Journal of Computer Science 7 (9): 1318-1324, 2011
ISSN 1549-3636

Efficient Hybrid Network (Wired and Wireless) Intrusion Detection using Statistical Data Streams and Detection of Clustered Alerts

[1]M. Thangavel and [2]P. Thangaraj
[1]Department of Computer Applications,
Erode Sengunthar Engineering College, Thudupathi, Eorde, 638 057,
[2]Department of Computer Science and Engineering,
Bannari Amman Institute of Technology, Sathyamangalam, 638 401, India

Abstract: Problem statement: Wireless LAN IEEE 802.11 protocols are growing rapidly and security has always been a concern with the security of wired network. Wireless networks encountered threats from unauthorized access to network resources, installation of access points and illegal sniffing (refer as classical intrusion threats). In its current hybrid wired and wireless network attacks on the generally distinguish from normal cable intrusion attacks, selective forwarding attacks, MAC spoofing attacks. This means that the simple traditional misuse detection and anomaly detection model alone not sufficient to identify these mixed attacks on the hybrid network (wired and wireless). **Approach:** Our proposed work presents a hybrid cluster-based intrusion detection statistical anomaly, for detecting selective forwarding in wireless networks and intrusion into traditional wired networks. The detection was identified by changes in the statistical characteristics of data traffic on the wireless network. The clustering of data traffic based on the characteristics of alert classes and normal classes improve the performance of our hybrid intrusion detection in both wired and wireless network efficiently. The simulation was performed to evaluate the performance of wired intrusion detection systems to the proposed wireless intrusion detection on the data traffic in the area of wired and wireless hybrid network environment. **Results:** The proposed wireless intrusion detection system sharply detect the statistical change point detection of intrusion behavior in terms of attack rate and throughput of data traffic. The probability of intrusion attack and detection delay were measured in the simulation scenario, the result is 17% better than the current part of the exiting wired intrusion detection. **Conclusion:** The proposed anomaly intrusion traffic detection scheme performs better in heterogametic hybrid network (i.e., wired and wireless) compared to that of conventional homogeneous intrusion detection network models.

Key words: Hybrid network, anomaly intrusion detection, traffic statistics, cluster data streams

INTRODUCTION

The wireless networks features and its growing popularity is an obvious target for malicious attacks. In general, the intrusion detection systems have been used in wired networks, but wireless networks have limited deployment. Anomaly-based detection methods with growing hacker attacks should be able to fight attacks without the need of previous and through characterization. However, their application for wireless environments is more recent. The proposal presented in this work combines an intrusion detection system, which provide functional with the wired network to resistance detection of common attacks against 802.11 networks.

In the early days of local area networks, security by controlling physical access to the facilities was raised and the initiates were the biggest threat. With the advent of the Internet and the adoption of wide area networks, administrators were forced to defend their network not only against those with physical access, but against the larger community of people with Internet access or even just modem. The hackers began to use automated scripts to phone numbers randomly searched modems to access the networks could call. This was known as "war dialing". The attackers had to enter the network from a known point, such as a telephone number or IP address, so that at least part of that (Ohsita *et al*., 2007; Zubair *et al*., 2010).

In recent years an entirely new class of attacks has materialized (Zhong *et al*., 2005). The proliferation of wireless technologies has enabled attackers to enter networks, quite literally, out of thin air. With simple software, free, is a new generation of hackers able to find wireless networks, spy on communications and command resources. The practice of wandering in search of wireless networks is known

Corresponding Author: M. Thangavel, Department of Computer Applications, Erode Sengunthar Engineering College, Thudupathi, Eorde, 638 057, India

as "war driving", a play on the earlier modern discovery technique. With the right antenna, the attack can come from as far as several miles away. Thus, the intruder detection and identification presents unique challenges, which render many of the traditional techniques of intrusion detection ineffective (Khoshgoftaar *et al*., 2005; Yu and Zhou, 2010).

Wireless Sensor Networks (WSNs), which regulates media in a variety of applications such as military surveillance and control of forest fires. In WSN, a large number of sensor nodes in a wide range are used to detect events of interest (such as enemy vehicles, forest fires) and provide data reports to the base station via multi-hop wireless paths. The node model using wireless sensor networks, however, can be the focus of certain types of attacks. Such a strategy is the selective forwarding attack. In those attacks, a malicious node selectively drops sensitive packets, for example, a packet of information, the movements of the enemy tanks. Selective forwarding attacks are usually more effective to attack when nodes explicitly in the path of a data stream.

