Regional-based Authentication Against DoS Attacks in Wireless Networks

Ivan Martinovic, Frank A. Zdarsky, and Jens B. Schmitt
TU Kaiserslautern
Distributed Computers and Systems Lab
p.o. box 3049
67653 Kaiserslautern, Germany
{martinovic,zdarsky,jschmitt}@informatik.uni-kl.de

ABSTRACT

In this work we focus on resource depletion attacks within IEEE 802.11 networks. This type of DoS attacks is used to exhaust access points' resources resulting in denying service to legitimate clients and rising the opportunity for more sophisticated attacks. It is usually based on flooding an access point (AP) with a high number of fake authentication requests. This paper introduces a protection method which assists APs to selectively block fake requests sent by an attacker, while at the same time allowing other legitimate clients to successfully join the network. For this purpose we introduce the concept of regions, estimates on client's relative locations. The concept itself is similar to a known protection against DoS attacks based on client puzzles in wired networks, yet had to be adjusted to the peculiarities of wireless networks. Rather than utilizing CPU or memory-based resources that are highly variable among wireless clients we take advantage of wireless characteristics such as broadcast communication, signal propagation, and dense deployment of IEEE 802.11 technology. The proposed protection enables a trade-off between security and performance thus providing its adaptation to different network configurations.

Categories and Subject Descriptors

C.2.1 [**Computer-Communication Networks**]: Network Architecture and Design—*Wireless communication*

General Terms

Design, Security, Performance

Keywords

Denial-of-Service (DoS), impersonation attacks, wireless LANs

1. MOTIVATION

Fighting against Denial-of-Service attacks in IEEE 802.11 networks has always been a critical task. While wired networks provide means for protecting the availability at physical layer through physical control over traffic (e.g. using cables and switches), wireless networks suffer from the broadcast characteristic of communication. Through jamming of a wireless channel or by abusing the fair-play assumption of a CSMA protocol an attacker always has the option of attacking not only the service but communication itself. This has mainly been a reason for considering the availability in wireless networks hard to protect and often left to be sacrificed. Nonetheless, especially in wireless networks DoS attacks can be used as a starting point for attacking other security goals. One frequently used DoS attack in WLAN is based on stealing the user's credentials through authentication and/or association flooding of access points. By sending a high number of authentication or association requests most APs would exhaust their resources and crash. After bringing down legal service, the attacker would install a rogue AP and try to takeover new wireless clients. The simplicity of such attacks has resulted in various tools available in order to easily execute them e.g. [6].

Today, to avoid this type of attacks most of the new APs are labeled with so-called "DoS protection". This protection is based on periodically allowing only a certain number of association requests. After the number of allowed associations is reached, an AP blocks all further requests for a certain period of time [7]. Hence, this protection is only an access control implemented through blocking of all association requests. The major problem with this mechanism is that it cannot distinguish between requests sent by legal stations and those sent by an attacker. As a result, by using high flooding rates the attacker can easily bring the AP to block requests most of the time. New clients' attempts to associate would end up in vain, waiting for an association response.

In this work we explore characteristics of wireless environments such as broadcast communication, signal propagation, and dense deployment of IEEE 802.11 technology to introduce a notion of *Regions*. Regions are relative locations of wireless clients and by using them an AP is able to selectively block requests coming from certain regions while accepting others. To compute the region, clients are required to *invest time* in monitoring the wireless channel. Each region is conditioned by a client's physical position, therefore all changes of position without previously monitoring the channel will result in rejecting the region and denying association. Both of these requirements are in contrast with the attacker's behaviour who must send many requests to be successful in its attack and has a strong incentive to change its physical position as soon as possible.

Q2SWinet'07, October 22, 2007, Chania, Crete Island, Greece.

