Proceedings of the 5th WSEAS Int. Conf. on APPLIED INFORMATICS and COMMUNICATIONS, Malta, September 15-17, 2005 (pp85-90)

Theoretical framework for location enhanced security in WLAN networks

DIMITRIOS DRAKOULIS,
IAKOVOS STAMOULIS,
DIMITRIOS DRES
Telesto ITC
Makrygianni 69, Athens
GREECE

ODYSSEAS I. PYROVOLAKIS
Hellenic Naval Academy
Terma Chatzikyriakou
185 37 Pireaus
GREECE

Abstract: - Following the assessment of the threats posed to the security of WLAN (802.11a/b/g) networks as well as the conventional mechanisms used today, location is proposed as an additional layer in the conventionally applied network security strategy. The authors indicate alternative approaches for the implementation of location estimation schemes and proceed with a critical appraisal of the advantages and shortcomings.

Key-Words: WLAN Security, Location Estimation, Kalman Filter, Bayesian Estimators

1 Introduction

Wireless Local Area Network (WLAN) technologies are spreading rapidly in organizations of all sizes. However in parallel with market success, suspicion among the general public of weaknesses in the mechanisms employed for security, and in some cases debates have occurred among the engineering community of the technical immaturity of security mechanisms utilized.

In the sections that follow, the authors review the goals of security policies in WLAN installations, the threats that may arise, the conventional mechanisms used for guaranteeing security (as well as the best practices that should govern the application of these mechanisms in the office environment), and propose the exploitation of the knowledge of the location of the network nodes as an additional layer in the security strategy. Consequently, the importance of the location estimation mechanisms for the fortification of security is explained. The theoretical framework of the location estimation problem is reviewed and eventually the authors attempt a high level evaluation of the alternative approaches.

2 Identification of Threats to WLAN Networks

Threats to network security have existed since the very beginning of computer networks, however the advent of wireless networking amplifies the perceived threats. By nature, RF communications and as such, wireless networking is particularly vulnerable to security breaches and attacks because the signal is transmitted by radio waves, i.e. in an open, hard to confine, public medium.

The situation is similar in mobile communication technologies, and security risks were high especially in the 1st Generation systems, however 2nd and eventually 3rd Generation technologies have produced strong, proven authentication (mutual authentication for both the terminal as well as the network entities) and confidentiality mechanisms.

The use of readily available software by potential intruders (former employees, competitors or even by-passers employing so called “war driving” techniques) for exploiting WLAN technical vulnerabilities, allows these persons to take “vengeance” from employers, colleagues or organizations or simply to satisfy their curiosity and vanity.

The very nature of wireless means that information related to sensitive transactions, personal data, financial information are free to propagate, given the circumstances, both indoors and outdoors. Additionally for the first time in the history of computer networks, the conventional system monitoring tools may not reliably identify the communicating parties in a network transaction, or identify the location of the communicating parties. Actually anyone within line-of-sight (LOS) from the emitting sources (or even under non-LOS conditions in some cases) may detect the signal and potentially intrude the network.

A classification of the goals of WLAN security as

well as the common threats is attempted hereafter.

- Confidentiality relates to the goal of the protection of personal or corporate data from disclosure to unauthorized parties. Eavesdroppers exploit the nature of the RF airwaves, to detect the existence of network traffic and then use "sniffers" (TCP/IP protocol stack decoders) with which they may track specific traffic patterns leading to the extraction of meaningful application data
- User Authentication relates to the ability of identifying users, before they are granted access to a network and its resources. The leakage of information used for the identification of the users will lead to the potential forging of existing users' identity, leading to any kind of TCP/IP spoofing or session hijacking techniques, thus paving the way to intruders acquiring full access to corporate resources
- Mutual Authentication will guarantee that besides the authentication of the user by the network, the network is also positively identified by the user, thus countering the risk of "rogue" Access Points, i.e. unauthorized APs operating in the enterprise. IEEE 802.11 AP equipment, being low-cost, small-sized devices, may be placed in locations that lack proper physical security. Furthermore the firmware used by many WLAN NICs (Network Interface Cards) may also be converted so that a NIC operates as an AP. Even if a corporation does not intend to deploy WLAN services, the thread of unauthorized AP is one that should not be overlooked.

