International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-3 Issue-3, February 2014

802.11i Encryption Key Distribution Using Quantum Cryptography

Divya Ahir, Khayti Darbar, Ankur Dave

Abstract*—Quantum cryptography is an emerging technology in which two parties may simultaneously generate shared, secret cryptographic key material using the transmission of quantum states of light. Key distribution is the problem of classical cryptography algorithm, and tends to provide safe channel to transport key. Quantum cryptography could distribute key in quantum channel. Eavesdropper cannot access to key on quantum channel. Research on the application of quantum cryptography in mobile networks is still premature. In this paper, we analyze the interests of using quantum technique for the distribution of encryption keys in 802.11 wireless networks, and propose a scheme integrating quantum cryptography in 802.11i security mechanisms for the distribution of the encryption keys. The use of an apparatus network to provide alternative line-of-sight paths is also discussed.

Index Terms*— 802.11i, quantum cryptography, network security.

I. INTRODUCTION

The uncertainty principle in quantum mechanics created a new paradigm for cryptography: Quantum cryptography, or more specifically Quantum Key Distribution (QKD). Unlike the classical cryptography which relies on mathematical complexity, quantum cryptography is based on the laws of quantum physics. These laws ensure that nobody can measure a state of an arbitrary polarized photon carrying information without introducing disturbances which will be detected by legitimate users. As all eavesdropping can be detected, quantum cryptography is considered as a promising key distribution means towards long term unconditionally secure cryptosystems. Since the first QKD protocol proposed in 1984 with the name of BB84 [11], research on quantum cryptography gets significant advances. Experiments of different QKD systems have been realized in fiber networks and over free space [1-4]. Especially, a turnkey service using quantum cryptography to frequently generate fresh secret key has been commercialized in Switzerland [5].

While the use of quantum cryptography in fiber optical networks is successfully deployed in practice, the application of quantum cryptography in mobile wireless networks is still premature. Most research and experiments aim at providing QKD service outdoor for a long distance in satellite networks [6] or between buildings in a city. In these works, communication entities of the QKD protocol are mainly system devices but not final mobile users.

For instance, communication entities in satellite networks are ground stations and the satellite. Our motivation of integrating quantum cryptography in mobile wireless networks is quite different. We aim at providing mobile wireless user's terminals with QKD service. In a mobile environment, one technical challenge in addition to those of free space environment is the maintenance of a line-of-sight path between mobile user and the fixed part of the network when the user moves around.

As indicated in Table 1, GSM or cellular networks in general is a wide area network, used essentially outdoor to provide mobile users with telephone service. As voice call is the main application of GSM networks, the terminals are small size cell phones allowing mobile users to move with a high level of mobility. The speed of mobile users in a GSM network can be at step speed or vehicle speed. With this level of mobility and the outdoor environment, cellular network presents some disadvantages for the use of quantum cryptography. It will be difficult to provide a line-of-sight path with a high user mobility level. The outdoor environment is not ideal for free space quantum cryptography. Noise level can be raised because of rain or smoke. The large coverage area of the GSM network and the presence of natural obstacles such as trees or houses do not facilitate the provision of alternative line-of-sight paths.

Table .1. Comparison of mobile wireless networks

Mobile wireless network	User mobility Level	Coverage area	Terminals	Applications
GSM	High	Outdoor (order of kilometers)	cell phone	Voice calls
802.11	Low	Indoor (< 100m)	laptop, PDA	Internet, e-Commerce
Bluetooth	Low	Indoor (< 10 meters)	Peripheral Devices	Replacement of wires connecting devices in close proximity of each Other

Manuscript published on 28 February 2014.
***** Correspondence Author (s)
Divya S. Ahir* ,M.Tech CO Chotubhai Gopalbhai Patel Institute Of Technology,Uka Tarsadia University- Bardoli, Surat, Gujarat, India.
Khyati K. Darbar ,M.Tech CO Chotubhai Gopalbhai Patel Institute Of Technology,Uka Tarsadia University- Bardoli, Surat, Gujarat, India.
Ankur P. Dave ,M.Tech CO Chotubhai Gopalbhai Patel Institute Of Technology,Uka Tarsadia University- Bardoli,Surat, Gujarat, India.

