Towards Multi-Stage Intrusion Detection using IP Flow Records

Muhammad Fahad Umer, Muhammad Sher and Imran Khan
Department of Computer Science and
Software Engineering
International Islamic University
Islamabad, Pakistan

***Abstract*—Traditional network-based intrusion detection systems using deep packet inspection are not feasible for modern high-speed networks due to slow processing and inability to read encrypted packet content. As an alternative to packet-based intrusion detection, researchers have focused on flow-based intrusion detection techniques. Flow-based intrusion detection systems analyze IP flow records for attack detection. IP flow records contain summarized traffic information. However, flow data is very large in high-speed networks and cannot be processed in real-time by the intrusion detection system. In this paper, an efficient multi-stage model for intrusion detection using IP flows records is proposed. The first stage in the model classifies the traffic as normal or malicious. The malicious flows are further analyzed by a second stage. The second stage associates an attack type with malicious IP flows. The proposed multi-stage model is efficient because the majority of IP flows are discarded in the first stage and only malicious flows are examined in detail. We also describe the implementation of our model using machine learning techniques.**

Keywords*—*IP flows; Multi-stage intrusion detection; One-class classification; Multi-class classification

I. Introduction

Network-based Intrusion detection system (NIDS) analyze network traffic to detect malicious activities. Traditional approaches for intrusion detection scan the complete packet content. This method is termed as deep packet inspection (DPI) [18]. However, DPI is difficult to implement when packets are being transferred at gigabit speed. Extensive resources and dedicated hardware infrastructure need to be deployed to perform packet inspection[20]. In most cases, data transmitting through the network is encrypted. DPI techniques cannot scan the encrypted payload. Another drawback of DPI is the compromise of privacy. Even if the data is not encrypted, performing strong packet filtering on the network traffic might not be permitted due to privacy issues [10].

A relatively new approach for intrusion detection analyzes the communication pattern in the network traffic for abnormal behavior[20]. The communication patterns are extracted from the network in the form of IP flow records. The IP flow records contain aggregate packet information and describe the network traffic in a summarized form. An IP flow is defined as a set of IP packets passing through an observation point in the network during a certain time interval. All packets belonging to a particular flow have a set of common properties [6]. The extraction of flow records from the network consists of two processes; flow export and flow collection [20]. The flow records are exported from the network using flow-enabled devices. Many vendors offer built-in support in the network switches and routers for flow export. The flow collector receives flows from the flow exporter and stores them in a flow database for analysis. A flow exporter can forward flow records to more than one flow collectors. Similarly, a flow collector can receive flow from more than one flow exporters.

The process of transferring flow records between the flow exporter and collector is defined by a flow export and collection protocol. Different vendors have formulated proprietary flow export and collection protocol. However, Cisco's Netflow is a common flow export and collection protocol and is supported by almost all major vendors. Due to the increased requirement of IP flow information for network management, the Internet Engineering Task Force (IETF) has standardized the flow export and collection protocol as IP Flow Information Exchange (IPFIX) protocol [19]. IPFIX is very flexible protocol and defines around 280 attributes for IP flow records.

The IP flow records have a number of applications including billing, congestion control, traffic analysis and intrusion detection. The intrusion detection system using IP flows records for attack detection are called Flow-based IDS. Flow-based IDS have several advantages over DPI-based techniques [12]. The flow records contain aggregate packet data; therefore, fewer resources are required to process the flow data. The flow-based IDS are also not effected by the use of encryption because flow records do not have any payload. Flow-based technique only scans the data up to transport layer, and no confidential information leaves the network [1].

Flow-based Intrusion detection is an on-going research area [20]. This paper proposes a novel multi-stage model for flow-based IDS. The multi-stage model separates malicious flows from normal flows in the first stage. The malicious flows are processed by a second stage which associates an attack type with the malicious flows. We also give implementation details of our model using machine learning techniques. We suggest the use of one and multi-class classification technique for first and second stage intrusion detection processes respectively. Our future work will include a rigorous evaluation of different one-class and multi-class techniques for flow-based intrusion detection. The best performing classification technique will be combined in a multi-stage model for a comprehensive flow-based intrusion detection framework. The multi-stage model will be evaluated on various flow-based intrusion datasets to obtain the performance results.

