International Journal of Systems Signal Control and Engineering Application 9 (2): 17-23, 2016
ISSN: 1997-5422

Offering a New Method for Detection of Flood Attacks in Voice Transmission Networks on the IP

Farid Bavifard
Islamic Azad University, Ahwaz, Khoozestan, Iran

Abstract: Now a days, the voice transmission technologies on the networks based on the IP (VOIP) has become one of the most widely used technologies in telecommunications due to lower costs and more flexibility. These networks due to variation of supporting VOIP terminals are vulnerable in terms of security and against several attacks such as lack of service, worms, DoS and DHCP attacks and etc. After attacking prevention methods, such as encryption, one of the conventional methods for securing VOIP is using Intrusion Detection Solutions (IDS) which include misuse detection methods and methods of detecting abnormal behavior. One area of concern in the designing the intrusion detection systems is machine learning and data mining. On the other hand, intrusion detection systems work with large volumes of data that include additional features and this, slow down and thus reduce the efficiency of the training and testing process. For this reason, feature selection, as one of the key issues of intrusion detection systems, includes finding a subset of more efficient features to improve the accuracy of prediction. In this study a method is proposed in four phases, to identify the best available features for intrusion detection and use them to design a compound classifier in order to detect the attack packets to the network. The results of the proposed simulation method is indicative of a 99.73% accuracy in detecting attacks.

Key words: Intrusion Detection Solution (IDS), the combination of feature extraction methods, combining the expertise, unsupervised neural network, Iran

INTRODUCTION

Application VOIP is an integrated program that runs on the IP protocol and includes protocols for Voice over Internet transmission. In the PSTN phone service voice passes the circuit switched substrate in the analog form while in the VOIP service passes through packet switching network substrate in digital form. Users, due to lower costs and flexibility of internet telephone service have migrated from PSTN architecture to packet-based architecture. The use of Internet phone system on the network (VOIP) has been vastly developed during the recent years.

On the other hand, with the advent of IP, Packet-Switched Networks have replaced the traditional circuit switches (PSTN). Therefore, this service, in addition to withstanding the attacks specific to cellular and fixed networks telephony and, etc. should also be protected against specific threats of IP networks. Thus, security, compared to other areas is one of the most challenging issues in VOIP. With the growing attacks on computer networks and the expansion of threats to these networks, protecting the privacy of the networks with a focus on major approaches such as encryption and intrusion detection and prevention has been specially addressed. In spite of major developments in the design of encrypting systems, designing the intrusion detection systems is also becoming an important research field in computer networks in terms of security problems.

A software or hardware intrusion detection system, by monitoring the network and identifying disruptions or violates against the security and management policies, reports such cases to the network management and its objective is only the identification and detection of the attacks and security bugs in the network. In fact, 3 general task of such systems are: assessment and monitoring, intrusion detection and responsiveness. These systems are responsible for detection of any unauthorized use of computer networks, misuse, damage and attack by trusted users (domestic), non-trusted users (external), inexperienced attackers and experienced users.

Two main methods for intrusion detection include the detection of cases of abuse (by matching the current network model with known attacks) and diagnosing abnormalities (with modeling the normal behavior of network and identifying deviations from it). Since the first approach needs to keep the attacks database and it is not beneficial in most of the networks, the second approach is often used and the recent studies have been inclined to production of the smart intrusion detection systems.

One of the main approaches of infiltrators is the use of the flood attacks, in which large volumes of traffic are sent to the victim machine in order to occupy its bandwidth that cause it slow down or crash (for example in UDP Flood Attack or ICMP Flood Attack it leads to the saturation of the network bandwidth.

The principles and basic concepts: Hacking a network is a non-authorized attempt to access, modify or extract data in an unreliable or unusable form. The intruder can be domestic or foreigner. By Bace and Mell (2001), the most important factors affecting the intrusion are introduced as follows:

- The attackers who want to have access to important information through the internet
- The authorized system users who want to have the advantages they are not allowed to
- Virtual users that want to take advantage of defined benefits for themselves

In most cases, an attack is carried out using or creating a breach in the security system of an organization. Most organizations may use tools for securing network which due to flaws and security bugs, make the attack easier for the attacker. Other means to intrude is to create unconventional outbound traffic. An intruder by using trial and error and even unsuccessful intrusions, tries to gain control of the target computer. The intrusive operation increases the typical network traffic and it is a sign of a coming attack. Another approach of an intruding agent could be creation of disharmony in order to send and receive information. Any traffic mismatches in the packets or any leakages can be a sign of a hidden attack (Zhang *et al*., 2006).

