Neuro-fuzzy-based clustering of DDoS attack detection in the network

Kumarasamy Saravanan

Erode Sengunthar Engineering College,
Thudupathi, Erode 638057, Tamil Nadu, India
Email: saravanankumarasamy@gmail.com

Abstract: The detection system developed for wired networks cannot be deployed in wireless networks due to the difference between the two types of networks. The data transmission of the wired network is a standard physical routing. However, the data stream routing of wireless network are based on radio signals with a variety of problems of evolution. The attacker's packet header data are acknowledged with a port number, option field parameters and IP address. The anomalies detection is carried out at a regular interval to monitor the traffic analysed through statistical variance. The change detection detects the statistical variance of the traffic volume. The results obtained from the proposed system are compared with the existing attack detection systems with the propagation delay metric. It shows a reduction of nearly 10% and an improvement of 13% average throughput.

Keywords: attack; MAC frames; fuzzy system; DoS attack; clustering; DDoS attack.

Reference to this paper should be made as follows: Saravanan, K. (2017) 'Neuro-fuzzy-based clustering of DDoS attack detection in the network', *Int. J. Critical Infrastructures*, Vol. 13, No. 1, pp.46–56.

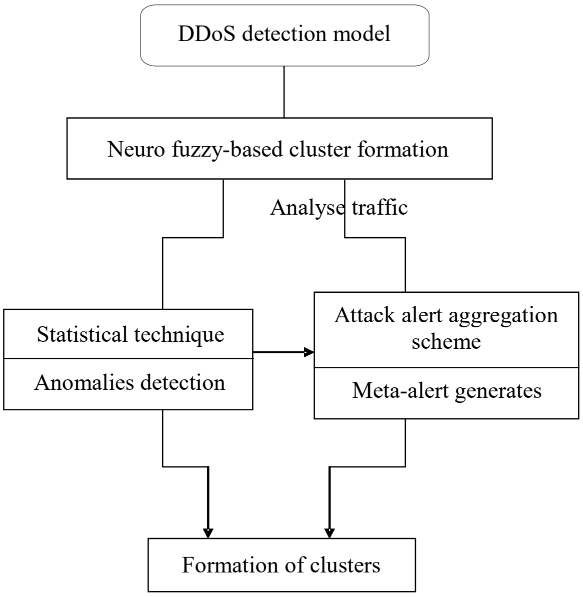
Biographical notes: Kumarasamy Saravanan received his PhD degree in Information and Communication Engineering from Anna University, Chennai, ME degree 2008 in Computer Science from MCET, Anna University, Chennai, India. He is currently working as an Assistant Professor at the Faculty of Engineering, Erode Sengunthar Engineering College, Erode, Tamilnadu. He published 24 papers in international journal, 16 papers in national conference and eight papers in international conference. His current research interests are information security, computer communications and DDoS Attacks.

1 Introduction

The anomaly cluster and normal clusters are measured by the distance-based values from the anomaly traffic data aggregated values. On the other hand, regular deviations on the data propagation modify the traffic data packets influenced by scrupulous nodes polluting the normal data packets (Bhuyan et al., 2012). To establish the cluster of improper data aggregation traffic has to be made the alternate changes in the propagation data.

To overcome the deficiency of improper traffic data clustering, a more interpretable and accurate model of neuro-fuzzy is introduced to generate anomaly interrupt data packet clusters and normal data clusters from the traffic data streams (Buchtala et al., 2005). The fuzzy logic rules enable the cluster objects to appropriate clusters with test data of the traffic streams detected with statistical anomaly traffic attack detection model. In this regard, the neural network is used to recognise the normal and anomalous data field patterns with an advanced accuracy rate (Saravanan and Asokan, 2012; Smitha and Reddy, 2001).