The organization of the paper is as follows: Section 2 discusses related work in multi-stage intrusion detection systems. The architecture of our proposed model is given in Section 3. Section 4 presents the implementation detail of our model using machine learning algorithms. The conclusion of our work is presented in Section 5.

II. Related Work

The multi-stage detection of network attacks has been applied using two different approaches. The first approach considers a single attack type spanned over multiple stages. Various stages of an attack include vulnerability scan, weakness exploitation, invasion, control, and spread. Every stage of an attack corresponds to a detection stage in the multi-stage IDS. In [9], a technique for detection of a single type of attack using multi-stage traffic analysis was proposed. Similarly, a multi-stage IDS using Hidden Markov Model is presented in [16]. Every attack stage is analyzed by detection agents using predefined attack signals. The signals of all attack stages are estimated by a determination stage using Hidden Markov Model for final intrusion detection decision. The IDS is evaluated on DARPA dataset and achieved a detection rate of 90%.

The other method for multi-stage IDS detects a different type of attack in every stage. In [7], a network intrusion detection technique using Learning Vector Quantization(LVQ) was proposed. The authors used multiple stages to detect different types of attack. The technique was evaluated on DARPA dataset and achieve very low error rate. A multi-stage filter using enhanced AdaBoost for network intrusion detection is presented in [17]. The technique is evaluated on DARPA dataset and achieved good results for some attack types. A malware prevention and detection system using a combination of signature and anomaly-based IDS is presented in [2]. The signature-based IDS uses general characteristics of attack for detection. The anomaly-based IDS is implemented using the RIPPER classifier. The signature and anomaly based IDS are implemented in three stages. The first stage classifies the traffic as normal or malicious. The second stage determines the attack type while the third stage determines the variant of a particular attack type. The technique is evaluated on the NSL-KDD99 dataset and achieved F1-measure of over 0.97 for different stages.

In [22], a multi-stage detection model using time-slot and flow-based detection, is proposed. The time-slot detection stage checks the incoming traffic for obvious traffic characteristic. This stage classifies the traffic into normal, suspicious and malicious categories. The traffic detected as suspicious is converted into IP flows and forwarded to the flow-based detection stage. The technique is evaluated in DARPA dataset and achieved a detection rate of 68.4%.

In [3], the authors proposed a real-time multi-stage intrusion detection system using unsupervised learning to improve the detection rate of unknown attacks. The system uses IP flow records for attack detection. The multi-stage model uses two detection engines. The first engines use sub-space clustering and to detect DoS, DDoS, and other attacks. The second detection engine analyzes the relation between attackers to detect Bot-master. The proposed technique focused on improving the detection rate of unknown attacks by additional flow features.

Our proposed approach differs from the existing work. Unlike most of the techniques, our model uses IP flow records instead of packets for intrusion detection. Our model separates the normal and malicious flow in the first stage and determines the attack type in the second stage. The implementation of our model uses a one-class and multi-class classification at the first and second stage. The use of one-class classification in a multi-stage model is a novel idea. The next section presents the architecture of our proposed model.

III. Architecture of Proposed Model

Although flow records contain summarized network traffic information, the flow data can be very large in high-speed networks [14]. Flow monitoring and analysis tools employ packet sampling techniques to obtain a subset of flow records [13], [4]. Furthermore, IPFIX defines around 280 flow attributes. Additional flow attributes can also be computed using the base flow attributes by the IDS to detect different types of network attacks. Large input size and high feature space can overload the IDS. Also most of the traffic in the network is normal as compared to malicious traffic. Processing of malicious as well as normal traffic by the IDS will be performance bottleneck.

