Securing Wireless Data Networks against Eavesdropping Using Smart Antennas *

Sriram Lakshmanan, Cheng-Lin Tsao, Raghupathy Sivakumar
Georgia Institute of Technology
Atlanta,GA,USA
{sriram,cltsao,siva}@ece.gatech.edu

Karthikeyan Sundaresan
NEC-LABS America
Princeton,USA
karthiks@nec-labs.com

Abstract

In this paper, we focus on securing communication over wireless data networks from malicious eavesdroppers, using smart antennas. While conventional cryptography based approaches focus on hiding the meaning of the information being communicated from the eavesdropper, we consider a complimentary class of strategies that limit knowledge of the existence of the information from the eavesdropper. We profile the performance achievable using simple beamforming strategies using a newly defined metric called exposure region. We then present three strategies within the context of an approach called virtual arrays of physical arrays to significantly improve the exposure region performance of a wireless LAN environment. Using simulations and analysis, we validate and evaluate the proposed strategies.

1 Introduction

With the explosive growth in the usage of wireless data networks over the last several years, increasing attention is now being paid to specifically securing communication in wireless environments. Cryptography based techniques including the wired equivalent privacy (WEP), the wi-fi protected access (WPA), and the 802.11i WPA2 all are examples of techniques that specifically protect wireless communication against some of these challenges. One of the primary properties of such cryptography based techniques is that they *hide the meaning of the information being communicated*, but *not the existence of the information itself*. In other words, it is typically assumed that the adversary has access to all the information and the techniques are designed to make it *computationally hard for the adversary to understand the true meaning of the information*. In this paper, we focus on a somewhat orthogonal form of securing communication that is sometimes referred to as *physical security*. While the term encompasses a wide variety of techniques, it typically refers to approaches that *limit knowledge of the existence of the information* at the adversary. In other words, the goal is to prevent the adversary from even getting access to the information in the first place. It is imperative to note here that the notion of physical security is by *no means a replacement* for traditional cryptography, but should be strictly seen as a *complimentary strategy* to better foil the attempts of an adversary.

The scope of this paper is restricted to securing communication over wireless data networks, and further limited to a specific form of adversarial behavior - *eavesdropping*. With the growing deployment of wireless data networks (WLAN hotspots for e.g.) at very high-densities, it is relatively easy for even a casual user to turn into an adversary by eavesdropping on ongoing communication. This coupled with the fact that increasingly more applications, including ones that would require high degrees of confidentiality such as voice-over-IP, are being used over wireless data networks makes it an important problem to tackle.

Specifically, we consider an emerging class of antenna technologies - smart antennas, to achieve higher levels of protection against eavesdropping. A common defining characteristic of smart antennas is their use of sophisticated signal processing to achieve better spectral efficiencies, interference suppression, and increased reliability among other benefits. A related property of smart antenna techniques is their *ability to focus communication energy spatially*, thus providing a natural platform to build techniques to provide physical security based strategies to tackle eavesdropping.

In this context, we define a metric called the *exposure region* that refers to the area within which an eavesdropper can access and decode the signals being transmitted, and first investigate the baseline performance improvements achievable when using adaptive arrays for beamforming. We show that the improvements achievable are sub-linear with k, the number of elements on the antenna-array, and the improvements can further be smaller when considering link-margins required to tackle fading. Perhaps equally importantly, in high density environments where trusted physical spaces might not necessarily be contiguous, this still

*This work was supported in part by the National Science Foundation under grants CNS-0721296, CNS-0519733, and CNS-0519841.

leaves a non-trivial region of exposure between the transmitter and the receiver that can be exploited by potential eavesdroppers.

We then propose a suite of strategies that use *arrays of arrays* to provide considerable reductions in the exposure region. The strategies are predicated on two principles to limit an eavesdropper's ability to access and decode information: (i) spatial diversity: split and send information over a diverse number of pathways such that an eavesdropper's probability to access all parts of an information is reduced; and (ii) signal overload: overload the number of signals or pieces of information at the eavesdropper. We present the solutions in the realistic context of a *virtual array of physical arrays*, where multiple access points (in the same administrative domain), each equipped with a physical antenna array, are used in tandem to achieve the strategies. Briefly, the strategies proposed include: (a) Secret-sharing, where information to a client is split and delivered through different access-points; (b) Controlled-jamming, where access-points not delivering information are made to perform jamming to eavesdroppers; and (c) Stream-overwhelming, where legal transmissions are coordinated such that physical overlaps between signals are maximized except at legal receivers. Using a combination of *simulations and analysis*, we demonstrate the efficacy of the proposed solution. Thus, the contributions of this work are two-fold:

- We introduce the notion of physical space security in wireless data networks through a metric called the *exposure region*, and study the performance levels achievable when using adaptive-array smart antennas.