Intrusion detection system: According to Henry and coauthors an intrusion detection system, the sabotage and infiltration taking place on the network and host which have not been identified by other security solutions, have been detected and presented. These systems, in terms of application method, the place of installation and the host or network protecting them are of the following types.

Host based Intrusion Detection System (HIDS): This system is implemented on the host system controlling all the activities and processes within it and protecting it against the malicious infiltration (Scarfone and Mell, 2012).

Network-based Intrusion Detection System (NIDS): This system by acting on the field of network and monitoring and analyzing the network traffic at all layers, tends to discover signs of intrusion or attack (Scarfone and Mell, 2012).

Distributed Intrusion Detection System (DIDS): These systems often act based on communication protocols. In a work that must be done in a distributed manner, multiple communications are taking place. When it comes to security and data protection, the number of connections will increase (Syarif *et al*., 2012).

VOIP service: A variety of means of communication tools support VOIP service and receive and send its messages. Mobile phones, hardware phones, computer systems… are all components of VOIP terminals. The variety of these terminals make the VOIP network more vulnerable in terms of security and lack of service attacks, viruses, internet worms, eavesdropping and change of identity. Thus, the security is one of the most challenging issues in VOIP.

Attacks on VOIP: Some of the most threatening attacks on the VIOP service are given.

Man in the middle attack: It includes reading and modifying messages exchanged between the two sides, by an intruder and without their knowledge, eavesdropping, forgery and repeating the packet (Ahson and Ilyas, 2008).

DoS and DdoS attacks: Including prevention of authorized access to a network service and sending outage requests on behalf of one or more hosts to a server or phone (in DoS and DdoS respectively). Attacks such as Smurf, FloodSYN, UDP Flood and ICMP Flood are among these attacks.

Flash crowd attack: it includes sending a large number of sudden request to a server. This attack is a DoS attack (Ahson and Ilyas, 2009).

Rogue sets attack: Including acts of deception by attackers to gain access to equipment and resources of the other (Ahson and Ilyas, 2008).

DHCP attack: It includes sending numerous requests to a DHCP server by a malicious computer on the network. The attack puts pressure on the server to allocate all IP addresses (Ahson and Ilyas, 2008). Actually, it is a DoS attack.

Pharming attack: Including connection to the client machine to access the information via a web page, e-mail or exchange instant messages using an apparently authorized request. Another type of attack on VOIP is misleading a large number of calls to a specific area in order to commit to a DdoS (Ahson and Ilyas, 2008).

Tall fraud attack: Including the use of a VOIP end-user from the VOIP servers for unauthorized calls via the traditional PSTN (Ahson and Ilyas, 2008).

Security solutions for VOIP: Although, the combination of voice and data traffic on the same physical infrastructure leads to saving the costs and easy management, during the phase of architectural designing of VOIP, logical separation of voice and data traffic is of great importance. The network events and security phenomena such as worm-wares and DoS attacks, in the event of an impact over a network, should not affect each other. In practice, there are several options for this logical separation. Using VLAN's, the VOIP-specific firewalls, application-layer gateways, routers and switches are among these solutions. Also, Access Control Lists (ACL) can be used to control access to equipment.

In addition, IPSec can be used for encryption at the network layer and a Public Key Infrastructure (PKI) for authentication. In addition, the TLS can be used for authentication with digital signature and encryption of signaling messages. One of the most common ways for immunization of the communications is the use of VPN and other tunneling methods. Also, for securing the remote management and access control, the IPSec and SSH are being used.

