host	Victim replies with ICMP packets which might not reach a source due to spoofing

researchers have proposed different approaches to detect DoS attacks; however, the most common approach used is anomaly-based detection. Anomaly-based detection detects a DoS attack based on network traffic statistics such as traffic volume and packet header information. The alert alarm for a DoS attack is generated after deviation is observed while measuring the statistical features of the network traffic.

Nevertheless, the best option for detecting an anomaly in the network is to determine randomness in the packet patterns. For instance, in a DoS attack, one host may target another host by flooding it with numerous attack packets to break down its computational power as it entertains large amounts of packets. To measure the flooding of packets, entropy can be used to measure the uncertainty related to packets by considering it a random variable. The divergence of attack packets from normal packets is calculated by finding the difference between the probability distributions. In this paper, our main goal is to determine the most appropriate features to use in identifying a DoS attack in a NSL KDD dataset using entropy calculation and granular computing. From the literature [3], we have selected seven of the key significant features which are used to identify DoS attacks in a NSL KDD dataset. Moving one step further, we want to identify the potential features from among these seven selected features which have the greater impact. We have selected a small part of the NSL KDD dataset with 50 instances to evaluate our proposed method and illustrate it with an example.

The paper has following key contributions which has been listed as follows:

1. Comprehensive knowledge of DoS attack is provided to have proper insight and understandability for the reader.
2. The weight has been calculated for DoS attack features based on entropy calculation.
3. The potential feature/attribute is selected based on granular computing to identify its maximum role in launching the DoS attack.

The rest of the paper is organized as follows: Sect. 2 explains background knowledge related to DoS attack, entropy, and granular computing. Section 3 discusses proposed method used to find potential features of DoS attack. Section 4 illustrates the proposed method with an example based on NSL KDD dataset. Section 5 highlights related work of entropy-based IDS. At last, we conclude the paper.

2 Background

In this section, we provide a brief background of the DoS attack, entropy, and granular computing. We have used entropy and granular computing in order to propose a meaningful solution to identifying the potential features of a DoS attack based on the NSL KDD dataset.

2.1 Denial-of-Service attack

A DoS attack is considered to be one of the most serious threats to the security of cyberspace nowadays [4]. It exploits the network or victim machine by exhausting bandwidth, memory, and its processing capacity. Generally, DoS

attacks target one host or server by generating numerous malicious packets to stop legitimate users using different services. Detecting a DoS attack is important to mitigate the attack before it crashes the system or chokes the network [5,6]. The detection of a DoS attack is mainly carried out in one of two ways: signature-based intrusion detection or anomaly-based intrusion detection. Signature-based intrusion detection is performed by comparing network traffic with early known attack patterns stored in the database. The advantage of this method is that it identifies intrusion accurately by generating fewer false positive alarms. However, the disadvantage of signature-based intrusion detection is its non-detection of zero day attacks, those types of attack which have not been experienced before. Anomaly-based intrusion detection considers the network traffic statistics to detect various intrusions in the network traffic, such as packet header information, packet size, and packet rates. The advantages of anomaly-based intrusion detection are that there are no worries about databases; less maintenance is required once the system is developed; and less memory is required for its development. However, the disadvantages of anomaly-based intrusion detection include difficulty in detecting malicious traffic which is similar to normal traffic, such as in low-rate DDoS attacks, the need for appropriate training to detect attacks, greater system complexity, and no guarantee about generating alarms for unknown attacks.

Currently, the Internet is attacked with different attacks including large-scale DoS attacks, low-rate DDoS attacks, and various others. A botnet is an example of how to launch a low-rate DDoS attack while ensuring the network appears normal. These kinds of low-rate DDoS attack are difficult to detect or mitigate easily [7]. To detect different types of DDoS attack, it is necessary to understand the features of a DDoS attack, which will also help in tracing the source of the attack and hence stop it in the future especially in cloud computing [8].

