Physical Layer Secret Symmetric Key Generation and Management Techniques for Wireless Systems-A Study

Srividya.L[#1], Dr.P.N.Sudha[*2]

#Dept of ECE, Dayananda Sagar College of Engineering, Bangalore-560078, India,

*Dept. of ECE, K.S. Institute of Technology, Bangalore-560109, India

llsrividyabe@gmail.com
2pnsudha@gmail.com

Abstract-Symmetric encryption is more attractive due to its simplicity in implementation especially under restricted environment where there is a constraint on computation, memory, power etc. One of the basic requirement is that both the legitimate parties to posses common secret key which is quite challenging in the wireless medium which is unsecure to share. There is a shift in the paradigm from developing complex and secure encryption algorithms, to emphasise in securing and sharing the secret information i.e., secret key. In this paper we make an extensive survey of methods in generating secret key in various context and the key management techniques. The concept of symmetric key management and generation techniques were studied under physical layer security context.

Keywords: key sharing, key generation, key management, physical layer security, channel state information (CSI), biometric key, elliptic curve cryptography, channel model.

I. INTRODUCTION

With the popularity and advancement of connecting technologies, wireless devices have paved it way in our day to day life. Even critical data applications such as banking, military, business have become wireless. Wireless mode of communication are more vulnerable for unintended audience, hence there is a need for achieving secrecy for the data.

Secrecy mechanisms are broadly classified under concealment systems, secrecy systems and privacy systems. Concealment systems are those similar to stenographic techniques which involves data hiding , security systems uses codes and mathematical transformations, whereas privacy systems requires devices to recover messages.

We are concerned with security systems to achieve confidentiality, integrity, availability, authorisation, non repudiation, freshness, accountability and assurance.

Critical data is transformed into codes with some of the cryptographic primitives such as symmetric/asymmetric encryption, digital signatures and hash functions.

In present communication system, security is implemented at each level as an additional cryptographic feature. It has become a part of network design and security reinforcement.

We are concerned with physical layer security as it aims at providing security at the initial level i.e.., bit level. Also physical layer security does not require additional equipment than that are already employed for communication.

The public key or asymmetric cryptography has an advantage of scalability, while digital signatures have intrinsic authentication properties, but both lacks due to high computational overhead and authentication by public certificates. Symmetric cryptography attracts due to its simplicity and less weight computation but lacks in providing authentication and not scalable.

As wireless nodes have constrained by its computational capability, memory size & power hence we prefer symmetric cryptography which is light computational weight and less complexity in implementing at the physical layer level. The key challenges to implement symmetric key cryptography is sharing a common key between sender and receiver, as wireless medium are open systems and are vulnerable to security attacks[18].

In this paper we address to the various symmetric key generation and management techniques on wireless mediums. We also discuss recent works carried in this field.

The rest of the paper is organised in this manner: section II deals with the basic symmetric key management concepts while section III with physical layer security which also discusses about key management techniques. Basics of wireless channel characteristics followed by key generation channel models are discussed in section IV. Section V summarises the recent related work in symmetric key generation techniques and conclusion and future works is presented in the end in section VI.

II. SYMMETRIC KEY MANAGEMENT TECHNIQUES

Symmetric key management techniques are classified based on method of key establishment and number of users participating in key generation phase.[17]

Key distribution centre: In centralized key distribution approach key generation centre distributes pair wise session keys, a global key between nodes and server. The disadvantage of this approach is that it cannot be implemented on distributed networks or decentralised networks.

Symmetric key can also be shared using public key cryptography such as RSA, Diffie- Hellman key exchanges main strength of this strategy lies in computational difficulty of reversing an algorithm.

Wireless sensor networks oriented solutions are based on key pre distribution which involves two stages key generation and key material distribution. Example for key generation is Blom's scheme where central authority computes public matrix and secret matrix over GF field. The secret key matrix for each node i will be ith column from public and secret matrix .

The key material distribution is either random key material distribution, deterministic key material distribution and location based key material distribution.

