Hybrid Technique of Pre Shared Key and Entropy Variation for DDOS Detection

Ruby Jain
Radharaman Institute of Technology and Science, Bhopal(india)

Anuraag jain
Radharaman Institute of Technology and Science Bhopal(india)

ABSTRACT
Here in this paper an effective technique for the detection of intrusion is proposed. The model is based on the hybrid combinatorial method of Pre shared key exchange and entropy variation. The data to be sent is first authenticated by the local router by comparing the shared key between them. The sender once authenticated can successfully sends the data to the receiver, but the variation of entropy is calculated based on the distance between sender and local router and if the entropy variates alarm is generated. The methodology implemented here provides high detection ratio and less false alarm rate as well as chances of attacks is reduced. The result shows the performance of the methodology, on the basis of storage, Trace back time and operation overload nearly 3-5 % enhancement in the detection of DDOS.

Keywords
Trace back, Intrusion Detection System, Entropy Variation, DDOS.

1. INTRODUCTION
With the enhancement of the network and internet various security issues also rises. Network security is a common problem now a day due to attacks and hacking. DDOS attack is also a special attack that slows down the any service via generating huge amount of fake request. This action lead large amount of traffic and slow down any service that is essential. IDS are one of the solutions to detect malicious activity and protect system against attacks. Attackers are also very clever and tried to implement new attacks. Hence betterment of security systems also required. IP trace back is a mechanism to identifying the validation of source that sends packet. It is a capacity to find out actual source of any packet sent across the Internet. Due to vulnerability of Internet design it is difficult to find the actual attacker and its location. IP trace back scheme is capable enough to identify the zombies when packets entered through DDOS in Internet [1].

Protecting networks from computer security attacks is a vital apprehension of computer security. Intrusion detection system (IDS) is a supporting system for network security. It can monitor and detect unauthorized network usages or uncharacteristic conditions without distressing network performance. IDS can be defined as tools, solution, and resources used to help identify, assess, and to claim unconstitutional or unapproved network action. IDS can monitor the network traffic and according to it generate alarms to inform misbehaviors of any nodes. An intrusion detection system (IDS) enables detection of suspicious packets and attacks. Intrusion detection techniques are traditionally categorized into two methodologies: anomaly detection and misuse detection [2].

Anomaly based intrusion detection systems based on their decisions on anomalies, belongings that do not usually occur. This type of Intrusion detection System observes the behavior of network traffic. Behavior of every node was monitored and node profile is maintained. If a node behaves apart to their normal profile then IDS find it and add this node in suspected list if this behavior continued then it generate alarm and block the activity of this node. In this scheme machine learning is quite important. Anomaly based intrusion detection systems uses the concept so that detection is done in the presence of network traffic even if it is incomplete [2].

The concept of intrusion detection uses the parameters for the classification accuracy of intrusions or anomalies. True positive rate and false positive rate denotes the accuracy of correct prediction of intrusions [3].

The figure shown below is the differentiation and classification of intrusions [4].

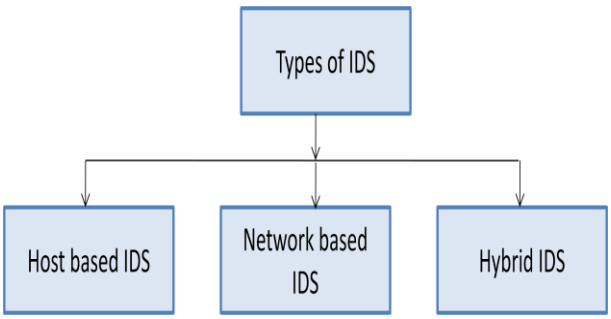

Figure 1: Types of Intrusion Detection System.

Entropy is a measure of the uncertainty in a random variable. According to information theory entropy is defined as total information available in a message. Entropy is used to calculate the total instance of value in the dataset and is used for the checking of non-linear flow of packets in the network. Entropy also defined as measure of the uncertainty associated with a random variable. Entropy is kind of summarization tool used to analyzed network traffic. It is enough capable to detect wide range of traffic anomalies, enlarging detections by volume-based techniques. For becoming aware of this detection by randomness packet size was used for transaction [5] [6]. The quantity of randomness i.e. entropy was used to perceive DDOS attack.

