Techniques in Key Generation

Juby Susan Mathew
PG Student
Mount Zion College of Engineering, Kadammanitta, India

Hari. S
Assistant Professor
Mount Zion College of Engineering, Kadammanitta, India

Abstract

Key generation from the randomness of wireless communication channels is a hopeful technique to share cryptographic keys securely between legitimate users. This paper reviews the current technique for wireless key generation. The principles, performance metrics and key generation procedure unit comprehensively surveyed. Ways for optimizing the performance of key generation also are mentioned. Key generation applications in numerous setting area units introduced beside the challenges of applying the approach in every state of affairs. We conjointly mentioned ways to optimize the key generation performance; completely different application outlines were surveyed so as to clarify the options and challenges of every surroundings.
Keywords: Key Generation, Wireless Communication

I. INTRODUCTION

Traditionally, the data is secured by classic encryption schemes, which work on the assumption that the algorithm is complex enough so that the time taken by eavesdroppers to break the cryptographic system is much longer than the validity of the information itself, therefore, the background secrecy is guaranteed. There has been extensive research interest to protect wireless transmission. Classic encryption schemes contain symmetric encryption schemes and asymmetric encryption schemes, based on the keys that the two cryptographic parties use.

Symmetric encryption schemes use the same key and are usually give data protection to their efficiency in data encryption. Uneven secret writing schemes, conjointly referred to as public key cryptography, use constant public key however completely different personal keys and area unit typically applied for key distribution. Research streams in wireless network security, wherever Alice and Bob represent 2 legitimate users UN agency wish to share data firmly between one another. Classic encryption schemes are faced with several vulnerabilities. Take public key cryptography as an example. Firstly, it depends on the computational rigidity of some mathematical problems. This computational security nature may not hold in future due to the rapid development of hardware technology.

II. KEY GENERATION PRINCIPLES

Key Generation is based on three principles, that is, temporal variation, channel reciprocity and spatial decorelation. Temporal variation is introduced by the movement of the transmitter, receiver or any objects in the environment, which will change the reflection and scattering of the channel paths. The randomness caused by such unpredictable movement can be used as the random source for key generation. There is research effort to exploit the randomness in frequency domain and spatial domain However, in a very static atmosphere wherever these options stay identical, the randomness is quite restricted. Temporal variation is therefore still needed so as to introduce a adequate level of randomness.

Channel reciprocity shows that the multipath and fading at both ends of the same link, i.e., same carrier frequency, are duplicate which the basis is for Alice and Bob to generate the same key. The signals have to be measured by hardware platforms, which usually work in half duplex mode and there is a possibility of noise. Therefore, the received signals of the uplink and downlink path are asymmetric due to the non-simultaneous measurements and noise effects, which minimize key generation applications within time-division duplexing (TDD) systems and slow fading channels. These effects can be mitigated using signal processing algorithms.

Spatial decorrelation state that any snoop set quite one half-wavelength aloof from either user exposed by unrelated multipath attenuation, which might even be delineated by the cross-correlation between the signals of legitimate users and eavesdroppers. This property is essential for the security of key generation systems and has been claimed in most key generation papers[6]. However, it may not be satisfied in all the environments. Channel variation is contributed by large-scale fading and small-scale fading. With a uniform scattering Rayleigh environment and without a line-of-sight path, if the number of scatters grows to infinity, the signal decor relates over a distance of nearly one half-wavelength. Some experiments have also shown this property. However, when large-scale fading is dominant, special caution is required as the channel is more correlated. There's analysis reportage that signals determined by eavesdroppers have mutual relationship to signals of legitimate users, that makes key generation systems vulnerable and needs special thought to combat eavesdropping. In general, spatial decorrelation has not been extensively studied and is worth more research input.

III. PERFORMANCE METRICS

Key generation is designed to establish cryptographic keys for encryption and authentication. These applications have special request on the key's randomness, refresh rate, etc. Thus, key generation systems can be correspondingly evaluated in terms of three important metrics: randomness, Key Generation Rate (KGR), and Key Disagreement Rate (KDR).

A. Randomness

Randomness is the most significant feature of key generation systems. Cryptographic applications have strict requirements on the randomness of the key sequence. A statistical randomness test suite provided by National Institute of Standards and Technology (NIST) is mostly used to test the randomness of random number generators and pseudo random number generators (PRNGs). In essence, a key generation system may be a sort of RNG, therefore bureau applied math check suite also can be applied. As randomness may be a probabilistic property, applied math analysis is utilized to check a particular null hypothesis, i.e., the sequence beneath check is random.

There is infinite statistical performance of a random sequence, therefore, in practice, it is impossible to test all the features using a finite set of tests. The NIST test suite has 15 tests to examine different randomness features, each for a specific feature of the randomness, i.e, the proportion of 1s and 0s (frequency test), periodic feature (DFT test). Some tests needs extremely long sequence. For example, the prompt input length is 106 for the linear complexness, random excursions and random excursions variant tests and is judged to be terribly long during a key generation system. Thus, most of the key generation analysis has solely adopted a set of the randomness tests to see a set of the randomness options.

