International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

# Establishing Secret Key in Wireless Environment by Using Techniques of Keyless Cryptosystem

**Fatima Joselyn Mystica[1], Gopalakrishnan Prakash[2]**

[1]PG Scholar, Information Technology, Sona College of Technology/Anna University Chennai, India

[2]Associate Professor, Information Technology, Sona College of Technology/Anna University Chennai, India

**Abstract:** ***Cryptography is the idea of protected communication. Security guaranteed by different crypto ways of encryption, decryption, secret key establishment, etc.One such way is Keyless Cryptosystem. This new technique of Cryptosystem uses the procedure where security is guaranteed by concealing the distinctiveness of the sender of the information by not using the usual crypto techniques. Keyless does not mean that there are no keys; it actually means the procedure of hiding the senders Identity by using the random secret key. The sender and receiver of the communication use a protocol that crafts a random key. These ambiguous keys do not allow the middle man to get an idea on the key imagining that the channel of communication is anonymous. This unidentified channel is ideal to hide the sender's identity, without affecting the actual message passed between the sender and the receiver. This is a leap over in the findings of cryptography.By using very limited or no Crypto techniques the security of communication between the dispatcher and recipient of message. Many Algorithms stand as a proof to the efficient working of this novel technique. A study of this is elaborated in this research paper. This technique is efficiently used in smart phones running on iOS, Android for assuring at most security***

**Keywords:** Trusted Third Party (TTP), Public Key Cryptosystem (PKC), Man in the Middle (MitM) attack, SHOT Protocol, Shave Method, Shack Method.

## 1. Introduction

Keyless Cryptosystem – a new technique of Cryptography that uses a different method to secure communications of the channel and Smartphone communications. Initially Public key Cryptosystem (PKC) was used to give security to the hand held devices which are resource constrained. When considering the parameter of Energy,PKC security measures consumes more energy as they use more crypto operations like encryption decryption with various algorithm with the aid of public, private keys. Thus Smartphone with PKC safety measures are not energy efficient, so a new technique was the need of the hour. As an alternative to the existing Cryptographic techniques Keyless Cryptography method used less Crypto procedures to secure the communications in the channel by securing the senders identity. A brief discussion is explained in this paper about this technique explain the various ways of effectively establishing the secret key using the explained methods.

## 2. Related Work

B. Alpern and F. B. Schneider[1] had proposed this innovative idea of securing exchange of data by not disturbing original message sent via unknown channel. To handle semi anonymous communication channel M. Young's Processing letter highlighted the idea. This keyless technique was mainly to reduce consumption of energy in devices where there were fewer devices like mobile phones. R. Mayrhofer, et al.[3] introduced the a novel protocol in their journal to use this technique efficiently in their smart mobile phone with the latest OS like iOS, Android so that energy is saved. J.Croft,et al [5] explanation on how this methodology is used for Wireless Sensors is given. M. Wilhelm, S. Jana [6,7] explains the different ways of extracting secret keys from the in entangled sensor motes and Real Environments respectively. Jon W. Wallace's [8] scheme on how to extract secret key based on the keyless scheme is briefed here.

## 3. Preliminary Keyless Proposal

### A. Key Exchange via Keyless Cryptosystem

Hiding only the sender in the anonymous channel is the main idea of Keyless cryptosystem. Bowen Alpern suggested this idea where he analyzed the issues of public key cryptosystem. In this method, communication between the two parties where the sender is using an encryption algorithm to safeguard his message and sending it through the communication channel to the receiver. This receiver will have to use a corresponding decryption algorithm to get the message from the sender. Public and Private keys are involved in this communication. Eaves dropper can hack the communication at any point if he gets an idea of either the algorithm used by the parties of any one of the keys. So the Keyless Cryptosystems took an edge over this. The main idea revolves around the point of hiding from where the message is coming from and not the actual message. So the middle man, even if he gets the message, It will be a dump to him as he does not know from where it coming from. so this idea with less crypto techniques excelled public key cryptosystem. This was just a proposed technique initially and various methods were given by the author for making this keyless cryptosystem idea to establish effectively

### B. Key Allocation Design on Anonymous Channel

Central key distribution facility, broadcast network and special communication channel. These Schemes acting on anonymous channel emphasis on the blackboard which acts as a TTP – trusted third party. This blackboard can be read by any user at any time. When a message is got it is posted on this black board and sender's identity is concealed from other parties. This happens via special communication channel protecting from the Wire tapper. This had many

disadvantage as A TTP had to be believed so this suggested technique couldn't be practically implemented

**C. Key Distribution Format On Semi- Anonymous Conduit**

M Young proposed this extension of the original scheme using the secured fixed key. Security in previous technique is assured from the anonymous channel. But it can't be always said that a communication channel is not known or distinct, if the same parties communicate then there are more chances from the attacker to trace the sender of the message which is a threat to the foundation of key less cryptosystem technique. So the author used a fixed key for Mutual authentication to overcome this problem. This is also a primitive technique, If there are large number of packets, the protocol is not secure to prevent an attack on it.