2. CONCEPT OF REGIONALIZATION

Due to the broadcast characteristic of wireless environment every packet can be received by every other station given that the received signal is strong enough. Two stations that are within their transmission ranges and that receive one another with signal strength above a certain signal threshold will consider themselves as *Neighbours*. This particular signal level that must be reached to fulfill the neighbourhood relationship we define as *Neighbourhood Signal Threshold* (NST). By listening on a wireless channel and comparing the received signal strengths of other already associated stations with the given NST, every station is able to define the set of its neighbours which corresponds to a *Region*. How well a new station defines its region depends on the time it invests in monitoring the wireless channel. After the region is defined, it is sent within an association request. Taking advantage of broadcast communication, every associated station within the transmission range of the joining station will be able to capture it and check whether the region fulfills the neighbourhood relationship from its own view.

2.1 Regionalization Parameters

2.1.1 Neighbourhood Signal Threshold (NST)

Generally, every wireless card reports some sort of a link quality measure calculated by different indicators. Some WLAN cards report a Signal-to-Noise Ratio (SNR), others Received Signal Strength Indicator (RSSI) or Link Quality Indicator (LQI). We are interested in mapping the signal quality to a discrete binary value of receiving stations either as a neighbour or not. It is important to mention that this relation cannot be taken as absolute physical distance or position (due to the high variance of signal strength). More intuitively, it can be compared with a typical wireless management tool reporting the link status (e.g. if the percentage of received signal strength to a maximum signal strength is above 75%, most WLAN cards will report the link status as "excellent" and if the percentage is below 20%, the link status is reported as "poor"). The only difference is that we are using absolute values given in dBm and that NST is periodically broadcast by an AP within the Beacon frame. For example, if NST is defined at -70 dBm, every station with received signal strength that is better or equal to -70 dBm will be considered as neighbour to our station. If NST is set to a minimum signal strength required for a station to receive a packet (such as -95 dBm) all station falling within station's transmission range will be considered as a neighbour. Through this dynamic adaptation of NST we can handle scenarios with different density of associated stations.

2.1.2 Regions

Region is a view that a single station has of the wireless environment. It is defined by the number of associated stations estimated as neighbours and sent with association request as a binary array of neighbourhood. The maximal region is equivalent to the previous example where NST was set to a minimal signal strength required for successful reception of a frame. The important question is how the optimal number of neighbours can be found in order to define the region. We are interested in having a high number of disjoint regions i.e. every new station has to create a different region consisting of k stations from n associated ones. This is equal to a number of combinations of a non-ordered set described by the binomial coefficient $C(n,k) = \frac{n!}{k!(n-k)!}$. This implies that the highest number of regions is achieved when about 50% of all associated stations is received within NST.

In Figure 1 we show results of varying NST parameter within an 100x100 m area. As it can be seen, the optimal NST is at -80 dBm, but more importantly, the 25th and 75th percentiles show a high dispersion of the sample at -75 dBm, -80 dBm, and -85 dBm. This means that even if in a real world scenario we cannot set NST at the optimal value (it depends on a density of stations and on area covered by AP), we can still achieve a high number of different regions by varying the NST and taking care to avoid extreme values. To get an estimation of density of stations within a neighbourhood, an AP could use the help of already associated stations which can periodically send neighbourhood lengths for various NSTs.

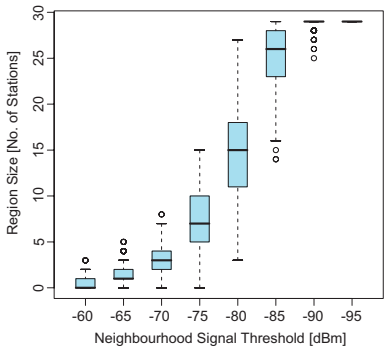

Figure 1: Region's size for varying NST

2.1.3 Maximal Signal Sample Size (MSSS)

The received signal strength is a highly environment-dependent random variable. It is influenced by various factors such as temperature, antenna orientation, different attenuation factors based on the material through which the signal is penetrating and many other obstacles. To statistically improve an estimate on the neighbourhood, a wireless station can increase the sample size of received packets. The chosen size of MSSS can be seen as a trade-off between protection accuracy (minimizing the number of wrong decisions) versus performance (time required to define a neighbourhood and to successfully associate). Every station can decide how long it should measure the signal strength of other stations before defining the region. Our initial RSSI measurements showed that signal cross-correlation between consecutive frames is high (≈ 0.8 within 50 ms). On the other hand, building the median of MSSS can only help us to avoid outliers. The problem of channel asymmetry due to different NIC capabilities still remains.