Figure 1 Combined network DDoS attack detection model



The proposed work presents both wired and wireless network DDoS attack detection models based on neuro-fuzzy-based cluster formation which efficiently detects non-interrupt packets. The detection is identified through statistical technique of the network traffic data in both networks. This helps detect anomalies and attack alert aggregation by way of traffic data. Traffic is analysed through statistical technique which is used to generate meta-alerts from the statistical anomaly attacker traffic data. Figure 1 explains the proposed system; DDoS attack detection of the neuro-fuzzy model. The DDoS attack detection of the neuro-fuzzy model is carried out. To evaluate the performance of neuro-fuzzy-based cluster formation for both wired and wireless networks it is necessary to work in terms of DDoS attack detection Rate, throughput and propagation delay.

2 Statistical anomaly DDoS attack traffic detection model

The traffic sources generated from the servers and client communication spread across the network. The implementation of the detection model helps detect the attacks at the source network using traffic monitoring of the DDoS attack which evade the rules of network access. In addition, the attacker traffic generated from the traffic sources is compared to the standard traffic to detect the anomalous traffic occurring in the network. The anomalous DDoS attack traffic propagated is measured through statistical analysis by comparing the load demand ratio of the standard traffic to the traffic generated at certain instances in the network (François et al., 2012; Garg and Reddy, 2002).

The traffic load demand analysis is carried out with the characteristics of data flow across the network. The traffic source analysis reveals the frequency dynamics for the temporal of the scaling properties concurrently unlike other data transformation techniques like Fourier transform. The statistical anomaly attack traffic detection model utilises the statistical properties using multi-variant distribution approach used to correlate the data traffic applied at several timescales (Saravanan and Asokan, 2011).

The network transfer data sources create the sampling points due to statistical data transformation. The normal traffic and abnormal traffic are detected in certain timescales which comprise the frequency of data transfer rate variance. In certain other positions of the timescales, mean temporal information is deduced for detecting the anomaly traffic attacks (Subhadrabandhu et al., 2006).

The statistical data transformation of the one-dimensional multilevel traffic data replica iterates capability of six levels analysis. The detected time-stamped traffic data sources are deduced to lower levels of traffic characteristics, till the anomaly traffic attack associated with the definitive property is identified. Each level signal has to be affected that two times for the expansion of the sampling interval. The detection system uses '*t*' minutes as sampling interval, '*j*' as the time range at a level the traffic source detection for anomaly attack detection spans at $t * 2^j$ minutes. This traffic data samples autonomously carry the time range; it can reinstate the frequency of traffic data statistically.

3 Neuro-fuzzy-based clustering technique

Neuro-fuzzy-based clustering technique for anomaly attack detection comprises the following phases: collecting the detected anomaly attacks from statistical traffic analysis and alert generation, data stream of alert aggregation and clustering and these are shown in Figure 2.

3.1 Collection of detected anomaly traffic and alert generation

In this phase, the detected anomaly attacker traffic source resulting from the statistical traffic analysis is first collected and stored with its actual characteristic of traffic data. The collections of detected alerts acquire the characteristics of incoming data from both the networks. To construct an appropriate event through the incoming data collection, this information extracted offer exciting and valuable potential (Saravanan et al., 2014; Wei et al., 2013).

The detection of anomaly DDoS attack assesses the attack procedures for suspicious behaviour and seeks out known attack signatures. If the attack behaviour is suspicious, it is collected from detected anomaly attack and creates alerts and forwards them to the alert generation. At the alert generation phase, the accumulation of alert combines the alerts and makes them specific to an attack instance or type as shown in Figure 3.

Figure 2 Neuro-fuzzy-based clustering technique for anomaly DDoS attack detection

