Formato A

Perfil de la propuesta de Tema de Tesis

Nombre del Asesor(es): César A. Santiváñez, Ph.D.

Titulo (tentativo) de la tesis: Diseño e implementación de un sistema de detección de Puntos de Acceso (Access Points, o APs) inalámbricos intrusos en la red WiFi del campus de la PUCP.

Descripción del proyecto:

Las redes WiFi, al compartir el medio de transmisión (el espectro electromagnético) son vulnerables a una serie de ataques. El rango de vulnerabilidades de la red WiFi de la PUCP va desde el visitante/alumno que establece su propia red WiFi, inadvertidamente causando interferencia o degradando la calidad de experiencia de usuarios autorizados desde el campus, hasta el atacante malicioso que establece una red WiFi con las misma identidad (SSID) que la red de la PUCP con la intención de hacerse pasar por un AP valido de la PUCP y así capturar el trafico de los usuarios WiFi PUCP (ataque "Honeycomb").

Dado que la PUCP esta migrando a un sistema de seguridad WiFi basado en clave WAP individual (por usuario), y autenticación 802.1x, y donde las autorizaciones de acceso (así como la asignación de VLAN) están asociadas al perfil del usuario, la red WiFi se vuelve atractiva para el ataque del tipo "Honeycomb" arriba mencionado: un atacante localizado dentro o cerca del campus puede irradiar desde un AP tratando de hacerse pasar por un AP valido de la WiFi PUCP para así conseguir que usuarios se conecten a el, revelando sus certificados o claves de acceso. Armado con estas claves (y de corresponder a usuarios con altos privilegios), el atacante puede entonces tener acceso a recursos críticos de la universidad.

Por esa razón, es importante contar un sistema que constantemente escanee el espectro electromagnético en el campus, identifique AP intrusos, y los neutralice. Por ejemplo, los AP de la red WiFi PUCP (Cisco Aironet 3600 y 3700) y sus controladores (Cisco's WLC 5508 y WLC 5760) cuentan con el sistema wIPS (wireless Intrusion Prevention System – sistema de prevención de intrusos inalámbricos). No obstante, para operar correctamente, este sistema requiere de información oportuna sobre la actividad sospechosa en las bandas de operación de la red WiFi PUCP.

Sin embargo, el sensado del canal es una operación costosa. Por un lado, si es efectuado por los Puntos de Acceso (Access Points, o APs) que ya están en operación sirviendo trafico de usuarios, requerirá interrumpir temporalmente la transmisión de datos para proceder a escanear todos los canales de la banda de operación, lo que disminuye el throughput y ocasiona retardos que pueden ser inaceptables para aplicaciones criticas como voz y video en tiempo real, sobretodo si el AP intruso es altamente móvil o dinámico (p.ej., cambia constantemente de canal de operación), lo que obliga a un sensado mas frecuente si se quiere garantizar una probabilidad alta de detección. Por otro lado, si es sensado es efectuado por hardware dedicado, el costo de este hardware es comparable al costo de los APs. Lo mas probable es que una solución hibrida sea necesaria: en áreas de poca trafico o donde se espera poca movilidad de los AP intrusos se pueda utilizar un AP para el sensado durante los tiempos muertos (osea, no hay comunicación), mientras que en zonas de alto trafico o alta movilidad se requerirán módulos de sensado dedicados. Asimismo, una solución donde un sensor es co-localizado con cada AP es muy costosa y probablemente innecesaria. Dado que para detectar AP intrusos (decodificación de "beacons" del bitrate mas bajo) se necesita una relación señal a ruido (SNR) menor que la necesaria para establecer una comunicación (decodificar un paquete de un bitrate alto), el rango de detección de APs intrusos es mayor al rango de comunicación/cobertura. Entonces, la densidad de detectores necesaria para

efectivamente escanear el espectro en toda la red es menor a la densidad de APs necesaria para garantizar total cobertura (a un bitrate adecuado) en la red.
Esta tesis busca determinar el numero y ubicación de módulos de sensado/detección de AP intrusos necesarios para monitorizar el espectro electromagnético del campus de la PUCP. El diseño será validado con simulaciones sobre mapas de calor (capturan el pathloss, o perdida de señal, entre cada 2 puntos del campus de la PUCP), y de concretarse la compra de los módulos WSSI de sensado/detección por DIRINFO (proceso actualmente en evaluación) se validara con experimentos sobre la red de sensores instalado.

(si la tesis es grupal presentar *un formato A para cada alumno con sus objetivos específicos*):
Objetivo general:
- Diseñar una red de detectores de AP intrusos para el campus de la PUCP.
Objetivos específicos:
- Modelar la ubicación de los detectores como un problema de optimización, donde la función a minimizar es el costo total de los sensores sujetos a restricciones mínimas de probabilidad y tiempo de detección del AP intruso bajo ciertas condiciones de movilidad y dinamicidad, así como garantías mínimas de calidad de servicio de los usuarios validos de la red WiFi PUCP.
- Determinar el numero y la ubicación de los detectores dedicados, indicando también los APs que complementarán a los detectores dedicados realizando sensado de canales durante periodos muertos (no comunicación).
- Evaluar la performance de la red de detección (probabilidad de detección versus movilidad/dinamicidad del atacante) vía simulaciones y – en caso DIRINFO concrete la adquisición de los módulos de sensado recomendados – experimentación.

Requerimientos de diseño del Sistema o circuito (si fuera el caso):
- Mapa topográfico o topológico del campus PUCP. Donde se capture el "pathloss" (perdida de espectro entre cada 2 puntos).
- Computadora para correr algoritmos de optimización de ubicación de detectores, y simulaciones.

Tiempo de dedicación por parte del alumno (Horas/Semanales):
20 horas a la semana

En caso la tesis sea una implementación (o construcción), mencionar la fuente de financiamiento:
a. Financiado por el docente.
b. Financiado por el alumno.
c. Financiado por laboratorio (indicar cuál).
d. Financiado por fondos PUCP (indique unidad).
e. Financiado por fondos externos a la PUCP (Concytec, FINCYT, FIDECOM, etc.)
f. No requiere financiamiento.

-Rpta: d. Financiado por DIRINFO, como parte de su proyecto de ampliación de la cobertura y seguridad de la red WiFi de la PUCP