Rogue Access Point Detection Using Segmental TCP Jitter

Gaogang XIE
Institute Of Computing Technology, CAS, 100080 Beijing
xie@ict.ac.cn

Tingting HE
Institute of Computing Technology, CAS, 100080 , Beijing
hetingting@ict.ac.cn

Guangxing ZHANG
Institute of Computing Technology, CAS, 100080, Beijing
guangxing@ict.ac.cn

ABSTRACT
Rogue Access Points (RAPs) pose serious security threats to local networks. An analytic model of prior probability distribution of Segmental TCP Jitter (STJ) is deduced from the mechanism of IEEE 802.11 MAC Distributed Coordinated Function (DCF) and used to differentiate the types of wire and WLAN connections which is the crucial step for RAPs detecting. STJ as the detecting metric can reflect more the characteristic of 802.11 MAC than ACK-Pair since it can eliminate the delay caused by packet transmission. The experiment on an operated network shows the average detection ratio of the algorithm with STJ is more than 92.8% and the average detection time is less than 1s with improvement of 20% and 60% over the detecting approach of ACK-Pair respectively. Farther more no WLAN training trace is needed in the detecting algorithm.

Categories and Subject Descriptors
C.2.3 [**Network Operations**]: Network management and monitoring

General Terms
Management, Measurement

Keywords
Rogue AP, Segmental TCP Jitter, Analytic Model, Sequential Hypothesis Testing.

1. INTRODUCTION
802.11-based wireless access network has been deployed widely recent years due to its unlicensed spectrum, cheap wireless interfaces, high bandwidth and the inherent convenience of computing. However, the vulnerabilities for example DOS attack, wiretapping and incursion have gone all along with and threaten the popularization of WLAN. Rogue Access Point (RAP) is one of the most popular threats [1,2]. The RAP detecting methodologies can be classified into two categories: the Over-the-Air (OTA) and the Over-the-Wire (OTW). OTW has attracted great research force due to its advantages over OTA. MAC/IP address filtering and flow characteristics are two common criterions used in RAP detection [1,2,3]. The methodology based on MAC/IP address filtering will be invalid in the scenes of network address transfer and address spoofing. The flow-based detecting approaches identify the connection categories from the prior possibility distribution of flow characteristics obtained in advance from captured WLAN trace. Unfortunately, usually it is impossible to get these trace for organizations without WLAN.

WWW 2008, April 21–25, 2008, Beijing, China.
ACM 978-1-60558-085-2/08/04.

An analytic model of STJ has been deduced from the mechanism of 802.11 MAC DCF and used as the metric to differentiate the link types in this paper. An algorithm of detecting RAPs is proposed based on the analytic model. The experiment result on an operated network shows its advantage over the approaches based on ACK-Pair.

2. RELATED WORK
OTA-based detection approaches parses SSID and MAC of AP from captured data frames to detect RAPs. Almost all existed detection instruments provided by vendors used OTA, for example AirDefense, AirMagnet and AirWave. OTA is generally ineffective because of time-consuming manual scans, signal range and expensive besides MAC/IP address spoofing. OTW-based detection approaches determine RAPs using MAC/IP or traffic flow characteristics. Cisco offers some tools to detect RAPs by querying routers or switches for MAC/IP address assignment. However, it is of no effect on address spoofing and NAT.

The main idea of the flow characteristics-based detection methodologies identify RAPs using binary decision diagram based on the prior probability distribution of the wire and wireless flows from measurement experiments. The methodologies can be classified into active and passive measurement according the approach of obtaining flow characteristics [1,2,3,4]. TCP Ack-pairs and Inter-packet spacing are two primary properties to detect RAPs. Ack-pairs based approaches can throw off the disadvantage of MAC/IP based approaches, but they also require some restriction conditions e.g. the packet size of TCP should be larger than 1000 bytes, the interval of two sequent packets should be less than *0.24ms*, and all hosts must implement the mechanism of Delayed ACK.

3. ANALYTIC MODEL OF STJ
Let's discuss a TCP connection with WLAN destination host *H*. The STJ denoted as j is defined as the RTT jitter from the detecting site to *H*. Obviously, j is composed by jitters in wire (j_l) and wireless link (j_w). j_w is determined by queuing delay caused by 802.11 MAC DCF. Signal strength, handover and traffic let j_w increase and different with the characteristic of wire's jitters.

A packet trace about 8GB is captured from the access link of a campus Intranet with 1500 users. There are 5,121,419 TCP connections from 847 Ethernet and 213,163 TCP connections from 57 WLAN users respectively. Their STJs are shown as Figure 1. From Figure 1, the distribution characteristic of STJ in WLAN is evidently distinguished from that of Ethernet access.

Denoted packet i queuing delay on AP and wireless host as $q_A[i]$ and $q_s[i]$, then

$$j_w[n] = q_A[n] + q_S[n] - q_A[n-1] - q_S[n-1] \quad (1)$$

The probability distribution of STJs caused by wireless access can be deduced from the DCF Markov chain model ignoring the effect of cross traffic as formula (2).

