Abstract—Generating a secret key between two parties by extracting the shared randomness in the wireless fading channel is an emerging area of research. Previous works focus mainly on single-antenna systems. Multiple-antenna devices have the potential to provide more randomness for key generation than single-antenna ones. However, the performance of key generation using multiple-antenna devices in a real environment remains unknown. Different from the previous theoretical work on multiple-antenna key generation, we propose and implement a shared secret key generation protocol, Multiple-Antenna Key generator (MAKE) using off-the-shelf 802.11n multiple-antenna devices. We also conduct extensive experiments and analysis in real indoor and outdoor mobile environments. Using the measured Received Signal Strength Indicator (RSSI) to generate keys, our experimental results show that using laptops with three antennas, MAKE can increase the bit generation rate by more than four times over single-antenna systems. Our experiments validate the effectiveness of using multi-level quantization when there is enough randomness in the channel. Our results also show the trade-off between bit generation rate and bit agreement ratio when using multi-level quantization. We further find that even if an eavesdropper has multiple antennas, he cannot gain much more information about the legitimate channel.

I. INTRODUCTION

Recently, there is an increasing interest in generating a shared secret key between wireless devices by exploiting reciprocal and location-specific properties of a wireless fading channel [1]. Based on the reciprocity, the bidirectional channel states should be identical between two transceivers at a given instance of time. In a multipath or mobile environment, the channel states randomly fluctuate due to fading. Therefore, two legitimate parties can take advantage of this natural correlated random process to generate a shared key. Furthermore, the channel state observed at an eavesdropper is uncorrelated with the legitimate channel if the eavesdropper is more than half a wavelength away from legitimate parties [2].

Generating shared secret keys via wireless channels has advantages over traditional mechanisms, e.g., Diffie-Hellman key exchange. It can eliminate the requirement of an authenticated communication channel and does not rely on the intractability of certain computational problems such as factoring large integers [1]. Actually, integers could be factored in polynomial time using Shor’s quantum factoring algorithm on quantum computers [3]. Although practical quantum computers may not be built in years, it is worthy to research on other key establishment mechanisms that do not rely on the computational intractability.

Previous experimental work shows two wireless devices can generate a shared key at approximately 1bit/sec by using off-the-shelf 802.11a hardware [1]. Under this secret bit generation rate, Alice and Bob may not be able to generate a long enough key in a mobile environment where the connectivity may be intermittent. For example, Advanced Encryption Standard (AES) requires a key length with at least 128 bits, then it takes about two minutes to generate a key. Therefore, it is necessary to increase the bit generation rate for real-world usage.

Intuitively, multiple-antenna devices have the potential to provide more randomness for key generation by exploiting spatial diversity. This potential, however, has not been well explored in the literature. Although a recent work studies the theoretic limits of multiple-antenna key generation [4], the feasibility and performance of key generation using off-the-shelf multiple-antenna devices in a real environment remains unknown. Furthermore, the binary quantization method proposed previously [1] may not fully make use of the randomness in the channel. Multi-level quantization can be applied to increase the bit generation rate when there is enough randomness in the channel.

In this paper, we propose and implement a shared secret key generation protocol, Multiple-Antenna Key generator (MAKE), that exploits spatial diversity in a real system with off-the-shelf 802.11n multiple-antenna devices. We also implement a practical multi-level quantization mechanism to increase the bit generation rate. We conduct extensive experiments and analysis in both indoor and outdoor environments. To the best of our knowledge, this is the first work on studying the shared key generation problem in a real multiple-antenna wireless system.

II. SHARED SECRET KEY GENERATION IN MULTIPLE ANTENNA SYSTEMS

Figure 1 illustrates our multiple-antenna system model. Two legitimate parties, Alice and Bob, want to generate a shared secret key using the channel related information (e.g. signal strength). They are equipped with $N_a$ and $N_b$ antennas, respectively. There is an adversary, Eve, who eavesdrops on the communication between Alice and Bob trying to figure out
the generated key. Eve is also equipped with multiple \(N_e\) antennas. In this paper, we assume a passive attacker model and mainly focus on the key generation between Alice and Bob.

To generate shared secret keys in the multiple antenna system, Alice and Bob perform the steps shown in Figure 2.

III. Protocol Design and Implementation

For Alice and Bob to generate a shared key, our protocol contains two stages: channel related information collection and key generation. The channel related information collection stage corresponds to the first step in Figure 2, and key generation stage includes all the remaining steps. For the practical concern of our protocol in the existing off-the-shelf 802.11n hardware, we use RSSI as the channel related information.

A. Channel Related Information Collection

One way to exploit the multiple-antenna diversity is to measure the RSSI between each antenna pair in a round-robin way. In our implementation, both Alice and Bob have three antennas which makes nine antenna pairs. Suppose we probe the sub-channels periodically in the order of \(A_1 - B_1, A_3 - B_3, A_2 - B_1, A_1 - B_3, A_3 - B_2, A_1 - B_2, A_3 - B_1, A_2 - B_3, A_2 - B_2\) shown in Figure 3, we will get nine RSSI sequences corresponding to each sub-channel respectively at both Alice and Bob sides.

B. Key Generation

Alice initiates the key generation process. She decides quantization levels and performs the quantization on her RSSI list. She then sends a KEYGEN REQUEST to Bob. In the KEYGEN REQUEST frame, she indicates 1) which antenna-pair measurements are used for key generation, 2) the quantization levels, 3) which portion of the RSSI list is used, and 4) the start positions of excursions. After receiving the KEYGEN REQUEST, Bob will quantize his lists using the same quantization levels (but may use different intervals according to his own measurements). Bob finds a subset of the positions where he also finds excursions, and sends a KEYGEN REPLY to Alice indicating those positions. Both Alice and Bob generate their keys in the same way based on those positions. Further reconciliation mechanisms [5] can be applied by exchanging more KEYGEN REQUEST and REPLY frames if the keys do not agree.

IV. Experimental Results and Performance Evaluation

To evaluate the performance of MAKE, we carried out extensive experiments in both real indoor and outdoor environments. When multiple antennas are used in MAKE, we call it Multiple One antenna To One antenna (MOTO) mode. When we set the probing sequence to contain only one antenna pair, MAKE degenerates to the single antenna case. We call it Single One antenna To One antenna (SOTO) mode.

Figure 4 is a CDF of the shared bit generation rates corresponding to the keys made by 2-ary and 4-ary quantization levels (filtered by approximate entropy \(\geq 0.9\)) under different environments, probing intervals and operating modes. We can see that, for all scenarios, the median bit generation rate of MOTO (corresponding to 3-antenna systems) is at least 4.5 times of that achieved by SOTO (corresponding to single antenna systems). The indoor environment provides higher variation (entropy), so all the indoor cases outperform the corresponding outdoor cases. When we probe the channel faster (with shorter interval), we get higher bit generation rate because we can catch more randomness from the channel. However, the bit generation rate is fundamentally constrained by the time-variation of the channel. If the channel itself does not change much in a short interval, even if we can probe the channel at a very high rate, we cannot extract more randomness.

REFERENCES