- We present a set of strategies that use (virtual) arrays of (physical) arrays to substantially reduce the exposure region *(from 1735 sq.m. with omni to 855 sq.m. with beamforming alone and 5 sq.m. on the average with 4APs and 4 elements in a 2500 sq.m. area)*, and demonstrate the performance using a combination of simulations and analysis.

The rest of this paper is organized as follows: Section 2 defines the scope for the paper and presents background information including the performance when using beamforming with smart antennas. Section 3 presents the three strategies that use virtual arrays of physical arrays to reduce the exposure region. Section 4 describes the details of the solution including the integrated operations for the three strategies. Finally, Section 5 presents the performance results, while Section 6 discusses related work and conclusions.

2 Scope and Background

2.1 Scope

Environment: The wireless environment considered is that of a Wireless Local Area Network (WLAN), which consists of p wireless Access Points (APs), each equipped with a k-element antenna array and one or more clients, each equipped with a single omni-directional antenna or an array of upto k-elements. Channel parameters such as Line of Sight (LOS), the degree of fading and the richness of scattering vary widely for different indoor environments. Thus, to begin with, we consider a strong LOS path between an AP and each client. Later, in Sections 3 and 5 we show how this assumption is relaxed. We assume that any frequency selective fading is combatted using OFDM as in current WLAN devices. Further, since the mobility of indoor users is typically low, we do not consider the effect of fast-fading and assume static clients.

Metric: To quantify the security achieved against eavesdropping, we define a new security metric called the *the total exposure region of the network*, $ER_{Network}$. This is turn, is defined as the union of the exposure regions of all the clients in the network The exposure region of the i^{th} client, $ER(C_i)$, is given by the region in which an eavesdropper can decode the information of client i.

$$ER_N = \bigcup_{i=1}^{N_c} ER(C_i) \quad (1)$$

where N_c is the total number of clients in the network. We initially consider a 2-D network, where region refers to area. Note that the above metric applies to both homogenous and heterogenous antenna capabilities (although we restrict our focus only to a homogenous network). Further, the exposure region of a client is also a function of the receiver's (or eavesdropper's) antenna gains. Thus, all references to the metric are for a fixed eavesdropper antenna capability.

Eavesdropper: Our eavesdropper model is captured by the following set of assumptions for the eavesdropper M: (i) M is a wireless node with *k* antenna elements (where $k <=$ the number of elements at each AP) (ii) M has access to location information of all the clients and APs. (iii) M can perform sophisticated antenna processing with its available elements. (iv) APs do not have any information about the position of M or its strategy. We initially consider the eavesdropper to operate in isolation, but later consider the case of colluding eavesdroppers.

2.2 Background

Adaptive array smart antennas employ an array of antenna elements coupled with both amplitude and phase

weighting, thereby making it possible to tune and obtain a large set of angular and spatial patterns. The number of elements on the array is typically called the number of Degrees of Freedom (DOF). With a *k* element array, it is possible to place $k-1$ nulls in the pattern and use the remaining one DOF for the desired communication. For further background, we refer the reader to [6]. Here we recall the key properties of adaptive arrays that are relevant to this work : (1) A transmitter can control where it causes interference by the appropriate placement of nulls in its pattern. (2) A receiver can null interference only from up to $k-1$ transmissions. Beyond that, it is unable to decode or resolve the transmissions.(3) It is sufficient for either the interfering transmitter to suppress interference to an unintended receiver, or for that receiver to suppress interference from an unintended transmitter. (4) When more than k parallel transmissions happen within an interference range, all transmissions suffer a reduction in Signal to Interference and Noise ratio (SINR) that will make the signal undecodable.

2.3 Why Physical-Space Security?

In this section we describe limitations of existing techniques and the relevance of the proposed approach.

While tapping the wired channel could require sophistication in device and physical manipulation of the medium, wiretapping can be done in a passive manner in the wireless channel. Consequently even a casual user could turn into an eavesdropper. More specifically,

- *Actual solutions are not as secure as the underlying cryptographic technique used*: Although the central cryptographic technique in several wireless security solutions and standards might require very high computational power to crack, reasons such as improper key management, difficulty of realizing truly random generators in practice, and fundamental implementation flaws limit the achievable security.
- *Several unique privacy and targeted denial of service attacks are enabled*: Apart from the basic eavesdropping problem, additional security risks exist which are not directly addressed by cryptographic schemes. These include passive attacks [5], such as user fingerprinting [8], that seriously affect user privacyand active denial of service attacks which target protocol vulnerability (such as beacon attacks) and network management.

