ЎЗБЕКИСТОН РЕСПУБЛИКАСИ АХБОРОТ ТЕХНОЛОГИЯЛАРИ ВА КОММУНИКАЦИЯЛАРИНИ РИВОЖЛАНТИРИШ ВАЗИРЛИГИ

МУҲАММАД АЛ-ХОРАЗМИЙ НОМИДАГИ ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ ҚАРШИ ФИЛИАЛИ

АХБОРОТ-КОММУНИКАЦИЯ ТЕХНОЛОГИЯЛАРИНИНГ РИВОЖЛАНИШ ИСТИҚБОЛЛАРИ

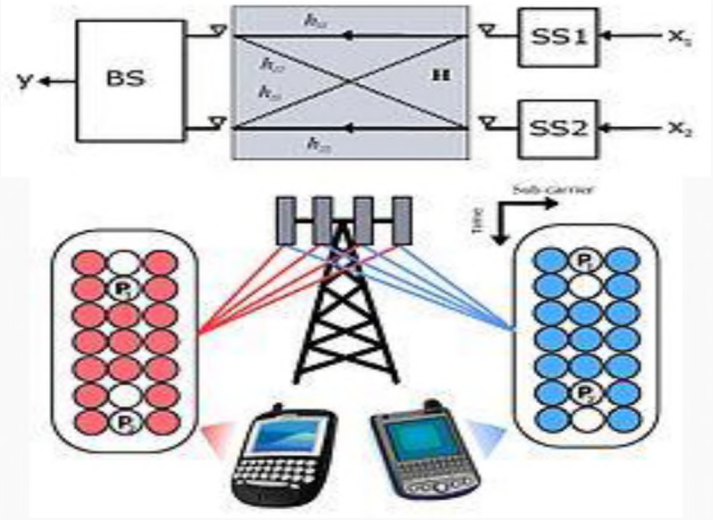
мавзусидаги

Республика илмий-амалий анжуман
МАЪРУЗАЛАР ТЎПЛАМИ

(20-21 апрель)

ҚАРШИ-2018

Другие усовершенствованные методы MIMO, применяемые к WiMAX



MS пространственно некоррелированные

Литературы

1. L. Jorguseki, "Vision on Radio Resource Management (RRM) and Quality of Service (QoS) for Wireless Communication Systems in Year 2020", Globalization of Mobile and Wireless Communications, R. Prasad et al. (eds) Springer, Netherlands, 2011.
2. Going Greener, Vodafone, http://www.vodafone.com/content/index/uk_corporate_responsibility/greener.html.
3.Y. Chen et al., "Fundamental Tradeoffs on Green Wireless Networks," IEEE Communications Magazine, 2011.

SIGNATURE STATISTICAL PORT CLASSIFIER (SSPC) IS REAL-TIME TRAFFIC CLASSIFICATION ALGORITHM

Makhamadjonov A.A. Master of TUIT named after Muhammad al-Khwarizmi,
Akhmadjonov A.M. Student of TUIT named after Muhammad al-Khwarizmi,

Internet service providers (ISPs) and network operators are mostly interested in knowing the amount of traffic carried by their networks for the purposes of optimizing network performance and security issues. Therefore, Internet traffic classification is something valuable, particularly for interactive traffic applications such as VoIP and online games. Simple classification assumes that most applications use well-known port numbers, and the classifier uses this port number to identify the application type. However, most Internet applications use unknown port numbers, or more than one application uses the same port number, which indicates the failure of port base classification. Another classification method is payload based (deep packet inspection), which is individual packet inspection, looking for unique signatures. However, using this technique faces two problems; first, it is difficult to detect non-standard ports by using packet inspection because these packets are encrypted. Second, deep packet inspection touches on users' privacy. In order to solve the problem of past classification methods (base port and payload inspection), machine learning (ML) technique was developed. ML uses artificial intelligence to classify IP traffic, which provides a powerful solution by extracting the right information from application features. Moreover, some of the ML algorithms are suitable for Internet traffic flow classification at a high speed. Most of the proposed ML classification methods are limited to offline traffic classification and cannot support online classification. Online classification means, the decision of which packet belongs to which flow, assuming to be on the traffic speed. Such, like any hardware classifier (PacketShaper, SANGFOR), is installed on the network path to classify with the passage of the traffic. The main problem that

meets the online classification decision is the high speed of Internet traffic. It is difficult to take an online classification decision with huge amounts of Internet traffic. The question is how to divide the Internet traffic into flows, calculate flow patterns, and make classification decisions online with high Internet traffic speed. Most previous literature worked with classifiers using real time traffic, however only few of them provided a classifier which can make an online decision. This paper describes the development of an online Signature Statistic Port Classifier (SSPC) algorithm, which can identify Internet traffic shortly after traffic is captured. The task is also to classify network applications that use any TCP or UDP protocols. The classifier differs from others since it takes the classification decision based on three different parallel hybrid methods.

General Concepts Definition 1: Flow is a group of packets share the same 5-tuples (source address, destination address, source port, destination port, and transport protocol). Flow can be represented by TCP or UDP packets. We consider unidirectional flows, which defines client-server traffic as different from server client traffic. Definition 2: Real time traffic is the Internet traffic captured from the campus network during the period of experiments. Definition 3: Offline decision is the decision by the classifier about the flows identification, which is taken offline after capturing time. Definition 4: Online decision is the decision by the classifier about the flows identification, which is taken online within capturing time. Since the Internet applications are continuously being developed, it is difficult to classify the traffic by using only one classification method. This paper develops online Signature Statistical Port Classifier (SSPC), which is making classification decision near to the capturing time. The classifier makes his final decision based on three parallel partial decisions (port classifier, signature classifier, and statistic classifier)

Port classifier Port based classification cannot achieve a high accuracy all the time. In this paper port classification was used as a part of our classification system and it represents low priority of SSPC classification decisions. In most cases, SSPC classification decisions are not made based on the port classifier alone, but shared with the other two classifiers. We developed the port classifier algorithm as a part of the SSPC algorithm. The port classifier makes its own decision based on the port database. Easley, our port classifier algorithm, looks for the port number of the considered flow in the port database. If it is found, then the considered flow will be classified based on port classifier rules.