In contrast to cellular networks, 802.11 networks [7] present many interests relating to the use of quantum cryptography. First, 802.11 is a wireless local area network, mainly used in offices and campus such as, class rooms, meeting rooms, universities, and halls in hotels or in airports. For the limited coverage area, 802.11 networks are mainly used indoor, reducing noise and natural obstacles caused by the outdoor environment This building-oriented environment also facilitates the deployment of a high density of quantum apparatus to provide alternative line-of-sight paths. Second, 802.11 terminals are mainly laptops or PDAs (Personal Digital Assistant) which have more computational capacity and more energy for the autonomy than cell phones in cellular networks. Quantum key distribution in mobile networks is a task requiring significant amount of computational resource and energy for the control protocol and the QKD protocol. In this paper, I am define the Quantum handshake, which will replace the 4-way handshake defined by 802.11i, in order to establish the TK (Temporal Key) and the KEK (Key Encryption Key) between the mobile terminal and the access point. The TK will be used by the encryption algorithms as fresh encryption keys. The organization of the paper is as follows. In section 2, we provide an overview on security mechanisms specified by the 802.11i standard. Section 3 familiarizes the readers with quantum cryptography. In section 4, we describe the Quantum handshake, a scheme integrating QKD with 802.11i. Finally, we conclude the paper in section 5

II. 802.11I SECURITY MECHANISMS

A. The failure of WEP and the arrival of 802.11i

The first standard of 802.11 security defines WEP [10] (Wired Equivalent Privacy) for the authentication and data confidentiality of user data over the wireless link. Unfortunately, WEP was not well designed and presents serious vulnerabilities as follows.

- WEP uses only one secret key for both authentication and encryption. This is not a good security strategy. If the encryption key is discovered, we also loose the authentication key. In this case, the authentication key cannot be used to authenticate the user and generate a new encryption key.
- WEP is based on the RC4 algorithm , a stream cipher which has a set of weak keys and becomes especially vulnerable if one part of the key is disclosed to attackers. In WEP, the RC4 key is the concatenation of an Initialization Vector (IV) of 24 bits which is sent in plain text together with the encrypted frame, and a WEP key of 40 bits. Attackers can collect IVs to detect weak keys. In addition, because IV is directly used as a part of the RC4 key, passive attacks can be easily realized to reveal the WEP key.
- The IV is not necessary to be secret but it should be used only once together with a given secret key. Unfortunately, WEP does not have any mechanism to avoid repeated IV during the use of a given secret key. In addition, with the bit rate of 11Mb/s of 802.11b, the space of IV is exhausted after about 8 hours. This fact requires a renewal of the secret key every 8 hours which is impossible in WEP because WEP does not define any mechanism to dynamically establish new secret key between mobile device and access point.

B. 802.11i authentication

Authentication is the first thing to do when a mobile terminal wants to join a network. In order to rectify the flaw of the WEP (Wired Equivalent Privacy) [10] based authentication mechanism specified in the 802.11 standard, 802.11i defines the 802.1X authentication [8] based on EAP (Extensible Authentication Protocol) [11]. EAP is a flexible protocol allowing the running of different authentication methods between the mobile terminal and the authentication server. Depending on the EAP method used, we can have a strong or weak, simple or mutual authentication. For instance, the EAP-TLS method [12] allows a mutual authentication while the EAP MD5-CHALLENGE method [13] only provides the authentication of mobile terminal. As shown in Figure 1, EAP messages can be carried by different protocols. They are transported by the 802.1X EAPOL (EAP over LAN) protocol between the mobile terminal and the access point. Between the access point and the authentication server, they can be carried by the EAP over RADIUS (Remote Authentication Dial-In User Service) protocol if the underlying communication protocol between the Authenticator and the authentication server is RADIUS. Typically, RADIUS runs over TCP/IP (Transport Control Protocol/Internet Protocol) which in turn runs over a link layer protocol such as IEEE 802.3.

C. Key management

802.11i uses many keys at different levels, constituting a key hierarchy. In this paper, we only present the Pair wise Key Hierarchy containing the keys related to the encryption of uncast traffic.