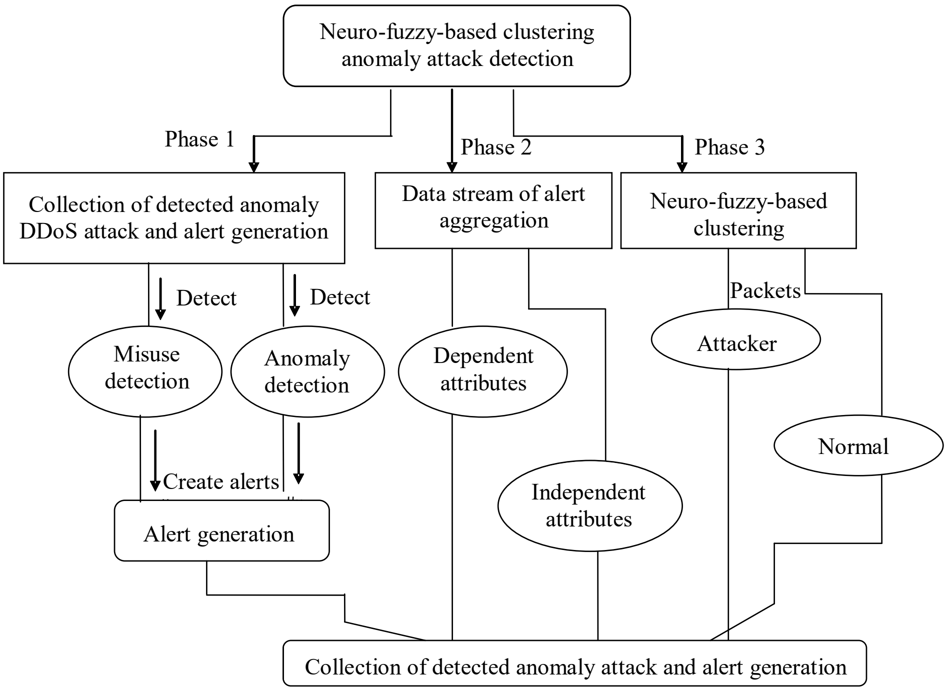
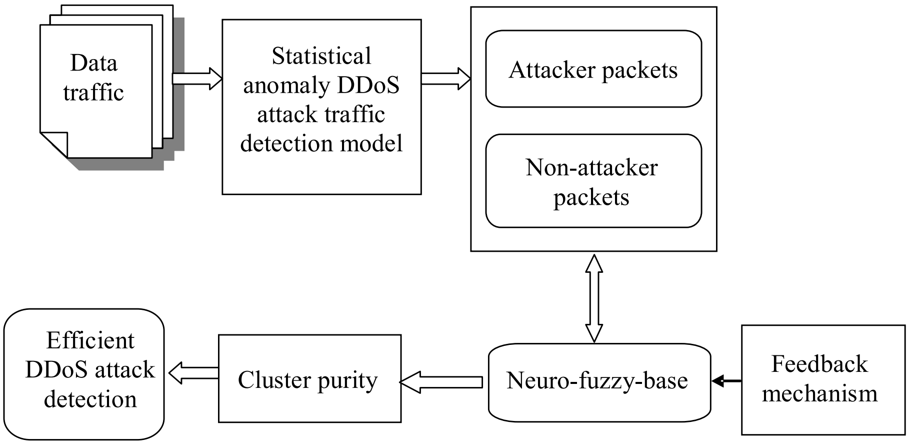

Neuro-fuzzy-based clustering anomaly attack detection
Phase 1
Phase 2
Phase 3
Collection of detected anomaly DDoS attack and alert generation
Data stream of alert aggregation
Neuro-fuzzy-based clustering
Detect
Detect
Packets
Misuse detection
Anomaly detection
Dependent attributes
Attacker
Normal
Create alerts
Alert generation
Independent attributes
Collection of detected anomaly attack and alert generation

Figure 3 A working model of neuro-fuzzy-based clustering for anomaly DDoS attack detection



3.2 Data stream alert clustering

Based on the format, alerts are aggregated. Using the attribute values alert aggregation produces the input for alert clustering. The specific attacks are measured by the classification of the traffic data attributes in the independent event. Thus the traffic data attributes are reliant on the attack instance and the alert aggregation method is applied to discriminate the attack instances at different levels.

