iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 **Issue:** IV **Month of publication:** April 2016

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 4 Issue IV, April 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A Modern Approach of Quantum Cryptography for Wireless Network Security

Vrushali M Junghare[1], P. P. Pawade[2]
Department of CSE, P R PATIL College of Engineering & Technology, Amravati University

Abstract - "SECURITY" in these contemporary scenarios has become a more sensible issue for the "REAL WORLD" or in the "CYBER WORLD". Data that is transient over an unsecured wireless network is always susceptible to being intercepted by anyone within the range of the wireless signal, providing secure communication to keep the user's information and devices safety when connected wireless has become one of the huge concerns. Quantum cryptography provides a solution towards accurate security over the network by encoding information as photons, which can be sent through the air. This paper explores on the aspect of application of quantum cryptography in wireless networks. This paper explores the importance of quantum cryptography in wireless security networks.

In this paper, we present an approach for integrating quantum cryptography and security of IEEE 802.11 wireless networks for the distribution of encryption keys.

Keywords - Security, Cyber World, Quantum Cryptography, IEEE 802.11, Encryption etc

I. INTRODUCTION

Network security occurs with the problems of messages being captured and replayed. Network security is the effort to create a secure computing platform. This paper covers the ADVANCED technical combats that have been devised all through the way, thus giving birth to the notion of **"NETWORK -SECURITY".** Various antidotes that are in fact inextricable with security issues are – Cryptography, Authentication, Integrity and Non Repudiation, Key Distribution and certification, Access control by implementing Firewalls etc. [1]

To satiate the flaws in the network security more and more advanced security notions are being devised day by day. Our paper covers a wide perspective of such arenas where the contemporary cyber world is revolving around viz.

In order to make secure communications around a wireless network, communication between nodes (users) and base station (BS) to other nodes should be handled carefully by means of an efficient key management protocol. Quantum Key Distribution (QKD) using quantum cryptography is a new method in key distribution scheme, which allows broadcast of a network key with absolute confidentiality. This method of Quantum cryptography solves the issue related to network

Network security deals with problems of security which is related with the secrecy of data pattern which transmitted through air. security. It solves the problem of key distribution by the properties of quantum information and provides a secure communication network between two users with unconditional security [2]. This paper presents a methodology for key distribution in a wireless networks using quantum cryptography and its protocols. The paper also discusses the various other methods to keep wireless networks safe and secure. Classical cryptography can be divided roughly into four intertwined areas:

Secrecy, Authentication, Nonrepudation, and Integrity control.

A. Secrecy has to do with keeping information out of the hands of unauthorized users.
B. Authentication deals with whom you are talking to before revealing sensitive information or entering into a business deal.
C. Integrity control deals with long enterprises like banking, online networking.

These problems can be handled by using cryptography, which provides means and methods of converting data into unreadable from, so that valid User can access Information at the Destination.

II. CRYPTOGRAPHY

Cryptography is an approach to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the internet) So that it cannot be read by anyone expect the intended recipient. While cryptography is the science of securing data, cryptanalysts are also called attackers. Cryptology embraces both cryptography and cryptanalysis.

©IJRASET : All Rights are Reserved

Volume 4 Issue IV, April 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

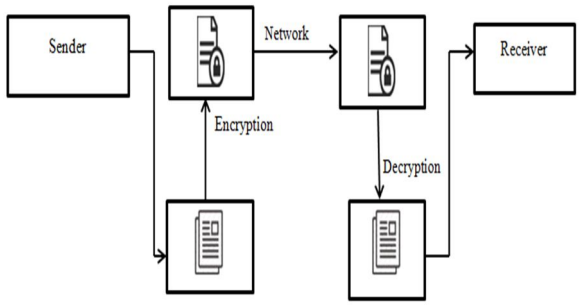


Fig. 1 Cryptography Structure

A. Key Process Techniques

There are three key process techniques. They are:

1) Symmetric-key encryption
2) Asymmetric-key encryption
3) Hash functions

1) Symmetric-key encryption (one key): There is only one key in this encryption. That is private key. This key is only used for both encryption and decryption. This is also called as private-key encryption. In this method the sender encrypt the data through private key and receiver decrypt that data through that key only.