Data mining: One area of concern in the design of intrusion detection systems is machine learning and data mining. Data mining exploits advances in artificial intelligence and statistics. Both of these areas are used in pattern recognition and data classification and also directly in data mining. Also, both groups are active in recognition and the use of neural networks. In a definition, data mining is an automated process to extract patterns that represent the knowledge. This knowledge is implicitly stored in large databases and other repositories of information. Data mining simultaneously exploits several scientific disciplines such as database technology, artificial intelligence, machine learning, neural networks, statistics, pattern recognition, knowledge-based systems, knowledge acquisition, information retrieval, high-Performance computing and data visualization. In other words, data mining is the combination of classification techniques with new algorithms such as neural networks and decision tree. The combination of the classifiers is among these methods. The classifiers whose results are combined are called base classifiers and the set of the classifiers is called compound system. The neural networks are among the most common base classifiers. The relief method is the most important method among the distance-based methods and it uses a statistical solution for selecting the features. It is also a weight-based method which is inspired by algorithm-based Samples. However, the Multilayer Perceptron Method as Wrapper feature selection method uses the evaluation function. Relief algorithm works on the basis that initially allocates the zero weight to each of the features. After determining the weight features in Relief method, the features with a weight of above 0.01 and 0 are used to train the classifiers.

Literature review: In this study, the most important literature related to intrusion detection system using data mining algorithms will be reviewed. Among the most important tasks in order to secure VOIP, the following ways can be cited.

Creating a predictive model: Teng *et al*. (1990) have used the sequence of the statistical events to design an intrusion detection system in a manner that the future events are predictable based on events that have already happened. The main advantages of this method are the ability to detect and respond quickly to unusual performance and its main problem is the inability to detect some intrusions with no systematic sequence of events.

The analysis of the change in mode method: According to Ilgun *et al*. (1995) the system mode switching has been used for detection of the intrusion. This method creates the mode switching graph which is the graphical display of intrusion function as a series of mode switching, however it can only detect the attacks with predefined patterns and is unable to detect new and complex attacks.

Neural networks-based method: According to Fox *et al.* (1990) and Ryan *et al*. (1997), the researchers have proposed a data extraction which can be used in intrusion detection. This technique includes a set of processing units that are strongly linked and convert a set of inputs to the desired output. This method is used for intrusion detection, both in terms of irregularity and misuse.

Support Vector Machine-based methods: According to Vapnik (2000), a SVN-based intrusion detection system is proposed. In this system, features are selected using Fisher's scoring method and applied to a polynomial SVM core. This reduction in features in addition to reduction in computation, leads to speed increase.

Decision tree-based approach: According to Quinlan (1986, 1994) decision trees, including classification algorithms are used to extracting data. In the algorithm C4.5, the best feature for selected categorization and features and the discontinued features for each value are formed as a branch and for each continuous feature, a threshold is specified and is divided into two branches.

Mixture of experts: According to Govindarajan and Chandrasekaran (2012) in this category of methods that have been widely considered in recent years, instead of using a specific (expert) classifier, a combination of the similar or different classifiers are used for final decision-making. In one of the presented methods, the set of input data are passed through a decision tree that leads to the production of nodes. This information as an additional feature alongside with the original set of features are passed through support vector machine in order to achieve the final output.

In previous methods the KDD 99 data set was used. One of the disadvantages of this method was the use of repetitive and useless values. For this reason, the NSL-KDD data collection method was used in the proposed method. The NSL-KDD data set is formed by omission of the repetitive and useless values from the KDD 99. Another disadvantage of the previous methods is its low accuracy.

MATERIALS AND METHODS

The proposed method: In this study, aiming to achieve an efficient intrusion detection system, a method based on a combined and new techniques of machine learning has been considered and its details and efficiency have been analyzed. In the proposed method, in four stages, the best available features for intrusion detection are identified and they are used to design a compound classifier in order to detect the attacking packets to the network. The general scheme of the proposed system is shown in Fig. 1.

In the first phase of the proposed method, from among the data sets, six subsets are extracted based on the features and types of attacks. The first 4 subsets are based on the type of attack (any subset of normal records with a specific type of attack) and two other subsets are based on the features (Tavallaee *et al.*, 2009).