We propose a multi-stage model for intrusion detection in high-speed networks using IP flow records. Figure II shows the architecture of our proposed approach. The IP flows are collected from the network using a flow-enabled device. These IP flows are passed through an attribute selection step. The multi-stage model uses two stages for attack detection. The first stage selects a minimal set of attributes and determines whether incoming IP flows are normal or malicious. The first stage uses a fast and computationally inexpensive technique for detection. It discards the normal flows and forwards the malicious to the second stage detection process. An initial intrusion alert is also sent to the consolidated intrusion alert module.

The second stage process performs detail intrusion detection on the malicious flows. The size of malicious flows is very small in overall network traffic. Due to small input size, the second stage can commit additional resources for detailed and accurate detection of an attack type. The second stage analyzes the malicious flows and determines the attack type. The second stage can also use additional flow attributes for precise detection of an attack. If the flows do not belong to any attack class, they are marked as unknown in the detail intrusion alert. The unknown flows can belong to an unseen attack, or they can be false posties of the first stage. The second stage sends a detail intrusion alert to the alert module. The alert module raises a consolidated alert combining the alert information received from both detection stages.

Our proposed multi-stage model discards normal flows in the first stage and ensures that only malicious flows are subject to detail intrusion detection. This increase the efficient of our model because no resources are consumed in the processing normal flows. Another benefit of our approach is the reduction of false positives. If the malicious flows detected in the first stage contain false positives, the second stage process does not associate a class type with such flows. The next section gives implementation detail of our model using machine learning techniques.

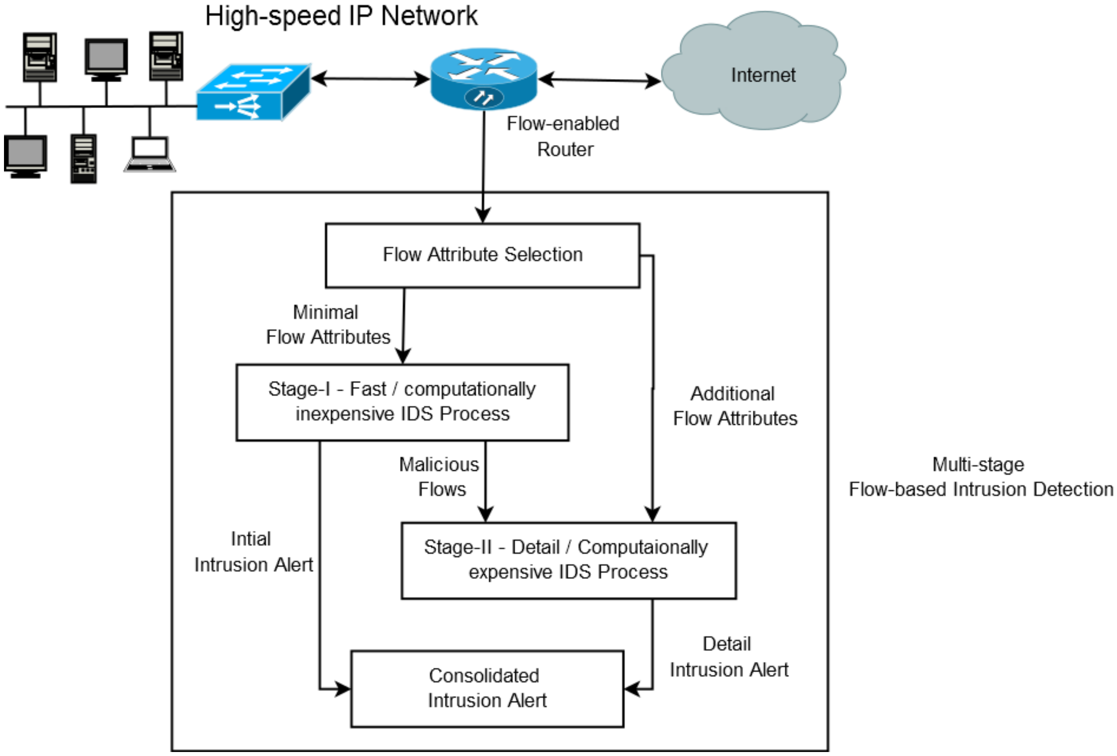
High-speed IP Network
Internet
Flow-enabled Router
Flow Attribute Selection
Minimal Flow Attributes
Stage-I - Fast / computationally inexpensive IDS Process
Additional Flow Attributes
Malicious Flows
Intial Intrusion Alert
Stage-II - Detail / Computaionally expensive IDS Process
Detail Intrusion Alert
Consolidated Intrusion Alert
Multi-stage Flow-based Intrusion Detection