2.2 Entropy

Entropy is a concept used in information theory to measure randomness. In simple words, it can be explained as a measurement of the uncertainty of a random variable. The greater the randomness, the higher the value of the entropy is and vice versa [9]. Shannon entropy is one type of generalized information entropy used to quantify the diversity of the randomness or uncertainty of a system. Shannon entropy is considered an important metric in statistics for calculating the index of diversity. It is used in different fields including infinite circular wells [10], mass oscillators [11], acoustic emission detection [12], image randomness [13], fuzzy setting [14], fuzzy concept lattice [15], finance [16]. Moreover, in detecting a DDoS attack, Shannon entropy is also used to measure the randomness of packets generated during the attack [17]. More studies regarding the detection of DDoS through entropy are discussed in the related work section.

The equation for entropy is shown in Eq. (1):

$$E(b) = -\sum p(b/a)\log(p(b/a)) \tag{1}$$

where $E(b)$ is entropy value and $p(b/a)$ is probabilistic value of the random values. The reader is advice to reader the following [9] for the step-by-step calculation of the entropy.

2.3 Granular computing

The process of solving a problem through its basic elements is called granular computing. It is considered an important paradigm in the information processing field. A problem which is difficult to solve in its entirety is divided into small parts called granules, which can then be further easily handled and solved. The granules can be viewed as a bunch of elements combined together based on their similarity, spatial neighborhood, indiscernibility, and functionality. However, generating the granules of a problem is a crucial process because the success of granular computing depends on the shape and size of the generated granules. Each granule represents some part of the problem which in turn represents a level of granularity. Different granules have different levels of granularity and represent the problem or system differently.

Granular computing helps to solve problems involving uncertainty, vagueness, and incompleteness of information. In some sophisticated problems, it is hard to differentiate among the groups of elements to obtain a more precise and meaningful output. Therefore, the most convenient way is to break down the problem into different granules, which represent the structure of the patterns of the problem. Granular computing can be used efficiently in the decision-making process in real life based on neural networks, fuzzy sets, rough sets, and interval analysis [18]. More information and the application of granular computing can be seen in [19,20].

3 Proposed Method

The proposed method is based on Shannon entropy and granular computing to select some potential features of the DoS attack. The aim of the proposed method is to determine those potential features which could help security administrators to investigate the DoS attack. Such that we can reduce time in detecting the DoS attack and mitigating it in a real time. The proposed algorithm for the proposed method is shown in Table 2, and its explanation is illustrated in Fig. 1.

Step 1. Let us consider any dataset. For example, the NSL KDD dataset is considered in this paper.

Table 2 Proposed algorithm for finding potential features using Shannon entropy and threshold

Input: An array of features for the DoS attack

Output: Some potential features of the DoS attack

1. **for** i = 1, 2, 3, …, m, where m is the number of features
2. Compute the probability of each feature such as $P(a/b) = P(a)/P(b)$, where $P(a)$ is …….and $P(b)$ is …….
3. Calculate the value for Shannon entropy, i.e.,$E(b) = -\sum p(b/a)\log(p(b/a))$
4. Find the weight, i.e., Weight (w) = $weight(w) = \sum b_i / \sum b$
5. Return the weight value for the feature, i.e., (w)

end for

6. Set the threshold for weight (w) in [0, 1].
7. **if** (w > threshold)

   Select the feature attribute

8. **else**

   Remove the feature attribute

end if

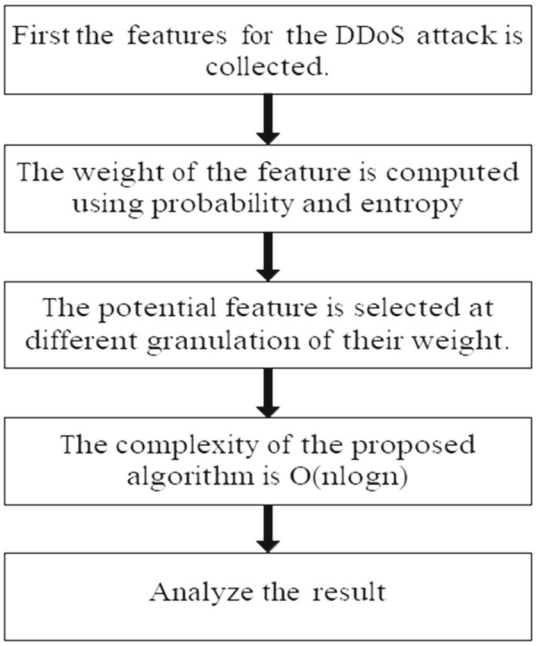

Fig. 1 Flowchart of the proposed research methodology

Step 2. Normalize the dataset into one format using the following formula.