B. Key Generation Rate (KGR)

KGR describes the amount of secret bits produced in one second/measurement. It mainly depend on environment conditions which determines the amount of randomness available for extraction. A high KGR is necessary for the real time key generation process as the cryptographic schemes require a certain length of keys, advance encryption standard (AES) needs a key series with a minimum length of 128 bits.

C. Key Disagreement Rate (KDR)

KDR is that the share of the various bits between the keys generated by Alice and Bob, that is state as wherever N is that the length of keys. The KDR should be smaller than the correction capacity of information reconciliation techniques, otherwise, key generation fails. There are also other assessment metrics such as scalability and implementation issues. However, randomness, KGR and KDR are the most significant and popular metrics which describe the success and efficiency of the system.

$$\text{KDR}=\frac{\sum_{i=1}^{N}|K^{A}(i)-K^{B}(i)|}{N} \qquad (1)$$

IV. KEY GENERATION PROCEDURE

Key generation procedures are often divided into four stages: channel searching, division, data reconciliation and privacy amplification. One user is the instigator, and also the alternative because the communicator, while not loss of generality, Alice is chosen because the instigator. So as to modify the flow chart, the stage synchronization between Alice and Bob isn't shown.

A. Channel Probing

Channel probing is the key step to harvest the randomness from channel which needs two users on the other hand measure the common channel through the received signals. At time $t_{i,A}$ Alice sends the probing signal to Bob who will measure some channel parameter through the received signal and store it in Y_i'. At time $t_{i,B}$, Bob transmits his i^{th} probing signal to Alice who will also measure the same channel parameter and store it in X'_i . The sampling time difference $\Delta ti = |t_{i,A} - t_{i,B}|$ is carefully kept smaller than the channel coherence time so the channel during the two probes can be regarded as constant. Alice and Bob will repeat the above process until sufficient results are collected.

Research in channel probing mainly reflects the channel parameter, signal pre-processing, and channel probing rate. Although the channel features at each end of the link are reciprocal, the measured received signals are asymmetric mainly due to non-simultaneous measurements and the independent noise vested in the two separate hardware platform. The effects of non-simultaneous measurements and noise can be changed by interpolation and filtering, respectively.

B. Quantization

Similar to an analog-to-digital converter (ADC), quantization in key generation is also a method to map the analog channel measurements into binary values. The quantization level, which is the number of key bits quantized from each measurement. Due to the failure between received signals of any two users, the quantization level is changed according to the signal-to-noise ratio (SNR) of the channel. In multi-bit quantization, Gray coding may be used in order to minimize the key disagreement. The thresholds are the reference levels used to divide the measurements into different groups. Mean value and cumulative distribution

function (CDF) are commonly used to determine the thresholds. Mean value and standard deviation based quantization scheme has simple implementation. The thresholds are determined as In essence, the quantizer design is the adjustment of the quantization level and threshold in order to approach an optimal performance of the randomness, KGR and KDR. This results in different design variations.

C. Information Reconciliation

Although signal pre-processing algorithms are often adopted to enhance the cross-correlation of the channel measurements, there should still be key disagreement between Alice and Bob once quantisation. The pair are often corrected exploitation information reconciliation techniques, which might be enforced with protocols like Cascade or error correcting code (ECC) like low-density parity-check (LDPC), BCH code , Reed-Solomon code, and Turbo code. ECC-based reconciliation schemes are more efficient than Cascade, but they also leak more information and have higher complexity. The selection of the ECC depends on the complicated nature and correction capacity.

D. Privacy Amplification

Some information is transmitted publicly in the information reconciliation stage, which can be heard by the eavesdropper as well. This can potentially compromise the security of the key sequence. Privacy amplification is then used to remove the revealed information from the agreed key sequence at Alice's and Bob's side. This can be implemented by extractor, or universal hashing functions, such as leftover hash lemma, cryptographic hash functions. Privacy amplification and information reconciliation always appear together, which requires a cross design between these two stages. However, in practice, it is difficult to determine the amount of the leaked information, or to recognize where the leakage occurs in the data. Thus the key generation implementation is usually low cost, as it only needs non-complex operations, i.e, sampling and storing data in the channel probing stage. All these operations may be enforced exploitation the off-the-peg hardware, with solely a amendment to the drivers. The key generation procedures bear in line with the system implementation. All the key generation systems want channel sampling and quantisation whereas info reconciliation and privacy amplification could also be not sensible because of specific implementation and setting wherever the systems succeed excellent arrangement once quantization.

Table - 1
Key generation application in wireless networks

Technique		Modulation	Parameter	Features
IEEE 802.11	n	MIMO OFDM	RSS, CSI	MIMO OFDM enables CSI measurements in both frequency and spatial domains
	a	OFDM	RSS, CSI	OFDM enables CSI measurements in frequency domain
	g	OFDM, DSSS	RSS, CSI	
	b	DSSS	RSS	RSS available
IEEE 802.15.4		DSSS	RSS	Widely used in WSN; Sensor motes are powered by battery and with low computational capacity; Usually low mobility.
Bluetooth		FHSS	RSS	FHSS allows sampling RSS in different frequencies.
UWB		Pulse	CIR	Low power, large bandwidth (> 500 MHz)
LTE		MIMO OFDM	RSS, CSI	Only applied in slow fading channel for key generation; Ability to adjust parameters, such as power allocation; No practical implementation reported yet.