2) Private Key method: Private Key method Asymmetric-key encryption (two keys):

There are two keys in this encryption. They are:

a) Public key
b) Private key

Two keys – a public key and a private key, which are mathematically related, are used in public-key encryption. To contrast it with symmetric-key encryption, public-key encryption is also sometimes called public-key encryption.

In public key can be passed openly between the parties or published in a public repository, but the related private key remains private. Data encrypted with the public key can be decrypted only using the private key. Data encrypted with the private key can be decrypted only using the public key. In the below figure, a sender has the receiver's public key and uses it to encrypt a message, but only the receiver has the related private key used to decrypt the message.

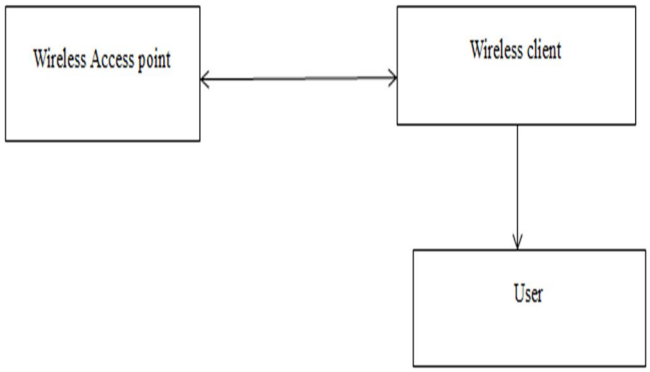


Fig. 2 Wireless Network Component

As long as a secure hash function is used, there is no way to take someone's signature from one documents and attach it to another, or to alter a signed message in any way. The slightest change in signed documents will cause the digital signature verification process to fail.

©IJRASET : All Rights are Reserved

III. ADVANCED CRYPTO TECHNIQUE

A. Quantum Cryptography

Quantum cryptography [7] is an evolving technology that provides safety and security for network communication by performing cryptographic tasks using quantum mechanical effects. Quantum Key Distribution (QKD) is a technique that is an application of quantum cryptography that has gained popularity recently since it overcomes the flaws of conventional cryptography QKD makes the secure distribution of the key among different parties possible by using properties of physics. The quantum states of photons are used and the security key information is transmitted via polarized photons that contain the message denoted by bits (0 or 1) and each photon contains one bit of quantum information called as Qubit. The sender sends the polarized photon to the receiver. At the receiver end, the user determines the photon polarization by passing it through a filter and checks for any modifications in the received bits of photons when compared to the bits measured by the receiver. Any modifications found would show that there has been an intrusion from a third party because the intrusion would irreversibly change the encoded data in the photon of either the sender or the receiver.

B. QKD?

Quantum Key Distribution (QKD) is a process that is an application of quantum cryptography that has gained popularity recently since it overcomes the flaws of conventional cryptography. QKD makes the secure distribution of the key among different parties possible by using properties of physics.

Heisenberg's uncertainty principle that states that the quantum state can't be measured without disturbing the state of either the sender or the receiver and hence introducing an anomaly in the quantum system that can be noticed by users as an intrusion.

C. BB84 QKD Protocol?

With respect to facilitate QKD many protocols exist such as: BB84 [8], B92, Six-State, SARG04 [9], Ekert91. Among these protocols, BB84 is the most popular and widely used protocol for key distribution in practical systems.

The protocol consists of two main channels used for transmission:

1) Quantum channel: One-Way communication.
2) Classical channel: Two-way communication.

IV. CRYPTOGRAPHIC ALGORITHMS

A. Based on layers

1) Link layer encryption
2) Network layer encryption
3) IPSEC, VPN, SKIP
4) Transport layer
5) SSL, PCT (private Communication Technology)
6) PEM (Privacy Enhanced Mail)
7) PGP (Pretty Good Privacy)
8) SHTTP

Cryptographic process can be designed at various at various layers starting from the link layer all the way up to the application layer. The most popular encryption scheme is SSL and it is implemented at the transport layer.