A straight-forward, simple technique to reduce the possibility of eavesdropping using smart antennas is to employ beamforming. When a transmitter or receiver or both perform beamforming, the signal is contained in a specific region between them depending on the shape and magnitude

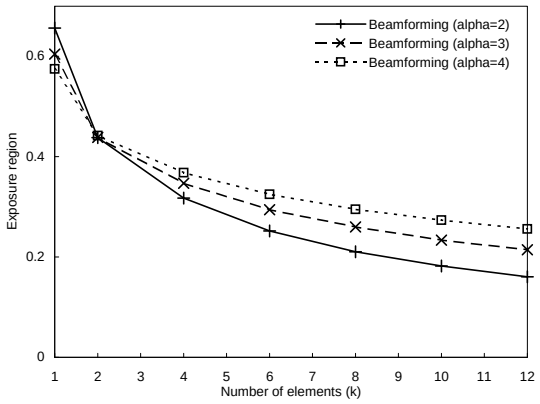


Figure 1. Beamforming Benefits

of the beam patterns and the channel. Here we summarize the security benefits of beamforming using analysis and simulation and refer the interested reader to [6].

Figure 1 shows the exposure region in a simulated setting with link shadow fading deviation of 3dB, 4 antenna elements, and a path loss exponent of 4. The figure clearly indicate the sub-linear (in k) security benefits possible with simple beamforming, with an example *reduction in exposure region by a factor of half for a six fold increase in antenna elements*. While, beamforming provides a first level security mechanism with a sub-linear k fold improvement, the key question we ask is whether *it is possible for a more intelligent scheme to achieve larger benefits?*

3 Virtual Arrays of Physical Arrays

In this section, we introduce two classes of strategies for improving security in wireless environments using smart antennas that rely on the usage of a *virtual array of physical arrays*. Essentially, inspired by several recent studies about high density access-point deployments, we exploit the availability of multiple access-points (APs) in a single WLAN environment to form a virtual array. We then assume that each access-point further is equipped with a physical antenna array. We also assume that there are p APs, and they are connected to each other through a high-bandwidth distribution network such as Ethernet. Also, let c be the number of clients, each with 1 to k element arrays.

The strategies are based on two guiding principles to provide physical space security, namely *prevent eavesdropper from getting access to the information signals* or *overwhelm eavesdropper with more signals than it can sustain such that the information signals cannot be decoded*. Interestingly, the techniques discussed below do apply to an environment with a *physical array of physical arrays* (a multi-radio smart antenna AP), but exploration of that dimension of the approaches is beyond the scope of this work. Also,

while the techniques themselves can be applied to a virtual array of omni-directional antennas, our contention is that the efficacy of the schemes are minimal due to the lack of spatial/angular control with omni-directional antennas.

3.1 Information deprivation

The underlying principle of information deprivation is to ensure that the eavesdropper is rendered unable to receive ths principle canbe applied in the time, frequency or spatial domains. In this work, the principle is applied to the space dimension as enabled by the virtual array. The basic technique is to use spatially separated transmitters required to decode any piece of information. We clarify the idea with an instance of this approach called "*secret sharing*".

3.1.1 Secret Sharing

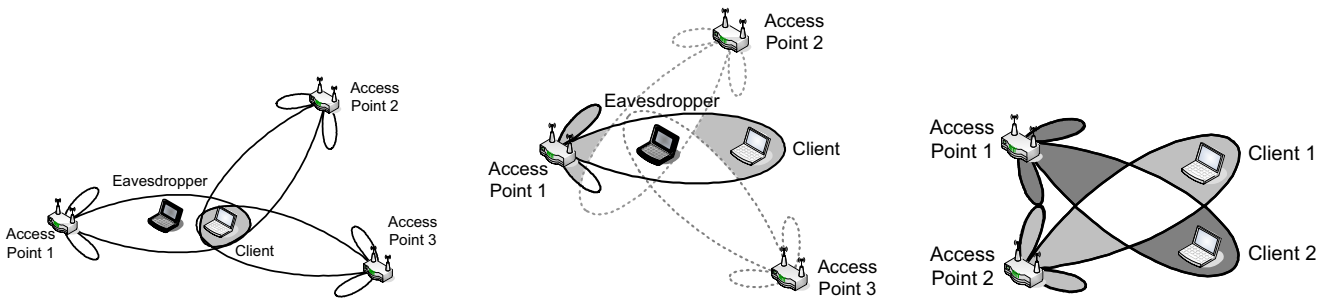
(i) Overview: The basic idea of secret sharing is well established in the context of cryptography [2].
In a general *t-out-of n* secret sharing scheme, a secret message x should be divided into n shares as
$x \Rightarrow (x_1, x_2, x_3 ... x_n)$ such that the following properties are satisfied.
Recoverability: Given any t shares x can be recovered.
Secrecy: Given any $t' < t$ shares, absolutely no information can be learnt about x. More formally, Pr(x|t' shares) = Pr(x)

(ii)Mechanism: The mechanism exploits the fact that when a single client is reachable from multiple access points, different shares of the message can be distributed to the clients through those access points. An eavesdropper in any position in the vicinity of the client or access points would only be able to gain access to a fraction of the information due to the *spatially disjoint nature of the transmissions* that are possible with adaptive arrays unlike with omni antennas. The multiple elements of the array are utilized to perform beamforming and the scheme is implemented in a time division manner. Although several secret sharing schemes exist, we are interested in those that do not significantly increase the traffic load on the network given the limited resources in wireless environments. In this regard, we consider the *all or nothing encryption* (as proposed by Rivest [10],) which is a mechanism to prevent parts of a message from being recovered until the whole message is received in its entirety.