In these attacks, malicious nodes behave like normal nodes in most time, but selectively drop sensitive packets, such as a packet of information about the movement of the opposition forces. Such selective drop is hard to detect. The proposal in this work, provide a security scheme for the detecting selective forwarding attacks. The detection scheme uses a recognition technique for multi-hop alarms start responses from intermediate nodes. This system is efficient and reliable, since the intermediate node will report any abnormal packet loss and suspect nodes to both the base station and the source node.

Related work: A wireless IDS can be used in one of two ways centralized or decentralized. In a decentralized environment each WIDS operate independently, logging and alerting on its own. Beside this also means that wherever WIDS must be managed. In a large network this can quickly become overwhelming and inefficient and therefore not recommended for networks with more than one or two access points. The idea behind a centralized WIDS is that the sensors are deployed that relate information back to one central point. This point could send alerts and event logging and serve as a single point of administration for all sensors. Another advantage of a centralized approach is that the sensors can work together to capture a wider range of events more closely (Seamans and Yang, 2004). In this approach, there are three possibilities, the sensors can be used. The first is by using existing Access Points (AP).

Some accesses points are on the market are able to simultaneously function as an access point and WIDS sensor. This option has the potential to be cheaper than others, however there is a downside. Using the AP for both functions will reduce the performance, potentially creating a “bottle neck” on the network. The second option is the use of "dumb" sensors. These devices simply relay all information to the central server and rely on the server for all events. Although inexpensive, all information in one place, the impact on the performance of the wired network and the creation of a single point of failure is sent to the server. The third option is the use of intelligent sensors. These devices actively monitor and analyze wireless traffic, identify attack patterns and rouge devices as well as look for deviations from the norm. Then these events are reported to a central server and allow administrators to invoke countermeasures.

There are three types of MAC 802.11 frames, data, control and management (Gupta and Shroff, 2010). The wireless IDS is unique in that it detects attacks against the 802.11 frame at layer two of the wireless network. Most wireless attacks target management frames, since they are responsible for authentication, association, dissociation, beacon and probe request/response (Tague *et al*., 2011). Wireless threats such as attacks man-in-the-middle, rouge access points, war drivers and denial of service attacks function within the 802.11 frames and cannot be detected on layer three past access point. Wired IDS will not receive these frames, since the management frames are not forwarded to upper layers of the OSI model.

As traditional wired intrusion detection systems that are used to monitor a network, wireless intrusion detection systems need a dedicated interface. This wireless interface must be in monitor mode, the operator also known as RFMON mode, this mode is similar to promiscuous mode for installation materials and the device can accept incoming traffic (Gupta and Shroff, 2010). Another important aspect of wireless IDS is that the monitoring interfaces between the 12 channels available to wireless networks. Several wireless attacks work by utilizing a rogue access point on a different channel. For instance, attacks man-in-the-middle utilizes a rogue AP that at least 5 channels away from the target AP. Without channel hopping the wireless IDS would be blind to attacks that function on other channels.

WIDS can be deployed using a network of dedicated wireless device running in monitor mode. Since the Wireless IDS is separate from the access points it is important for the monitoring devices to match coverage of the wireless networks. Wireless Site Surveys are carried out to ensure that the WIDS covers the entire wireless network. The case study is an example of a WIDS shown in this way. Ideally, manufactures would include two wireless interfaces on access points, one for sending and receiving traffic and monitor interface. With the integrated monitor interface in the AP is less to manage IDS equipment and adequate coverage of the wireless network with WEP (Wang *et al*., 2008; Syurahbil *et al*., 2009).

A different analysis is executed in where the detection process is combined with the web server application itself. Syurahbil *et al*. (2009) presented a novel method to find intrusion characteristics for IDS using decision tree machine learning. Wireless IDS systems pair signature and knowledge-based detection methodologies are mostly used to detect the wide range of wireless attacks (Nakayama *et al*., 2009). Signature-based detection utilizes static signatures to match bad traffic. This type of matching works well for known attacks that match a predefined pattern. For example, in order to detect rogue access points, the IDS utilize a list of authorized access points then alerts when a detected AP does not match the list (Nakayama *et al*., 2009). Knowledge-based detection uses a historical baseline and warnings when network traffic varies from the historical baseline. Many wireless attacks do not match a signature, but instead cause network traffic anomalies that a knowledge based IDS can detect. While the other classifications take into account the assault and the attacker, classification takes into consideration just the attack itself. By bringing a better clarity, this classification takes into account not only some observable characteristics of the attack, but also some operational aspects which remain primordial for the IDS test and evaluation (Mohammed *et al*., 2010). For instance, to generate enough packets to crack a WEP key, an attacker to capture play the traffic on the wireless network. This attack makes the amount of traffic on the network to dramatically increase the historical baseline.

