An Experimental Study of Secret Key Generation For Passive Wi-Fi Wearable Devices

Mohammad Hossein Chinaei, Vijay Sivaraman, Diethelm Ostry
Electrical Engineering and Telecommunications, University of New South Wales, Sydney, Australia
Emails:{m.chinaei, vijay}@unsw.edu.au, diet.ostry@csiro.au

***Abstract*—Passive Wi-Fi is a technology to generate 802.11b transmissions using backscatter communication, with power consumption 10000x lower than existing Wi-Fi chipsets. Since wearable devices are typically limited in resources such as power and storage, classical cryptographic security schemes are problematic for them. We instead propose to use wireless channel characteristics to secure data transfer. It has been shown that communicating wireless transceivers are able to generate shared secret keys by measuring channel characteristics at a single frequency. These methods are not applicable to passive Wi-Fi, which uses two different frequencies. In this paper, we describe a method to generate a shared secret key based on wireless channel characteristics in the passive Wi-Fi scenario where the two parties are using dual frequencies.**

I. Introduction

Backscatter or passive communication system is defined as a system in which a transceiver (termed the reader) sends out an incident signal to the passive device ("the tag") and receives a modified version reflected back by the tag. In this scenario the tag is a resource-constrained node without the usual active RF transmitter architecture for data transmission. Instead, it imposes data modulation on the RF field it reflects from transmissions by the reader. This revolutionary method, called passive Wi-Fi, was recently proposed in [1], which implements a passive communication network capable of Wi-Fi transmission. The passive Wi-Fi tag utilises backscatter communication rather the power-consuming RF transmitter function, and is potentially able to reach an 11 Mbps data bit rate while consuming 10000 times lower power than current active Wi-Fi devices.

Wearable devices are required to be small and light, and therefore can be severely constrained in computation capability, memory, communication, and battery resources. The need for ultra-low power consumption, small size and compatibility with current Wi-Fi devices make passive Wi-Fi a very attractive and practical option for body-worn sensor networks. However these wearable IoT devices may be transmitting critical personal and medical information. One of the most important challenges for these devices is to find feasible low-power security schemes to protect them against attack. Classical cryptographic schemes for establishing a secret key between the two ends consume significant computational resources making them generally unsuitable for ultra-low power tags.

Shared key generation based on channel characteristics is however a promising scheme and has been well studied in the literature. Previous work (eg our previous paper [2]), shows that this approach has high potential in sensor networks where nodes have severely limited computational and power resources. The information-theoretic aspects of key bit generation based on symmetric channel properties is studied in [3], [4]. The authors show that it is possible to extract identical information from the wireless channel at each end of the link, the information is unique to the legitimate parties, and can be used to generate a secret key. The eavesdropper however cannot learn any information about the shared key by listening to channel.

In this paper we introduce a new scheme to generate a shared secret key in a passive Wi-Fi scenario and use software-defined radios to demonstrate the approach. Unlike the conventional secret key generation methods which measure channel characteristics at a single frequency, our proposed method uses channel measurements at the two different frequencies used in the passive Wi-Fi scenario and utilises them to generate a secret key shared by both legitimate parties. We have implemented our technique on Universal Software Radio Peripheral (USRP) platforms to assess the scheme experimentally.

II. Secret Key Generation Technique

As in [5], the system model consists of a reader and a passive tag. The reader uses the Bluetooth protocol to generate a single-tone continuous wave (CW) at a certain frequency lying outside the desired Wi-Fi channel and radiates it toward the tag. The tag itself performs Wi-Fi modulation to generate a packet at baseband. The tag modulates the reflection cross-section of its antenna with this packet. The received out-of-band CW signal is thus shifted in frequency, modulated, and re-radiated in the desired Wi-Fi channel. The backscattered packet is a standard Wi-Fi packet in a standard Wi-Fi channel, and is fully compatible with commercial Wi-Fi devices. Since the reader utilises Bluetooth technology to transmit the CW signal and Wi-Fi to receive the backscattered packets, the method has been called inter-technology backscatter [5].

In the basic system, information is sent in plaintext from tag to reader. Confidentiality, integrity and authenticity of the message are not provided and the message could be compromised by any malicious entity in the vicinity of the tag and reader. For new sensor technology to succeed in real world scenarios such as wearable sensor networks and IOT devices, it must be supported by sufficiently powerful security features to protect against plausible attacks.

To avoid high computational power consumption and a trusted third party to set a pair of keys between legitimate

parties, we aim to utilise wireless channel characteristics as a source of shared secrecy to generate a key at both ends of the reader-tag link. The wireless channel in a typical multipath environment shows both time-, frequency-, and space-varying random behaviour. As a result, the changing channel causes consecutive transmitted signals to experience different gains, phase shifts or delays in propagating from transmitter to receiver. However, the reciprocity property of the wireless channel allows both transmitter and receiver to observe the same channel characteristics simultaneously. In other words, if two wireless nodes, Alice and Bob, using the identical transceivers and antennas, send identical signals to each other they would measure the same channel properties. Most previous work on channel-based key generation for IoT systems utilise these symmetric channel characteristics when propagation occurs at one frequency. However, this strategy is not applicable to the passive Wi-Fi scenario because the reader and tag receive signals at different frequencies.