III. PHYSICAL LAYER SECURITY

There are two approaches to security one is information –theoretic security and computational security.[17]

The fundamental metrics of secret systems (perfect, ideal, practical)are (1)amount of secrecy (2)Key length (3)complexity and message expansion systems at ciphering (4)error propagation after deciphering.

Information theoretic approach has two study components one is the secure communication and second is the secret key agreement. We shall deal the later part of it in this paper.

Physical layer secrecy studies considers either complete or partial or no knowledge of CSI at all.

A. Secret key agreement

The two ways of correlated observations in wireless communications are two way channel probing and one way transmissions.

In two way channel probing, the reciprocal nature of electromagnetic waves is considered. The physical layer measurements are the common source of information for both authorised users and can be used for common data. The eaves dropper correlation is a factor of distance from either authorised user to achieve correlation with the channel. This is the instantiation for source model. One way transmissions, the output of receiver and eaves dropper is output of classic Wiretap channel. Therefore channel model for key agreement requires either parties to set the channel randomness and key generation takes place at higher levels.

IV. WIRELESS CHANNEL CHARACTERISTICS FOR KEY GENERATION

The wireless characteristics are categorised based on their channel characteristics and their variations over various time, frequency and space domains. The channel measurements are usually done on the absolute values and their variations are like inherent or user–induced.

Some of the key generation methods are involving phase ,received signal strength, narrow band channel impulse response, multiple channels, relative node distance, angle of arrival, special equipment like reconfigurable antennas, jamming mechanisms, IR-UWB channel impulse response and so on.

A. Key generation models with wireless channel

1) Source model: Considers wireless channel as a random source. This model relies on the reciprocity and spatial decorrelation of the channel which gives legitimate users have special advantage over eaves dropper , they have correlated observations of common source i.e., wireless fading channel, while eavesdropper have lower chances of getting correlated observations located at a certain minimum distance of legitimate users.

2) Extended source model : It's a sender excited source model with optimised probing signals. With long channel coherence times, bidirectional entropy harvesting source model is not efficient. so one of the parties induces controlled channel variations during channel coherence, this approach is called virtual channel approach.

3) Wiretap channel model: Key agreement is implemented through classic wiretap coding strategies without public channel and with various levels of channel state information. But these are not optimal.In case of public channel availability, equiprobable dense parity codes can be employed to share key securely in binary symmetric wiretap channels.

4) Source-emulation channel model: Source generates discrete memory less source and send it over wireless channel to receiver to yield correlated observations. The secret key is obtained by information reconciliation and privacy amplification.
Fading is beneficial to secrecy capacity, practical secret sharing schemes when instantaneous CSI is available. It consists of one way transmission of random sequence during time slots when the secrecy capacity is positive , it is then followed by error correction by LDPC codes and privacy amplification with universal hash functions.

5) Mixed models: It is the mixed training and transmission key generation strategies with an initial phase of channel probing followed by a transmission phase . The secret keys are generated from both the phases. Both the cases indicate that when the channel coherence time is long, the contribution from source model is negligible and channel model should be used to achieve high key rates.

6) Reciprocity based channel model: Source model is highly dependent on coherence time hence not suitable for key generation for static channels. Alternatively, reciprocity or spatial decorrelation and user generated randomness have been used.

7) Alternate models: Information theoretic concept of mutual information with the notion of unknown deterministic parameters from detection and estimation theory perspective is used in the key generation.

V. RECENT RELATED WORKS IN THE SYMMETRIC KEY GENERATION

Recently there have been shift in the paradigm to give more emphasis on securely generating and sharing of the key in open wireless systems rather than building strong algorithms.

After extensive literature survey on key generation approaches, we have categorized those as ones which are based on channel characteristics , biometrics, Bluetooth , altering existing AES algorithm, elliptic curve cryptography.

A. Key generation based on channel characteristics

This is the most common and popular key generation techniques based on the channel state information which are known only to the correlated source and destinations.