MATERIALS AND METHODS

The hybrid model for intrusion detection attack in wireless network selects the optimal features to specially detect 802.11 specific intrusion attacks. The hybrid model of feature selection used information gain ratio. It evaluates the relevance of 802.11 specific features and its measures of information gain ratio indicate the features essentially needed for detecting anomaly intrusion attack in the network. The k-means clustering is further applied to select the optimal feature set to improve the efficiency of the intrusion detection by classifying the attributes to the associated attack class obtained from the records sets of the tracked data from the wireless network MAC frames. Statistical characteristic of data traffic learning is further used to reduce the detection time and improve the overall performance of wireless intrusion detection with optimal set of features for detection criteria.

The improved version of the hybrid model is developed using existing wireless intrusion detection specific to 802.11 features, by utilizing integrated statistical and clustering principles. The clustering effectively identify the set of reduced optimal features. The optimal feature obtained is more efficient in detecting the intrusions of low level network framework. In addition simulations are carried out to compare the performance of existing classical intrusion detection schemes in wired network to the proposed hybrid network.

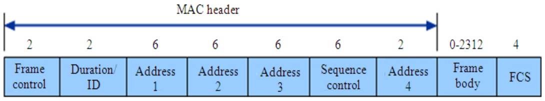

Fig. 1: 802.11 MAC frame structure

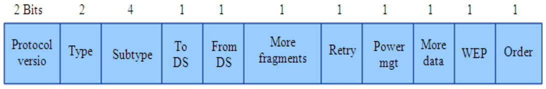

Fig. 2: Frame control field

De-authentication attack: De-authentication attack is an easy to mount attack that can work on any type of 802.11 networks (WEP and WPA) which modifies the 802.11 MAC frame. It enables an attacker to terminate the connection of all stations connected to the wireless network. The attacker sends a de-authentication frame with a destination address. The stations that receive this frame will automatically disconnect from the network. The operation is repeated continuously to prevent the stations from maintaining their connections to the access point.

802.11 MAC frame: The 802.11 MAC frame consists of a MAC header, body frame and a Frame Check Sequence (FCS), as shown in Fig. 1.

The numbers on the Fig. 1 represents the number of bytes for each field. The frame control field contains control information used to define the nature of the 802.11 MAC frame and providing information necessary for the following fields to understand how to process the MAC frame. The numbers on the Fig. 2 represents the number of bits for each field of the control settings in the MAC Frame.

Each sub-field under frame control field is explained in Fig. 2 Protocol Version provides the current version of the 802.11 protocol used. Receiving STAs use this value to determine if the version of the protocol of the received frame is supported. Type and Subtype determines the function of the frame. There are three different frame type fields: control, data and management. There are multiple subtype fields for each frame type . Each subtype determines the specific function to perform for its associated frame type. To DS and From DS indicates whether the frame is going to or exiting from the Distributed System (DS) and is only used in data type frames of STAs associated with an AP.

Other fragments indicate whether other fragments of the frame, either data or management type, followed. Retry indicates whether or not the frame, for either data or management frame types, is being retransmitted. Power management specifies if the sending STA is in active mode or power-save mode. More data indicates to a STA in power-save mode, the AP has to send more frames. It is also used for access points, to indicate that additional broadcast/multicast frames to follow. WEP indicates whether or not encryption and authentication are used in the frame. It can be set for all data frames and management frames, which have the subtype set to authentication. Order indicates that all received data frames must be processed in order.

Address fields: Depending upon the frame type, the four address fields will contain a combination of the following address types. BSS Identifier (BSSID) BSSID uniquely identifies each BSS. When the frame is from an STA in an infrastructure BSS, the BSSID is the MAC address of the AP. When the frame is from a STA in an IBSS, the BSSID is the randomly generated, locally administered MAC address of the STA that initiated the IBSS. Destination Address (DA) indicates the MAC address of the final destination to receive the frame. Source Address (SA) indicates the MAC address of the original source that initially created and transmitted the frame. Receiver Address (RA) indicates the MAC address of the next immediate STA on the wireless medium to receive the frame.