$$\text{Normalization} = [(\text{Actual} - \text{value} - \text{Min})/ \times (\text{Max} - \text{Min})][\text{high} - \text{low}] + \text{Low}$$

Step 3. The normalized dataset will provide the value of each feature between [0,1] when we fix Max = 1 and Min = 0.

Step 4. Now the probability of possessing the given anomaly (a) by feature (b) can be computed as follows:

$$P(a/b) = P(a)/P(b)$$

Step 5. The weight of the given feature to possess the particular anomaly can be computed using entropy calculation as follows:

$$E(b) = -\sum p(b/a)\log(p(b/a))$$

Step 6. The average weight of the feature can be computed as follows:

$$\text{Weight}(Wi) = \text{Summation of entropy weight}(Ei)/ \times \text{Total number of anomaly} \quad (2)$$

Step 7. Now the properties of granulation can be used to refine the potential feature based on its computed weight. The feature can be considered an important feature for the given anomaly if the weight of the feature is higher than the given threshold.

3.1 Complexity

Let us suppose n is the number of attributes. Then, the proposed method finds probability which takes o(n) complexity. Further, it computes entropy, which has o(n log(n)) time. Hence, the overall computational complexity time for the proposed method is o(n log(n)).

4 Illustration

Recently, numerous methods have been proposed to detect intrusion in the NSL KDD dataset. These methods focus on

Table 3 Selected attributes for denial-of-services attack

Attack	Selected features	Value/type	Descriptions
Denial of services (DoS)	Duration	Continuous/integer	Highlights length of the connections in seconds
	src_bytes	Continuous/integer	Number of data bytes transfer from source to destination
	Count	Continuous/integer	Number of connection to a host with considering time of past two seconds
	srv_rerror_rate	Continuous/real	Connections have "REJ" errors (%age)
	dst_host_same_srv_rate	Continuous/real	Connection have same destination host and service (%age)
	dst_host_srv_serror_rate	Continuous/real	Connection to current host with specified service having "S0" error (%age)
	dst_host_srv_rerror_rate	Continuous/real	Connection to current host with specified service having "RST" error (%age)

Table 4 Fifty random anomaly instances of NSL KDD dataset

Attack type	Instances	Duration	src_bytes	Count	srv_rerror _rate	dst_host_same _srv_rate	dst_host_srv _serror_rate	dst_host_srv _rerror_rate
DoS	1	0	0	123	0	0.1	1	0
	2	0	0	121	1	0.07	0	1
	3	0	0	166	0	0.04	1	0
	4	0	0	117	0	0.06	1	0
	5	0	0	270	0	0.09	1	0
	6	0	0	133	0	0.05	1	0
	7	0	0	205	1	0.05	0	1
	8	0	0	199	0	0.05	1	0
	9	0	334	2	0	1	0	0
	10	0	0	233	0	0	1	0
	11	0	0	96	0	0.01	1	0
	12	0	18	1	0	1	0	0
	13	0	0	223	0	0.09	1	0
	14	0	0	280	0	0.07	1	0
	15	0	0	248	0	0.01	1	0
	16	0	0	279	0	0.05	1	0
	17	0	8	1	0	1	0	0
	18	0	0	57	0	0.23	1	0
	19	0	0	2	1	0	0	1
	20	0	0	205	0	0.07	1	0
	21	0	0	228	0	0.05	1	0
	22	0	0	50	0	0.25	1	0
	23	0	0	262	0	0.04	1	0
	24	0	0	108	0	0.04	1	0
	25	0	28	80	0	0.31	0	0
	26	0	334	2	0	1	0	0
	27	0	0	258	0	0.02	1	0
	28	0	0	61	1	0.02	0	1