2.2 Association Process - Verifying Regions

When a new station (STA_{new}) decides to join the network it first listens for a *Beacon frame* to find out the value of NST. Then it starts collecting signal strength samples by changing to monitoring mode on a dedicated wireless channel. When MSSS is reached, the station defines the region based on the median signal strength and sends it together with the association request. Every associated station within STA_{new}'s transmission range can check if the neighbourhood relation described by a region is fulfilled from its own view.

There are two cases where the views of the new station and associated stations can differ; if the associated station receives a signal from STA_{new} above NST but is not defined in a region, or in contrary, if the signal strength is below NST but the station is still defined in a region. In both cases the associated station will broadcast a warning which will result in the AP denying association. Otherwise, if the region matches the views of associated stations no warnings will be sent and association will be granted. To decrease

the contention on a wireless channel any station that already detects the warning frame can suppress sending of its own.

3. INITIAL RESULTS

To evaluate our concept we have created a packet level simulation with radio propagation model based on Log-Normal Shadowing allowing us to model signal variation (setting the standard deviation to 6 dBm). To simulate different wireless NICs, we model half of the client population with 5dBm difference in their transmissions. The surface area is 100x100 meters and every experiment is run over 10 different scenarios with randomly placed stations. In Figure 2, we see three main response variables for varying NST. The *False Positives* are warning messages sent by associated stations which have detected discrepancies in regions sent by joining stations due the asymmetry of the channel. The *Duplicates* are same regions sent by different stations. They can be seen as a result of a "hidden terminal" problem within a wireless environment and only occur if two different stations are having the same view of the neighbourhood and at the same time try to join the wireless network. The *Region size* is an average size of a region, given as ratios with all associated stations.

As we can see the number of false positives dramatically increases

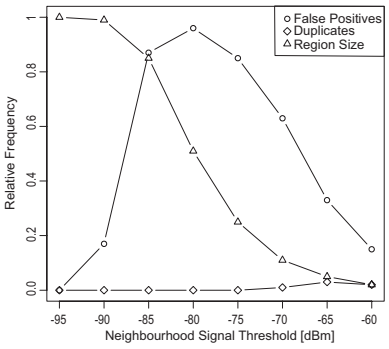

Figure 2: Wireless environment base on log-normal shadowing propagation model and using MSSS=1

for the optimal size of the regions. With NTS at -80 dBm, the fraction of false positives is 0.98, which would make this method unusable. An improvement can be achieved by increasing the number of received signals (increasing the MSSS parameter to 20) and thus spending longer time monitoring the channel before defining the region. By collecting more samples we could decrease the frequency of association failures by about 20% at network sizes of 5 and 10 stations. Larger network sizes, although improved, still suffered from a rather high number of false positives and only tuning the MSSS parameter seems insufficient to significantly improve authentication frequency.

To better cope with channel asymmetry, we introduce *Tolerance Intervals* (TI). These are built around the median of MSSS by computing $[median - TI, median + TI]$ and are used by associated stations only. The reason for introducing TI is to avoid warnings from associated stations located at the edge of the signal strength given by NTS. Those stations are the most sensitive to signal variations because the channel asymmetry at those positions dominates the decision on neighbourhood. By deploying TIs the associated stations will compare the neighbourhood relation given by the region not with its own median of received packets but with a range given by TI. For example, if NST is defined at -80 dBm and STA_{new} receives signals from the associated station (STA_1) with a median of -75 dBm, it will consider it as a neighbour. Due to the channel asymmetry let us assume that STA_1 receives a signal from STA_{new} with a median at -81 dBm. Without using TIs, STA_1 would send a warning and STA_{new} would fail to associate. If we define TI to be 1 dBm, STA_1 would ignore the mismatch with STA_{new} because the neighbourhood relation of both stations is still valid within an interval of $[-80\,dBm, -82\,dBm]$.