3.3 Neuro-fuzzy clustering model

The proposed work has implemented the neuro-fuzzy-based clustering technique for a detection system. The fundamental insufficiency of clustering is used to initiate the value of K, a number which computes the count of clusters to be formed. This classification is done by applying the neuro-fuzzy clustering technique to deal with two segregations as normal and abnormal, in which K is assigned to two values. By using this feature of DDoS attack as a criterion, this work considers the partition model. Figure 3 shows the proposed model of neuro-fuzzy-based clustering technique. It can consider the volume of attack packets in such a way that it is less than that of normal packets. The investigation shows the inherent nature of these attack packets and provides a clear picture of the factors that signify the abnormality. Subsequent to these partitions being made, every field in the normal and abnormal clusters is investigated to recognise its characteristics. This knowledge helps to distinguish the regular from the irregular ones.

Neuro-fuzzy-based clustering technique is measured for the minimisation of the following objective function, with respect to ‘Q’, a fuzzy partition of the data traffic and to ‘R’, a set of ‘L’ prototypes as shown in equation (3.1).

$$Dy(Q, R) = \sum_{z=1}^{l}\sum_{y=1}^{d} Q_{yz}^{o} \left\| N_y - R_y \right\| \tag{3.1}$$

where Q_{yz}^{o} is a membership of N_y in the cluster Dy between 0 and 1; where o is any real number greater than 1; N_y is the Y^{th} d-dimensional measured input data; DDy is the centre of fuzzy cluster Y; $fe_{yz} = \|N_y - R_y\|$ is the z^{th} point and y^{th} cluster centre are the measured the Euclidean distance and $X \in (1, \infty)$ is a weighting exponent.

There are two necessary conditions for C to reach a minimum as shown in equations (3.2) and (3.3).

$$DDY = \sum Q_{yz}^{O} N_z \tag{3.2}$$

$$N_y = \sum Q_{yz}^{O} \tag{3.3}$$

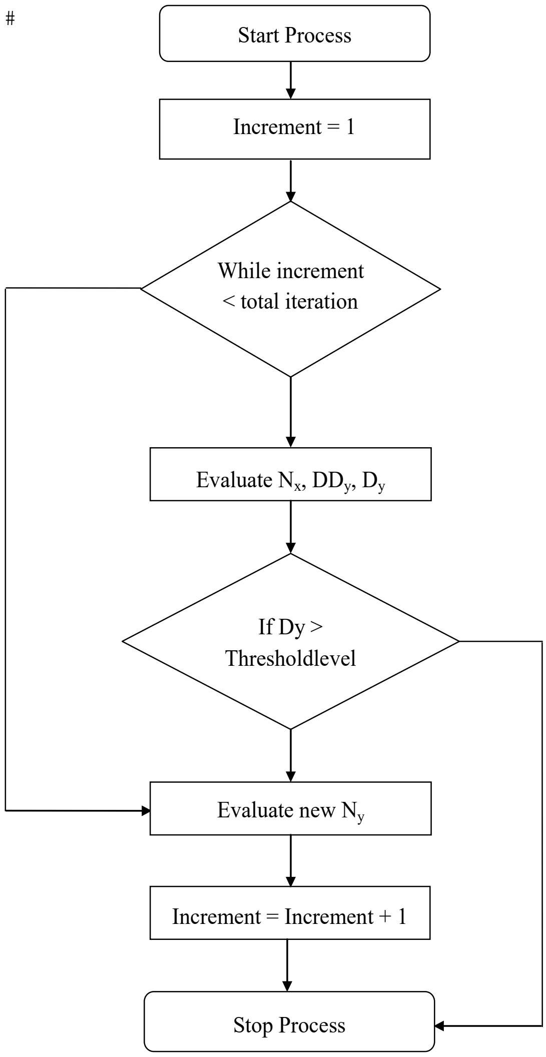
where $y,z = 1,2,3\ldots l$.

$$Q_{yz} = \frac{1}{\sum_{l=1}^{d} \left[\frac{fe_{yz}}{fe_{yl}} \right] \cdot \frac{2}{x-1}} \tag{3.4}$$

$$R_y = \frac{\sum_{z=2}^{l} Q_{yz}^{o} N_y}{\sum_{z=2}^{l} Q_{yz}^{o}} \tag{3.5}$$

The measures in this iteration will stop when $\max, |Q_{yz} - \hat{Q}_{yz}| < \varepsilon$, where ε is a termination measure between 0 and 1. The maximum number of iteration routines shown in equation (3.4) can be used as a termination measure. An illustration of the pseudo-code and the flow chart for the aforementioned process are shown in Figures 4 and 5 respectively.