Table 4 continued

Attack type	Instances	Duration	src_bytes	Count	srv_rerror _rate	dst_host_same _srv_rate	dst_host_srv _serror_rate	dst_host_srv _rerror_rate
	29	0	28	2	0	0.01	0	0
	30	0	8	1	0	1	0	0
	31	0	0	146	1	0.04	0	1
	32	0	0	300	0	0.01	1	0
	33	0	0	129	0	0.05	1	0
	34	0	28	82	0	0.71	0	0
	35	25950	1	2	1	0.01	0	1
	36	0	0	110	1	0.07	0	1
	37	0	0	190	0	0.08	1	0
	38	0	0	135	1	0	0	1
	39	0	0	123	0	0.03	1	0
	40	0	0	245	0	0.03	1	0
	41	0	1032	263	0	1	0	0
	42	0	0	109	0	0.03	1	0
	43	0	0	145	1	0.03	0	1
	44	9015	1	2	1	0.01	0	1
	45	0	0	44	0	0.05	1	0
	46	0	1032	511	0	0.83	0	0
	47	0	0	101	0	0.06	1	0
	48	15159	350	1	0	0.56	0	0
	49	0	0	223	0	0.04	1	0
	50	0	0	223	0	0.07	1	0

classification, clustering, feature reduction, feature extraction, and many others. Our proposed work is closer to the feature reduction methods. In the literature, feature reduction methods are used to identify the significant features of different attacks found in the dataset such as DoS, probe, U2R, and R2L. Mostly, these methods have identified several significant features for detecting the different attacks presented in the dataset. However, based on our knowledge, no work has been done to find some potential features which have a greater significance during a DoS attack. Identifying the potential features will help IDS to focus on these features in detecting the attack rather than using greater time and computation addressing the many other features.

In this paper, our scope is limited to DoS attacks; however, our method is applicable to the other attacks in the dataset as well. To evaluate our proposed method, seven significant features of a DoS attack were considered [3]. These features and their properties are depicted in Table 3. To illustrate the proposed method, 50 random instances were considered from the NSL KDD dataset, as shown in Table 4. The features of the NSL KDD dataset contained different numerical values. To scale each feature of the DoS attack, the dataset had to be normalized into one scale. For this purpose, the selected dataset was normalized as follows:

$$\text{Normalization} = [(\text{Actual} - \text{value} - \text{Min})/(\text{Max} - \text{Min})] \times [\text{high} - \text{low}] + \text{Low} \quad (3)$$

The normalization of features provided a value within the range of [0–1], as shown in Table 5. Now the concern is to identify some of the potential features of the DoS attack. For this purpose, we calculated the probability of each feature attribute, as shown in Table 6. Further, the weight of each feature could be computed based on the theory of entropy using Eq. (1). The average weight for each feature could be computed using Eq. (2). Table 6 represents the computed probability, entropy, and weight for each attribute using the proposed method. In general, the features having the greater weight can be considered potential features as, for example, the feature "count." Moreover, potential features can be selected based on user requirements at different granulations of their weight, as shown in Table 7. We can observe that the feature "count" has more weight compared to the other features of the DoS attack. This feature should necessarily be given more attention during a DoS attack.

Table 5 Data normalization of instances within range of [0–1]

Attack type	Instances	Duration	src_bytes	Count	srv_rerror _rate	dst_host_same _srv_rate	dst_host_srv _serror_rate	dst_host_srv _rerror_rate
DoS	1	0	0	0.239	0	0.1	1	0
	2	0	0	0.235	1	0.07	0	1
	3	0	0	0.323	0	0.04	1	0
	4	0	0	0.227	0	0.06	1	0
	5	0	0	0.527	0	0.09	1	0
	6	0	0	0.258	0	0.05	1	0
	7	0	0	0.4	1	0.05	0	1
	8	0	0	0.388	0	0.05	1	0
	9	0	0.32	0.001	0	1	0	0
	10	0	0	0.454	0	0	1	0
	11	0	0	0.186	0	0.01	1	0
	12	0	0.017	1	0	1	0	0
	13	0	0	0.435	0	0.09	1	0
	14	0	0	0.547	0	0.07	1	0
	15	0	0	0.484	0	0.01	1	0
	16	0	0	0.545	0	0.05	1	0
	17	0	0.007	1	0	1	0	0
	18	0	0	0.109	0	0.23	1	0
	19	0	0	0.001	1	0	0	1
	20	0	0	0.4	0	0.07	1	0
	21	0	0	0.445	0	0.05	1	0
	22	0	0	0.096	0	0.25	1	0
	23	0	0	0.511	0	0.04	1	0
	24	0	0	0.209	0	0.04	1	0
	25	0	0.027	0.154	0	0.31	0	0
	26	0	0.32	0.001	0	1	0	0
	27	0	0	0.503	0	0.02	1	0
	28	0	0	0.117	1	0.02	0	1