Signature classifier Payload classification can achieve high accuracy, but it cannot work with encrypted traffic. As before, our classifier did not fully depend on payload, but it only represented a part of the SSPC decision. We developed a signature classifier algorithm, which is the second part of the SSPC algorithm; this algorithm makes its classification decision based on some saved signatures. We added very general signatures (such as DNS query and http host) for the considered applications, which are extracted from the application layer. If the considered flow carries a signature from the signature database, then it will classify based on the signature group.

Statistical classifier The main problem that meets ML classification is the high false positive. To reduce this problem we consider two issues: firstly, the offline training datasets were continuously updated and collected manually from the same network we needed to classify, and secondly, the statistical classifier was supported by the other two classifiers. The statistical classifier algorithm is the third part of the SSPC algorithm. Same as before, ML classifiers represent a part of our system decision. SSPC For the purpose of increasing the classification efficiency, SSPC was proposed. SSPC is the result of the three previous classifiers' decisions. Differing from the previous studies and, SSPC did not base on hardware component; it also did not make its decision based only on one method. The online flow classification occurred after comparison of three stage classification decisions. Moreover, SSPC was tested for online classification decisions.

SSPC Architecture Figure 1 illustrates the classifier stages, which start by fully packets capturing using traffic mirror.

Before delivered to the three classifiers, the traffic was divided into flows based on the 5-tuples. Each flow will classify three times by each of the three classifiers. The port classifier (algorithm) will compare the captured flow port with a list of saved port numbers. If the captured flow belongs to any group of saved ports, it will be identified as its group. The second classifier (statistical) will work in parallel with the first classifier. Based on offline training and testing

datasets, some classification rules were built. Based on these rules, the statistical classifier (algorithm) makes its online decisions to identify the captured flows. On the other hand, the signature classifier will classify the same flow at the same time as the previous two classifiers; Figure 1 SSPC architecture 654 the classifier will compare a part of the captured flow with the signature database. If the signature matches any of the saved signatures, the classifier will make its online decisions to identify the captured flows. SSPC is an algorithm which compares between the three classifier results and makes its online classification decision based on some priorities rules.

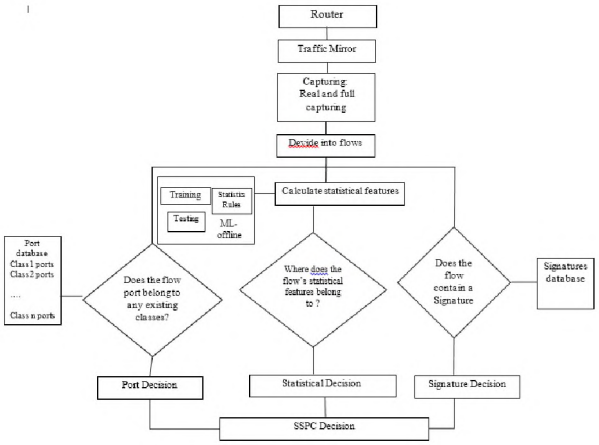


Figure 1. SSPC architecture

SSPC Algorithm The SSPC algorithm is shown in algorithm 1. The SSPC algorithm consists of three partial classifier algorithms each classifier has it's own classification decision. Because of the accuracy of the signature classifier, the first priority in SSPC decision making goes to the signature classifier. If the signature classifier makes any decision about this flow, then SSPC final decision will to the decision made by the signature classifier. The second priority of SSPC happen in the case when of all the partial classifiers cannot make any decision about this flow. In this case, SSPC will classify the flow as unknown. The third priority of SSPC occurs in the case when the statistics and the port classifiers have the same decision and signature classifier have no decision (unknown). In this case, SSPC identifies this flow based on the statistic and port classifiers. When the statistic and port classifiers have different opinions about the flow, SSPC will classify this flow as the statistic classifier as. The SSPC decision is based on the port classifier in only one case. This occurs when the port classifier has a decision whilst both statistic and signature classifiers have no decision about the flow.

Port based classification has the advantage of non complexity; however, it cannot achieve high accuracy with applications of unknown port numbers. On the other hand, payload classifiers have the advantage of accurate classification, but incapable to classify encrypted traffic. Statistical classifier has the benefit of classifying encrypted traffic, but it has the problem of high false positive and features overlapping. In parallel, each of the three partial classifiers (based on the three methods) makes a decision about each traffic flow. SSPC based on some priority rules calculates the final decision from the outcome of the three classifiers. Real time datasets (more than 7900 flows) were captured in the campus environment, which includes WWW (http, https) and non WWW (FTP data, FTP control, online gaming, and Skype) traffic. The SSPC system is tested in two stages, offline and online. The results of the offline experiments show that SSPC has higher accuracy compared to the three partial classifiers. To further validate the robustness of the algorithm, online classification using SSPC algorithm is carried out. The classification decision is made immediately after the end of flow capture. Thus, SSPC has achieved the two objectives; the first, capitalizing on the effectiveness of the individual classifiers which sums up to effectively increase SSPC accuracy. Second, SSPC can still classify the online Internet traffic without any compromise in delay.