A modified version of the above algorithm adapted for a WLAN scenario, is presented here. The mechanism works as follows. Assuming a secure pseudo-random number generator PRNG, which uses a key K of length ℓ bits to generate a pseudo-random sequence PRNG(K). The message that we require to be sent is a bit stream of length $\mid M \mid$. The message M is XORed with the sequence generated by PRNG(K), to create a cipher text C of length $\mid C \mid$, which is the same as $\mid M \mid$. This cipher text is now split into blocks of length ℓ bits. Each of these blocks are now XORed with each other and then with the key K. The result is known as C_ℓ. Now the controller divides the new packet $C \mid C_\ell$ into fragments of length ℓ bits. All these fragments must be received successfully at the intended client. When the receiver receives these fragments, it XORs all the fragments to regenerate the ℓ-bit encryption key. Once the key is regenerated, the receiver uses it to decrypt the fragments and aggregates them into a single packet based on the fragment numbers. The overhead of such a scheme is ℓ bits (linear) for a message of length M bits and provides a strength of 2^ℓ. We illustrate the scheme using a figure. The figure 2(a) shows three APs,each possessing a share of the information which they communicate to a client in consecutive time slots. Specifically, AP1 transmits its share to the client in slot 1, AP2 in slot 2 and AP3 in slot 3. At the end of the three slots, the client can process the fragments received to decode its packet. On the other hand, an eavesdropper who is positioned along the path between AP1 and the client would be able to obtain share 1 but not share 2. The eavesdropper cannot receive that share from AP2 being in that location The alternative is for the eavesdropper to move quickly and place himself in the path from AP2 to the client. In this case, the speed with which the eavesdropper must move to reposition himself in the direction of the new path within a time slot, is significantly high (close to signal propagation speeds). There are two main practical challenges with applying the proposed technique, namely overheads and packet loss. Since each fragment has its own preamble,header and CRC in addition to the secret shared data,the payload size should be chosen to be much larger than the overheads.The other issue is the loss of fragments. If a fragment is lost,in principle only that particular AP need retransmit it in the next slot by adjusting the schedule. However, we conservatively require that all fragments are received at the client before proceeding to the next packet for that client. Hence all fragments for that client are retransmitted in the next slot.

3.2 Information overloading

The core idea here is to overload/overwhelm the eavesdropper with multiple signals or information units so that the eavesdropper is unable to decode even a portion of the information. The main challenges here are that of ensuring that the legitimate clients are unaffected and also how to achieve this at a link/network level. We recall that interference suppression in an indoor setting, will now be pattern based rather than angle based i.e one can identify patterns that would cause power to be received or not at a node, taking into account scattering effects. This can be performed



(a) Secret sharing (b) Controlled jamming (c) stream overwhelming

Figure 2. Illustration of techniques -(simple beam shape used for illustration only)

by obtaining and updating RF maps at coarse time granularities. When overloading of information is considered, one can use smart antenna strategies in different ways. However, there are two fundamental strategies that illustrate the range of strategies under this approach. These two flavours are called *Controlled jamming* and *Stream overwhelming*. For both these strategies, we highlight the design principles and how the challenges can be overcome.

3.2.1 Controlled Jamming

(i) Overview: The key concept is to generate interfering signals in a controlled manner such that those signals cause no (or negligible) interference at an intended receiver, but cause significant interference to eavesdroppers.When sufficient interference is generated the signal to interference and noise ratio (SINR) at the eavesdropper is reduced significantly thereby preventing the eavesdropper from obtaining access to the information itself.

(ii) Mechanism: The scheme is illustrated in Figure 2(b), where a single AP attempts to convey a data packet to a client. The other APs in the vicinity generate jamming signals with two constraints: (1) the intended receiver should suffer negligible interference, and (2) the eavesdropper (whose position is unknown) must suffer as much interference as possible. Recall that a k element array can be used to suppress interference of $k-1$ other nodes, if it dedicates one DOF for communication. However, this technique differs from a conventional interference suppression technique in that, a jamming AP does not serve any client and therefore can use all its k DOFs for performing interference suppression and still jam several eavesdroppers. In the figure AP1 communicates a data packet to the client. Simultaneously, AP2,AP3,AP4 generate jamming signals by placing a null to the client. Then the maximum allowed power is used so that most of the region that is unoccupied by clients is filled with jamming signals. In this way, when multiple overlapping jamming signals are received, an eavesdropper in any of those locations would experience a poor SINR. The eavesdropper can attempt to use its k element array to suppress the interference along the directions of the jamming APs. However, if the number of APs that are in the vicinity times the number of antenna elements on them is higher than the number of antenna elements at the eavesdropper, it would still be unable to receive with a sufficient SINR. On the other hand, the client would be unaffected because the different jamming APs control their beam patterns to place a null in its direction. The fine grained control that the k element array provides, enables successful reception at the client while jamming at the eavesdropper simultaneously.