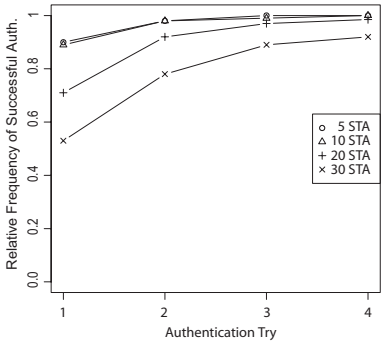

Figure 3: Successful associations using MSSS=20 and TI=1.5

As depicted in Figure 3, allowing TIs highly increases the frequency of successful associations for even very dense networks. The frequency of successful associations with network sizes of 5 and 10 associated stations starts at 90% (for a first authentication attempt) and for larger networks it also shows a significant improvement. Both networks have an association probability after third retry equal or greater to 90%.

Since the performance, in this case increasing the number of successful associations does not come for free, there is a price to pay from the security point of view. By allowing TIs, we create a new possibility for an attack. An attacker can search for a position where most or all associated stations receive its signal within their TIs. Hence, they will also tolerate regions sent from the attacker. Such positions we call *Weak Positions* (WP). If attacker finds a WP it would be able to flood with the regions made of all combinations of "tolerant" associated stations.

4. WIRELESS HELPS SECURITY

Nevertheless, there is again a certain advantage within a wireless environment that can be used against attacker who is trying to exploit WPs. The solution is based on changing NST periodically to similar but not the same values. As discussed in 2.1.2, there are many valid NST values that an AP can select and still provide a number of combinations to allow a high number of different regions. Then by changing NST the unpredictability of the signal propagation takes care that the entire regionalization of the environment is changed. As a result, both parameters - *Regions* and *Weak Positions* will also change. Hence, changing NST "moves" the WP to another physical position and attacker is forced to search for a new one (or to wait and hope that the same NST value and network configuration will be selected again). To support this statement we create the following experiment. The AP defines NST and changes it periodically by uniformly selecting various NST values between -70 and -85 dBm. We then sample the environment for every given NST and capture the physical positions where an attacker is tolerated. We are interested in finding out which of those positions remain the same for different NST values and if there is a possibility for an attacker to stay within a certain proximity of next WPs. Figure 4 depicts the cumulative frequency of occurrences of WPs among all physical positions (sampled at every 5 m).

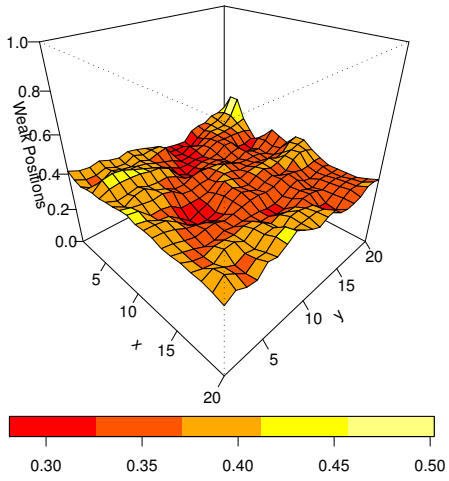

Figure 4: Cumulative frequency of Weak Position for various NST values

Although we have detected $\approx$ 10% of WP where *any* station would tolerate *any* region sent by an attacker, this figure shows that an attacker cannot predict a next position nor stay at the same postions to continue its attack. Any position is equally "good and bad", thus attacker has no better strategy for searching then random (brute-force) tries. Interestingly, after only one single change of NST value there are only 3% of the same WPs left. By changing NST for the second time, none of previously found positions are any longer WP.