For the detection and classification of DDOS attack entropy is used so than the randomness of the flow of flow of packets can be computed. The entropy value is added with node profile and

randomly calculated according to network traffic and then compare with profile value. It obvious this new value is differs from previous value. This difference is known as entropy variation, on the basis of this difference it is identified that there is attack or not [5] [7].

Relative entropy is used to detect similarity of known attack set and suspected data set [8]. Due to the asymmetrical property of entropy it is not a perfect metric. Entropy variation is used to detect attacks and helps IDS to generate alarms. This concept is applied to routers. The amount of randomness is calculated when routers are on normal load. The packet transfer per unit time is known as flows. When router observes improper or unexpected flow, it calculates entropy variation and according to value of entropy variation it detects attacks. When attack is detected victim router pushback the process to identify the source of attack. The upstream routers identify where the attack flows came from based on their local entropy variations that they have monitored. This process is continued until source is traced [1].

Pre-shared key or PSK is a cryptographic scheme to provide authentication. It is like secrete sharing among sender and receiver over secure channel before use. It is a secret code used to authenticate or validate user. It is already exchange over the secure channel and before going to use it. It is a safe and well known method of authentication. The pre shared keys are in pairs, defined to provide mutual authentication and an authenticated key exchange. All considered solutions are server-less, i.e. the protocols do not require the presence of an on-line TTP. There are varieties of pre-shared keys to provide mutual authentication and authenticated key exchange [9]. Using these pre-shared keys is contributed in advance to keep away from public key operations; mainly it is useful for performance-confined situations and devices, e.g. like mobile phones and Personal Digital Assistants (PDAs). Generally three key exchange suites using pre-shared key exchange mechanism were discussed. The first suite uses only pre-shared key (PSK) mechanism, namely Plain PSK. The second suite is DHE PSK which uses a pre-shared key (PSK) to authenticate a DH key exchange. Finally, the third suite is RSA PSK which combines public key based authentication of the server using RSA and certificate with mutual authentication using a PSK [10].

Due to highly dependency on computer, computer network and Internet; large amount of private and sensitive data is stored and shared. This will lead numerous malicious attacks on node to get access of those private data. Hence security is essential to prevent from such activity. Entropy variation based detection is useful method to detect and prevent attacks. The rest of paper is organized as follows. In Section II describes about related work of trace back, entropy variation and security. Section III describes about proposed method. Section IV describes about experimental result algorithm followed by a conclusion in Section V.

2. RELATED WORK

Here in this section describes some related work trace back, entropy variation and security mechanism.

A novel method for IP trace back using information based on hypothetical constraints was proposed by Yu et al [1]. Here they classified based on data packets that are get ahead of all the way through a router into flows, which are distinct by the upstream router where a data packet came from, and the destination address of that data packet. In using those data packet they used flow of entropy variation or entropy variation exchanging. When a various type of attack was detected casualty node initiated pushback procedure to recognize the positions of zombies. On the starting point of flow entropy discrepancies victim node determined the attack tree and sent the demand to upcoming router concerning attack on that data packet. The upstream routers are acquainted with where the attack flows came from based on their local entropy variations that they have monitored. Once the instantaneous upstream routers have acknowledged the attack flows, they will forward the appeals to their instantaneous upstream routers, correspondingly, and then to spot the attacker sources additional; this method is show again in a parallel and distributed manner in anticipation of it reaches the attack source(s) or the unfairness boundary between attack flows and justifiable flows is contented [1].

This approach is primarily unusual from the subsisting PPM or DPM trace back methods and it do better than the available PPM and DPM methods. It also eradicates the problems of conventional succeed to packet marking techniques. These problems are bounded scalability, enormous requires on storage space, and susceptibility to packet contaminations. Mainly this technique can work separately as an extra component on routers for supervising and soundtrack flow information, and exchange a few words with its upstream and downstream routers when the pushback method is conceded out. This technique also efficient for expectations packet flooding DDOS attacks because it is independent of network traffic prototypes and this method can also collection of real-time trace back to network attackers. Once the temporary flow information is in position at routers, and the victim node become aware of that it is underneath attack, it will establish the trace back process. The workload of trace back Is distributed among all the networks and the on the whole trace back time for the most part depends on the network delays between the victim node and the network attackers. Along with this experimental analysis and simulations confirmed that this trace back mechanism is efficient and capable of tracking attackers [1].