Fig. 1. Architecture of multi-stage intrusion detection model

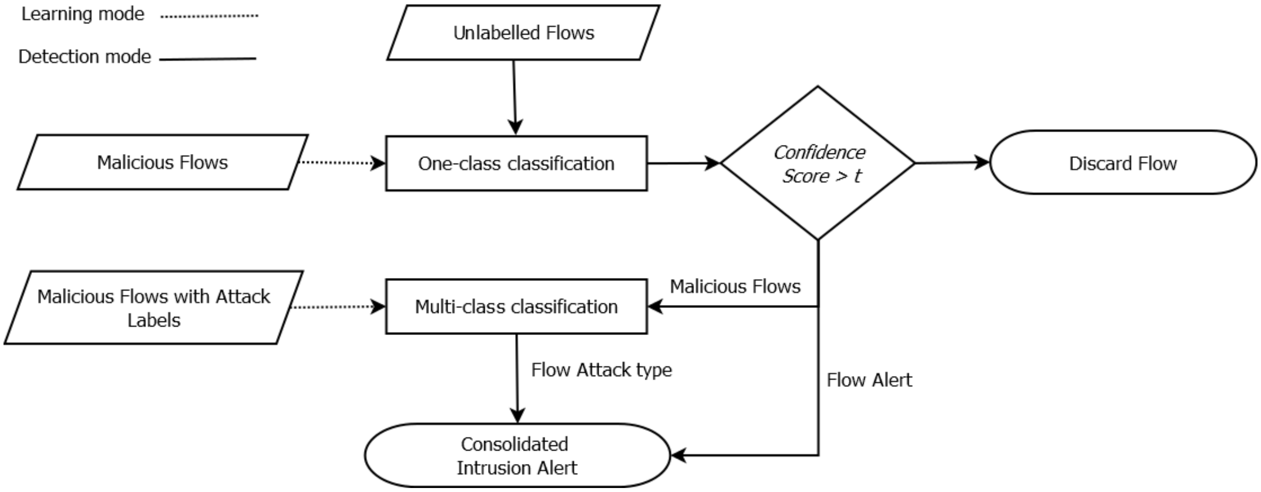

Fig. 2. Architecture of multi-stage intrusion detection model

IV. Implementation

Our work proposes the use of machine learning technique for implementation of the proposed model. Machine learning techniques have been extensively used in intrusion detection systems for adaptability and improvement of detection rate [21], [5].

The implementation of the multi-stage model using machine learning techniques has two modes, learning mode and detection mode. In learning mode, the classification algorithms are trained using a labeled set of IP flows. Our model uses two training sets. The fist stage requires a training set consisting of only malicious flow. The second stage uses a training set of malicious flow with attack labels. In the detection mode, the IDS process unlabeled IP flows and raises consolidated intrusion alerts.

Figure III shows the implementation of our model using machine learning classification algorithms. The first stage detection process only detects malicious IP flows. There is only one target class in the first stage. We have proposed the use of the one-class classification for detection of malicious flows in the first stage. One class classification techniques learn the model for one target class. It only recognizes objects of target class and all other objects are rejected. The training set for one-class classification technique also consists of target class objects [15].