Transmitter Address (TA) shows the MAC address of the STA that transmitted the frame into the wireless medium. The frame body contains the data or information included in either management type or data type frames. STA transfer with a Cyclic Redundancy Check (CRC) in all areas of the MAC header and the area of the body structure to generate the FCS value. The receiving STA then uses the same CRC calculation of its own FCS field value to determine whether or not errors have occurred during the transmission.

Feature extraction: Feature extraction is responsible for the extraction of attributes and characteristics that are effective in detecting the interference of the 802.11 MAC frame fields. The attributes are selected depending on the type of the frame and the detection algorithm. This set of characteristics is sent to the local misuse detection and the central module for detecting anomalies.

Statistical anomaly traffic characteristic in MAC frames: MAC frame fields in the 802.11 packet header are analyzed to observe anomalies in the traffic. Individual fields in the traffic header data take discrete values and show discontinuities in the sample space. MAC address space span multiple addresses in a sample are likely to exhibit many discontinuities over this space. It is difficult to analyze the data over the address space. In order to overcome such discontinuities in a discrete space, the packet header data transform in to continuous signal through correlation of samples successive samples. To investigate the sequence of a random process, we use a simplified correlation time series for computational efficiency without sacrificing performance.

For each MAC address in the traffic, count the number of packets sent in the sampling instant. For computing address correlation signal, consider two adjacent sampling instants. The detection model define address signal in sampling point. If an address spans the two measuring points, ie n-1 and n, the user get a positive contribution. In order to minimize storage and processing complexity, use a linked data structure. A location count is used to record the packet count for the address j in ith field of the IP address through scaling. This provides a concise description of the address required to store the address occurrence uniquely. The statistical model anomaly detection filters this signal by calculating a correlation of the address in two samples of success. Consequently four correlation signals are calculated. This approximate representation of addresses allows us to reduce the demands of the computing and storage for a considerable factor. To create the correlation of signaling messages at the end of the sampling point, multiply each segment of the correlation with scaling factors. From a statistical point of view, they have more or less same mean and dispersion standard deviation as cross-correlation coefficient.

Cluster intrusion alert generation: Attributes in an event of data traffic in the hybrid network are independent of a particular attack instance used for clustering. Attributes are dependent on the instance of the attack used in the clustered alert aggregation process to distinguish different attach instances. Dependent metrics such as source IP address identify the attacker. Independent metrics, i.e., destination port -80, in case of web-based attacks. Both contain the attacker’s real target services specifically for a particular service objective. Regarding, an attack instance, a random process generate alerts, that are distributed according to a certain multivariate probability distribution. The alert space is composed of several attributes. Reconstructing an attack situation from observed samples estimate all the parameters of the mixture distribution. The approach adopted is Maximum Likelihood (ML) estimation. Hybrid network anomaly intrusion detection is aware of the situation and tries to keep the model updated to current attack. There is a trade-off between the running time (reaction time) and accuracy. It is possible to decide upon the existence of a new attack instance when only one observation is made. Overall random process is non-stationary regarded as mixing coefficients at certain points in time.

The mixing coefficient is either zero or the reciprocal of the number of active components (for the time interval of the respective instance of attack). With appropriate novelty and obsoleteness detection mechanisms aim at detecting the data traffic in varying time with both sufficient certainty and timeliness. With the creation of a new component, an appropriate meta-alert that represents the information about the component in an abstract way is created. Each time a new alert is added to a component the corresponding meta- alert is updated incrementally too. Meta-alerts exchanged with other cluster objects detect distributed attacks such as one-to-many attacks. Meta-alerts used at various points in time from the initial creation until the deletion of the corresponding component.

Hybrid network anomaly traffic intrusion detection algorithm:

Step 1 (Initialization): Initialize input data stream based on specified time intervals from hybrid network (wired and wireless).

Step 2 (Characteristic extraction): Extract wired and wireless data characteristics from the initialized time specific data streams.

Step 3 (Evaluation of intrusion rule): Evaluate intruder rules as specified by the administrator for basic filtering of time specified data streams with its extracted characteristics from step 2.

Step 4 (Derivatives of black listed rules): Derive server admin specific black listed rules from standard black lists available in World Wide Web.