3 Conventional Countermeasures

The technical means conventionally employed for the protection of the users from the aforementioned risks, include:

- The implementation of strong authentication schemes (including all kinds of digital signatures and certificates, MAC filtering and even smartcards) to ensure that only a user whose identification matches that of a specific registration in a user store or database, will gain access to network resources. However this is not always the case, as the user's "password" may be acquired by helpful "friends" or colleagues, MAC addresses may be forged ("MAC spoofing"), smartcards may be stolen.
- The encryption of data conveyed via the airwaves, is used for ensuring confidentiality of information exchanged. However there have been reports of cases where algorithms have been used to successfully decrypt WLAN traffic and even recover the keys themselves or the initialization vectors that produce these keys (as discussed in a following paragraph on WEP).
- The separation of sensitive network traffic (relative to email, file transfer among others) from traffic relative to public interest applications such as the internet. This separation in common LAN networks may be achieved using separate VLANs when switching Ethernet IEEE 802.3 traffic.
- The creation of efficient network access control mechanisms is the evident approach, where the user is allowed access according to user rights following his positive identification. However it is possible that the authentication information may be jeopardized during the transaction that takes place between the AP and the AAA (Authentication Authorization Accounting) server especially when the AAA server does not reside on the same LAN as the AP.

Due to this very nature of WLAN networks, the need for security was partially (and thus unsuccessfully) addressed from the initial stage of the IEEE 802.11 standard through the application of the Wired Equivalent Protocol (WEP) as a means of encryption. WEP employs the RC4 symmetric stream cipher, producing an encryption key shared by all devices in the wireless network. However over the last 5 years, WEP was demonstrated to be inadequately secure at any key length (as evidenced most notably by Shamir [1], while other contributions produced faster, near on-line code-breaking processes) and thus proved unsuitable for enterprise class security. Furthermore the WEP keys are vulnerable to dictionary attacks based on the tendency of administrators to select meaningful words or phrases. To make things worse practice has shown that users (70% of users to be exact) take advantage of the WLAN plug-and-play operation and neglect to set the key-generating pass-phrase. This is especially true in SME corporations with no dedicated network administrators and security experts.

To improve on the security issues that arise by the known vulnerabilities of the WEP protocol, WPA was introduced by IEEE 802.11i as the new standard of Wireless Encryption. In the WPA, keys are distributed in a similar fashion as WEP keys. It has been shown [2], that small password are vulnerable to off-line dictionary attacks. WPA can be combined with a Radius Server for authentication. Users are prompted to a login screen

where they can authenticate and receive the automatically generated WPA keys. As these keys are machine-generated they are not prone to standard dictionary attacks and are significantly more secure. The login scheme has the advantage that it enables the implementation of open wireless LAN security in large scale networks such as Universities and Hospitals where the manual distribution of encryption keys is very impractical. However WPA has not yet been standardised by IEEE and may only be deployed with only compatible equipment.

In essence, network security ends-up being enforced by systems which base their operation on the certification of who a user (or a network) actually is, versus what credentials he holds to prove this claim. The use of the identity layer (be it either a username or a smartcard) along with a password layer (a password or a "pin"), is seen by experts as no longer adequate especially for the WLAN networks which by nature have serious vulnerabilities. A third layer representing the geographic location of the users will significantly strengthen the security of the WLAN infrastructure.

4 Location as a User Identity Parameter

Although the very purpose of the WLAN networks is to support the users' connectivity regardless of location, the (geographic) location feature is inherent in the operation, management and security of a WLAN installation. Indeed even before the WLAN network is deployed, a site survey is performed, which captures the geography of a room or an office space, and determines how the Access Points are placed to provide maximal coverage and to guarantee the performance levels expected of the network.

Consideration of the overall geography indicates the placement of APs to prevent eavesdroppers from capturing internal WLAN traffic from outside the perimeter of the network installation. Coverage in this case is "steered" away from potential threats, as in the case of the company whose competitor is right across the street to the north. Positioning the AP in the northern part of the office and selecting the antenna gain pattern to provide coverage to the south of the office or campus will minimise such threats. In combination to a correctly predefined site survey, the definition of the WLAN network coverage pattern is definitely a significant part of the overall network protection strategy.

The main purpose, however, served by location would be the identification of potential intruders, as well of the identification of unauthorized ("rogue") APs. Forming a novel additional layer in the identification strategy of the WLAN network, location provides enhanced authentication reaching beyond conventional methods. Indeed besides the obvious potential for the exclusion of users accessing the network from outside the perimeter set by its administrators, or the identification of rogue APs, hidden in a plastic closet inside an office, other complex yet custom and thus efficient security policies may be implemented. For example, based on the knowledge of the location of users, aspects such as authorization to specific resources (a concept described by the authors as "departmental access", whereby no user may access any personnel file while outside of the HR department) or even bounding users within a specific network area to support the coexistence of public hot-spots within an enterprise building (where unauthorized users are served by the network only when they are in the ground floor or specifically in the building's cafeteria).