5 Related Work

Identifying the most potential features of a DoS attack is one of the major issues addressed by researchers. For this purpose, several approaches have been proposed; some of the approaches related to the proposed method are also discussed in Table 8. We can see that some researchers have used the theory of entropy to traceback the attack while some have used it to identify the significant number of features for intrusion detection. In method [21], entropy and frequency-sort distribution are used to detect the DDoS attack by computing packet header information. In method [22], features are selected using the information gain and Chi-square approaches. The selected features are the input for the maximum entropy model to determine those which are relevant and reduce the computational cost during intrusion detection. In method [23], entropy-based profiling of network traffic is used to detect network security attacks.

The method used in [24] employs the modified Global K-Means algorithm (MGKM) clustering approach incorporated with entropy to determine the degree of divergence between source and destination IP addresses. The method mentioned in [25] analyzes honey net traffic data by using entropy calculation and volume-based distribution. In method [26], the hybrid approach is used including K-Means, K-nearest neighbor, and Naïve Bayes combined with entropy to find relevant features for intrusion detection. In [27], entropy is combined with the K-Means clustering algorithm to find the similarities between the data inside the cluster. A hybrid machine learning-based intrusion detection method is proposed to detect intrusions in [28]. The method first uses entropy to select the relevant features among the different feature attributes of the dataset. In method [29], anomaly detection is performed based on the cluster algorithm while using information entropy and the frequency-sensitive discrepancy metric. Information entropy assists in finding the

Table 5 continued

Attack type	Instances	Duration	src_bytes	Count	srv_rerror _rate	dst_host_same _srv_rate	dst_host_srv _serror_rate	dst_host_srv _rerror_rate
	29	0	0.027	0.001	0	0.01	0	0
	30	0	0.007	1	0	1	0	0
	31	0	0	0.284	1	0.04	0	1
	32	0	0	0.586	0	0.01	1	0
	33	0	0	0.25	0	0.05	1	0
	34	0	0.027	0.158	0	0.71	0	0
	35	1	1	0.001	1	0.01	0	1
	36	0	0	0.213	1	0.07	0	1
	37	0	0	0.37	0	0.08	1	0
	38	0	0	0.262	1	0	0	1
	39	0	0	0.239	0	0.03	1	0
	40	0	0	0.478	0	0.03	1	0
	41	0	1	0.513	0	1	0	0
	42	0	0	0.211	0	0.03	1	0
	43	0	0	0.282	1	0.03	0	1
	44	0.34	1	0.001	1	0.01	0	1
	45	0	0	0.084	0	0.05	1	0
	46	0	1	1	0	0.83	0	0
	47	0	0	0.196	0	0.06	1	0
	48	0.58	0.33	1	0	0.56	0	0
	49	0	0	0.435	0	0.04	1	0
	50	0	0	0.435	0	0.07	1	0

Table 6 Computed probability, entropy, and weight of each selected attribute

yi	P (yi)	E (yi)	wi
Duration	0.0384	0.18	0.0738
src_bytes	0.10164	0.335	0.1375
Count	0.35588	0.53	0.2175
srv_rerror_rate	0.2	0.464	0.1904
dst_host_same_srv_rate	0.2098	0.472	0.1937
dst_host_srv_serror_rate	0.58	0.455	0.1867

Table 7 Selection of potential features using chosen granulation

Granulation	Selected attribute
$0.20 < w < 1.0$	Count
$0.19 < w < 0.2$	srv_rerror_rate, dst_host_same_srv_rate
$0.18 < w < 0.19$	dst_host_srv_serror_rate
$0.10 < w < 0.18$	src_bytes
$0.00 < w < 0.10$	Duration

appropriate center of clusters, which helps in increasing the detection rate and has a lower false alarm rate.