The second phase of the proposed method is reduction of the considerable features for classification of the input patterns. In order to reduce the features and remove the useless features we use a combined approach. In this regard, a filter method (here Relief) and a Wrapper method (In the proposed method, the Multilayer Perceptron Classifier) are used. The work is based on selection of the best features from among these two methods. The proposed combined algorithm for feature selection is shown in Fig. 2 in the form of a flow chart.

In the 3rd phase if the results of the Relief are weighted above 0.01 or 0, they are more accurate in Adaboost method with Multilayer Perception Classification. This subset of features is used as the final feature for training the classifier and in case the obtained results are lower than Multilayer Perception, the selected features of Multilayer Perceptron are chosen as the selected features.

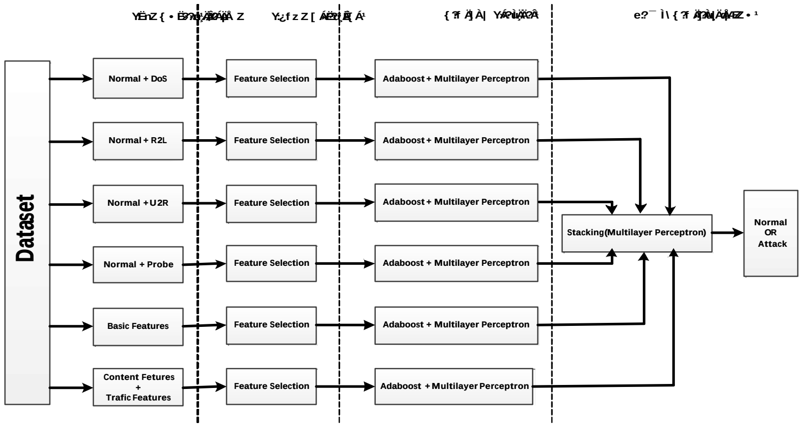

Fig. 1: The general scheme of the proposed method

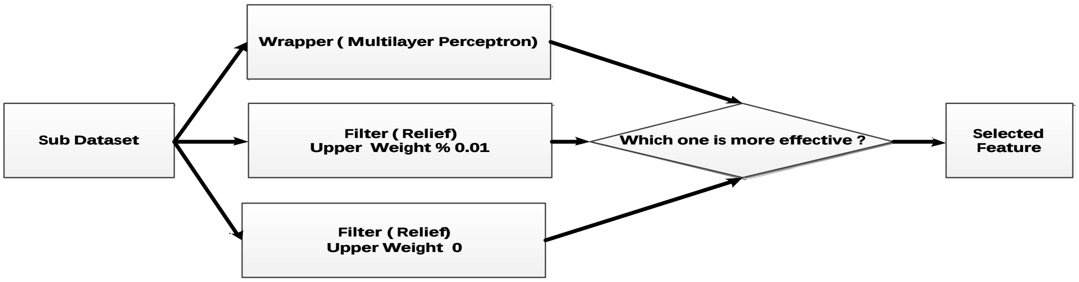

Fig. 2: The proposed feature selection algorithm

In the fourth phase, since each classification has a high ability treating a specific type of attack, the Stacking algorithm is used for combination of the classifier and covering the errors of classification.

RESULTS AND DISCUSSION

In a data mining system, firstly, a convenient application is needed for analysis. Today, several applications such as WEKA and RapidMiner are used for this purpose. In the current study, the WEKA application version 3.7.9 was used for running some methods and extracting the results. Another requirement for running and analyzing the proposed method is the convenient set of data. The KDD99 data set as a standard set was provided by DARPA for analysis of methods functionality of the artificial intelligence in intrusion detection systems. This data set has three main sets of features:

- The basic feature including the features 1-9
- The content feature including the features 10-22
- The traffic feature including the features 23- 41

Every data sample in this data set is categorized under one of the two normal and abnormal categories. The abnormal samples class contains samples from the 38 types of attack which itself is divided to four classes of attacks as DoS, R2L, U2R and Probe.

DoS: In this attack, the system resources are excessively consumed and cause the normal requests for resources to be rejected.

R2L: In this type of attack, the attacker, by remote unauthorized intrusion to the victim's machine, begins to exploit the legitimate user's account and sends the packets on the Net.