3.2.2 Stream overwhelming

(i) Overview: This strategy exploits the fact that when a node receives more information than the resources possessed to handle it (overwhelmed node), the different information signals mutually interfere with each other resulting in insufficient SINR for each of these signals. (Here, we use the notion of a stream to indicate each independent data/information flow that a node receives.). Several valid data transmissions are coordinated such that every intended receiver has a sufficient SINR for its desired signal, whereas at other points in the network, the multiple signals interfere to prevent decodability.
(ii) Mechanism: Figure 2(c) shows an illustration of the idea, where two APs and two clients are considered. When each client chooses the nearest AP, then there is no stream overwhelming. However, as in the second part of Figure 2(c), if the AP client associations are performed in a suitable manner, the beams overlap, causing a larger region to be overwhelmed, thereby reducing the exposure area. We also note here that it is not necessary for the eavesdropper to be present in the overlap of transmission ranges, rather, the eavesdropper would be left with poor SINR even if it is at a point in the overlap of interference ranges.

In both the above techniques an important point about the design must be clarified i.e Transmit side interference

suppression is more beneficial for security than receive side interference suppression. Consider an AP with k elements transmitting to a client with an omni antenna. The AP can use just one DOF for supressing interference to the client, since it is generating the interference. On the other hand, the eavesdropper ,doing receive side interference suppression would need to suppress interference from the different transmitting elements of the jamming AP, since each of them would appear different to each of his elements. The central idea is that the number of DOFs needed for interference suppression depends also on the number of elements at the interferer (see for instance pages 229 and 231 of [1] for MISO interference cancellation). Hence the number of antenna elements required at the eavesdropper is proportional to $p' * k$ where p' is the number of APs transmitting simultaneously within interference range of the eavesdropper and k is the number of elements on each AP. Thus interference from each interfering element must be managed by the eavesdropper.(Further details are available in [6]).

4. Architecture and Algorithms

4.1. Architectural Model

The architectural model that we consider consists of a central controller connected to several access points as shown in the figure 3. The controller receives from the backbone a stream of packets to be transmitted over the wireless LAN to the clients. For such packets, it employs a combination of the schemes discussed in Section 3, and forwards the packets to the appropriate access-points. We assume that the controller has strict synchronization and control over the access-points. All transmissions by the APs are done at the granularity of *synchronized fragment slots*, where the length of a fragment slot is smaller than that of a *packet slot*. The controller controls both the downstream and upstream (we discuss upstream communication toward the end of the section) modes of communication, and the two modes alternate in epochs. For downstream communication, the controller divides packets into fragments, applies its security decisions, and provides the APs with a set of fragments to transmit. Additionally, the controller knows the locations of the APs in the network and also the approximate locations of the clients (using for instance [11]). Further, it also posseses a coverage map to identify how the actual transmissions could be affected by the scattering nature of the channel. This information is already in place, in commercial products and will be leveraged to make intelligent pattern adaptation taking into account the beamforming impairments due to multipath. Also, since some of the APs will be part of the controlled jamming strategy and the entire coverage map is known, the coverage of jamming signals is also known.

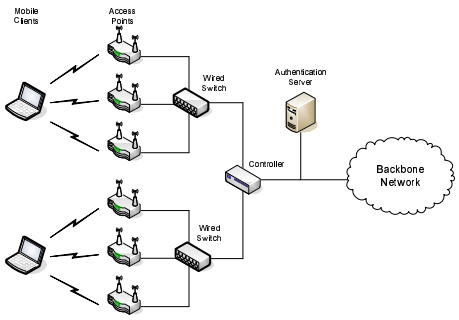


Figure 3. Network Model

4.2 Integrated Operations

While we discussed the three key strategies of secret sharing, controlled jamming, and stream overwhelming in Section 3, an important element of the operations is *how are the three techniques used in tandem to achieve the best performance possible?* The decision depends on topology, resources and security vs throughput tradeoff and a discussion can be found in [6]. Here we just recall the main observation that for a desired throughput constraint, if security has to be maximized, a combination of stream overwhelming and secret sharing (with preference to secret sharing) should be used and the remaining APs devoted to controlled jamming.