In this paper author Singh et al [5] proposed a new method for detecting of DDOS attacks in the network using Entropy Based Anomaly Detection Algorithm. Here author has calculated the value of entropy with respect to time and packet windows. Entropy is calculated with the intention of detect the DDOS attack in a network. Entropy is calculated using given formula:

$$\mathbf{H(x)} = -\sum_{\mathbf{i=1}}^{\mathbf{n}} (\mathbf{p_i}\ \mathbf{\log_2 p_i})$$

where pi is the value of probability.

DDOS detection line of attack aspires at detecting DDOS attacks in the network using Entropy Based Anomaly Detection Algorithm. With the intention of detect the attack in the network, two different come within reach of are used. Here they firstly calculated entropy concerning with time window is estimated and in the second come up to the entropy concerning with packet window is calculated. When using the time window approach, entropy of the network traffic is calculated as regards equal time stamps and when they are using in the packet window approach equal numbers of flowing packets are taken from network traffic to calculate the entropy [5].

An entropy-based technique is proposed to identify network attack by Liu et al [6]. Here author has suggested the Shannon entropy and Renyi cross entropy are make use of to analyze the distribution features of alert characteristics and to become aware of network attack. When the network observed runs in standard way the entropy values are comparatively smooth in the given network or else, the entropy value of one or more quality would transform. The Renyi cross entropy of these features is computed to calculate the network condition and identify network attacks. Here the Renyi cross entropy is used to fuse the

Shannon entropy of five statistical characteristics to detect the network attack. And the experimental results illustrate that this technique can detect network attack rapidly and correctly [6]. Vincenzo Caglioti [7] offered a formalization of the difficulty of choosing sensor measurements differentiated by minimum outstanding insecurity about the state of an examined system explained both by continuous ones and by discrete variables.

The system under observation can be described by only continuous variables; a set of possible criteria can be defined as a function of the variance of the continuous state variables. This criterion is applied to recognition and localization tasks: an a priori description is supposed to be available of the state of a system constituted by an object. They offered an information–theoretic criterion which combines the uncertainty relative to the localization with the uncertainty relative to the recognition [7]. Relative entropy is connected with learning to optimize in a more general context. For every possible string of outcomes the sequence of likelihood ratios between the agent's belief and the truth were considered. They used this sequence to define the agent's relative entropy. They show that if the relative entropy is close to zero, then, in the long run, the payoff to a patient agent is almost equal to the payoff generated by the true optimal strategy. They also try to identify conditions on the relation between the belief and the truth that ensure optimality in the long run [8].

In this paper author Hoeper and Gong has build up ID-based protocols that use pre-shared keys KAB to make available mutual authentication and an authenticated key exchange method. Here they investigated what kinds of security properties are practicable by such a lightweight protocol. Calculation more security properties necessitates the accomplishment of asymmetric procedures such as ID-based public key encryption; ID-based signatures or DH-like key agreements which unsurprisingly enhance the computational complication of the protocols.ID-based methods do not have need of an on-line certification authority (CA) to take action to get certificate queries as required in PKI systems. Subsequent to an initialization phase the certification authority does not need to be easy to get to by the network nodes any extensive. And the second possessions help to decrease the have need of bandwidth of given network protocols. Here they suggested using ID-based pre-shared keys as an alternate of symmetric keys in secure protocols to keep away from the difficulty of an initial key distribution selection [9]. At author Kuo et al [10] proposed an efficient study and concert evaluation between the pre-shared key exchange methods and the standard public key exchange methods in TLS. In addition the communication of the taken as a whole TLS handshake period and the networking environment is appraised. Experimental results for unusual key exchange methods are moderately calculated and the propose alternatives of pre-shared key supported key exchange methods have been authenticated. Experimental results give features concerning to show the get better of the pre-shared key based methods measure up to the typical public key based method [10].