Step 5 (Intruder detection with statistic characteristic): With the extracted characteristics of data stream (step 2), statistical features are verified with intrusion rules (step 3) and black list rules (step 4) to identify intrusion alerts.

Step 6 (Clustering of alerts): Cluster the intrusion alerts (from step 5) based on anomaly, normal and abnormal characteristics, to form meta alert which predicts more precise and other probable intrusion attacks on the server in latter stages.

Step 7 (Iteration): Iterate step 3 to step 6 for all the characteristics of the data stream to improve the anomaly intrusion detection rate.

RESULTS

In this study, we propose an intelligent anomaly IDS for reducing false positive rates, while there are few similarities between the approach proposed (Mehdi *et al*., 2007) and ours, there are several major differences, the most significant of which is their system's limitation to a single class of attacks, namely that of control flow data corruption. Anomaly detection to de-authentication attack is based on the observation of the behavior of the system to create profiles and data structures that describe the normal state of the system using the features extracted from the 802.11 MAC frame. IDS detect the behavior of the network to establish the standard way to build an effective anomaly detector. The normal user behavior is evaluated with various training samples which deviate from malicious activity. Even sometimes anomaly intrusion detector generates a false alert when illegal activity takes place on the date of the establishment of traffic for a specified period. Anomaly detection is effective for detecting abnormal behavior on the basis of the previous, traditional and black list rules.

The blacklist is the register of entities being denied a particular privilege, service, mobility, access or recognition as per the rules and governance of worldwide web consortium. Black list rules adapted in our work follows the below mentioned rule sets. Latest black list of websites in due course of our experiments verified:

- Cleaning up an infected WordPress site (Posted on 16 March 2011 by Sucuri-research)
- Cleaning up an infected osCommerce web site (Posted on 9 March 2011 by Sucuri-research)
- Cleaning up an infected Joomla web site (Posted on 9 March 2011 by Sucuri-research)
- Cleaning up blacklisted sites (Posted on 8 March 2011 by Sucuri-research)
- WPSecurity lock (Posted on 19 January 2011 by dremeda)

The anomaly detection mode is based on the functions of network traffic splitter and statistical data transformation. The traffic splitter generates network traffic signal from packet header traces or data flow records. The statistical data transformation analysis is carried out with wavelet transforms of IP address and port number correlation over several timescales. Then the detection of attacks and anomalies are checked using thresholds. The analyzed information will be compared with historical thresholds to see whether the traffic's characteristics are out of regular norms. This comparison will lead to some form of a detection signal that could be used to alert the network administrator of the potential anomalies in the network traffic.

Selective forwarding attack, a type of intrusion attack, in wireless mesh network, intermediate misbehaving router forwards a portion of packets it receives and discards others. Previous work handles these attacks in error free wireless channel. However in reality most of the wireless channel drop packets due to the medium access collision, poor channel quality, In our work anomaly based channel aware detection is provided to identify the selective forwarding misbehavior from the normal channel loss of hybrid network data traffic.

The anomaly based channel aware detection scheme uses a multi-hop acknowledgement technique to launch alarms by obtaining responses from intermediate nodes. This scheme is efficient and reliable in the sense that an intermediate node will report any abnormal packet loss and suspect nodes to both the base station and the source node. Each intermediate node along the forwarding path is in charge of detecting malicious nodes. If an intermediate node detects the misbehavior of its downstream (upstream) nodes, it will generate an alarm packet and deliver it to the source node (the base station) through multiple hops. Downstream denotes the direction toward the base station and upstream denotes the direction toward the source node.

DISCUSSION

The simulation of anomaly intrusion traffic detection was conducted based on the monitored traces of hybrid network (wired and wireless) traffic generated from real time data traffic from ISP servers. The real trace of samples was carried for a period of one month connecting with 10Mbps broad band link comprising of wireless and wired network servers. The samples taken from the ISP server have 1000s of wired and 1000s of wireless connection, at the traffic rate varying from 256Kbps to 1MBPs. These traces were anonym, but preserved with MAC and IP prefix relationships. The deployment of the anomaly traffic detection applied in the hybrid network is done based on the clustering Meta alert and statistical characteristics of data traffic. The simulation was conducted on IBM PC Compatible Machines with 2.20 GHz and 2GB of RAM in NS2 simulator.