4.3. Problem Formulation and Algorithms

In the model described thus far, the intelligence is concentrated at the controller and can be divided into two major components, *the throughput scheduler and the security scheduler*. The throughput scheduler takes as input a throughput constraint S and determines the maximum number of packets j that are schedulable subject to a bound of S. This value j is then fed into the security scheduler that then determines the right strategies to use to maximize security while transmitting the j packets. Consider that the controller has an infinite stream of packets in its queue. We assume that any fairness mechanisms are implemented even before the packets reach the controller. In this fashion, the security algorithm works without affecting the fairness and is agnostic to the fairness mechanism used. The algorithm serves packets only in the order that they were queued to prevent potential starvation and out-of-order delivery problems .

The first part in the formulation is to determine the number of insequence packets j that can be scheduled out of the first S packets. S is thus a tunable knob which can be used to tune the desired levels of security in the network. For instance, if S = 1, then the problem reduces to maximizing security for this single packet's transmission.

S': schedulable number of packets
PS: schedulable packet stream
PS_s: first s packets in the packet stream
p_l: l^{th} packet in PS
F: number of fragments
$r(a, b)$: available DOF of AP a for fragment b
f: fragment index
E: network Connectivity matrix
$AP(n)$: set of APs within communication range of client n
$n(p_i)$: destination(client) id of packet P_i,
W_{ij}: (i, j)-th element of link conflict matrix,
$W_{(ab)(cd)}$: link conflict indicator between links ab and cd,
$m(p, f)$: assigned AP id of packet p during fragment f
$Action(a, f)$: action of AP a for fragment duration f
N: set of clients for which packets are destined in PS
M: set of APs which are in range of clients in N

Figure 4. Definition of variables

Greedy_Throughput() :
INPUT: S, PS, $m(Ps)$, E, W
OUTPUT: $m(Ps)$
1 For each a in M
2 $NC(a) =$ Calculate_Number_of_possible_clients
3 For each value s from 1 to S
4 $APS(s) =$ Calculate_available_APs($n(Ps)$)
5 $MAP =$ Find_Minimum_NC(APS)
6 If $MAP \neq$ NULL
7 $m(PI_j) = MAP$
8 Increment assigned
9 Update_Available_APS
10 Update_Available_DOF
11 Update_NC
12 $S' = assigned$

Figure 5. Throughput scheduler

However, when S is larger (bound by the number of APs) then throughput is maximized, and any security achieved is opportunistic using unassigned resources. In the second part of the problem, the security mechanisms need to be applied to the j insequence packets such that those j packets are transmitted by the end of the slot but the security is maximized for these j packets (appropriate choice of strategies for the APs during the fragment durations).

4.3.1.Throughput Scheduler. The throughput scheduler takes as input the control parameter S and the first S packets in the input queue of the controller. It provides as output the set S' of the j schedulable in-sequence packets. The algorithm used is a greedy algorithm that attempts to maximize j, the number of insequence packets that would be served during this transmission slot considering the spatial reuse and the adaptive interference suppression capability.The throughput scheduler first calculates how

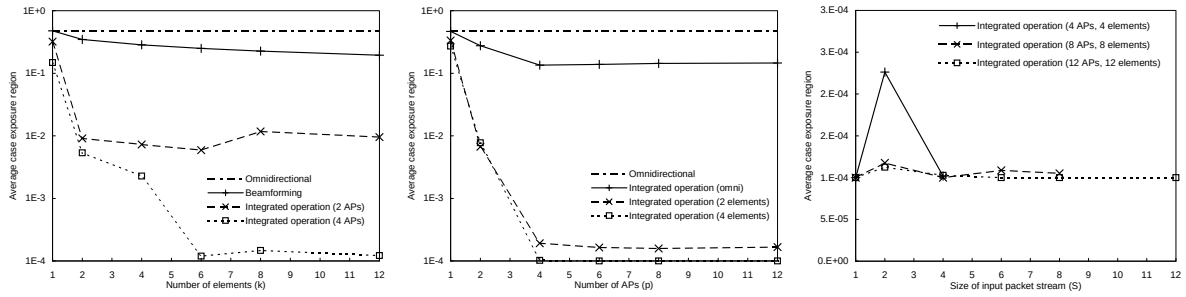
Initialize() :
1 For each m in M
2 For $1 \leq f \leq F$
3 $r(m, f) = k$
4 For each n in N
5 $AP(n) = \{m \in M | (m, n) \in E\}$
6 $PI = PS$

Security :
INPUT: S', PS, $m(Ps)$, E, W
OUTPUT: $Action(Ap, f)$, $m(Ps, f)$
7 Initialize()
8 sort_ascending(Pi,NUM_APS)
9 For each packet i from 1 to S'
10 $n = n(p_i)$
11 For each fragment f
12 For each AP m
13 $Avail(m, f) =$ Determine_availability(m,n,f,i)
14 $APList =$Sort_ascending(APs,fragment_num)
15 Adjust_stream overwhelming(APList)
16 For each AP in APList
17 $fragment =$Select_random_availablefragments
18 $Action(AP, fragment) = n(p_i)$
19 For each free AP a
20 For each free slot t
21 $Action(a, t) = JAM$