3. PROPOSED ALGORITHM

The proposed methodology includes the following set of steps for the detection of intrusions in the dataset.

1. Initially set up a network with no. of sender of local routers between them and pre shared key between them which needs to be exchanged for authentication.
2. For 'N' number of packets send from source 'S' to Destination 'D'.
3. The local router 'R' checks the authenticity of the Source 'S'.

Algorithm for Pre shared Key Exchange & Authentication

a. For each 'pkt' to be send from 'S' → 'R'
b. Router 'R' → 'S' responds to Source to exchange the shared key.
c. Source 'S' → 'R' responds to router his key.
d. On the basis of key of Source 'S' router generates Random No. for the Source 'S' and send via secure channel 'C'.
e. The Source 'S' then generates Master Key through Random number and send to Router 'R'.
f. Router checks and verifies the Master Key generated.
g. If 'S' fails to authenticate, an alarm is generated for the Source and blocked.

4. If Source is valid user then entropy of the message can be computed by the other router 'R2'.

Algorithm for Entropy variation

a. If 'N' number of packets send from 'R' → 'R2.
b. Repeat for all packets 'pkt'
c. En=calculate_entropy('pkt')

Pseudo Code for Entropy Variation

```
Calculate_entropy("pkt")

for (int c_ = 0; c_ < s.length(); ++c_) {
    char cx = s.charAt(c_);
    if (occ.containsKey(cx)) {
      occ.put(cx, occ.get(cx) + 1);
    } else {
      occ.put(cx, 1);
    }
    ++n;
double p = (double) entry.getValue() / n;
    e += p * log2(p);
```

d. If En > threshold value
e. Alarm for the tracing of packet attacker is generated
f. Else
g. No alarm is generated
h. End

4. SIMULATION RESULT

The table shown below is the analysis of DDOS trace back using Entropy variation and proposed methodology. The analysis is done on the following parameters as Storage, Trace back time and Operation Workload.

Table 1. Analysis on various Parameters

	Existing Work	**Proposed Work**
Storage	Very High	Very low
Trace back Time	Network Delay	Low
Operation Workload	very low	very low

The Table shown below is the comparison of Entropy variation on the number of flows.

Table 2. Comparison of Entropy Variation

	Entropy Variation	
No. of Flows	**Existing work**	**Proposed Work**
100	4.4	5.73
200	5.2	7.18
300	5.6	7.42
400	5.8	7.82
500	6	8.32
600	6.3	8.52
700	6.4	8.71
800	6.5	8.84
900	6.7	9.2
1000	6.9	9.64

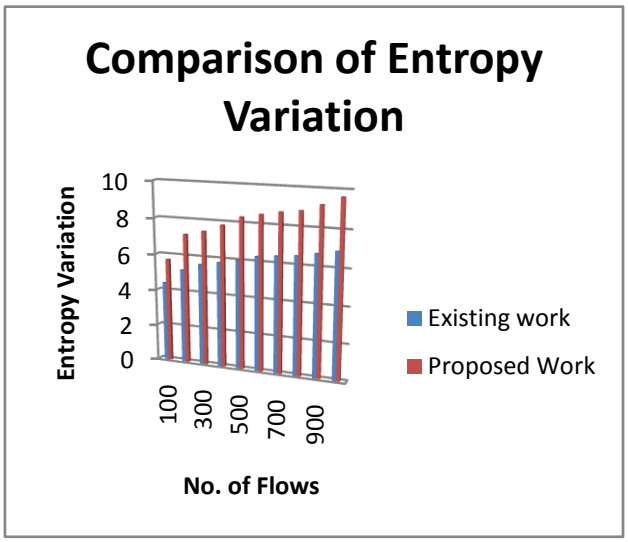

Figure 2. Comparison of Entropy Variation

Table 3. Comparison of Entropy Vs Strength of Attacks

	Entropy Variation	
Strength of Attacks	**Existing Work**	**Proposed Work**
100	6.3	6.8
200	5.8	6.2
300	5.2	5.7
400	4.9	5.4
500	4.6	5.1
600	4.3	4.9
700	3.6	4.5

The figure shown below is the comparison of strength of attacks on the basis of entropy variation for existing and proposed work.