In method [30], intrusion is detected by using a flow-level-limited penetrable visibility graph. The statistical characteristics of the intrusion are converted to a graph where further machine learning and entropy are applied to extract the potential features used to analyze different anomalies. In method [31], entropy analysis is used for wavelet coefficients in order to detect intrusion in the network. Some extensive method on DoS attack in various research fields is discussed in [32–37]. Table 8 analyzes some important methods related to the proposed method. The current study is aimed at addressing the following problems, marked (*) in Table 8:

1. Computation of the weight of each attribute of a DoS attack.
2. Identifying some of the potential attributes of the DoS attack at different granulations of their weight.

The proposed method is different from any of the available methods in the following aspects:

1. The proposed method computes the weight of each feature of the DoS attack using entropy calculation. Hence, the proposed method provides the best possible measurement of uncertainty in intrusion detection.
2. The complexity of the proposed method, i.e., o($n \times \log(n)$), is in good agreement with any of the available methods. Moreover, the proposed method provides a way

Table 8 Entropy-based literature work

References	Attack type	Entropy	Weight	Granular computing
[21]	DoS	Feature selection	Chi-square	Selection of fields in packet header
[22]	DoS, probe, R2l, U2R	Relevant feature selection	Information gain, Chi-square	*
[23]	DoS	To profile network traffic	Chi-square goodness-of-fit test	Basic and time-based traffic features
[24]	DoS	Degree of divergence for source and destination ip address	Linear correlation coefficient	*
[25]	Different anomalies	To analyze honey net traffic data by selecting relevant network features	Threshold	Selection based on traffic volume
[26]	DoS, probe, R2l, U2R	Relevant feature selection	K-nearest neighbor, Naïve Bayes	Clustering
[27]	DoS, probe, R2l, U2R	To improve detection rate and decrease false positive rate	K-Means	Clustering
[28]	DoS, probe, R2l, U2R	Extract optimized information	Support vector machine, Multi-layer perceptron	*
[29]	DoS, probe, R2l, U2R	To find the cluster centers	Frequency-sensitive discrepancy metric	Clustering
[30]	DoS, probe, R2l, U2R	To select potential attributes in the network graph	*	*
[31]	DoS	Used entropy analysis of wavelet coefficient	Daubechies wavelets	Traffic signal decomposition

to select some potential features at different granulations of their computed weight.

6 Conclusions and Future Work

This paper aimed at finding some of the potential features of a DoS attack by entropy calculation and granulation computing. To achieve this goal, a method is proposed to compute the weight of each feature based on entropy calculation. Such that, the potential features can be selected using their computed weight at a chosen granulation within $o(n\log(n))$ complexity. The proposed method is applied on the NSL KDD dataset and provides agreement with recent studies [14–16,23]. In addition, the proposed method provides a way to select some of the potential attributes for the Dos attack. In future the work will focus on implementing the proposed method on software-defined networks (SDN) [38–40].

Acknowledgements This work is fully funded by Bright Spark Unit, University of Malaya, Malaysia, and partially funded by the High Impact Research Grant UM.C/625/1/HIR/MOE/FCSIT/03, Malaysian Ministry of Higher Education under the University of Malaya. Moreover, the authors thanks School of Information Technology, Monash University Malaysia for providing the seed grant.