Figure 4 Neuro-fuzzy-based clustering for anomaly DDoS attack detection



Neuro-fuzzy-based clustering determines the cluster centres DD_Y and the membership matrix D_Y using the aforesaid pseudo code. Initially the membership matrix M_X is computed. Then for each M_X, the cluster centers DD_Y is calculated using equation (5.1). The equation (5.1) is used to calculate the objective function. The iteration will be stopped if its progress over the prior iteration is below a certain threshold or it is below a certain threshold level. Otherwise a new N_Y is computed. The cluster centres can carry the iterative procedure, initialised alternatively.

4 Simulation of cluster-based statistical anomaly DDoS attack detection

The network traffic collected from ISP servers through traffic data is real time of the both wired and wireless networks, the neuro-fuzzy-based clustering for anomaly attack traffic detection is implemented the in NS2 simulation. The samples are taken from the NetCon Server, which has a number of connections, changeable from 256 kbps to 2 Mbps of the traffic rate. The one month period of the broad band link 10 Mbps is connects the real trace of samples which comprise of the network servers. The need for anomaly traffic detection in the combined wired and wireless networks are done by the traffic data with statistical characteristics through the clustering of meta-alert. The relationship of the sealed IP prefix and MAC of the traces are anonymous.

The performance evaluates carrying the simulation such as communication overhead and accuracy detection of the proposed scheme. As the node counts are gradually increased to obtain the throughputs, attack detection rate and propagation delay. Field size of 800 × 800 m is used for simulation where 90 nodes are distributed uniformly. Single stationary source and single stationary sink is placed on conflicting, between 3 to 4 hops. The data transmission of the packets can be sent hop-by-hop at 15 kbps. These simulation events carry every two seconds sending one report and the sources develop 600 reports in total. The retransmission mechanism follows the hop-by hop transport layer which helps to formulate the scheme for poor radio conditions.

5 Performance result and discussion

The simulation deploys different data communication located to reveal the probability of statistical integration with anomaly attacker model of the cluster-based detection system. The investigation simulates a small confidential data site through a number of weeks of working out, test data having been generated. In the wireless and wired networks situation, the network data traffic are generated and analysed for detection of characteristics of the DDoS attack.

Figure 5 Performance of throughput with and without neuro-fuzzy clustering techniques for wired network (see online version for colours)

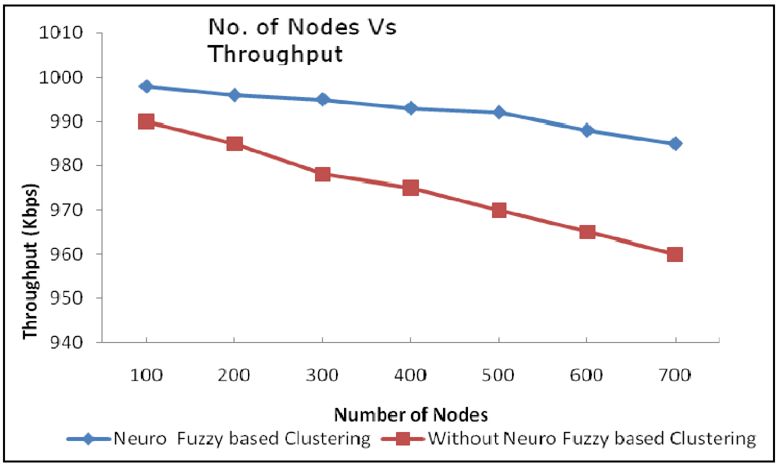


Figure 5 depicts the network traffic simulation of the outperformance for the number of nodes variations, which is based on the wired network. When the throughput decreases, the number of nodes increases. Experimental results show that the proposed new way DDoS attack detection using neuro-fuzzy-based clustering technique and its anomaly-based detection outperforms others because it ensures an effective and uninterrupted communication from source to the destination by enabling the users to choose the best detection for transmission.