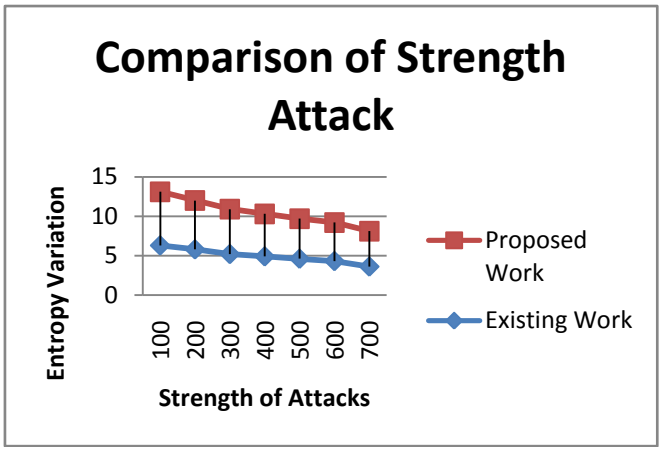

Figure 3. Comparison on Strength of Attacks

5. CONCLUSION AND FUTURE WORK

This paper proposed a novel method for optimization of detecting intrusion in the web log data on the basis of pre shared exchange of keys between sender and local router and the by checking the entropy variation of message. The proposed methodology implemented here is feasibly for large datasets also and provides high alarm rate and accuracy of detecting intrusions.

6. REFERENCES

[1] Yu, Shui, Wanlei Zhou, Robin Doss, and Weijia Jia. "Trace back of DDOS attacks using entropy variations." IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 3, pp. 412-425, 2011.

[2] Baig, Zubair A., Sadiq M. Sait, and AbdulRahman Shaheen. "GMDH-based networks for intelligent intrusion detection", ELSEVIER Engineering Applications of Artificial Intelligence, vol. 26, issue 7, pp. 1731–1740, 2013.

[3] Yuebin Bai and Hidetsune Kobayashi "Intrusion Detection System: Technology & Development", Proceedings of the IEEE 17th International Conference on Advanced formation Networking and Applications (AINA'03), pp. 710 – 715, 2003.

[4] Sonawane, Sandip, Pardeshi, Shailendra and Prasad, Ganesh "A survey on intrusion detection techniques World Journal of Science and Technology, vol. 2, issue 3, pp.127-133, 2012.

[5] Singh, Jaswinder, Sachdeva, Monika And Kumar, Krishan "Detection of DDOS Attacks Using Source IP Based Entropy", International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR), ISSN 2249-6831, Vol. 3, Issue 1, pp. 201-210, Mar 2013.

[6] Liu, Ting, Zhiwen Wang, Haijun Wang, and Ke Lu. "An Entropy-based Method for Attack Detection in Large Scale Network." International Journal of Computer Communication, vol. 7, no. 3, pp. 509-517, 2012.

[7] Caglioti, Vincenzo. "An entropic criterion for minimum uncertainty sensing in recognition and localization. I. Theoretical and conceptual aspects." IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics, vol. 31, no. 2, pp. 187-196, 2001.

[8] Lehrer, Ehud, and Rann Smorodinsky. "Relative entropy in sequential decision problems." Journal of Mathematical Economics, vol. 33, no. 4, pp. 425-439, 2000.

[9] Hoeper, Katrin, and Guang Gong. "Identity-based key exchange protocols for ad hoc networks." In Proceedings of the Canadian Workshop on Information Theory (CWIT'05), pp. 127-130. 2005.

[10] Kuo, Fang-Chun, Hannes Tschofenig, Fabian Meyer, and Xiaoming Fu. "Comparison Studies between Pre-Shared Key and Public Key Exchange Mechanisms for Transport Layer Security (TLS)." Institute for Informatics, University of Goettingen, Technical Report IFI-TB-2006-01, 2006.