References

1. Tavallaee, M.; Bagheri, E.; Lu, W.; Ghorbani, A.-A.: A detailed analysis of the KDD CUP 99 data set. In: Proceedings of the Second IEEE Symposium on Computational Intelligence for Security and Defence Applications 2009 (2009)
2. Institute, P.: 2014 Global report on the cost of cyber crime. HP Enterprise Security p. 31 (2014)
3. Yi, M.A.; Phyu, T.: Layering based network intrusion detection system to enhance network attacks detection. Int. J. Sci. Res. **2**(9), 10091302 (2013)
4. Xiang, Y.; Li, K.; Zhou, W.: Low-rate DDoS attacks detection and traceback by using new information metrics. IEEE Trans. Inf. Forensics Secur. **6**, 426–437 (2011)
5. Khan, S.; Shiraz, M.; Wahab, A.W.A.; Gani, A.; Han, Q.; Rahman, Z.B.A.: A comprehensive review on adaptability of network forensics frameworks for mobile cloud computing. Sci. World J. **2014**, 547062 (2014). doi:10.1155/2014/547062

6. Khan, S.; Gani, A.; Wahab, A.W.A.; Shiraz, M.; Ahmad, I.: Network forensics: review, taxonomy, and open challenges. J. Netw. Comput. Appl. **66**, 214–235 (2016)
7. Shevtekar, A.; Anantharam, K.; Ansari, N.: Low rate TCP denial-of-service attack detection at edge routers. IEEE Commun. Lett. **9**, 363–365 (2005)
8. Khan, S.; Gani, A.; Abdul Wahab A. W.; AminuBagiwa M.: "SIDNFF: source identification network forensics framework for cloud computing. In: Presented at the IEEE International Conference on Consumer Electronics, Taiwan, (2015)
9. Shannon, C.E.: A mathematical theory of communication. ACM SIGMOBILE Mob. Comput. Commun. Rev. **5**, 3–55 (2001)
10. Song, X.-D.; Sun, G.-H.; Dong, S.-H.: Shannon information entropy for an infinite circular well. Phys. Lett. A **379**, 1402–1408 (2015)
11. Macedo, D.; Guedes, I.: Fisher information and Shannon entropy of position-dependent mass oscillators. Phys. A Stat. Mech. Appl. **434**, 211–219 (2015)
12. Zhang, X.; Feng, N.; Wang, Y.; Shen, Y.: Acoustic emission detection of rail defect based on wavelet transform and Shannon entropy. J. Sound Vib. **339**, 419–432 (2015)
13. Wu, Y.; Zhou, Y.; Saveriades, G.; Agaian, S.; Noonan, J.P.; Natarajan, P.: Local Shannon entropy measure with statistical tests for image randomness. Inf. Sci. **222**, 323–342 (2013)
14. Singh, P.K.; Cherukuri, A.K.; Li, J.: Concepts reduction in formal concept analysis with fuzzy setting using Shannon entropy. Int. J. Mach. Learn. Cybernet. **8**(1), 179–189 (2017)
15. Singh, P.K.; Gani, A.: Fuzzy concept lattice reduction using Shannon entropy and Huffman coding. J. Appl. Non-Classical Logics **25**(2), 101–119 (2015)
16. Zhou, R.; Cai, R.; Tong, G.: Applications of entropy in finance: a review. Entropy **15**, 4909–4931 (2013)
17. Yu, S.; Zhou, W.; Doss, R.; Jia, W.: Traceback of DDoS attacks using entropy variations. IEEE Trans. Parallel Distrib. Syst. **22**, 412–425 (2011)
18. Pedrycz, W.; Skowron, A.; Kreinovich, V.: Handbook of Granular Computing. Wiley, New York (2008)
19. Yao, J.T.; Vasilakos, A.V.; Pedrycz, W.: Granular computing: perspectives and challenges. IEEE Trans. Cybernet. **43**, 1977–1989 (2013)
20. Pal, S.K.; Meher, S.K.: Paper: natural computing: a problem solving paradigm with granular information processing. Appl. Soft Comput. **13**, 3944–3955 (2013)
21. Feinstein, L.; Schnackenberg, D.; Balupari, R.; Kindred, D.: Statistical approaches to DDoS attack detection and response. In: DARPA Information Survivability Conference and Exposition, 2003. Proceedings, pp. 303–314 (2003)
22. Li, Y.; Fang, B.-X.; Chen, Y.; Guo, L.: A lightweight intrusion detection model based on feature selection and maximum entropy model. In: International Conference on Communication Technology ICCT'06. **2006**, pp. 1–4 (2006)
