ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (925-929), Month: April - June 2015, Available at: www.researchpublish.com

RAPD Extension with Temporal Traffic Characteristics

[1]Prof. Abhijit S Bodhe, [2]Prof. Shivaji Patil, [3]Prof. Shashikant Deshmukh, [4]Dr.Sanjay Thakur

[1, 2, 3] SRES COE, Kopargaon
[4]Principal, LKCT, Indore

Abstract: **As the value of 802.11 hardware continues to fall, the charm of inserting unauthorized wireless access into enterprise networks grows. These rogue access points (APs) expose the enterprise network to a barrage of security vulnerabilities in this they're usually connected to a network port behind the firewall. Most of this approaches to detective work rogue APs ar rudimentary and are simply evaded by hackers. we have a tendency to propose the utilization of temporal traffic characteristics to notice rogue APs at a central location. This malfunction is independent of the wireless technology (802.11a, 802.11b, or 802.11g), is scalable , does not posses the inefficiencies of the current solutions, and is freelance of the signal vary of the rogue Aps**

Keywords: **Aps, temporal traffic characteristic, enterprise network, wireless technology.**

I. INTRODUCTION

As users notice the advantages of wireless networking at home, they begin to desire an equivalent flexibility within the work. instead of expecting their IT organizations to put in a wireless network, users area unit taking matters into their own hands. staff ar deploying rogue APs and building massive grassroots wireless networks while not the data or consent of their IT departments. These rogue APs represent a significant breach of network security. they're generally connected to a network port behind the company firewall. in addition, staff seldom change even the foremost basic security settings on rogue APs, creating it straightforward for unauthorized outsiders to use the AP and pay attention to network traffic.

Corporate network directors don't seem to be the sole ones UN agency ar, or ought to be, involved concerning the rogue AP downside. Universities' support staffs ar already having a tough time making an attempt to manage the safety of the PCs on the network. struggling from students, staff, and administration, the universities' networking staffs have deployed wireless networking across field with minimum security measures. Some modify the wired equivalency protocol (WEP) and perform a point of application-level authentication before permitting nodes to become related to the network. whereas this is often a decent begin, attributable to numerous factors, as well as price constraints, several universities don't have specific wireless intrusion detection systems, nor do they have any technique of preventing students, staff, or college from putting in their own AP. This villain AP might permit unauthorized pleasant or malicious users onto the network. Further, the network administrator can have problem chase down the wrongdoer.

Similarly, a growing variety of hotels currently provide broadband access in upgraded and even regular rooms. several of the services ar provided by a third-party UN agency accepts payment in exchange for daily net access for one machine. this is often loosely enforced by distribution a brief informatics address to the requesting machine and storing that machine's medium access management (MAC) address. Once the time expires, the information science expires and the communication is blocked till the fee is paid once more. One cannot share the web access with another machine within the space as a result of the informatics is coupled to 1 mackintosh address. This management is well circumvented so multiple users will share the access. The room's users will merely use a router that has mack address spoofing and network address translation (NAT) options. If a user desires to share this one reference to everybody on the hall, he just has got to use a wireless router with an equivalent features.

In general, each organization that incorporates a network ought to have some variety of villain AP detection, particularly organizations that don't have wireless networks. These organizations don't expect, or assume to think about, any variety of malicious wireless activity as a result of they need not deployed a wireless network. This thinking, may result in 2 undesirable outcomes: 1) AN worker installs a villain AP ANd a malicious user stumbles upon a wide-open invite to the company network as they "war drive"; or 2) a hacker installs an AP out of website on a live port (e.g., edifice lobby, ironmongery shop, hospital, building, etc.) and incorporates a entrance to the network from the automobile parking space or, victimization signal boosting antennas, even farther away.

To these authors' information, the villain AP detection downside has been unnoticed by educational researchers. Most solutions are fast fixes by wireless to put in space network (WLAN) security vendors. we have a tendency to illustrate, by empirical analysis, a completely unique approach to rogue AP detection exploitation temporal traffic characteristics. the remainder of the paper is organized as follows: In section II we tend to discuss current approaches. we have a tendency to discuss the background of our theme in Section III. In Section IV we have a tendency to describe our experimental setup. Section V provides the results and performance analysis of our theme. In Section VI we have a tendency to provide the conclusion and that we conclude this paper with a discussion on future add Section VII.