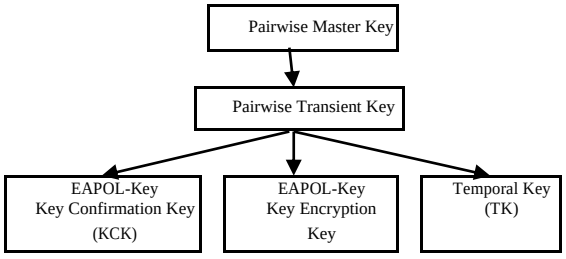

Fig.(1) Pairwise Key Hierarchy.

Figure 1 depicts this key hierarchy. At the top level, we have the master key called Pair wise Master Key (PMK) which is used to derive the other keys. There are two ways to establish the PMK, one based on the pre shared key, and one based on the authentication server. In the first method, a pre shared key which is used as the PMK is directly installed in the access point and in the mobile device by some means outside the 802.11i standard. No EAP-based authentication.

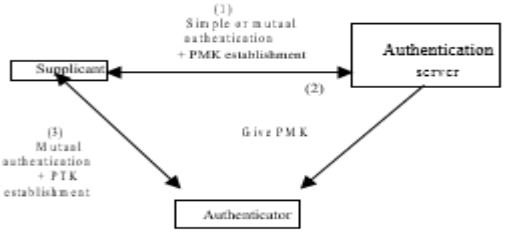

Fig. (2) Summary of authentication and key distribution in 802.11i

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Fig. (2) Summarizes the authentication and key management process in 802.11i. If the PMK is derived from a preshared key, only step (3) is needed. The authentication and the key establishment are strongly tied together. In step (1) the PMK is derived during the authentication between the Supplicant and the Authentication server. In step (2), the Authentication server supplies the Authenticator with the PMK. In step (3), the PTK and thus the remainder keys of the key hierarchy are derived during the 4-wayhandshake.

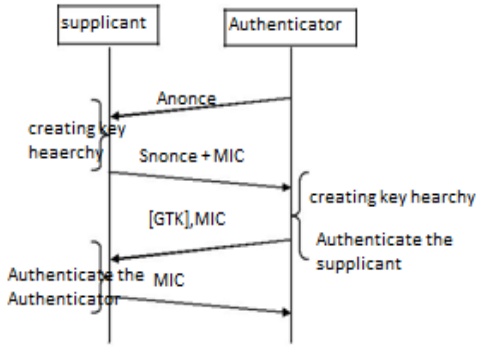

Fig. (3) The 4-way handshake

The 4-way handshake is started by the Authenticator by sending the value ANonce (Authenticator Nonce) to the Supplicant. Upon receiving the value ANonce, the Supplicant has all materials to build the key hierarchy. However, this hierarchy is not used until the Authenticator is authenticated and ready to use these keys.

C. Encryption Algorithms

The 802.11i standard specifies two encryption algorithms: TKIP (Temporal Key Integrity Protocol) and CCMP (Counter mode with CBC-MAC Protocol). CCMP is mandatory and TKIP is optional. TKIP is considered as a transient solution towards CCMP-based systems because TKIP is based on the RC4 algorithm and only requires a software upgrade on WEP-based systems. CCMP is based on AES (Advanced Encryption Standard) and requires hardware modification for the transition from WEP-based systems.

III.QUANTUM KEY DISTRIBUTION

A. A brief quantum cryptography presentation

Quantum cryptography aims at exploiting the laws of quantum physics in order to carry out a cryptographic task. As the use of quantum physics at cryptographic ends is limited, for the moment, mainly to the distribution of secret keys, we very often call the quantum distribution of key under the generic term of quantum cryptography. The quantum key distribution rests on a common function of the whole protocols, namely the combined use of a traditional channel and a quantum channel. The quantum nature of the data carrier ensures Alice and Bob that the information conveyed on the quantum channel could be spied only by taking measurements, and thus by introducing disturbances. This sensitivity of the quantum channel to espionage is based on various points: It is impossible to duplicate an arbitrary quantum state, like that was shown by W Zurek and W K Wootters in 1982. The second point is that the encoding of the quantum bits can be made sensitive to espionage since information is coded on at least two non-orthogonal states. Indeed, any measurement of a quantum object carried out in a base other than that of which it is state will have an effect on the measured object. For that the sender and receiver could obtain a real secret key, it is thus necessary to resort to some protocols, known as reconciliation and amplification of confidentiality protocols. The corresponding mathematical algorithms result from the traditional information theory and their application requires the use of a traditional channel of communication which can be listened freely by the spy. The quantum key distribution (QKD) is said “unconditionally secure”.