Table 1: The number of the normal and abnormal records in the training set

Varaibles	Normal	DoS	Probe	R2L	U2L
Number of the records	67343	45927	11656	995	52

Table 2: the number of the normal and abnormal records in the testing set

Varaible	Normal	DoS	Probe	R2L	U2R
Number of the records	9711	7458	2421	2754	200

U2R: These types of attacks are successfully executed on the victim's machine and takes the roots.

Probing: in this type of attack, the computers are scanned for data collection or finding the known vulnerabilities.

The main disadvantage of the KDD99 is the large number of duplicate samples. For this reason, the NSL-KDD data set is used in this study. In this regard, the available samples in this database are divided into training and test data. Table 1 and 2 show the number of normal and abnormal samples divided by the type of attack, respectively.

The results of training the selected features (their accuracy) from the three feature selecting methodswrapper, relief with the weight above 0.01 and 0 with Adaboost method and Multilayer Perceptron for each subset are shown in Table 3.

The classification process: After the preparation of the subsets we start training phase. The base for this method is using the Adaboost as the best algorithm in the Boosting set. The Multilayer Perceptron algorithm is used as the basic classifier.

Table 4 which is extracted from Table 3 is indicative of the best features and the highest accuracy in any of the above subsets using the three feature selecting methods as wrapper, relief with the weight above 0.01 and relief with the weight above 0.

The combination of the classifiers: In the 4th phase, we face 2 parallel combinations. The combination of the results obtained from the trained experts based on the attack and results from the trained experts based on the

Table 3: The comparison of the results of the best selector of the feature

Subset	Multilayer perceptron	The features with the weights above 0 in the relief (%)	The features the weights above 0.01 in the relief (%)
Normal+DoS	99.6243	99.9173	99.9267
Normal+R2L	97.9072	99.8735	99.7696
Normal+U2R	99.8681	99.6428	99.4752
Normal+Probe	99.8841	99.7961	99.6215
Basic Features	99.1532	99.2816	99.1874
Content feature+Traffic features	99.3652	99.3945	99.3278

Table 4: The application of Adaboost + Multilayer Perceptron on the select classes

Subsets	Selected features	Accuracy	False positive
Normal+DoS	2,4,5,6,7,10,11,12,14,16,17,18,20,21,22,24,26,27,28,30,32,33,34,35,38,40,41	99.9314	0.003
Normal+R2L	1,2,3,4,5,6,8,9,10,11,12,14,15,16,17,18,19,20,21,22,2324,25,26,27,28,29, 30,31,32,33,34,35,36,37,38,39,41	99.9752	0.003
Normal+U2R	1,2,3,4,5,6,7, 8,9,10,11,12,14,15,17,18,19,20,21, 23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,40,41	99.8735	0.009
Normal+Probe	2,3,5,6,7, 10,11,12,16,17,18,20,22,24,27,28,30,32,35,38,41	99.8841	0.003
Basic Features	1,2,3,4,5,6,7,8,9	99.2816	0.018
Content Feature+Traffic Features	10,11,12,13,14,15,16,17,18,20,21,22, 23,24,25,26,27,28,29,30,31 32,33,34,35,36,38,39,40,41	99.3945	0.024

Table 5: The results of voting divided by the type of attack and the property

The result of combination	Accesure	False posative
Normal prob¡ normal U2R, normal R2L, normal DoS	99.7246	0.003
Contrnt features+traffic features, basic features	99.6562	0.003

Table 6: The proposed method

The result of combination	Accesure	False posative
Normal Prob, normal U2R, normal R2L, normal DoS Contrnt features+traffic features, basic features	99.7353	0.003

Tale 7: The comparison between the proposed method and several other methods

Proposed method	Accuracy
RBF-SVM	85.19
Adaboost ensemble with genetic algorithm post optimization for intrusion detection	97.57
Ensemble (feature selections and filters)	97.85
proposed method	99.73

feature. It should be noted that the combined algorithm at the fourth phase is the combination algorithm in stacking method. In Stacking method, 2 levels of algorithms are used.

The first level is the same Adaboost^{+} Multilayer Perceptron and in the second phase, the Multilayer Perceptron is used as the basic algorithm. The final result of the two parallel combinations are presented in Table 5.