II. CURRENT APPROACHES

A. Wireless Approaches:

Most of this approaches for detective work villain APs ar rudimentary and simply evaded by hackers. Some organizations have equipped IT personnel with wireless packet instrument tools (e.g., sniffers) on laptops and hand-held devices (e.g., AirMagnet [5] and NetStumbler [6]), forcing IT personnel to steer the halls of the enterprise or field finding out villain APs. This methodology is usually ineffective because manual scans ar long and dearly-won – and, therefore, ar conducted knave. Also, with 802.11 hardware operative at separate frequencies (802.11a - 5Ghz and 802.11b - 2.4Ghz), IT personnel should upgrade their detection devices to accommodate multiple frequencies. Moreover, scans ar simple to elude, since a rogue AP easily simply be unplugged when the scan takes place.

Most vendors these days go a step any. instead of wishing on AN worker equipped with a scanner, they allow IT to initiate Associate in Nursing enterprise-wide scan from a central location. this is often doable by exploitation separate hardware devices [2][3][7][8] (e.g., sensors) or victimization APs to discover beacons from close APs [2], and transmitting this info back to a central management platform containing the wireless network policy for analysis [1]. This methodology becomes expensive, considering that one must place sensors or APs throughout the complete enterprise to watch the air waves. this system is additionally fully impractical for the networks that don't have wireless APs. very similar to the disadvantage of the "walking the halls" answer, every sensor/AP should operate at each frequencies to be utterly effective. Moreover, with sensors deployed throughout the network, one still might not be ready to discover the villain AP. The clever worker could have used a antenna, or reduced the signal strength to hide the little vary among his/her workplace. Another downside of wireless -based solutions is that they're going to incorrectly report the wireless network within the low house adjacent as a rogue.

B. Hybrid Wireless and Wired Approach:

Taking a step within the right direction, Wavelink [2] combined the antecedently mentioned techniques for detection scoundrel APs with listening at network layers two and three and querying switches and routers to see what devices ar connected to them, thus, trying to supply a hybrid wired and wireless approach to detection scoundrel APs. This fails for constant reasons that the wired-only solutions mentioned well below fail.

C. Wired Approaches:

Cisco offers a additional complete, scalable, and comprehensive approach employing a suite of tools [9] that aren't restricted by signal vary. They conceive to discover APs by querying routers and switches for company mackintosh address assignments (i.e., if the mackintosh address belongs to Linksys, the mackintosh address cannot belong to a laptop and becomes suspicious). This fails as a result of macintosh addresses may be spoofed or cloned simply by AN AP. Another approach within the suite is that the use of httpd question to speak with the net server residing on the AP. this can be a decent approach, however the node should already be suspected as being AN AP (may be victimization one in all the same methods), or each node on the network should be queried. This approach assumes that the wireless router responds to http queries. to boot, this invasive approaches taken into account active, adding important unwanted traffic on the network and may conjointly alert a complicated scoundrel AP user of a scan for the AP. The suite conjointly has Associate in Nursing application that permits the viewing of markup language code generated once configuring AP settings. though' this approach can add theory, the window of opportunity is proscribed since this information is merely transmitted once the AP's configuration is updated. to boot, as signature-based IDSs will attest, reassembling application-level information becomes harder and impractical as network speeds increase.

Another LAN solely approach is bestowed by Biometrics [4]. Their product features a LAN only approach, however is ambiguous with details. the fundamental premise of their work is that they probe the network to spot the profile of a wireless AP. whereas the main points were unclear, Biometrics' general approach proves not climbable since it needs a laptop to take a seat on every section of the network. Their approach unjustly assumes that the network could be a shared network. As mentioned in that previous section, APs may be organized to ignore network queries

III. BACKGROUND ON OUR THEME

The primary goal of our analysis is to discover scoundrel APs from a central location (a switch that supports a subnet) with the detection freelance of the wireless technology. we have a tendency to show a scalable resolution, so not trying to set up information before analysis.

Also, there solution can perform severally of the signal vary of the scoundrel APs. Our analysis involve scrutiny traffic characteristics of flows from totally different sources in an exceedingly LAN section and detection traffic coming back from a wireless AP.