Figure 6 Performance of throughput with and without neuro-fuzzy clustering techniques for wireless network (see online version for colours)

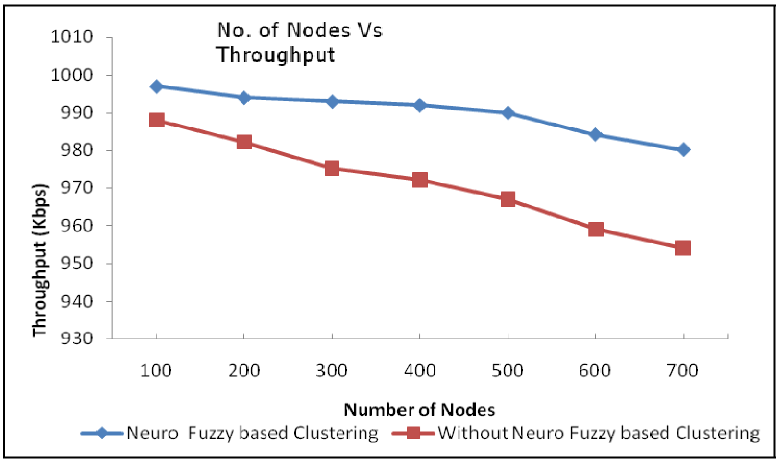
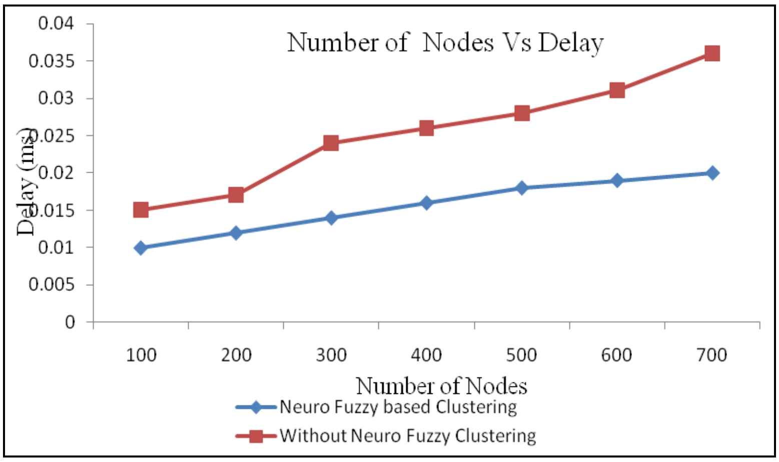


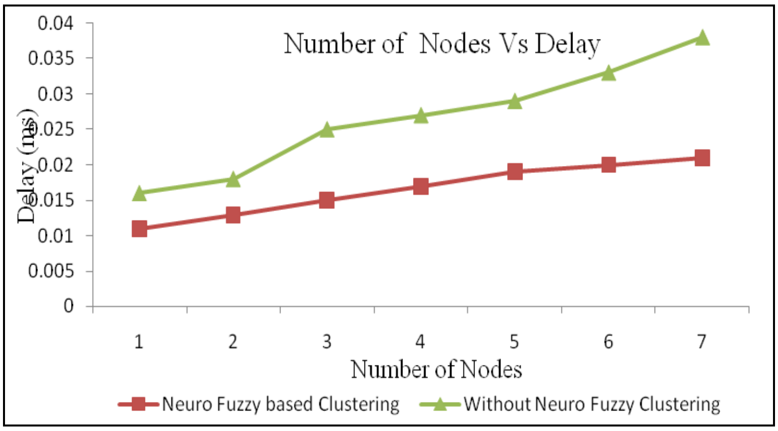
Figure 6 depicts the wireless network of the simulation that outperforms the network traffic based on varying number of nodes. The data communication of the network marks a considerable change in the throughput. The QoS-based throughput decreases and the number of nodes increases. It is proven that the neuro-fuzzy-based clustering for both wired and wireless network anomaly DDoS attack detection outperforms the other methods.