Generally key generation from CSI involves the following steps: channel probing or random sharing , information reconciliation, privacy amplification .

a) Channel gain compliment assisted secret key extraction [1] this scheme is used to learn the non-reciprocity to lessen the bit mismatch rate of channel response measured at sender and receiver, in order to achieve a higher bit generation rate. The key concept is to reduce the non-reciprocity component by getting the channel response from a small amount of probe packets. This method collects a small number of channel responses from probe packets at first to learn the non-reciprocity component μf of the every sub carrier, and then use this μf to lessen the impact of non-reciprocity component to reach a low bit mismatch rate while keeping the bit generation rate high, using multilevel quantization method.

b) This secret key generation approach exploits the channel phase randomness and utilizes the uniformly distributed phase information of channel responses to extract under narrow band multipath fading models, to get cryptographic keys [2]. The key benefit of this method, due to its efficient introduction of multiple randomized phase information within a single coherence time interval as the keying sources, is the high key bit generation rate.

c) With the measured received signal strength indicator (RSSI), shared randomness is extracted. Different signal processing techniques are adapted in LoRa-Key to improve the key generation technique effectively. This method can achieve key establishment rates of 13bit/s in stationary and 21bit/s in mobile scenario[16]. Another scheme [3] proposes a practical method to generate secret keys while avoiding information reconciliation and privacy amplification. This scheme can generate 128 symmetric secret keys in a short time frame and also allows to secure the communication between the sensor devices and QOS is improved in WBANs.

d) In order to achieve desired reciprocity and codeword diversity ,[4] shows how the quantization thresholds can be adapted as a function of SNR and hence excess delay for UWB multipath signals. The cost metrics is defined and computed analytically using Gaussian mixture approximation for a IEEE802.15.4a channel model (CM1).
An observation is made for the metric behaviour of different uniform and non-uniform fixed quantization schemes. Finally, trivial and non-trivial points are found by optimization routines and it is shown that at certain SNR, the uniform quantization can approach weak pareto-optimal points.

e) Active insiders as attackers are considered in paper [5]. The basic concept of this method is to split the secret into a number of shares such that minimal number say x, is required to reconstruct the secret key. Confidentiality and availability is achieved in through this scheme against the erasing attackers.

f) The Loop-Back time division duplex transmissions(LB-TDD) scheme [6] can effectively reduce the CSI non-reciprocity due to its hardware interference and system synchronization effect. The advantage of this method is that it can effectively eliminate CSI non reciprocity for the generation of secret key.

B. Key generation using elliptic curve cryptography

Here the key generation is based on the properties of linear feedback shift register and cyclic elliptic curve over a finite prime field GF(p). [7]

The strength of the algorithm lies in the generation of random sequences using linear feedback shift registers over GF(p), difficulty of elliptic curve discrete logarithmic properties and entire key need not be transmitted in encryption process. This method was initially proposed for steam cipher for images. Main advantages of this scheme is that key space is sufficiently large to resist all brute force attack, statistical and correlation attacks. It is pertinent for real time multimedia applications.

C. Key generation using self organising maps(SOM)

It is based on the neural networks. SOM generates secret key by two ways ; a fake key and the key index. Applying the fake key to SOM and finding out the nearest neuron to that point leads to discover common true key.

This method generates a large number of keys which is the same number of neurons in the map. We showed that an SOM can converge to represent any surface immersed in $3\ \Re$. Then vectors associated with neurons could be used as keys. The two methods to co-opt a key in both sides of the communication channel; the fake key and the key index methods. Mask function allows the association of several neurons within the key computation. The mask enhances the security of the keys and allows the use of the same map with different mask function to exchange messages between several communicators.[8]

D. Key extraction using Bluetooth wireless signal strength measurements

Robust secret key extraction (RSKE) using Bluetooth that uses a very wide bandwidth (B >20 MHz) in conjunction with random frequency hopping over a set of narrow channels within B to avoid those frequencies that are heavily used. It shows that with this approach using Bluetooth, we can exchange packets and collect measurements for secret key extraction even under heavy WiFi traffic, an order of magnitude faster in comparison to using WiFi. Secret key generation using Bluetooth is comparable to that of WiFi while using much lower transmit power.[9]