23. Lee, T.-H.; He, J.-D.: Entropy-based profiling of network traffic for detection of security attack. In: TENCON 2009-2009 IEEE Region 10 Conference, pp. 1–5 (2009)
24. Zi, L.; Yearwood, J.; Wu, X.-W.: Adaptive clustering with feature ranking for DDoS attacks detection. In: 4th International Conference on Network and System Security (NSS), **2010**, pp. 281–286 (2010)
25. Sqalli, M.H.; Firdous, S.N.; Baig, Z.; Azzedin, F.: An entropy and volume-based approach for identifying malicious activities in honeynet traffic. In: International Conference on Cyberworlds (CW). **2011**, pp. 23–30 (2011)
26. Om, H.; Kundu, A.: A hybrid system for reducing the false alarm rate of anomaly intrusion detection system. In: 2012 1st International Conference on Recent Advances in Information Technology (RAIT), pp. 131–136 (2012)
27. Han, L.: Research of K-means algorithm based on information Entropy in anomaly detection. In: Fourth International Conference on Multimedia Information Networking and Security (MINES), **2012**, pp. 71–74 (2012)
28. Qazanfari, K.; Mirpouryan, M. S.; Gharaee, H.: A novel hybrid anomaly based intrusion detection method. In: 2012 Sixth International Symposium on Telecommunications (IST), pp. 942–947 (2012)
29. Li, H.; Wu, Q.: Research of clustering algorithm based on information entropy and frequency sensitive discrepancy metric in anomaly detection. In: International Conference on Information Science and Cloud Computing Companion (ISCC-C), **2013**, pp. 799–805 (2013)
30. Luo, Y.; Wang, B.; Sun, Y.; Zhang, B.; Chen, X.: FL-LPVG: an approach for anomaly detection based on flow-level limited penetrable visibility graph. In: International Conference on Information and Network Security, ICINS 2013, Beijing. pp. 1–7 (2013). doi:10.1049/cp.2013.2470
31. Kaur, G.; Varma, S.; Jain, A.: "A novel statistical technique for detection of DDoS attacks in KDDdataset," In: Contemporary Computing (IC3). Sixth International Conference on **2013**, 393–398 (2013)
32. Priyanka, N.; Mishra, A.; et al.: Enhanced CBF packet filtering method to detect DDoS attack in cloud computing environment. IJCSI Int. J. Comput. Sci. Issues **10**(2), 142–146 (2013)
33. Gupta, B.B.; Misra, M.; Joshi, R.C.: FVBA: a combined statistical approach for low rate degrading and high bandwidth disruptive DDoS attacks detection in ISP domain. In: 16th IEEE International Conference on Networks, 2008, ICON 2008, IEEE (2008)
34. Chhabra, M.; et al.: A novel solution to handle DDOS attack in MANET. J. Inf. Secur. **4**(3), 153–165 (2013)
35. Chhabra, M.; Gupta, B.B.: An efficient scheme to prevent DDoS flooding attacks in mobile ad-hoc network (MANET). Res. J. Appl. Sci. Eng. Technol. **7**(10), 2033–2039 (2014)
36. Gupta, B.B.: An introduction to DDoS attacks and defense mechanisms: an analyst's handbook. Lap Lambert Academic Publications, Saarbrücken (2011)
37. Gupta, B.B.; Badve, O.P.: Taxonomy of DoS and DDoS attacks and desirable defense mechanism in a cloud computing environment. Neural Comput. Appl. (2016). doi:10.1007/s00521-016-2317-5
38. Singh, P.K.; Kumar, C.A.: Concept lattice reduction using difference subset of attributes as information granules. Granul. Comput. (2017). doi:10.1007/s41066-016-0036-z
39. Singh, P.K.: Complex vague set based concept lattice. Chaos Solitons Fractals **96**, 145–153 (2017)
40. Singh, P.K.: Three-way fuzzy concept lattice representation using neutrosophic set. Int. J. Mach. Learn. Cybernet. **8**(1), 69–79 (2017)