Figure 6. Security Scheduler

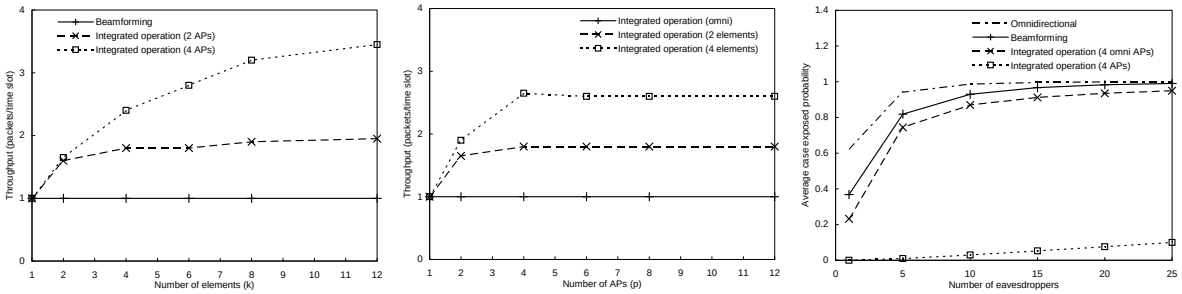
many clients for this packet stream can potentially use an AP, for each of the APs in the AP set M (lines 1-2). Then, for each packet starting from the first packet in the queue, the set of available APs is computed (line 4). Of this set, the one with minimum potential clients is chosen to be the one for this packet (line 5-7), as long as there is some such AP.

4.3.2. Security Scheduler. The objective of the security scheduler is to identify the assignment of actions of APs for different fragment durations such that all the packets handed down by the throughput scheduler are scheduled, while minimizing the exposure region. These are performed in a greedy manner, where secret sharing is the default strategy. However, when there is a tie between two choices of available APs for a fragment, both giving the same secret sharing benefit, then stream overwhelming is used as the strategy of choice. Once the possible fragments are scheduled (i.e the throughput scheduler's constraint on number of packets is met), controlled jamming is attempted in the free fragment durations. To begin with all the APs reachable from a client are included in the list of available APs for each client. Then the packets are arranged in ascending order of the number of APs(line 8). This is because clients with fewer number of APs should definitely be scheduled and must not lose their AP to other clients who may want



(a) Impact of k (b) Impact of p (c) Impact of Rate parameter S

Figure 7. Average case security performance



(a) Throughput variation with k (b) Throughput variation with p (c) Eavesdropper collusion

Figure 8. Throughput variation and Impact of eavesdropper collusion

to perform secret sharing. The available APs are allocated (line 15 -18) in a round robin manner such that for each AP one of the available fragment durations is picked randomly. When one of the fragments is lost, the fragment alone is scheduled in the next slot duration. Using the PCF mode of 802.11, it is possible to realize the scheme using current standard products. (Further details on protocol and system design can be found in [6].)

5. Performance evaluation

5.1. Simulation Model

We use a custom simulator written in C++ for the evaluation. The custom simulator incorporates the following modules:smart antennas pattern computation, ability to perform adaptive array processing [9] and indoor channel models. The details of the models are described below. *Beamforming*: Adaptive beamforming using the matrix inversion techniques described in [9]. *Channel model*: We use the ITU indoor attenuation model , which includes log-distance path loss with an exponent of 4 and a lognormal fading with a standard deviation of 2.5dB. We use a link margin of 3.2 dB (3dB with a 90% link reliability),an operating frequency of 2.4 GHz, an SNR threshold of 15 dB,a noise level of -100dBm (0.1pW), a sensitivity of -85dBm (3 pW) and a maximum transmission power of 20dBm (100mW) as used in standard 802.11 equipment . The default number of antennas is 4 and number of APs is 4. *Positions*: We generate the position of the client and APs randomly within the grid of points in a 100m * 100m grid. We also select the eavesdropper's(s) position randomly within the grid. We consider 20 clients by default. *Traffic flow*: We consider downstream flows to a randomly chosen subset of clients. For each data point, we calculate the average of 20 simulation runs. *Metric*: The metric of interest is the average exposure region.

5.2. Simulation results

We present results for the integrated algorithm in this section. Performance results for the individual schemes are available in [6].

5.2.1.Varying number of elements k

We explore the effect of varying the number of antenna elements on the APs. From Figure 7(a) as the number of elements on the APs is increased, the exposure region is reduced significantly. We also observe that the exposure region is extremely small when the integrated algorithm operates. Further, and more importantly, the exposure region of simple beamforming is much larger compared to the integrated solution. This means that it is only the intelligent use of the mechanisms that gives large security gains and not just simple beamforming.