Although the list of benefits obtained from the knowledge of the location of a network's resources is not exhaustive, we may stress the opportunity to support the timely hand-off from one AP to another even across different network domains as the terminal moves around in the network. Efficient roaming techniques may be then applied in the case where *continuous mobility* throughout a campus installation needs to be supported (the case of voice and multimedia applications [3]). All types of network management tasks (primarily resource management as well as mobility management) might benefit significantly from the utilisation of a precise location estimation scheme; however such a discussion is off-the-scope of this work.

5 Applicable Techniques for Location Estimation in a WLAN Environment

Two are the main parameters whose knowledge may be exploited to extract location information from standard IEEE 802.11 compliant equipment in a Wireless Network.

- **Signal strength**. Signal strength is very useful and measurable information that we can readily extract from both network (APs) and terminal (NICs). Implementation is based on the periodic execution of a routine by which APs successively hand over the potential network user to each other until signal strength is measured by all.

Assuming a sufficient number of APs whose layout is representative of the characteristics of the area covered by WLAN, a very good approximation of the location of the client may be achieved. However in a complex indoors environment, multipathing from large steel furniture (metal bookshelves) or the metal reinforcements in walls and other structural elements of the building, as well as scattering and attenuation effects distort the expected signal attenuation in a way that is difficult to predict.

- **Angle of reception**. The existence of sectorized coverage antennas may provide significant information about the users' location and, to some extent, limit the effects of unpredictable attenuation. Combinations of directional antennas may be used to not only limit the coverage areas in particular area, but also sample the client signal strength in areas that should be out-of-reach, thus identifying direction of an unknown signal source. An example of this scenario is the typical threat when an unauthorised intruder is at the corporate car park and is trying to get access to the corporate network. The placement of an AP located or aimed towards the car park will provide significant information of the users location, and deny access to anyone located in that area, even if he can supply legitimate encryption keys.

The aforementioned techniques may be used without deviating from the 802.11 standard. Furthermore, there are additional techniques that would require the use of non-standard client equipment. One of them is round-trip time, that is the time required for a "ping" signal to come could be a good indication of distance from an access point to a client. However, the delay of the "pong" arrival may depend on many additional factors, apart from distance. Typically wireless devices are based on a SOC based device whereas a processor services a number of interrupts and therefore the exact response time may not be predictable to the accuracy required for the calculations.

6 Theoretical Framework of the Location Estimation Problem

According to systems' theory, the determination of the location of a terminal moving in a WLAN network may be classified as an estimation problem. The location as well as other characteristic quantities (velocity being another example) are variables of time and may be theoretically supported by a model, which is termed as a "*dynamic system*". The estimation of the precise values of these characteristic quantities based on meaningful observations of the system's behaviour is referred to as "*state estimation*". In the most basic form of the problem i.e. the location estimation, the state of interest is the location of a person or object, and observations are provided by sensor(s) either placed in the environment or carried by the person (as in the case of a client with modified firmware to monitor signal strength or ping times and report these values back to the network for processing).

As was already explained in the previously supplied review of individual techniques used for location estimation, the performance levels achieved by the use of any single technique may not always allow the provisioning of reliable, robust location services in diverse environments based on the measurements of a single observation source – a sensor. The deterring factor is mainly the non-uniform performance expected at the diverse propagation environments (both indoors as well as outdoors), in which a WLAN terminal is expected to operate. The combined, simultaneous use of more than one location techniques, from more than one observation sources / sensors (multiple Access Points, or the terminal itself) is hereby proposed as the means of reaching acceptable performance levels. In order to maximize the useful information content, improve reliability, and in the meantime minimize the quantity of data ultimately retained, the synthesis of individual data and knowledge from multiple observation sets from different sensors is required. This synthesis of sensor data or "Data Fusion" as it is referred to in literature may be based on several methodologies, examined in the section that follows.

According to Dynamic System theory, the knowledge of the system's output cannot determine by itself the overall behaviour of the system. To this end the exploitation of any knowledge of the history as well as the dynamics of the system is of high importance for the optimal estimation of the current state of the system. This is especially true in the case of WLAN networks and hot-spots, where generally users mostly interact with the WLAN while being stationary (being in their office, an internet café), thus the system state variations may be bounded within limits, thus allowing the faster convergence of the estimator function to the true position.

7 Deterministic vs Probabilistic Approaches – High Level Evaluation

The traditional, geometric approach to location estimation is based on solving a geometrical problem based on the angle and distance estimates from one or more sensors. Distance estimates are based either on propagation times ("times of flight") where universal, precise clock reference exists (as in the case of mobile networks, however not the case of WLAN networks) or on the measurement of the power attenuation of the signal from transmitter to receiver (signal strength). Multiple error sources are introduced in the estimation of distance, as mentioned earlier, while linear approximations of the propagation functions may not be used freely as the propagation laws differ significantly between indoors and outdoors environments.