B. About QKD protocols

Up to now, there are several protocols being proposed since the birth of the first one BB84. BB84 was introduced by Benet and Brassard in 1984, thus it was named BB84 [12]. In 1994, this protocol was proved to be secure against eavesdropping by Dominic Meyers, Eli Biham, Michael Ben-Or. BB84 is a non-deterministic protocol, which means that it is useful for distribution of a random sequence only. BB84 is a four-state protocol. Other protocols are used especially the B92 (a two-state protocol), the three-state protocol and the six-state protocol.

C. BB84 operating mode

The operating mode of BB84 as published in 1984 in the International Conference on Computers, Systems and Signal Processing (in Bangalore, India), consists on two main steps [13]. The first step is the quantum transmission.

Quantum transmission.

In this phase, the information is encoded in non-orthogonal quantum states. This could be a single photon with a polarization direction of

0 (↔), π/4 (↗), π/2 (↕) or 3π/4 (↖). The sender and the receiver must agree first on the meaning of the photon polarizations for instance 0 or π/4 for a binary zero and π/2 or 3π/4 for a binary 1 (as announced in BB84). The sender (Alice) generates a random bit string and a random sequence of polarization bases then sends the receiver (Bob) photon by photon. Each photon represents a bit of the generated bit string polarized by the random basis for this bit position. When receiving photons, Bob selects the polarization filters (rectilinear or diagonal) to measure the polarization of the received photon (Figure 4).

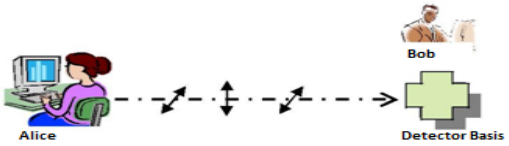

Fig. (4) Photon exchange

Public discussion.

After finishing the quantum transmission, Bob reports the bases that he picked for each received photon. Alice checks Bob bases and says which ones were correct. Bob and Alice take the bits resulting from these correct bases, these bits are only known by Alice and Bob. At this moment Alice and Bob share a secret bit string (Figure 3). This exchange is unconditionally secure if no active attacks are applied and the bases are perfect (if the photon polarization corresponds to the selected basis then Bob get the information else the photon is lost without any further information).

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

However, an additional step is used to estimate the error rate. In this step, Bob chooses a random sequence of validated bits and sends it back to Alice. Alice checks whether these bits are in conformity with those sent by Alice originally. If there is an attack on the quantum channel the error rate will be about 25% (or higher than). In this case, Alice and Bob detect the eavesdropper. Else (the error rate is less than 25 percent), the two parties discard the revealed bits and take the resulting stream as the secret key. The secrecy of this final stream is unconditional.

C. Some Quantum Key Distribution techniques

Based on the BB84 protocol, multiple techniques have been developed enabling quantum cryptography. We will in particular mention four techniques:

Auto compensating weak laser pulse systems: This technique has been extensively studied and is used in commercially available products. Its particularity is that it is invariant to the polarization rotation of the photon induced by the use of fiber optic.

Entangled photons: Two photons are generated which state is conjointly defined. One is sent to Alice, the other to Bob. Each personthe measures the photons' polarization.

Continuous Variable: In this technique the information is not based on the photons' polarization but coded on the phase or amplitude of the light pulses.

Free Space: This technique describes the quantum transmission through free space, e.g. in the earth atmosphere or the space without any physical support.

IV. INTEGRATING QDK AND 802.11I

A. Quantum handshake

When considering Figure 3 presented in section 2, we can see that the authentication and key management in 802.11i can be split into two parts. The first part including the step (1) and (2) results in the PMK available in the mobile station and in the access point. The second part including only step (3) results in two keys (the KCK and KEK) used by the 4-way handshake and one key (the TK) used for the encryption of user data. In order to integrate Quantum key distribution in 802.11i, we modify the 4-way handshake to integrate the BB84 protocol as presented in Figure 7, and call it the Quantum handshake. . As the purpose of this paper does not concern the authentication aspect, the derivation and the use of the KCK will remain unchanged. The BB84 protocol will be used to establish the KEK and the TK.