## 4. Notion of the Methods on Mobile Devices

**A. Mobile Devices Paired Securely**

Spontaneous mobile interactions are to provide pairing methods that are both intuitive and secure. Simultaneous shaking is proposed as a novel and easy-to-use mechanism for pairing of small mobile devices. This was proposed by Rene Mayhofer. He suggested the usage of Shave and Shack protocols these are two concrete method of which sensing and analysis of shaking movement is combined with cryptographic protocols for secure authentication. The former is based on is based on initial key exchange followed by exchange and comparison of sensor data for verification of key authenticity. The later is based on matching features extracted from the sensor data to construct a cryptographic key. These protocols are used in secured way of implementing keyless cryptosystem in mobile devices

**B. Paired by Shaking devices for Authentication**

Authentication by shaking as an approach to secure pairing that is designed to exploit joint movement of devices shared secret. In this section, we discuss the design of our approach, with respect to three principal considerations: the use of shaking to create a movement limited channel the use of accelerometers for embedded sensing of movement Shaking is an intuitive gesture. Humans are familiar with shaking as an or of physical interaction with objects that is very common, does not require learning, and is performed without cognitive demand; shaking is hence natural and easy-to-use as a user interaction technique Shaking motion is vigorous and distinctive. Shaking involves pronounced accelerations over a longer duration than alternative gestures that could be performed with two devices, such as bumping together. Shaking movements are variant. Shaking is a free-form gesture that naturally varies from one instance to another.

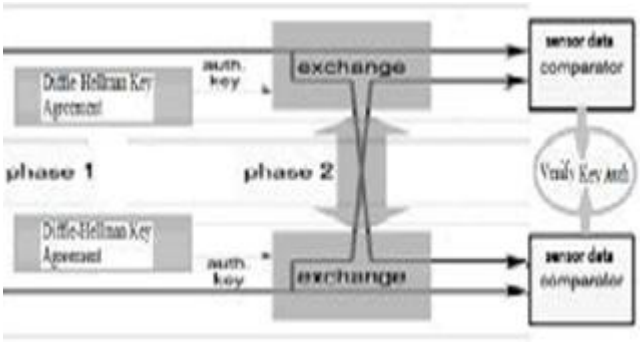


**Figure 1:** Shave Method

This figure denotes the accelerometer readings which is present in the mobile devices for key verification and agreement over the wireless channel. This establishes a wise method of exchange of key to get a verified secured key.

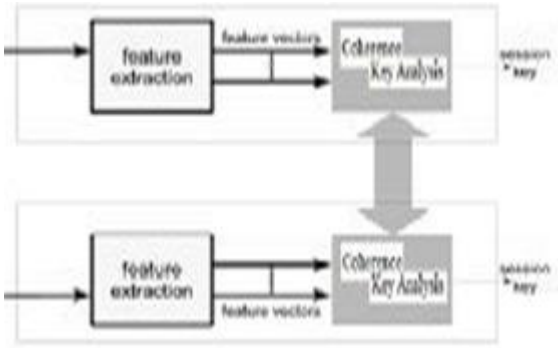


**Figure 2:** Shack Method

This is the continuation of the previous shave method where authenticity is very vital and that is ensured and pairing of the mobile devices is done efficiently.

## 5. Secret Key Establishment Via Channel Measurement

**A. Secret Key Extraction from sensor networks**

In the paper of J. Croft Robust Uncorrelated Bit Extraction method are used for wireless sensors. An adaptive robust uncorrelated bit extraction technique is used. It allows robust secret key extraction from radio channel measurements which suffer from real-world non-reciprocities and a priori unknown fading statistics. These procedures have low computational complexity, automatically adapt to differences in transmitter and receiver hardware, fading distribution and temporal correlations of the fading signal to produce secret keys with uncorrelated bits. Thus extraction of secret bits by using keyless technique in the sensor wireless nodes has become robust. The method produces secret key bits at a higher rate than previously reported, and is validated using extensive measurements

**B. Secret Key Extraction from entangled sensor motes**

Implementation and analysis of how Secret keys from entangled sensor motes was given by M. Wilhelm et al. Considers encoding RSS measurements to a secret key, but uses multiple frequency, in addition to multiple temporal, measurements, to achieve high entropy even with static transmitter and receiver. Thus the key to hide the sender's

identity is got from the entangled senor motes. This ensures at most security to the communication between the parties