V. APPLICATIONS

A. Wireless Local Area Network

WLAN connectivity is now included into most laptops, tablets and smart phones, making it the most popular wireless access technology. The main WLAN standards are IEEE 802.11 a/b/g/n functioning in 2.4 GHz and 5 GHz bands. Due to its wide extent, many practical key generation implementations in WLAN have been reported[11]. WLAN is primarily designed for indoor environments, where there is limited mobility. Therefore, in order to assured the randomness of the key sequence, the probe rate should be comparatively large, as the channel can remain static over long periods, which results in a low KGR. RSS is available in all the WLAN standards and can be thriving in the commercial NICs. The research emphases are mainly on the improvement of KGR and decrease of KDR.

B. Wireless Sensor Network

WSNs are widely used in environment monitoring, health care, or military, where there is a clear need to protect the data exchanged. The sensor nodes in WSNs are provided with 802.15.4 transceivers operating in the 2.4 GHz to 2.8 GHz industrial, scientific and medical (ISM) band. RSS info is typically on the market in these transceivers and might be wont to establish the keys in WSNs. However, the sensing element nodes area unit static or with very little movement, battery power-driven, and with low procedure capability, that places special needs on the implementation.

C. Vehicular Communication

In vehicular communication, vehicles can move fast and the coherence time can be as short as a few hundred seconds . In a 20 MHz channel IEEE 802.11 OFDM system, a packet with a maximum rate and minimum length causes an outcome in an over the air time of 34s, which cannot be examined negligible compared to the coherence time. There has been research applying key generation in vehicular communication. An RSS-based key generation system has been implemented using off-the-shelf IEEE 802.11 radios. The distance is measured through the long time averaged RSS values so that the fluctuations due to fading and shadowing are eliminated. As the distance does not change much in a short time interval, the legal users can agree on the same keys.

VI. CONCLUSION

Key generation from the randomness of wireless channels is a successful option to public key cryptography for the establishment of cryptographic keys between any two users. It is relatively easy to implement using off-the-shelf wireless NICs and can achieve information-theoretic security. This paper focused on the techniques of key generation systems, precisely, we reviewed the key generation principles. Here suggested that the performance metrics and procedure of key generation. We also discussed methods to enhance the key generation performance. Different application scenarios were surveyed in order to clarify the features and challenges of each environment.

REFERENCES

[1] Junqing Zhang, Trung Q. Duong, (Senior Member, IEEE),Alan Marshall, Roger Woods, Institute of Electronics, Communications and Information Technology, Queen's University Belfast, Belfast, BT3 9DT, U.K, " Key Generation From Wireless Channels",2016.
[2] E. Jorswieck, S. Tomasin, and A. Sezgin, Broadcasting into the uncertainty: Authentication and condentiality by physical-layer processing," Proc. IEEE, vol. 103, no. 10, pp. 1702_1724, Oct. 2015.
[3] K. Zeng, ``Physical layer key generation in wireless networks: Challenges and opportunities," IEEE Commun. Mag., vol. 53, no. 6, pp. 33_39, Jun. 2015
[4] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, ``Safeguarding 5G wireless communication networks using physical layer security," IEEE Commun. Mag., vol. 53, no. 4, pp. 20_27, Apr. 2015.
[5] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, ``Principles of physical layer security in multiuser wireless networks: A survey," IEEE Commun. Surveys Tuts., vol. 16, no. 3, pp. 1550_1573, Aug. 2014.
[6] W. Stallings, Cryptography and Network Security: Principles and Practice, 6th ed. Englewood Cliffs, NJ, USA: Prentice-Hall, 2013.
[7] L. Chen, J. Ji, and Z. Zhang, Eds., Wireless Network Security : Theories and Applications. Springer, 2013.
[8] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, ``Physical layer security in wireless networks: A tutorial," IEEE Wireless Commun., vol. 18, no. 2, pp. 66_74, Apr. 2011.
[9] M. Bloch and J. Barros, Physical-Layer Security: From Information Theory to Security Engineering. Cambridge, U.K.: Cambridge Univ. Press, 2011.
[10] S. Mathur et al., ``Exploiting the physical layer for enhanced security[Security and Privacy in Emerging Wireless Networks]," IEEE Wireless Commun., vol. 17, no. 5, pp. 63_70, Oct. 2010.
[11] B. Wu, J. Chen, J. Wu, and M. Cardei, ``A survey of attacks and countermeasures in mobile ad hoc networks," in Wireless Network Security, Y. Xiao, X. Shen, and D.-Z. Du, Eds. New York, NY, USA: Springer, 2007, pp. 103_135.