B. Based on algorithms:

Secret-key encryption algorithms (symmetric algorithms)

1) DES (Data Encryption Standard)
2) IDEA (International Data Encryption Algorithm)
3) Public-key encryption algorithms (Asymmetric algorithms)

V. PROTOCOLS IN WIRELESS NETWORK

There are wireless network protocols developed in order to provide privacy protection of the user data by encrypting the data being sent across the network. WLANs are defined under the IEEE 802.11 standard [3]. The security of a WLAN depends on the secrecy

©IJRASET : All Rights are Reserved

of the entire encrypting and decrypting process. Various algorithms are presently used for encrypting and decrypting without bargaining the security of the data being sent. The design and analysis of various mathematical techniques for encryption/decryption of data that ensure secure communications is termed as cryptography.

In today's era, everyone wants their necessary data to be handy, portable and accessible from almost every place they visit throughout the day and this is made possible by using wireless networks. Wireless networks [1], as the name suggests, are those networks that are not connected by any physical means such as Ethernet cables and thus provide the user with great mobility and convenience. Also, it saves one from the expenses on the cables that would be required if wired network is chosen as well as makes it easier for moving the base of the devices from location to another by just moving the machine along with the wireless network card.

VI. SECURITY ISSUES

Wireless networks do not promise quality of service during transmission and chances of intrusion into such networks are very high since the transmission here takes place through the medium of air and not cables. So, it doesn't only require protection against uninvited users from accessing the network but also needs to secure the users' private data that is being transmitted. The general security issues for wireless networks are as follows [2]:

A. Confidentiality

The data being sent across the network is encrypted during transit so as to ensure that the information is read only by the intended user and hence authentication of the receiver is required as well who will be given the key for the decryption of the received data.

B. Integrity

Wireless networks are exposed to attacks that would harm the data's integrity. The integrity prevention methods applied are similar to the ones used in wired networks.

VII. METHODOLOGY

A. IEEE 802.11WLANs

The main concept of this paper is to offer secure key distribution in wireless networks making use of Quantum Cryptography. In order to properly facilitate the functioning of QKD it is found that IEEE 802.11 family best suits to be integrated with QKD. In order to encourage efficient authentication and management of keys between access point and client, along with user traffic control 802.11 networks employs Extensible Authentication Protocol (EAP) [11]. EAP provides an authentication framework, which will be used in the current work. The security of 802.11 WLANs is based on the WEP protocol [10].

B. 4-WAY Handshaking

The 4-Way handshake performs the authentication process in IEEE 802.11 networks. The process allows the AP and the BS to generate the key hierarchy in order to provide encryption for secure communication. Since the keys are generated using a pseudorandom function, in order to further randomize data two random nonce values are transmitted between the AP and BS.

C. Proposed Protocol

For overcome the security issues of key distribution this paper employs SARG04 QKD protocol, which is an improved version of BB84 as discussed in Section 6. Fig. 11 shows the SARG04 QKD protocol being implemented in the proposed 4-way handshake protocol.

The steps involved in the proposed protocol are as follows:

©IJRASET : All Rights are Reserved

Volume 4 Issue IV, April 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

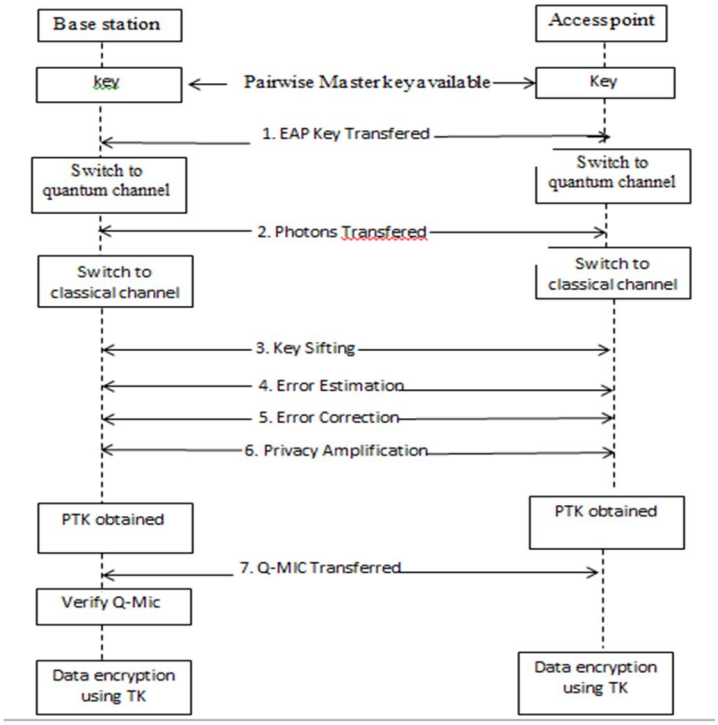


Fig.3 Proposed 4-Way handshake Protocol

1) Initially the PMK is shared between the BS and the AP. Then the transmission process is switched to the quantum channel.
2) BS sends all the polarized photon to the AP using bases at random. As soon as the transmission of photons is finished, the channel is switched to classical.
3) The next 3 stages of QKD are applied to remove all the error and obtain the final encryption key.

VIII. CONCLUSION

The main goal of this research work is to show a method to improve the security aspect of WLANs. It has been shown that the integration of Quantum Cryptography in Wireless Networks has great prospective in terms of better network security. Key management and distribution is difficult using classical cryptographic algorithms but the proposed approach provides a better solution for this problem. Research has shown that use of QKD to distribute network key raises the security and makes it harder for an eavesdropper to interrupt communication. With the proposed modification, this paper has achieved the main objective of improving security of WLANs. Everybody's business, and only with everyone's cooperation, intelligent policy, and consistent practices, will it be achievable.

Cryptography protects users by providing functionality for the encryption of data and authentication of other users. This technology lets the receiver of an electronic messages verify the sender, ensures that a message can be read only by the intended person, and assures the recipient that a message has not be altered in transmit. The Cryptography Attacking techniques like Cryptanalysis and Brute Force Attack. This paper provides information of Advance Cryptography Techniques.