E. Key extraction from images and Chinese remainder theorem

Images have more features than text like colour, edges, ridges etc. Hence these features facilitate us to generate many keys of variable length. To strengthen the security of key Chinese Remainder Theorem (CRT) is applied on the selected values from the selected image. Advantage of this method are keys of variable length suitable for any algorithm can be generated from featured image in a secure way by using Chinese Remainder Theorem. As the key used in symmetric encryption algorithm is image dependent, prediction of image and process of key generation for an attacker is impossible. Disadvantage: The concept has been limited to three numbers which can also be extended. Even the output of CRT can also be extended for more good results.[10]

F. Key generation based on biometrics

In the traditional KDC (key distribution center), a unique key is used between communicating parties for the purpose of distributing session keys. Reference [11] uses fingerprint biometrics of communicating parties for the purpose of unique key generation and distribute session key with the fingerprint based key of user. As the key is generated from fingerprint of user, there is no scope of attacks to break the unique key. In this way, the unique key is associated with biometric data of communicating party and the key is not required to remember by that party. This approach converts the knowledge based authentication to biometric based authentication of KDC. At the same time, this approach protects the privacy of fingerprint identity as the identity of user is not disclosed even when the KDC is compromised. Disadvantage: error which is the instance to instance variation of biometric is not handled properly to implement it without error.

The problem with biometrics is that once it gets compromised it cannot be reused. As a proficient solution for cancelling and reissuing biometric template cancelable biometrics has been proposed to generate 128 bit symmetric key from cancelable fingerprint templates of both communicating parties. The current approach confirms the privacy of fingerprints by one way transformation of original template into cancellable one as well as resolves the difficulty of key storage and key distribution as the key is not sent to the recipient and is also not saved anywhere.[12] Advantage: The privacy of fingerprint identity is also preserved using the concept of cancellable fingerprint template.

In reference [13], A biometric key using iris, which is the combination of the iris code and the pseudo random numbers as a key for VoIP Communication. This iris key act as a symmetric key for both encryption and decryption. Unfortunately if the iris biometric is stolen, this makes the attacker to access the data if the data encrypted with biometric key alone. To overcome this problem it uses pseudo random numbers, which is fused with iris biometric. Therefore billions of unique keys can be generated, making VoIP technology hard for an attacker to guess the key .

G. Enhancing the key generation of AES algorithm

In reference [14]Dynamic key is generated on AES algorithm using function of time. Key can be generated at random based on the value of the time when sender logs in to the system. On the decryption, synchronization activity takes time value with a certain tolerance limits to find the same key pair of the time value generated in the encryption process. It will protect message from Brute-force Attack, Differential Attack, Algebraic Attack and Linear Attack.

Reference [15] is a new method for AES key generation algorithm by using solved Sudoku problem. The user has to get a Sudoku problem from the server during registration and the problem has to be solved by the user in the initial stage itself. From the solved problem, user can get $32 \times 9 = 288$ bits size of key matrix. This key matrix is unique for each user and the same matrix will not be given to any other user by the server. The ciphering key or encryption key is taken from the key matrix and the index or row value is given to the receiver for decryption. Advantage is that the key pool generation time is very minimal compared to other techniques hence can be used in dynamic networks.

VI. CONCLUSION AND FUTURE WORK

The various symmetric secret key generation and management techniques were discussed with their relative advantages over the other. The drawbacks were also discussed which can be taken as a research area to work with.

REFERENCES:

[1] Hongbo Liu, Yang Wang, Jie Yang and Yingying Chen, "Fast and Practical Secret Key Extraction by Exploiting Channel Response," *Proceedings* IEEE INFOCOM, 2013.