Then, in the 4rth phase which is the same proposed method we will combine the results of the trained experts based on attack and based on features, using the Stacking algorithm (Table 6).

In this phase, the functionality of the proposed method is compared to the previous method based on NSL-KDD data set. The result of comparison with several algorithms are presented in Table 7.

CONCLUSION

The current study aimed at proposing a method for intrusion detection on VOIP networks based on detection of DoS, R2L, U2R and Probe attacks. In this regard, a combination of learning machines methods are used for designing the intrusion detection system and the NSL-KDD data set is used for training and testing procedures. In the proposed method, regarding the nature of the attacks it was shown that no classification can lonely detect all the attacks. Therefore, if the result of the final detection of the attack is based on the combination of attacks instead of a single attack, the efficiency of the system in detection of intrusion of these attacks can be improved.

As shown in Table 7, the proposed method, compared to the similar methods, improves the system efficiency up to 99.73% in detection of these attacks with a 1.88% improvement.

REFERENCES

Ahson, S.A. and M. Ilyas, 2008. VoIP Handbook: Applications, Technologies, Reliability and Security. CRC Press, Boca Raton FL., Pages: 440.

Bace, R. and P. Mell, 2001. Intrusion detection systems. NIST Special Publication on Intrusion Detection Systems, SP 800-31, National Institute of Standards and Technology, Scotts Valley, CA.

Fox, K.L., R.R. Henning and J.H. Reed, 1990. A neural network approach towards intrusion detection. Proceedings of the 13th National Computer Security Conference, October 1-4, 1990, Shoreham Hotel, Washington, DC., USA., pp: 124-134.

Govindarajan, M. and R.M. Chandrasekaran, 2012. Intrusion detection using an ensemble of classification methods. Proceedings of the World Congress on Engineering and Computer Science, Vol. 1, October 24-26, 2012, San Francisco, USA., pp: 24-26.

Ilgun, K., R.A. Kemmerer and P.A. Porras, 1995. State transition analysis: A rule-based intrusion detection system. IEEE Trans. Software Eng., 21: 181-199.

Quinlan, J.R., 1986. Induction of decision trees. Mach. Learn., 1: 81-106.

Quinlan, J.R., 1994. C4.5: Programs for machine learning. Machine Learn., 16: 235-240.

Ryan, J., M.J. Lin and R. Miikkulainen, 1997. Intrusion detection with neural networks. Proceedings of the 11th Annual Conference on Neural Information Processing Systems, December 1-6, 1997, Denver, CO., USA., pp: 943-949.

Scarfone, K. and P. Mell, 2012. Guide to Intrusion Detection and Prevention Systems (IDPS). Special Publication 800-94, National Institute of Standards and Technology, Technology Administration, U.S. Department Commerce, Gaithersburg, MD., USA., February 2007.

Syarif, I., E. Zaluska, A. Prugel-Bennett and G. Wills, 2012. Application of Bagging, Boosting and Stacking to Intrusion Detection. In: Machine Learning and Data Mining in Pattern Recognition, Perner, P. (Ed.)., Springer, Berlin, Heidelberg, pp: 593-602.

Tavallaee, M., E. Bagheri, W. Lu and A.A. Ghorbani, 2009. A detailed analysis of the KDD CUP 99 data set. Proceedings of the 2nd IEEE Symposium on Computational Intelligence for Security and Defence Applications, July 8-10 2009, Ottawa, Canada.

Teng, H.S., K. Chen and S.C. Lu, 1990. Security audit trail analysis using inductively generated predictive rules. Proceedings of IEEE 6th Conference on Artificial Intelligence Applications, May 5-9, 1990, Santa Barbara, CA., pp: 24-29.

Vapnik, V.N., 2000. The Nature of Statistical Learning Theory. 2nd Edn., Springer, New York, USA., ISBN: 9780387987804, Pages: 314.

Zhang, X.Q., C.H. Gu and J.J. Lin, 2006. Intrusion detection system based on feature selection and support vector machine. Proceedings of the 1st International Conference on Communications and Networking in China, October 25-27, 2006, Beijing, pp: 1-5.