5.2.2.Varying number of access points p

In Figure 7(b) we show how the average exposure region varies with the number of access points. We observe again that the exposure region reduces drastically as the number of APs is increased. Specifically, with 12 APs, a 2000x improvement is possible when a single eavesdropper is considered.

5.2.3.Varying values for parameter S

As we vary the value of S from low to high, the importance shifts from security to throughput. However, we observe that while the throughput increases with increase in S, the security benefit does not degrade. This is counter-intuitive and means that the stream overwhelming benefit also increases when the number of scheduled transmissions increases. This suggests that the intelligent use of all the three techniques enables maximizing both throughput and security without any significant tradeoff for the given conditions.

5.2.4.Varying number of colluding eavesdroppers

We simulate the effect of colluding eavesdroppers. For each packet destined to a client, we calculate if at the end of the slot duration, the eavesdroppers together have all the fragments for a client's packet. From Figure 8(c), one can observe that collusion increases the exposure area. Here the metric of exposure region by itself is not sufficient. Hence the metric used here is the packet exposure probability. Packet exposure probability for a given scenario is the number of packets that eavesdroppers can decode by collusion divided by the number of packets scheduled in a slot. This metric is shown in Figure 8(c). One can observe that with 4 Access points and with 4 element arrays each, the average packet exposure probability grows very gradually with increasing number of colluding eavesdroppers. Here we recall that collusion can only affect secret sharing,whereas controlled jamming and stream overwhelming would be unaffected by collusion. This explains why only with a large number of colluding eavesdroppers there is some increase in packet exposure probability.i.e even with 25 colluding eavesdroppers the packet exposure ratio is less than 20%. This result also indicates that *the schemes are quite robust to increasing eavesdropper antenna capability*. Additionally, the mobility of eavesdroppers from 5m/s to 20 m/s has no significant impact.

6 Related works and conclusion

Both the security problems in WLANs and higher layer solutions to specific problems have been well documented along with standardization of security techniques in the form of IEEE 802.11i [4]. [3] discusses spatial data striping techniques that increase the degree of security using a phased array antenna in 802.11 environments and [7] describes a theoretical communication scheme in which coding using the multiple degrees of freedom is used to generate artificial noise which degrades only the eavesdroppers channel quality. Both the above works do not provide a protocol or solution details. Also while [3] does not define or evaluate metrics, [7] does not consider the eavesdropper equipped with smart antennas.

In sum, we introduce the idea of using spatial smartness to provide security against eavesdropping. Specifically we describe the security implications of using smart antennas in the context of a WLAN, using the abstraction of a virtual array of physical arrays. We present three novel mechanisms that fundamentally improve security against eavesdropping. We evaluate the performance of an integrated algorithm that uses the three mechanisms using extensive simulations. Finally, we believe that this is the first solution that uses capability of smart antennas at higher layers for security with an intelligent consideration of MAC and security issues. For conventional indoor channels, using the solution with 4 APs and 4 elements , the exposure region is reduced from 1735 sq.m. to 5 sq.m. illustrating the power of the techniques.

References

[1] A.Paulraj, R.Nabar, and D.Gore. Introduction to space-time wireless communications. *Cambridge University Press*, May 2003.

[2] A.Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.

[3] J. M. Carey and D. Grunwald. Enhancing wlan security with smart antennas: A physical layer response for information assurance. In *IEEE VTC*, volume 1, pages 318–320, Sept. 2004.

[4] J.-C. Chen, M.-C. Jiang, and Y.-W. Liu. Wireless LAN security and IEEE 802.11i. *IEEE Wireless Communications*, 12(1):27–36, Feb. 2005.

[5] J. Franklin et al. Passive data link layer 802.11 wireless device driver fingerprinting. In *USENIX Security Symposium*, July 2006.

[6] S. Lakshmanan, C. Tsao, and R. Sivakumar. Securing wireless networks against eavesdropping using smart antennas. In *GNAN* technical report, 2007. Available at: http://www.ece.gatech.edu/research/GNAN/archive/2008 /icdcs08a.html.

[7] R. Negi and S. Goel. Secret communication using artificial noise. In *IEEE VTC*, volume 3, pages 1906–1910, Sept. 2005.

[8] J. Pang et al. 802.11 user fingerprinting. In *ACM MOBICOM*, Sept. 2007.

[9] M. Richards. *Fundamentals of Radar Signal Processing*. McGraw Hill inc., 2005.

[10] R. L. Rivest. All-or-nothing encryption and the package transform. *Lecture Notes in Computer Science*, 1267:210, 1997.

[11] A. Haeberlen et al. Practical Robust Localization over Large-Scale 802.11 Wireless Networks. In *ACM MOBICOM*,sep 2002.