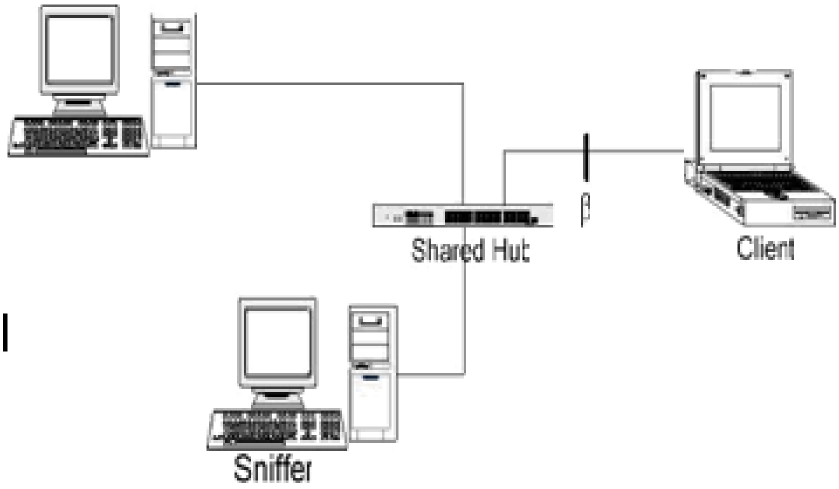

Figure.1 Configuration with wired link

Rogue Access shaped largely as a result of higher layer (e.g., TCP) mechanics, with a comparatively easy shaping from the link layer. A wireless link but, shapes traffic otherwise. as a result of variations in channel conditions, wireless link capability varies and random delays are introduced. The distinction in link speed between wired and wireless links conjointly shapes the characteristics considerably. Consequently, our detection theme relies on the premise that if traffic at a switch port is ascertained in each directions over time, and input-response related , completely different patterns could also be ascertained for segments with and completely different wireless links.

The input-response correlation involves estimating that a part of traffic is in response to that impulse (or input). Thus, for each response quanta of traffic from AN finish purpose within the section, temporal characteristics could also be analyzed by classifying mean, variance, and different frequency response characteristics of inter-packet spacing. For all switch ports, such analysis over time is succinctly hold on in an exceedingly variety of state variables. As time progresses, scoundrel AP (or variety of them) are detected because the distinction in state variables between ports crosses a threshold.

The aim of this analysis is to experiment and derive such state illustration and its derivation from the ascertained temporal characteristics of traffic. during this paper, we have a tendency to gift the ascertained variations in inter-packet spacing in wired and scoundrel A situations.

Our theme starts with the hypothesis that a wireless link in an exceedingly network path of multiple links would cause a additional random and temporally totally different spreading of packets, as compared to a path that has solely wired links. think about Figure one on the subsequent page. the target is to differentiate the state of affairs shown in Figure one, within which a switch port is connected to a network section that has no wireless links, from the state of affairs shown in Figure two, within which a switch port is connected to a section with a minimum of one wireless link. the assumption is that a majority of ports in a very switch ar connected to network segments that have solely wired links. The process and deciding are performed at the switch with the input because the link layer traffic traversing, in each directions, a switch port. the amount of hops between the switch and finish purpose can presumably have an effect on the temporal characteristics of traffic as ascertained at the switch. Queuing and congestion tend to mask the temporal shaping of traffic through finish points. However, we have a tendency to think about situations that involve network segments with, at most, two links from the detection switch. Such situations ar unremarkably ascertained in most LAN native networks. The reliableness of wired links makes the temporal characteristics of traffic, in a path, to be

IV. EXPERIMENTAL SETUP PLANNED

To test the inter-packet spacing theory in an exceedingly controlled surroundings, we tend to engineered associate experimental tested. the bottom state of affairs is portrayed in Figure one, wherever the sole traffic on the network was the traffic generated from our shopper. the primary state of affairs shows a laptop server machine, a laptop computer acting as a consumer connected by a 100Mbps shared hub (the hub was solely accustomed produce a state of affairs wherever we have a tendency to may sniff the traffic on the link). an extra laptop was accustomed observe traffic traversing the link. The network sniffing package used was Ethereal [10].

We conducted experiments victimization FTP traffic for 10 totally different file sizes from 10MB to 100MB victimization increments of 10MB. every take a look at was done ten times and similar results were generated. The shopper machine (laptop) initiated the transfer and uploaded a file to the server. For this experiment, we have a tendency to label the trail taken by the info traffic from the shopper to the server because the forward path. the info was captured to be analyzed offline. For the wireless experiments, we have a tendency to extended the network with a wireless router as shown in Figure two.