Our system model consists of reader, tag and eavesdropper in a time-varying channel. In passive scenarios the tag is not able to send a signal to the reader independently, but instead it reflects a beacon signal to the reader after modulating it with a WiFi packet. We assume here that in the key generation procedure, the passive tag is capable of two different modes of operation, reflecting and listening. In the listening mode, it measures a channel characteristic such as received signal strength (RSS). In the reflecting mode it reflects an incident beacon provided by the reader node. Our proposed method proceeds in three steps as follows (see Fig. 1):

1) The reader transmits a CW beacon signal at frequency f_1. The tag operates in reflecting mode and reflects a packet back at frequency f_2. When the reflected signal is received by the reader, the RSS it measures is essentially the product of channel gains at f_1 and f_2 i.e. $|G_{f1}||G_{f2}|$, because the forward and backward signals are sent at different frequencies.
2) The reader sends out the same beacon signal at f_1 while the tag is in listening mode so it can use an RSS measurement to estimate the channel gain at f_1, i.e. $|G_{f1}|$.
3) The reader again sends a beacon signal but now at frequency f_2 with the tag in the listening mode so it can measure the RSS at f_2, giving it an estimate of $|G_{f2}|$, the channel gain at f_2.

After these three steps, the tag can estimate the round-trip channel gain by multiplying the estimate at f_1, $|G_{f1}|$, by the estimate at f_2, $|G_{f2}|$. If the whole process is completed in a time duration less than channel coherence time, the channel characteristics can be assumed constant for both sides and the product of the measured gains at f_1 and f_2 at the tag side would be expected to be in good agreement with the measured round-trip RSS at the reader side. This source of shared secrecy can be used for key generation at the both sides. Due to the spatial decorrelation of multipath channels, the channel measurement is confidential with respect to any eavesdropper located further than a half of wavelength from legitimate parties.

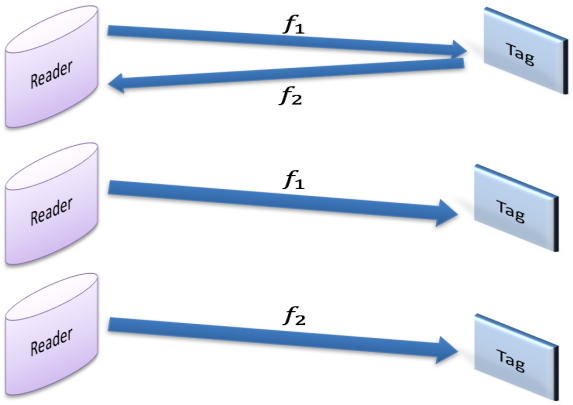

Fig. 1. Channel measurement steps in passive Wi-Fi scenario

The shared channel measurements provide data to both reader and tag from which they can generate a binary key via a quantisation process which to converts the measurements into a string of key bits. We use the basic level-crossing quantiser given in [2]. Both the reader and tag use an adaptive sliding window of length W_Q, within which consecutive RSS measurements are processed. For each window the two thresholds are defined as follows:

$$q+ = \mu + \alpha.\sigma$$

$$q- = \mu - \alpha.\sigma$$

where μ is the mean, σ is the standard deviation and $\alpha \geq 0$ is an adjustable parameter to balance the key bit generation rate against key bit agreement on both sides. An RSS measurement within a window outputs a key bit of 1, if it is greater than $q+$, and of 0 if less than $q-$. All the measurements which fall between two thresholds are discarded.

III. Evaluation

In this section, our goal is to evaluate the proposed method experimentally using USRP devices. Each of the nodes in our scenario including reader, tag and eavesdropper is implemented as a USRP connected to a computer running LabVIEW as the software interface. In our experiments f_1 and f_2 are separated by $11MHz$ as in [1], with $f_1 = 2.171GHz$ and $f_2 = 2.182GHz$. The two legitimate parties were separated by 100cm and the eavesdropper was located 70cm from them. During measurements, the channel characteristics were dynamically changed by moving the nodes slowly and randomly. Also abrupt changes were introduced by interposing a barrier randomly between the nodes.

As it is explained in the previous section, our approach comprises three steps. At the end of the third step the legitimate parties are able to use their channel measurements to generate a shared secret key. The eavesdropper is assumed to be passive and knows the whole key establishment process and she is able to measure the channel RSS at both frequencies.