Mathematically, X is a training set consisting of only malicious IP flows. The one-class classifier learns an output function f_o using the optimized parameter set θ for a given IP flow x_i. The f_o gives a confidence score defining the membership of IP flow x_i with the malicious class.

$$f_o(x_i) = \theta_1 + \theta_2(x_i) \tag{1}$$

The value of f_o is used in a decision function h_o to obtain the classification result. For all unclassified IP flows $z_i \in Z$, if the value of $f_o(z_i)$ is higher than the maliciousness threshold t, the flow is classified as malicious or normal otherwise. The value of maliciousness threshold t is user-defined.

$$h_o(z_i) = \begin{cases} malicious, & \text{if} f_o(z_i) \geq t \\ normal, & \text{if} f_o(z_i) < t \end{cases} \tag{2}$$

The malicious flows recognized in the first stage are forwarded to the second stage. The second stage detection process associates an attack type with the malicious IP flows. Since the number of attack types can be more than one, we use multi-class classification technique to classify the IP flows into different attack types [8].

The training set Y contains labeled malicious IP flows for K attack types. The multi-class classifier learns an output function $f_{mk}(y_i)$ for all K attack types using the training set Y where $y_i \in Y$. The function f_{mk} gives a confidence score for all attack types in K.

$$f_{mk}(y_i) = \theta_1 + \theta_2(y_i) \forall k \in K \tag{3}$$

For all unclassified IP flows $z_i \in Z$, The incoming flow is classified into the attack type for which the function $f_{mk}(z_i)$ gives the highest confidence score.

$$h_m(z_i) = \underset{k \in K}{\arg\max}\, f_{mk}(z_i) \tag{4}$$

The classification result of both stages is combined in a consolidated intrusion alert module. The alert module output the maliciousness of flow and the possible attack type in the alert. The information can be used by the security administrator to protect the integrity of the network.

Our future work will explore the application of one-class classification to IP flow records for intrusion detection. We will review available one-class classification methods and evaluate them on flow-based intrusion datasets for detection of malicious flows. Different techniques used for one-class classification include density estimation, reconstruction methods, and boundary methods. The outcome of the step will determine that which one-class classification perform better in intrusion detection using IP flow records.

In the second step, various machine learning technique will be evaluated using flow-based datasets for classification of malicious IP flows in different attack classes. In the third step, we will combine the best performing one and multi-class classification techniques and develop a multi-stage flow-based intrusion detection model. We will use various flow-based datasets [11] and testbeds to evaluate the performance of proposed intrusion detection system.

V. Conclusion

This paper proposes a multi-stage model for intrusion detection using IP Flow records. The first stage classifies the IP flow records into the normal and malicious classes. The second stage detection process performs detail analysis and classifies the flow into different attack types. We also give implementation detail of our model using one and multi-class classification. We conclude that our model is efficient since it discards the majority of the flows in the first stage using a computationally inexpensive algorithm. Only malicious flow are analyzed in detail. The multi-stage detection model also reduces the false positive rate through the application of two different classification techniques.

References

[1] Hashem Alaidaros, Massudi Mahmuddin, and Ali Al Mazari. An overview of flow-based and packet-based intrusion detection performance in high speed networks. In *In Proceedings of the International Arab Conference on Information Technology*, 2011.

[2] Ammar Alazab, Michael Hobbs, Jemal Abawajy, and Ansam Khraisat. Malware detection and prevention system based on multi-stage rules. *International Journal of Information Security and Privacy (IJISP)*, 7(2):29–43, 2013.

[3] Payam Vahdani Amoli and Timo Hämäläinen. Real time multi stage unsupervised intelligent engine for nids to enhance detection rate of unknown attacks. In *2013 IEEE Third International Conference on Information Science and Technology (ICIST)*, pages 702–706. IEEE, 2013.

[4] Karel Bartos and Martin Rehak. Ifs: Intelligent flow sampling for network security–an adaptive approach. *International Journal of Network Management*, 25(5):263–282, 2015.