The simulation evaluate the performance, such as the detection accuracy and communication overhead of our scheme through simulations. We use a field size of 1000×1000 m where 80 nodes are uniformly distributed. One stationary sink and one stationary source sit on opposite sides of the field, with about 2 to 3 hops in between. Carry out a simulation event in which the source generates 500 reports in total and one report is sent out every two seconds. Packets can be delivered hop-by-hop at 10 Kbps. In order to avoid detection, the malicious nodes drop only part of the packets passing by. To make our scheme more resilient in poor radio conditions, implement a hop-by hop transport layer retransmission mechanism. The retransmission limit is 5 by default. The channel error rate is 10% by default, which is usually regarded as a rather harsh radio condition. Each simulation runs 10 times and the result shown is an average of these runs.

The proposed metrics evaluate the detection accuracy and communication overhead of the existing and proposed schemes. Alarm reliability measures the ratio of the number of detected maliciously-dropped packets to the total number of lost packets detected including those lost due to poor radio conditions. Undetected rate measures the ratio of the number of undetected maliciously-dropped packets to the total number of maliciously-dropped packets. Relative communication overhead measures the ratio of the total communication overhead in a system that incorporates our detection scheme against a system that does not.

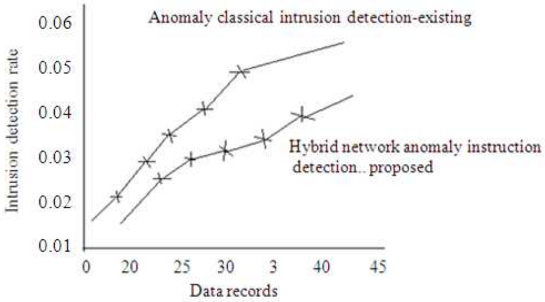

Fig. 3: Performance of anomaly intrusion detection in hybrid network

The simulation conducted also performed evaluation of cluster alert aggregation approach. The simulation deployed different hybrid network data sets to demonstrate the feasibility of integrated statistical and cluster based anomaly intrusion model. Several weeks of training and test data have been generated on a test bed that emulates a small confidential data site. In the hybrid network scenario of both wired and wireless, the generated network traffic is analyzed for its intrusion characteristic detection. The simulation used both MAC frame and IP address dump as input data and analyzed varied attack instances against various target hosts. The extracted statistical information from the network traffic data, apply Support Vector Machines (SVM) to classify the clustered data characteristic samples. The performance graph shown in Fig. 3 shows that the Hybrid network anomaly intrusion detection proposed in this work has better response time for the detection rate compared to that of the classical intrusion detection scheme. The percentage of improvement is made nearly 17% in terms of response time for the anomaly intrusion detection from the hybrid network data traffic.

The tabulated values of the detection rate response time against number of data records extracted from the hybrid network data traffic shown in Table 1 indicates that our proposal has better response time in detection anomaly intrusion both in wired and wireless network. With varying threshold to the data traffic rate of the clustered alert aggregation, the True Positive Rate (TPR, number of true positives divided by the sum of true positives and false negatives) and False Positive Rate (FPR, number of false positives divided by the sum of false positives and true negatives) are identified for the trained data traffic records.

Various operating points are marked to evaluate the normal traffic scenario and anomaly traffic intrusion at different data rates. The simulation conducted investigated, aggregation under idealized conditions where we assume to have a perfect detector layer with no missing and no false alerts at all. As attributes for the alerts, use MAC frame and IP address, source and destination port, the attack type and the creation time differences (based on the creation time stamps). The performance of the hybrid network intrusion detection shows improved detection rate with reduced set of features. The false positives rate identified is the percentage of frames containing normal traffic classified as intrusive frames, which is minimal in our scheme. False negatives rate identified is the percentage of frames generated from wireless attacks which are classified as normal traffic which is precisely evaluated in our scheme.

Table 1: Hybrid network detection error rate against number of data traffic records

Data records	Classical anomaly intrusion detection rate response time-existing (ms)	Hybrid network anomaly intrusion detection rate response time --- proposed (ms)
20	0.020	0.025
25	0.030	0.027
30	0.035	0.028
35	0.040	0.03
40	0.050	0.04

CONCLUSION

Anomaly Intrusion detection in hybrid network (wired and wireless) presented in this study, with the statistical characteristics of data traffic and clustering the alert aggregates detect the anomaly traffic intrusion occur in the ISP most efficiently in varying time zones of multiple data transfer rate (256 kbps to 1 Mbps). Different cluster alerts produced by low-level anomaly intrusion detection is evaluated to make the system more foolproof with the standard data traffic. The efficiency of hybrid network anomaly intrusion detection is investigated with all the relevant information from both the MAC frame headers and IP address headers. The simulation conducted for different data sets and showed that statistical and cluster based detectors are better than conventional signature based detectors. In most of the cases, the amount of data for interrogation is evaluated to its maximum metric of detection. Clusters split the instance detection rate and work on attack instances to minimize the missing data traffic.