Figure 7 Performance of propagation delay for wired network (see online version for colours)



It can be observed from Figure 7 that delay variations of legitimate traffic are very minimal during heavy attacks and the neuro-fuzzy based on clustering detection system is seen to perform far better than K-means clustering detection system as many attack packets are rerouted via longer paths enabling legitimate traffic to utilise QoS paths. It is evident from the results that QoS regulates the traffic based on legitimate requests within the agreed service. The better traffic management is based on the large amount of jitter which is an indication of an abnormal situation and small amounts of jitter qualify.

Figure 8 Performance of propagation delay for wireless network (see online version for colours)



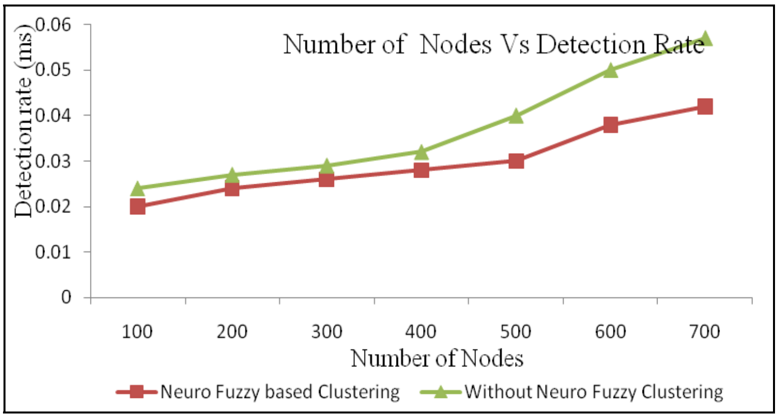
The analysing of simulation result based on the propagation delay, affecting the node variation is illustrated in Figure 8. When the number of nodes increase, the propagation delay increase in the nameless traffic network. This indicates that the proposed neuro-fuzzy system clustering technique establishes a better result. A large amount of jitter is an indication of abnormal situation and small amounts of jitter qualify for better traffic management.

The performance variations are recorded as in this scenario, under heavy attacks and there is a marked performance improvement with delay as well as jitter (nearly 80% reduction) parameters of legitimate traffic which indicates that the legitimate traffic is routed through fairly better paths compared to attack packets in neuro-fuzzy-based clustering detection system. The study proves that it performs far better than K-means clustering detection system.

The detection rate is found to outperform neuro-fuzzy-based clustering detection model in detection rate. The performance of the detection rate is tested with different types of attacks over various services and the result is plotted in Figure 9. It is observed that the web data generated has related patterns compared to K-means clustering anomaly detection system data and hence they are well-detected by this model.

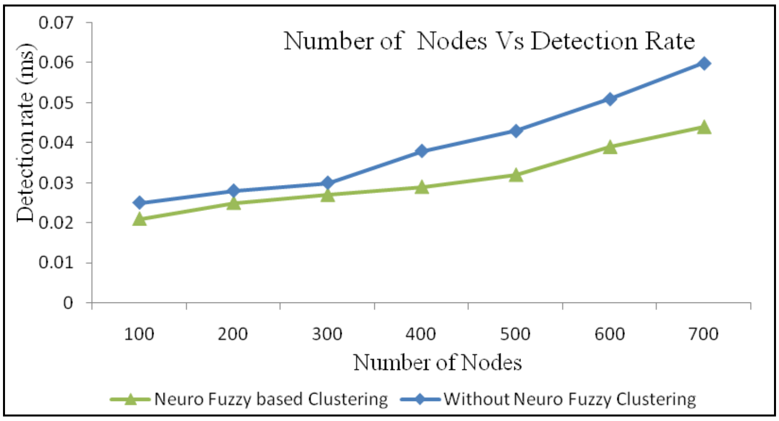
The percentage assessment obtained with K-means clustering using anomaly detection method is 20%–35% greater than the existing detection process due to the fact that neuro-fuzzy-based clustering using anomaly detection identifies the best detection method in the network. Finally, it is observed that the neuro-fuzzy-based clustering using anomaly detection performs better in relation to other detection systems.