[5] Anna L Buczak and Erhan Guven. A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials*, 18(2):1153–1176, 2015.

[6] Benoit Claise, Brian Trammell, and Paul Aitken. Specification of the ip flow information export (ipfix) protocol for the exchange of flow information. Technical report, IETF, 2013.

[7] Luigi Pietro Cordella, Alessandro Limongiello, and Carlo Sansone. Network intrusion detection by a multi-stage classification system. In *International Workshop on Multiple Classifier Systems*, pages 324–333. Springer, 2004.

[8] Corinna Cortes, Mehryar Mohri, and Afshin Rostamizadeh. Multi-class classification with maximum margin multiple kernel. In *ICML (3)*, pages 46–54, 2013.

[9] Jerald Dawkins and John Hale. A systematic approach to multi-stage network attack analysis. In *Information Assurance Workshop, 2004. Proceedings. Second IEEE International*, pages 48–56. IEEE, 2004.

[10] Christian Fuchs. Implications of deep packet inspection (dpi) internet surveillance for society.(= privacy & security-research paper series 1). *Available from {http:/www. projectpact. eu/documents-1/% 231_Privacy_and_Security_Research_Paper_Series. pdf}*, 2012.

[11] Sebastian Garcia, Martin Grill, Jan Stiborek, and Alejandro Zunino. An empirical comparison of botnet detection methods. *computers & security*, 45:100–123, 2014.

[12] Mario Golling, Rick Hofstede, and Robert Koch. Towards multi-layered intrusion detection in high-speed networks. In *Cyber Conflict (CyCon 2014), 2014 6th International Conference On*, pages 191–206. IEEE, 2014.

[13] Rick Hofstede, Pavel Čeleda, Brian Trammell, Idilio Drago, Ramin Sadre, Anna Sperotto, and Aiko Pras. Flow monitoring explained: from packet capture to data analysis with netflow and ipfix. *IEEE Communications Surveys & Tutorials*, 16(4):2037–2064, 2014.

[14] Jae-Hyun Jun, Dongjoon Lee, Cheol-Woong Ahn, and Sung-Ho Kim. Ddos attack detection using flow entropy and packet sampling on huge networks. *ICN 2014*, page 196, 2014.

[15] Shehroz S Khan and Michael G Madden. One-class classification: taxonomy of study and review of techniques. *The Knowledge Engineering Review*, 29(03):345–374, 2014.

[16] Do-hyeon Lee, Doo-young Kim, and Jae-il Jung. Multi-stage intrusion detection system using hidden markov model algorithm. In *Information Science and Security, 2008. ICISS. International Conference on*, pages 72–77. IEEE, 2008.

[17] P Natesan and P Balasubramanie. Multi stage filter using enhanced adaboost for network intrusion detection. *International Journal of Network Security & Its Applications*, 4(3):121, 2012.

[18] Thaksen J Parvat and Pravin Chandra. A novel approach to deep packet inspection for intrusion detection. *Procedia Computer Science*, 45:506–513, 2015.

[19] Anna Sperotto and Aiko Pras. Flow-based intrusion detection. In *Integrated Network Management (IM), 2011 IFIP/IEEE International Symposium on*, pages 958–963. IEEE, 2011.

[20] Anna Sperotto, Gregor Schaffrath, Ramin Sadre, Cristian Morariu, Aiko Pras, and Burkhard Stiller. An overview of ip flow-based intrusion detection. *Communications Surveys & Tutorials, IEEE*, 12(3):343–356, 2010.

[21] Chih-Fong Tsai, Yu-Feng Hsu, Chia-Ying Lin, and Wei-Yang Lin. Intrusion detection by machine learning: A review. *Expert Systems with Applications*, 36(10):11994–12000, 2009.

[22] Yuji Waizumi, Hiroshi Tsunoda, Masashi Tsuji, and Yoshiaki Nemoto. A multi-stage network anomaly detection method for improving efficiency and accuracy. *Journal of Information Security*, 3(01):18, 2011.