Data generated from hybrid network traffic have high volume, dimensionality and heterogeneity, making the performance of our algorithms more acceptable for on-line analysis. The anomaly intrusion traffic detection work carried out in this study combine multiple independent data sources to study combined traditional intrusion attack and anomaly intrusion, provides the statistical traffic characteristic detection and clustering the alert aggregation. The load-demand capacity of ISP server at lean and heavy traffic times are observed to provide better detection of anomaly intrusion in the hybrid networks. Using cluster alert aggregation, the simulation performed the analysis of several traffic anomaly properties which is highly complicated with classical intrusion detection systems in wired networks.

REFERENCES

Gupta, G.R. and N.B. Shroff, 2010. Delay analysis for wireless networks with single hop traffic and general interference constraints. IEEE/ACM Trans. Network., 18: 393-405. DOI: 10.1109/TNET.2009.2032181

Khoshgoftaar, T.M., S.V. Nath, S. Zhong and N. Seliya, 2005. Intrusion detection in wireless networks using clustering techniques with expert analysis. Proceedings of the 4th International Conference Machine Learning and Applications, Dec. 15-17, IEEE Xplore Press, pp: 6-6. DOI: 10.1109/ICMLA.2005.43

Mehdi, M., S. Zair, A. Anou and M. Bensebti, 2007. A Bayesian networks in intrusion detection systems. J. Comput. Sci., 3: 259-265. DOI: 10.3844/jcssp.2007.259.265

Nakayama, H., S. Kurosawa, A. Jamalipour, Y. Nemoto and N. Kato, 2009. A dynamic anomaly detection scheme for AODV-based mobile ad hoc networks. IEEE Trans. Vehicular Technol. 58: 2471-2481. DOI: 10.1109/TVT.2008.2010049

Ohsita, Y.,T. Miyamura, S. Arakawa, S. Ata and E. Oki *et al*., 2007. Gradually reconfiguring virtual network topologies based on estimated traffic matrices. Proceedings of the 26th IEEE International Conference on Computer Communications, May 6-12, IEEE Xplore Press, Anchorage, pp: 2511-2515. DOI: 10.1109/INFCOM.2007.311

Syurahbil_ N. Ahmad, M.F. Zolkipli and A.N. Abdalla, 2009. Intrusion preventing system using intrusion detection system decision tree data mining. Am. J. Eng. Applied Sci., 2: 721-725. DOI: 10.3844/ajeassp.2009.721.725

Seamans, J.K. and C.R. Yang, 2004. The principal features and mechanisms of dopamine modulation in the prefrontal cortex. Prog. Neurobiol., 74: 1-58. DOI: 10.1016/J.PNEUROBIO.2004.05.006

Tague, P., S. Nabar, J.A. Ritcey and R. Poovendran, 2011. Jamming-Aware traffic allocation for multiple-path routing using portfolio selection. IEEE/ACM Trans. Network., 19: 184-194. DOI: 10.1109/TNET.2010.2057515

Wang, Y., X. Wang, B. Xie, D. Wang and D.P. Agrawal, 2008. Intrusion detection in homogeneous and heterogeneous wireless sensor networks. IEEE Trans. Mobile Comput., 7: 698-711. DOI: 10.1109/TMC.2008.19

Yu, M. and M. Zhou, 2010. A performance modeling scheme for multistage switch networks with phase-type and bursty traffic. IEEE/ACM Trans. Network., 18: 1091-1104. DOI: 10.1109/TNET.2009.2036437

Zhong, S., T.M. Khoshgoftaar and S.V. Nath, 2005. A clustering approach to wireless network intrusion detection. Proceedings of the 17th IEEE International Conference Tools with Artificial Intelligence, Nov. 16-16, IEEE Xplore Press, Hong Kong, pp: 196-196. DOI: 10.1109/ICTAI.2005.5