**C. Secret Key Extraction from Real Environment**

S. Jana, S. P. Nandha, et al. explain about the Effectiveness of Secret Key Extraction Using Wireless Signal Strength in Real Environments. A measurement-based evaluation of RSS-based secret key extraction. Results show that (I) in certain environments, due to lack of variations in the wireless channel, the extracted bits have very low entropy making these bits unsuitable for a secret key, (ii) an adversary can cause predictable key generation in these static environments, and (iii) in dynamic scenarios where the two devices are mobile, and/or where there is a significant movement in the environment, high entropy bits are obtained fairly quickly. Presents an adaptive secret key generation scheme that uses an adaptive lossy quantizer in conjunction with Cascade-based information reconciliation and privacy amplification. Thus how effectively secret key is established from the dynamic environment as soon as possible on the effective way of hiding from whom the actual data content is coming from ; the author explains this idea briefly to extract random secret key from the surrounding. This real environment is prone to noise so extracting key effectively is a challenge.

## 6. Secret Key Generation Exploiting The Channel

**A. Key Generation – MIMO Channel**

Jon W. Wallace, Chan Chen, et al. presents mutual information 'secret bit' rate bounds from theory and theoretical channel models. Analyzes (using simulation) quantization schemes such as standard quantization, quantization with guard bands, and adaptive quantization and compares them to the bounds. Analyzes (using simulation) 'random pre-encryption', the transmission of the (obfuscated) secret key from one node to the other. Mutual data is given from both the sender and receiver. The establishment of the secret keys is the main emphasis of keyless cryptosystem method. To monitor this effectively quantization mechanisms are used and the author guards the way of using the adaptive methodology. The MIMO channel is made as a well prominent communication channel for rating the communication perfect to conceal the originator of message

**B. Key Generation scheme - Secure Physical Layer**

Michael A. Jensen suggested the techniques similar to the previous methodology Presents mutual information 'secret bit' rate bounds from theory and theoretical channel models. Analyzes (using simulation) two quantization schemes: standard quantization, and quantization with guard bands. Analyzes (using simulation) 'random pre-encryption', the transmission of the (obfuscated) secret key from one node to the other. Contains more details than [Wallace 2009a], but does not include adaptive quantization or random pre-encryption. This is the major difference from the previous technique and the present one. As Quantization is costly technique it cannot be adapted everywhere. Smart phones don't have facility to handle these highly powerful techniques so they can be avoided in physical layer and mutual authentication with random pre encryption used to increase security as suggested by the author. This encryption is not using the actual techniques but they involve only the before usage minor detailing of the above procedure.

**C. Random Secret Key from other channel Perspective**

Suhas Mathur's view on Radio-telepathy Extracting a Secret Key from an Unauthenticated Wireless Channel explains on extracting 1 secret bit per second using measurements from 802.11a packets. It uses the amplitude of the maximum peak of the CIR, recorded over time, as the channel measurement The communication channel is the connection between the sender and receiver of the message so by exploiting the channel parameters the random secret key can be got. size in bits of a shared secret based on a single reciprocal UWB channel measurement.

Sirin Nitinawarat, et al highlights on Secret key generation for correlated Gaussian sources an information theoretic paper considering the generation of shared bits from a correlated Gaussian random source. Uses nested lattice codes and vector quantization. Requires communication of the bits from one terminal to the other. Proofs show that the scheme achieves the mutual information limit as the rate of the quantizer goes high.

Tomoyuki Aono suggested key extraction from Multipath Fading Channels Proposes using statistics of the angle-of-arrival as a signature. Different beam patterns are used sequentially in this method, and RSS is measured for each beam pattern. Uses Chipcon CC2420 at both ends; an access point has a programmable phased array antenna. Uses block-code based syndrome to correct errors.

These are the various ways of extracting the secret key from the channel that is used in keyless cryptosystem technique for not reveling the sender's identity.

## 7. Results of Secret Key Establishment in Keyless

**Cryptosystem**

Mobile devices when they get paired they use these keyless cryptosystem techniques for assuring security measures. For authentication purpose this technique is best suited. Results of establishing a random secured key is explained by the above methodology like Secret Key Extraction from sensor networks, from entangled sensor motes and from Real Environment and Random Secret Key from other channel Perspective. This gives new dimensions of generation, establishing and usage of the secured key between the parties involved in the communication environment. These effective results are more appealing than PKC. The safety from the attacker is assured by using very less encryption and decryption methods.