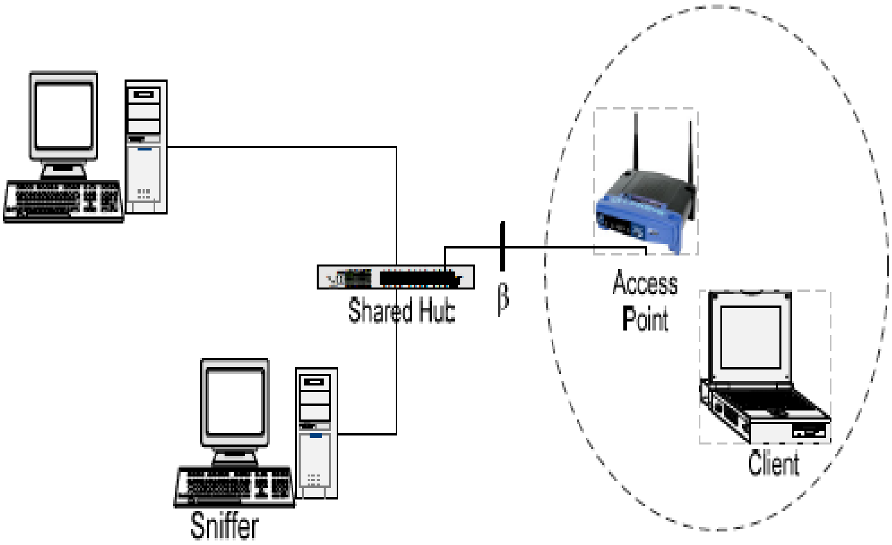

Figure.2 Configuration with wireless link

V. AP DETECTION PERFORMED ONE HOP AWAY

Aggregating the responsibility of watching scoundrel APs on many segments into a central location is an understandable want. we have a tendency to conceive to take a step therein direction by testing our approach one hop downstream from the monitored node. Specifically, we have a tendency to check to ascertain if the inter-packet spacing characteristic can hold, once the flows traverse a loaded switch and once doubtless variable queuing delays ar introduced. To a lot of accurately model a full intermediate switch, we have a tendency to generated totally different levels of cross traffic at the intermediate switch. the purpose of the cross traffic is to put a load on the intermediate switch, to not inject packets into the experiment flow stream. Thus, the test beds shown in Figures one and a couple of were expanded to incorporate an extra router with 2 machines connected. the additional elements were injected at the main goal "β" shown in Figures 1 and a couple of figures..

VI. CONCLUSION

In this paper, we have a tendency to be showed a way to discover APs from central location victimization temporal traffic characteristics. Further, this method, once employed in conjunction with AN allowed AP policy or access list, may simply establish rogues. The technique is novel as a result of it presents a climbable LAN-only resolution that's freelance of the wireless technology. Also, this resolution can perform freelance of the signal vary of the scoundrel APs.

VII. FUTURE WORK

Our planned theme needs that the rouge AP watching be performed within the switch wherever the scoundrel AP is instantly connected or one immediate hop downstream. This becomes difficult and expensive once one considers large-scale networks (e.g., field networks). we have a tendency to ar presently work techniques for activity the analysis additional upstream. Specifically, we have a tendency to commit to verify the connection between the amount of hops upstream and also the chance of correct detection. we have a tendency to expect this can prove additional economical. we are going to conjointly run actual experiments with totally different information models on an oversized field network and perform trace-driven simulations to characterize fascinating situations.

Additionally, we have a tendency to commit to produce the acceptable perform that may take the ascertained statistics as input and generate the chance of scoundrel AP Index (RAI) parameter. Once the statistics and chance scoundrel perform has been determined and deemed acceptable, we are going to extend our analysis to support non-traditional (other than 1st in 1st out (FIFO)) queuing at switches (i.e., queues that have priority related to them - AN example would be AN computer network that supported vex informatics (VoIP), wherever voice traffic has higher priority than knowledge traffic within the LAN

Our final space of interest deals with the flexibility to perform the scoundrel AP identification in an automatic fashion. Specifically, this practicality ought to be a utility that may run on a switch. Our current theme uses a visible approach that may prove difficult for a automatic data processing system to investigate. we have a tendency to ar observing AN approach wherever we will use the realm underneath the curves of the traffic shown to modify the analysis. As determined within the figures, the world below the wired curves is considerably larger than that underneath the wireless curves. Thus, by computing and examination the areas, we are able to probably perform this scoundrel AP identification, without inter-packet spacing, while not human intervention.

REFERENCES

[1] www.airwave.com/airwave_rogue_detection.pdf

[2] www.wavelink.com/downloads/pdf/wlmobilemanager_w p_rogueap.pdf

[3] www.highwalltech.com/products.cfm?menu=hwsent&page=hwsent

[4] www.wimetrics.com/WAPD.htm

[5] www.airmagnet.com

[6] www.netstumbler.com

[7] www.computerworld.com/mobiletopics/mobile/story/0,10801,72065,00.html

[8] www.airdefense.net

[9] winfingerprint.sourceforge.net/presentations/APTools.ppt

[10] www.ethereal.com