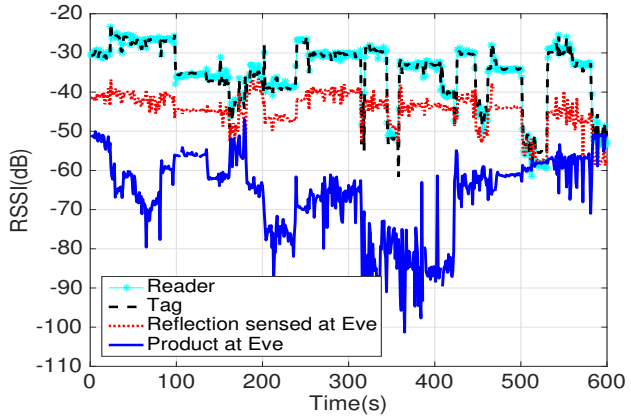

Fig. 2. Key Generation in passive Wi-Fi scenario

Therefore, during the first step, the eavesdropper would receive the reflected signal from the tag and in further steps she would listen to the reader's beacon to measure her RSS at both frequencies. She could utilise these different measurements of the channel to try to estimate the secret key. One estimate is based on her measurement in the first step which we call the backscatter measurement (the same signal as the reader measures to generate its key), and a second estimate can be made by forming the product of her measurements in the second and third steps (which we call the product measurement) in a similar way to what the tag does.

Fig. 2 shows that the RSS measurements made by the reader and the tag are in good agreement. We use the Pearson correlation coefficient between tag and reader ([2]). The correlation coefficient between reader and tag is 0.9849 corresponding to a very high agreement with each other. The correlation coefficient between reader and eavesdropper when it uses the backscattered measurement and product measurement are 0.8337 and -0.1299 respectively.

We used the level-crossing quantisation scheme to generate a key bit string from the RSS measurements. Using the quantisation process, the three parties determine the sample index and bit value of successful (ie not discarded) measurements. The reader and the tag exchange the location of their successful measurements to each over a public channel. Then they also discard the generated bits which are not in the successful measurement locations of the other side. In other words, the final key bits in each side are generated from the measurements which were considered successful at both sides. Because they use a public channel to send this information, all of the nodes, including eavesdropper, are aware of the exact sample indices of measurements that were used in key generation, but if the shared RSS measurements are unknown to an eavesdropper this gives no information about the key. We set α to 1 and show the key bit agreement for the different nodes in Table I and for several different window sizes for the quantisation process.

As shown in Table I, key agreement between reader and tag is at least 93.59%. We should emphasise the fact that we do not perform any reconciliation process to reconcile

TABLE I
KEY AGREEMENT BETWEEN DIFFERENT NODES

Signal quantised	Key Agreement	Eve Backscatter Key Agreement	Eve Product Key Agreement
$W_Q = 5$	93.59%	71.42%	46.30%
$W_Q = 10$	95.62%	72.13%	45.90%
$W_Q = 20$	96.63%	77.88%	42.78%

the keys [2]. Not surprisingly, larger window sizes achieve higher agreement, but at the cost of computational power consumption and memory usage. The eavesdropper in these experiments only achieves a key bit agreement proportion of about 45% for her product measurements, approaching the accuracy of a coin toss. However the eavesdropper key estimates made from listening to step 1, the backscatter case, surprisingly shows a more significant key agreement level. We are investigating the cause of this effect, which may be due to the short ranges used in the experiments.

IV. CONCLUSIONS

In this paper, we have proposed a novel method for secret key generation based on channel characteristics when the communicating nodes use several different frequencies such as the scenario on which passive Wi-Fi is based. We showed that it is possible to generate shared randomness and thus key material from RSS measurements of the wireless channel even when one node is a passive WiFi reflector. We have implemented our method using USRP devices to show experimentally that nodes can obtain keys with high agreement from the channel measurements. The key bit agreement between legitimate parties was at least 93% in our configuration (which could be improved with subsequent reconciliation or filtering schemes). In contrast to the legitimate parties, the eavesdropper cannot obtain useful information from her product measurements (close to using a random coin toss to generate the key). Nevertheless an estimate from the backscatter signal shows an unacceptable level of key agreement at present.

REFERENCES

[1] B. Kellogg, V. Talla, S. Gollakota, and J. R. Smith, "Passive wi-fi: bringing low power to wi-fi transmissions," in *13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16)*, 2016, pp. 151–164.

[2] S. T. Ali, V. Sivaraman, and D. Ostry, "Eliminating reconciliation cost in secret key generation for body-worn health monitoring devices," *IEEE Transactions on Mobile Computing*, vol. 13, no. 12, pp. 2763–2776, 2014.

[3] R. Ahlswede and I. CSISEAR, "Common randomness in information theory and cryptography. i: Secret sharing," *IEEE Transactions on Information Theory*, vol. 39, no. 4, pp. 1121–1132, 1993.

[4] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, 1993.

[5] V. Iyer, V. Talla, B. Kellogg, S. Gollakota, and J. Smith, "Inter-technology backscatter: Towards internet connectivity for implanted devices," in *Proceedings of the 2016 conference on ACM SIGCOMM 2016 Conference*. ACM, 2016, pp. 356–369.