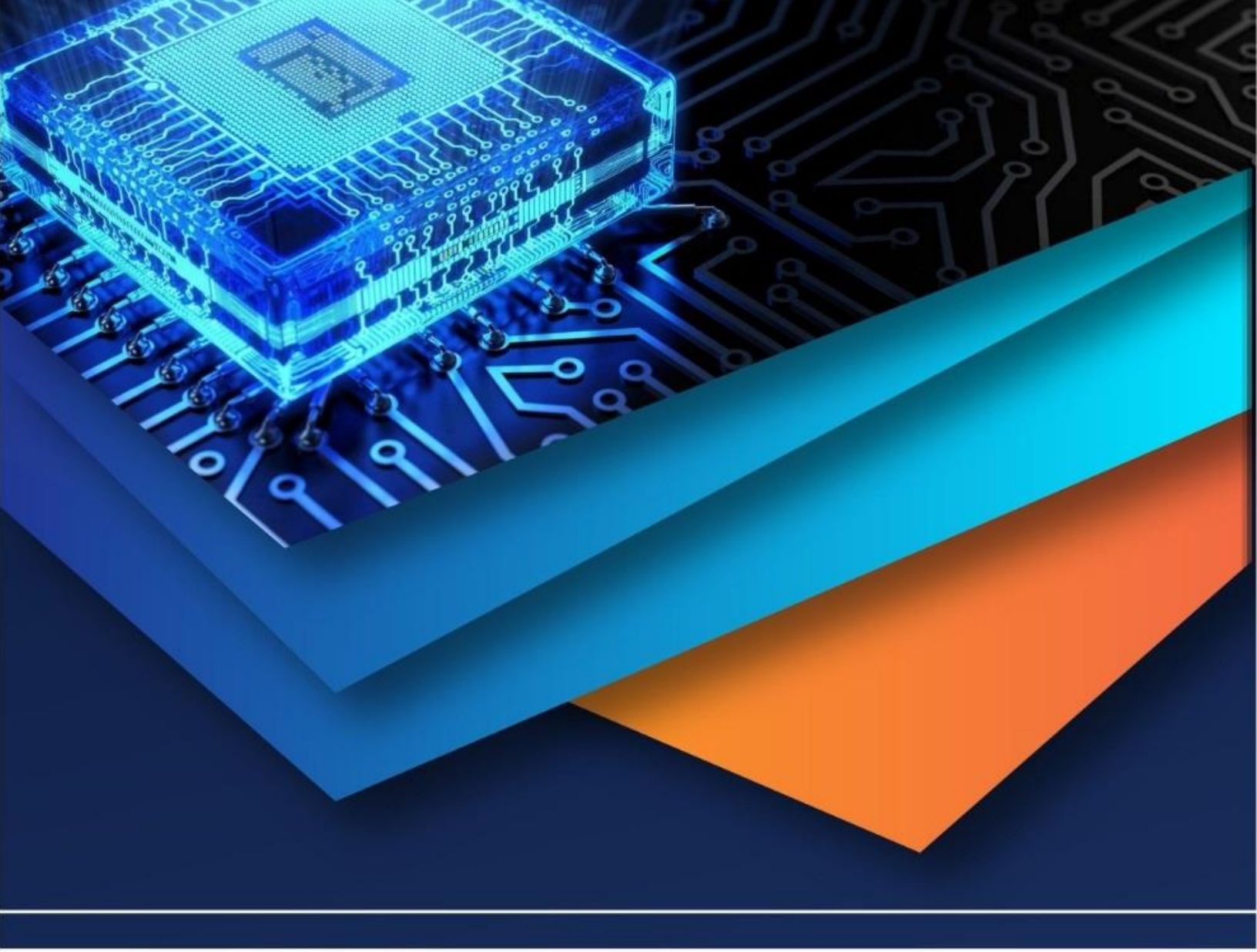
REFERENCES

[1] IEEE Standard for local and metropolitan area networks,"Wireless LAN Medium Access Control (MAC) and Physical Layer Specifications", ANSI/IEEE Std 802.11,1999 Edition (R2003).
[2] Shin, M.; Ma, J.; Mishra, A.; Arbaugh, W.A., "Wireless Network security and interworking", Proceedings of IEEE,Volume 94, Issue 2, pp 455 – 466, February 2006.
[3] Wang Shunman, TaoRan, WmgYue and ZhangJi,"Wireless LAN and its security problem". Proceedingsof the Fourth International Conference on Parallel andDistributed Computing, Applications and Technologies,2003. PDCAT'2003.
[4] Matthew S. Gast, 802.11 Wireless Networks, O'REILLY,2002.
[5] William Stallings, Cryptography and Network Security,Principles and Practices, 3rd Edition, Prentice Hall 2003.
[6] MatijaSorman, TomislavKovac and DamirMaurovic,"Implementing Improved WLAN security", 46th International Symposium Electronics in Marine.ELMAR-2004, Zadar. Croatia, 16-18 June 2004.

©IJRASET : All Rights are Reserved

[7] JoonS.Park and Derrick Dicoi, "WLAN Security:Current and Future". IEEE Computer Society, October2003.
[8] Nancy R. Mead and Gary McGraw."Wireless Security'sFuture". IEEE Computer Society, IEEE Security andPrivacy, August 2003.
[9] Joseph Williams, "Providing for Wireless LAN Security,Part 2". IEEE IT Pro, November | December 2002.
[10] J.-C. Chen, M.-C.Jiang, and Y.-W. Liu, "Wireless LAN Security and IEEE 802.11i", IEEE Wireless Commun., vol. 12, pp.27 -36 2005.
[11] Bernard Aboba, Larry J. Blunk, John R. Vollbrecht, James Carlson, and Henrik Levkowetz. Extensible Authentication Protocol (EAP). In- ternet RFC 3748, June 2004.
[12] R.LaluNaik, Dr.P.Chenna Reddy, U.Sathish Kumar, Dr.Y.V.Narayana, "Provely Secure Quantum Key distribution protocol in 802.11Wireless Networks", International Journal of Computer Science and Information Technologies, Vol. 2 (6), PP.2811-2815, 2011.

©IJRASET : All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)