According to deterministic approaches, knowledge of the system state (i.e. location) is continuously calculated based on the measurements of the sensors as well as our solid knowledge of the system's behaviour over time (the simplest example being the case when the user is stationary). Recursive state estimation methodologies are then used to continuously improve the state estimate as well as the inaccuracy of the calculations (the covariance). The most widely used methodology is the Kalman Filter. Kalman Filters assume a normal (Gaussian) distribution of the initial uncertainty of the system and the observation errors. Furthermore there is the requirement that the observation model and system dynamics are linear functions of the state. When the system is not linear (as in the case when radio propagation models are used to calculate distance), extended Kalman filters are applied, to linearize the system using first-order Taylor series expansions. A representative treaty of the use of Kalman filter estimation may be found in [4]. Experience shows that when the uncertainty of the person's initial location, as well as the person's dynamics is low, the sensor readings come at an adequately high rate, and additionally the sensors' errors are limited within well calculated limits (as happens in the case of measuring signal strengths in outdoors environments) then Kalman filters lead to accurate estimates.

On the contrary, alternative approaches probabilistically estimate the state of a dynamic system from a sequence of noisy sensor observations. At every time sample (epoch), the uncertainty is represented by a probability distribution over the location estimate. Using discrete state-space values (a set of discrete locations in a 2-D or 3-D space is pre-defined), probabilities are assigned to each of the potential outcomes as results of the estimation process. A typical representative of a probabilistic approach may be found in the paper by T. Roos et al. [5], where location estimation is regarded as a machine learning problem. Signal strengths distribution in different geographical areas based are modeled, based on a sample of measurements collected at several known locations (a measurement "grid").

Bayesian filter techniques provide a powerful tool to help manage measurement uncertainty and perform multi-sensor fusion, thus being a most representative example of the probabilistic estimation methodologies. Their statistical nature makes Bayesian filters applicable to arbitrary sensor types and representations of environments [6]. Furthermore depending on the type of sensor systems used, Bayesian filters may be applied to infer location estimates based on measurements of the signal strength together with topological maps depicting the layout of the indoors environments. However application of Bayesian techniques requires extended modifications to the system software of the NICs, required to preprocess and report measurements to the network.

Although performance expected in the case of Bayesian filters seems to be adequate for most of the applications envisaged, the requirement for sampling signal strength levels at predefined locations, as well as the need for repeating the measurements each time the APs are rearranged or the layout of the furniture or the equipment is modified, seem restricting for its use in a complex industrial, military or other environment, where in some cases administrators or network engineers may not be able to freely visit and survey.

8 Conclusions

The identification of a general use framework for location estimation, which shall allow the fusion of information from multiple sensors (WLAN APs and NICs) is a complex task whose success depends on numerous parameters, the most significant of which being the number and placement of sensors, the potential for employing special purpose sensors (rather than the use of cheap, off-the-shelf equipment), the type of the environment (indoors office or residential spaces being the most harsh environments in terms of estimation capability, while outdoors spaces in a campus-wide WLAN being a rather straightforward application of a deterministic estimator). Currently, no single

approach will guarantee uniform performance, without significant modifications to the network infrastructure or modifications of the client hardware or software, a choice which in turn restricts penetration to the installed base of WLAN networks and terminals.

References:

[1] S. Fluhrer, I. Mantin and A. Shamir, "*Weaknesses in the Key Scheduling Algorithm of RC4*", Selected Areas in Cryptography 2001, pp. 1–24.

[2] R. Moskowitz, "*Weakness in Passphrase Choice in WPA Interface*", ICSA Labs, 2003

[3] A. Mishra et al, "Key Distribution Using Neighbor Graphs", *IEEE Wireless Communications*, February 2004

[4] P.Kikiras, D. Drakoulis, "An Integrated Approach for the Estimation of Mobile Subscriber Geolocation", *Wireless Personal Communications*, Special Issue on Location, Kluwer, Netherlands 2004.

[5] T. Roos, P. Myllymaki, H. Tirri, P. Misikangas, J. Sievanen, "A Probabilistic Approach to WLAN User Location Estimation", *International Journal of Wireless Information Networks*, Vol. 9, No. 3, July 2002

[6] D. Fox, J. Hightower, L. Liao, D. Schulz, G. Borriello, "Bayesian Filters for Location Estimation", *IEEE Pervasive Computing*, pp. 1536-1268, September 2003.