**Recent Protocol In Keyless Cryptosystem**

As Key establishments of this keyless cryptosystem technique. Keyless technique does not hold the literal meaning of no secret keys instead it involves the methodology of generating and establishing secret keys by using the above techniques. Smart phones are more

concerned with energy conservation So the recent techniques of keyless cryptosystem are used to support at most security to communication BUMP protocol is used in iOS apple phones. This procedure is attacked by the eaves dropper to overcome it SHOT Protocol was introduced This procedure handled the interceptions introduced by the MitM. An advancement of this Protocol is COKE – Crypto-less Over-the-air Key Establishment Protocol. This technique is a suggested technique to be used in recent times The Proposed solution leverages no crypto but just plaintext message exchange. Indeed, the security of the solution relies on the difficulty for the adversary to correctly identify, for each one-bit transmission, the sender of that bit—not its value, which is indeed exchanged in clear text. Due to the low requirements of COKE (essentially, the capability to send a few wireless messages), it is particularly suited to resource constrained wireless devices (e.g. WNSs, wireless embedded systems), as well as for those scenarios where just energy saving is at premium, such as smart phones.

## 8. Conclusion

This research work creates an idea on Keyless Cryptosystem. A complete contrast from its name Keyless which confuse any one that no secret keys are involved in this cryptographic dimension but this technique uses only random secret key and less crypto primitives. The procedures of key extraction are explained by various above methodologies effectively. The main target is on the resource constrained devices these security measures are considerably successful. By enhancing various features of this technique by using puzzling methods we can resolve position guessing and Spoofing of adversary which is a major threat to Keyless Cryptosystem

## References

[1] B. Alpern and F. B. Schneider, in the Information processing Journal “Key exchange using keyless cryptography,” Tech. Rep., 1983.
[2] M. Young, “A secure and useful keyless cryptosystem,” *Information processing letter*, pp. 35–38, 1985.
[3] R. Mayrhofer and H. Gellersen, “Shake well before use: Intuitive and secure pairing of mobile devices,” *Mobile Computing, IEEE Transactionson*, vol. 8, no. 6, pp. 792–806, june 2009.
[4] Megan Hacker, Mark Crovella,Leonid Reyzin of Boston University “Secure Pairing of Mobile Devices”
[5] J. Croft,et.al paper on "Robust Uncorrelated Bit Extraction Methodologies for Wireless Sensors," in Proc. of the ACM/IEEE International Conference on Information Processing in Sensor Networks, 14 April, 2010.
[6] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, and S. V.Krishnamurthy, “On the Effectiveness of Secret Key Extraction fromWireless Signal Strength in Real Environments,” in *MOBICOM 2009*, 2009, pp. 321–332
[7] M. Wilhelm, I. Martinovic, and J.B. Schmitt, "Secret keys from entangled sensor motes: implementation and analysis 34 (2001), pp 1229-1245
[8] Jon W. Wallace, "Secure Physical Layer Key Generation Schemes: Performance and Information Theoretic Limits," in IEEE International Conference on Communications (ICC 2009), 14-18 June 2009, Dresden, Germany
[9] Jon W. Wallace, Chan Chen, and Michael A. Jensen. "Key Generation Exploiting MIMO Channel Evolution: Algorithms and Theoretical Limits," in 3rd European
[10] Conference on Antennas and Propagation (EuCAP 2009), 23 - 27 March 2009, Berlin, Germany
[11] Matthieu Bloch, João Barros, Miguel R. D. Rodrigues, and Steven W. McLaughlin, "Wireless Information-Theoretic Security," in IEEE Transactions on Information Theory, Vol. 54, No. 6, June 2008, pp. 2515-2534.
[12] Suhas Mathur, Wade Trappe, Narayan Mandayam, Chunxuan Ye, and Alex Reznik, "Radio-telepathy: Extracting a Secret Keyfrom an Unauthenticated Wireless Channel," to appear in ACM Mobicom 2008, Sept 2008
[13] Masoud Ghoreishi Madiseh, Michael L. McGuire, Stephen W. Neville, and Ali Asghar Beheshti Shirazi, "Secret Key Extraction in Ultra Wideband Channels for Unsynchronized Radios," in *Proc. of the 6th Annual Conference on Communication Networks and Services Research (CNSR2008)*, Halifax, Nova Scotia, Canada, May 5-8, 2008, pp. 88-95
[14] Akbar Sayeed and Adrian Perrig, "Secure wireless communications: Secret keys through multipath", in *IEEE ICASSP 2008*, March 31-April 3, 2008, pp. 3013-3016
[15] K.Zeng et.al proposed “ Exploiting multiple antenna diversity for shared secret key generation in wireless networks “ser. INFOCOM’10. Piscataway, NJ, USA: IEEE Press, 2010, pp. 1837-1845.
[16] Crypto-less Over-the-air Key Establishment In IEEE Transactions on Information Forensics and Security 8(1) 163-173 (2013) published by Roberto Di Pietro and Gabriele Oligeri.