Figure 9 Response time of detection rate for wired network (see online version for colours)



The performance graph as in Figure 10 shows that the neuro-fuzzy-based clustering technique detection system has achieved the higher response time for the rate of detection both in the wired and wireless networks. The proposed neuro-fuzzy-based clustering technique detection system is higher in performance than the enhanced K-means clustering for DDoS attack detection method. The improvement of the response time is almost 20% to 35% of the wireless network of the anomaly detection in the network traffic data.

Figure 10 Response time of detection rate for wireless network (see online version for colours)



6 Conclusions

In the proposed work, the wired and wireless networks are measured by way of capacity demand load of ISP server for improved detection of the anomaly DDoS attack in the deep traffic times. Neuro-fuzzy-based clustering technique has been implemented to form the cluster and to provide cluster purity to improve the performance of the proposed DDoS attack detection in both wired and wireless network. Simulations are conducted using the NS2 simulator for different data sets to evaluate the performance of neuro-fuzzy system cluster formation for combined wired and wireless network DDoS attack detection model. The simulation results showed that the neuro-fuzzy system clustering technique performs better in terms of detection Rate, throughput and propagation delay.

References

Bhuyan, M.H., Kashyap, H.J., Bhattacharyya, D.K. and Kalita, J.K. (2012) 'Detecting distributed denial of service attacks: methods, tools and future directions', *Computer Journal*, December.

Buchtala, O., Grass, W., Hofmann, A. and Sick, B. (2005) 'A distributed intrusion detection architecture with organic behavior', *The First CRIS International Workshop on Critical Information Infrastructures (CIIW'05)*, Linkoping, Sweden, pp.47–56.

François, J., Aib, I. and Boutaba, R. (2012) 'FireCol: a collaborative protection network for the detection of flooding DDoS attacks', *IEEE/ACM Transactions on Networking*, Vol. 20, No. 6, pp.1828 –1841.

Garg, A. and Reddy, A.L.N. (2002) 'Mitigation of intrusion attacks through QoS regulation', *Proceedings of 10th International Workshop on Quality Service*, Miami Beach.

Saravanan, K. and Asokan, R. (2011) 'Distributed denial of service (DDoS) attacks detection mechanism', *International Journal of Computer Science, Engineering and Information Technology (IJCSEIT)*, December, Vol. 1, No. 5, pp.39–49, DOI: 10.5121/ijcseit.2011.1504.

Saravanan, K. and Asokan, R. (2012) 'An efficient detection mechanism for distributed denial of service (DDoS) attack', *International Journal of Electronics Communication and Computer Engineering*, December, Vol. 3, No. 6, pp.1281–1285.

Saravanan, K., Asokan, R. and Venkatachalam, K. (2014) 'Detection mechanism for distributed denial of service (DDoS) attacks for anomaly detection system', *Journal of Theoretical and Applied Information Technology*, February, Vol. 60, No. 1, pp.174–178.

Smitha, K.I. and Reddy, A.L.N. (2001) 'Identifying long term high rate flows at a router', *Proceedings of 8th international Conference on High Performance Computing*, *Lecture Notes in Computer Science*, Hyderabad, India, December, Vol. 2228, pp.361–371.

Subhadrabandhu, D., Sarkar, S. and Anjum, F. (2006) 'A statistical framework for intrusion detection in ad hoc networks', *IEEE INFOCOM*, Barcelona, Spain.

Wei, W., Chen, F., Xia, Y. and Guang, J. (2013) 'A rank correlation based detection against distributed reflection DoS attacks', *IEEE Communications Letters*, Vol. 17, No. 1, pp.173–175.