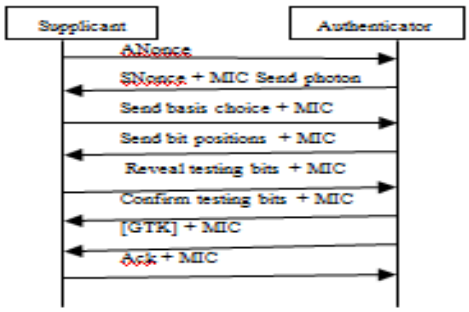

Fig. (6) Quantum handshake.

As illustrated in Figure 6, the BB84 protocol is inserted into the 4-way handshake after the second message. The two first messages of the 4-way handshake, which are reused by the Quantum handshake, allow the Supplicant and the Authenticator to derive a fresh KCK before starting the BB84 protocol.

In the 4-way handshake, the Supplicant and the Authenticator use a Pseudo-Random Function (PRF) to derive the PTK of 384 bits (for CCMP) or 512 bits (for TKIP) from the PMK. The PTK is then split into a KEK of 128 bits, a KCK of 128 bits, and a TK of 128 bits (for CCMP) or 256 bits (for TKIP). In the Quantum handshake, the PRF function is only used to produce the KCK which serves the mutual authentication between the Supplicant and the Authenticator. The keys serving the encryption, KEK and TK (the TK is our main objective, but we profit the QKD process to establish also the KEK), will be constructed by the BB84 protocol.

As described in Figure 7, the BB84 protocol results in a Q-PTK of 256 bits or 384 bits which then splits into a KEK of 128 bits and a TK of 128 bits (for AES) or 256 bits (for TKIP). The ANonce and SNonce exchanged in the first two messages only used to construct the KCK which helps the Authenticator and the Supplicant to authenticate each other and to provide the integrity (via the MIC calculation and verification) of the messages exchanged in the BB84 protocol. It is worth stressing that the Quantum handshake proposed in this paper only integrates the BB84 mechanism presented in which assumes a perfect quantum medium. If the quantum medium is noisy, it is necessary to add a step of key reconciliation and a step of privacy amplification before the two last messages.

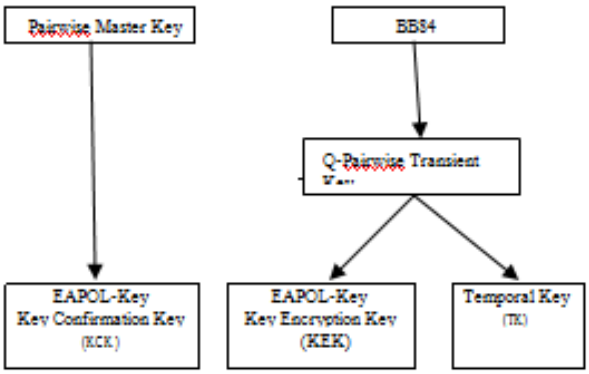

Fig. (7) Pairwise Key Hierarchy construction in the Quantum handshake.

V. OPEN ISSUES AND FUTURE WORKS

The Quantum handshake is our first tentative to integrate quantum key distribution in 802.11 wireless network. This integration is designed with the intention of keeping minimal changes for 802.11i. The BB84 information in the public discussion phase can be easily carried by EAPOL-Key frames. The authentication methods, i.e. the 802.1X authentication and the MIC in the Quantum handshake, remain unchanged in comparison with 802.11i.

In fact, the use of EAP and an authentication server in 802.1X authentication allows flexibility in the deployment of the system. Various authentication methods can be used. Client authentication and authorization information does not need to be distributed to every access points. In the next step, we can consider how to support an unconditionally secure for 802.11 and how this support impacts this flexibility.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

The use of an unconditionally secure encryption algorithm in 802.11 is also a future work towards a long-term absolutely secure cryptosystem.