5. RELATED WORK

Research on protection against DoS attacks in WLANs has significantly increased over the past few years [1],[2],[4],[7],[5]. The determining factor has been widespread deployment of IEEE 802.11 networks and their usage within public areas. In [2] authors provide an experimental analysis and show that IEEE 802.11 networks are highly vulnerable to DoS attacks due to their unprotected management and control frames. They also provide lightweight solutions to mitigate those attacks, but they do not consider vulnerabilities based on resource depletion resulting from flooding with association requests. In quest for more low-priced solutions against DoS attacks in contrast to cryptographic mechanisms and assumptions on pre-shared secrets, the usage of signal strength became the focus of some research papers. In [3] the RSSI has been used to create a protection against Sybil attacks within wireless sensor networks. They create a RSSI-based localization scheme that uses multiple receivers and the ratio of RSSIs to detect messages sent from a same device. This is an interesting work, showing that unreliable signal strength used as ratio can provide highly accurate detection. Identity attacks are also the focus of research given in [5]. The authors provide a solution based on radio signals as fingerprints to distinguish between different wireless clients. Their method is based on comparing the absolute values of RSSIs and using the number of matches between signals detecting those coming from same device. They utilize a number of APs as sensors to monitor the wireless environment. While the protection described in [5] is also based on received signal strengths to protect APs against identity-based attacks, they do not solve the problem of using directional antennas and per-packet signal strength manipulation. These techniques can easily enable an attacker to fake its physical position. In contrast, the idea presented in this paper takes a different approach and binds every request to a certain region which must be estimated by monitoring the wireless channel. This helps to limit the attacker's flooding rate even when it frequently changes its position of manipulates packet's signal strength.

6. CONCLUSION AND FUTURE WORK

The idea of this paper was to introduce and briefly quantify a new approach taken against DoS attacks within IEEE 802.11 networks. In search for a more constant performance factor among wireless clients on which DoS protection can be based, we have identified various characteristics of the wireless environment that can provide us with interesting and useful capabilities. Although often the unpredictability of signal propagation and broadcast nature of communication are considered as major disadvantages from a security point of view, we have shown the possibility of using them to increase the protection of wireless networks. This work presents our initial results and most of the issues described in this paper are still the focus of our current research. As a part of our future work we also intend to implement this idea and evaluate it empirically.

7. REFERENCES

[1] W.A. Arbaugh, S. Shankar, J. Wang, and K. Zhang. Your 802.11 Network has No Clothes. In *Proceedings of the First IEEE International Conference on Wireless LANs and Home Networks*, pages 15–28, December 2001.

[2] J. Bellardo and S. Savage. 802.11 Denial-of-Service attacks: Real Vulnerabilities and Practical Solutions. In *Proceedings of the USENIX Security Symposium*, pages 15–28, August 2003.

[3] M. Demirbas and Y. Song. An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks. In *WOWMOM '06: Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks*, pages 564–570. IEEE Computer Society, June 2006.

[4] D. B. Faria and D. R. Cheriton. DoS and authentication in wireless public access networks. In *WiSe '02:Proceedings of the 2004 ACM Workshop on Wireless Security*, pages 47–56. ACM Press, September 2002.

[5] D. B. Faria and D. R. Cheriton. Detecting Identity-based Attacks in Wireless Networks using Signalprints. In *WiSe '06: Proceedings of the 5th ACM workshop on Wireless security*, pages 43–52. ACM Press, 2006.

[6] R. Floeter. Wireless LAN Security Framework: void11. http://www.wirelessdefence.org/Contents/Void11Main.htm (last access: 2007-08-01).

[7] I. Martinovic, F. A. Zdarsky, A. Bachorek, C. Jung, and J. B. Schmitt. Phishing in the Wireless: Implementation and Analysis. In *Proceedings of the 22nd IFIP International Information Security Conference (SEC 2007)*. Springer LNCS, May 2007.