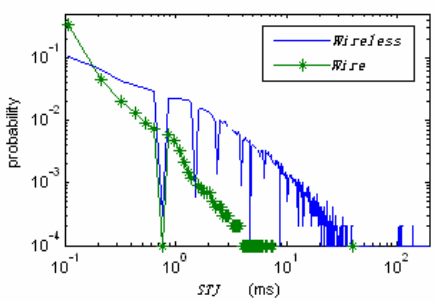

Figure 1. STJs of Ethernet and WLAN Access

$$P(j_W + j_e = t) = \sum_{j_e \geq 0} P(j_w(t - j_e)) * P(j_e) \quad (2)$$

The comparing result of cumulative distribution function (CDF) of STJ from the trace and formula (2) is shown in Figure 2.

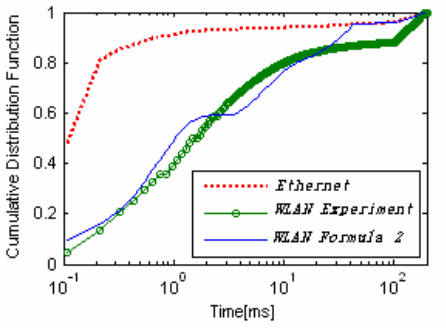

Figure 2. CDF of Theoretical and Experimental WLAN

4. RAP DETECTING ALGORITHM

The main idea of the RAP detecting algorithm is to differentiate the connection categories using sequential hypothesis testing based on analytic model of WLAN's STJ and the prior probability distribution (PPD) of the Ethernet's. The PPD can be achieved from the captured trace. Accordingly, the PPD and CDF of STJ WLAN can be calculated from formula (2). Then, STJ of all TCP connections can be measured online and be leveraged to differentiate the type of connection. The RAPs can be determinated by checking the IP addresses of these detected wireless connections. The detailed illumination of the algorithm is abbreviated.

5. EXPERIMENT RESULT

We implement the algorithm and install the measurement probe into the 100Mbps Ethernet access link of a campus network with a splitter, where users access Internet with Ethernet or 802.11b/g. The experiment results of STJ-based approach and Ack-Pairs[2] are compared as Table 1. There is no detecting error with STJ-based approach. From Table 1, the detecting performance metrics such as the detecting ratio, average detecting time and packets required in our approach are all better than Ack-Pairs based approach.

We also check the effect of NAT with our approach with experiment on the operated network and the data are shown as Figure 3. The CDF of wireless STJ with NAT is near to that of without NAT. Consequently, the performance of detecting the RAP through NAT keeps almost the same as that without NAT.

Table 1. Detecting Results of STJ and ACK-Pairs (A-P)

	2007/12/29		2008/1/2		2008/1/8	
	A-P	STJ	A-P	STJ	A-P	STJ
D-R(%)	66	88	74	92	81	99
Pkt	137	38	79	31	128	41
Avg-T	1.17	0.50	0.51	0.26	0.86	0.34

D-R: Detecting Ratio, Pkt: Packets Required, Avg-T: Average Detecting Time

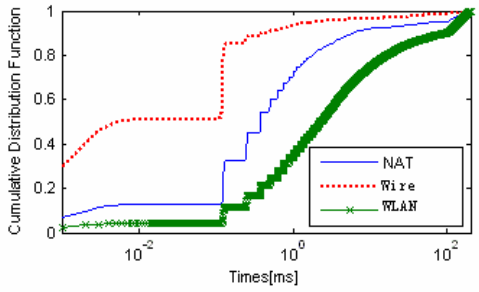

Figure 3. CDF of Wire Access with NAT, Without NAT and WLAN with NAT

6. CONCLUSION

There are three contributions of this paper. STJ, which can distinct reflect wireless MAC mechanism, is used to classify wire and wireless traffic. An analytic model of STJ is deduced from the DCF Markov chain model. A RAP detecting algorithm based on the analytic model is proposed without training trace.

7. ACKNOWLEDGMENTS

This research is supported by National Science Foundation of China with grant no. 90604015, National Basic Research Program of China 2007CB310702, and France Telecom R&D with grant no. 46135216.

8. REFERENCES

[1] R. Beyah, S. Kangude. Rogue access point detection using temporal traffic characteristics. In: Proceedings of IEEE GLOBECOM'04, Dallas, Texas, USA, 2004:2271~ 2275

[2] Wei Wei, Kyoungwon Suh, Bing Wang, Yu Gu, Jim Kurose, Don Towsley. Passive online rogue access point detection using sequential hypothesis testing with TCP ACK-pairs. In: Proceedings of ACM SIGCOMM IMC'07, San Diego, California, USA, 2007: 365~378

[3] C. Mano, A. Blaich, Q. Liao, Y. Jiang, D. Cieslak, D. Salyers, A. Striegel. RIPPS- Rogue Identifying Packet Payload Slicer Detecting Unauthorized Wireless Hosts Through Network Traffic Conditioning. ACM Transactions on Information and System Security, May 2008, to appear.

[4] Wei Wei, Sharad Jaiswal, Jim Kurose, Don Towsley. Identifying 802.11Traffic from Passive Measurements Using Iterative Bayesian Inference. In: Proceedings of IEEE INFOCOM'06, Barcelona, Catalunya, 2006: 1~12

[5] Tickoo O, Sikdar B. Queueing analysis and delay mitigation in IEEE 802.11 random access MAC based wireless networks. In: Proceedings of IEEE INFOCOM'04, HongKong, 2004: 1404~1413