From the quantum transmission point of view, the line-of-sight can be an open issue. In a mobile network, the quantum receiver's apparatus should be turnable. That means the receiver's apparatus can flexibly adjust the direction to keep a line-of-sight with a fixed point (the quantum transmitter's apparatus) in a hall or in a room. A protocol communicating between the mobile terminal and the fixed part of the network is necessary to control the direction of the receiver's apparatus. To facilitate the fact of having a line-of-sight path, transmitter apparatus can be implemented with a sufficient density. The control protocol will help the receiver apparatus to choose the most convenient transmitter for providing a line-of-sight.

From the implementation point of view, a specification of detail parameters such as the number of photons necessary to be transmitted should be done. The choice of reconciliation protocol and privacy amplification method taking into account the impact of wireless networks is also a future work.

VI. CONCLUSION

In this paper, we propose a scheme integrating quantum key distribution in 802.11 networks. A modified version of the 4-way handshake, the Quantum handshake, is defined to integrate the BB84 protocol for the distribution of the cryptographic keys used by 802.11i. The quantum handshake is our first step in the integration of quantum cryptography in mobile wireless networks. Open issues and future works have been discussed. When the research on the application of quantum cryptography in mobile wireless networks is still very premature, we hope that the work presented in this paper can contribute to the evolution of this research field.

REFERENCES

[1] N. Namekata, S. Mori, and S. Inoue, "Quantum key distribution over an installed multimode optical fiber local area network", *Optical Express*, 2005.
[2] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, "Quantum key distribution over 67 km with a plug and play system," *New Journal of Physics*, Vol. 4, 2002, pp. 41.1–41.8.
[3] H. Kosaka, A. Tomita, Y. Nambu, T. Kimura, and K. Nakamura, "Single-photon interference experiment over 100 km for quantum cryptography system using a balanced gated-mode photon detector", *Electronics Letters*, Vol. 39, 2003, pp. 1199–1200.
[4] C. Kurtsiefer, P. Zardaa, M. Halder, P.M. Gorman, P.R. Tapster, J.G. Rarity and H. Weinfurter. "Long Distance Free Space Quantum Cryptography", 2003.
[5] http://www.idquantique.com
[6] M. Aspelmeyer, T. Jennewein, and A. Zeilinger, "Long-distance quantum communication with entangled photons using satellites", *IEEE Journal of Selected Topics in Quantum Electronics*, Vol. 9, Issue 6, November 2003.
[7] ANSI/IEEE Standard 802.11, *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, 1999 Edition, Reaffirmed June 2003.
[8] IEEE Standard 802.11i, *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications - Amendment 6: Medium Access Control (MAC) Security Enhancements*, July 2004.
[9] K. G. Paterson, F. Piper, and R. Schack, "Why quantum cryptography ?", *Quantum physics*, quant-ph/0406147, June 2004.
[10] J. Edney, and W..A. Arbaugh, *Real 802.11 Security - Wi-Fi Protected Access and 802.11i*, Addison-Wesley, 2004.
[11] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, "Extensible Authentication Protocol (EAP)", *RFC 3748*, June 2004.
[12] B. Aboba, D. Simon, "PPP EAP TLS Authentication Protocol", *RFC 2716*, October 1999.
[13] R. Rivest, "The MD5 Message-Digest Algorithm", *RFC 1321*, April 1992.

Divya S. Ahir B.E. Computer Science Engineering , Bhagwan Mahavir College Of Engineering and Technology - Surat ,India ; ,M.Tech CO Chotubhai Gopalbhai Patel Institute Of Technology,Uka Tarsadia University- Bardoli,Surat,Gujarat,India.

Khyati K. Darbar B.E. Computer Science Engineering , Bhagwan Mahavir College Of Engineering and Technology - Surat ,India ; ,M.Tech CO Chotubhai Gopalbhai Patel Institute Of Technology,Uka Tarsadia University- Bardoli,Surat,Gujarat,India.

Ankur P. Dave B.E. IT , Salkalchand Patel College Of Engineering - Visnagar ,Mehasana,Gujarat,India ; ,M.Tech CO Chotubhai Gopalbhai Patel Institute Of Technology,Uka Tarsadia University- Bardoli,Surat,Gujarat,India.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)