[2] Qian Wang, Hai Su, Kui Ren, and Kwangjo Kim," Fast and Scalable Secret Key Generation Exploiting Channel Phase Randomness in Wireless Networks," IEEE INFOCOM, 2011.

[3] Ahmad Salehi S., M.A. Razzaque, Inmaculada Tomeo-Reyes, Nasir Hussain and Vahid Kavian, "Efficient High-Rate Key Management Technique for Wireless Body Area Networks ," *The 22nd Asia-Pacific Conference on Communications,* IEEE ,2016.

[4] Iulia Tunaru and Bernard Uguen," Reciprocity-Diversity Trade-off in Quantization for Secret Key Generation," *25th International Symposium on Personal, Indoor and Mobile Radio Communications,* IEEE, 2014.

[5] Stefan Pfennig, Sabrina Engelmann, Elke Franz and Anne Wolf, *Robust Secret Sharing for End-to-End Key Establishment with Physical Layer Keys under Active Attacks,* Proceedings of the 2nd Workshop on Communication Security, Lecture Notes in Electrical Engineering 44 ,Springer International Publishing AG M. Baldi et al. (eds.),vol 7, 2018.

[6] Linning Peng, Guyue Li, Aiqun Hu," Channel Reciprocity Improvement of Secret Key Generation with Loop-back Transmissions," *17th IEEE International Conference on Communication Technology, IEEE, 2017.*

[7] S. Maria Celestin Vigila and K. Muneeswaran, "Elliptic Curve based Key Generation for Symmetric Encryption ," *IEEE Proceedings of 2011 International Conference on Signal Processing, Communication, Computing and Networking Technologies,*IEEE*,2011.*

[8] Hasan Abdulkader and Daniel Roviras,"Generating Cryptography Keys Using Self Organizing Maps*,"* IEEE,2012.

[9] Sriram N. Premnath, Prarthana L. Gowda, Sneha K. Kasera , Neal Patwari and Robert Ricci, "Secret Key Extraction using Bluetooth Wireless Signal Strength Measurements," *Eleventh Annual IEEE International Conference on Sensing, Communication, and Networking (SECON),*IEEE*, 2014.*

[10] Kalyanapu Srinivas and Dr.V.Janaki, " Automatic Variable Length Key Generation from Images and CRT," *7th International Advance Computing Conference,* IEEE, 2017.

[11] Subhas Barman, Samiran Chattopadhyay and Debasis Samanta, "An Approach to Cryptographic Key Distribution Through Fingerprint Based Key Distribution Center ," *International Conference on Advances in Computing,Communications and Informatics (ICACCI),* IEEE, 2014.

[12] Arpita Sarkar and Binod Kr Singh , "Cancelable Biometric Based Key Generation for Symmetric Cryptography," *International Conference on Inventive Communication and Computational Technologies (ICICCT 2017),*IEEE,2017.

[13] S.Bhuvaneshwari and Dr.P.Arul," Secure Voice Over Internet Protocol(VoIP) Network with Biometric Key," *IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI-2017)*,IEEE,2017.

[14] Flevina Jonese D'souza and Dakshata Panchal ,"Advanced Encryption Standard (AES) Security Enhancement using Hybrid Approach," IEEE International Conference on Computing, Communication and Automation (ICCCA2017),IEEE,2017.

[15] Dr. B Indrani and Mrs. M. Karthigai Veni, " An Efficient Algorithm for Key Generation in Advance Encryption Standard using Sudoku Solving Method," IEEE International Conference on Inventive Systems and Control (ICISC-2017),IEEE,2017.

[16] Weitao Xu, Sanjay Jha and Wen Hu" Exploring the Feasibility of Physical Layer Key Generation for LoRaWAN," *17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering,*IEEE,2018.

Thesis:

[17] Iulia Tunaru, "Physical layer secret key generation for decentralized wireless networks," Signal and Image processing, Université Rennes1, Europe, 2015.

[18] Dr.P.N.Sudha," Speech compression and error correction for mobile communication," JNTU, anantapur, India, August-2012.