ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 5, Issue 3, March 2016**

# A Survey on Light Weight Authenticated Tweakey Framework for Body Area Network Security

R.Sujatha[1], M.Ramakrishnan[2]

Assistant Professor, Dept. of ECE, Velammal Engineering College, India[1]

Professor, School of IT, Madurai Kamaraj University, Madurai. India[2]

**ABSTRACT**: Advances in wireless communication technologies and sensors have empowered development of Wireless Body Area Network (WBAN). The wireless nature of network and variety of sensors offer numerous new, practical and Innovative applications to improve health monitoring and other health care applications system. In the past few years, many researches focused on building system architecture of health monitoring to improve the technical requirements of WBAN. However, WBAN faces various security issues such as loss of data, authentication and access control. Securing the transmission from wireless body sensor to the administrator means not only ensuring safe data delivery to administrator but also to preserve the privacy of transmitted data. Existing solution for WBAN provides any security feature by compromising the cost. In this paper, we present light weight encryption framework for WBAN and provide an additional third key to enhance the security for the data being transferred. We propose the TWEAKEY framework with a goal to unify the design of tweakable block ciphers. Our framework is simple, extends the key-alternating construction, and allows to build a primitive with arbitrary tweak and key sizes.

**KEYWORDS:** Wireless Body Area Network, Authenticated Encryption, Lightweight Cryptography , Data Integrity ,TWEAK Key

## I.INTRODUCTION

Wireless Body Area Network (WBAN) is a wireless network used for communication among sensor nodes operating in or around the human body in order to monitor vital body parameters and movements pertaining to the human health conditions. These monitored signals are gathered by a personal device, e.g. a PDA or smart phone which acts as a sink for data in the sensor nodes and transmits them to healthcare professional for health monitoring. There are various issues pointed out in implementation of WBAN technology particularly in the area of security. This study conducted a holistic review on previous researches that emphasis in security related issues in WBAN. Block ciphers ensure data encryption and/or authenticity. The security of the block ciphers, both Feistel and Substitution Permutation networks, has been well studied when the key is fixed, however, when the attacker is allowed to ask for encryption or decryption with different (and related) keys the situation becomes more complicated. In the past, many proposed ciphers have been broken in related-key model [5, 6] and it has demonstrated that the Advanced Encryption Standard (AES) has flaws in this model [7, 8].
in a minimum level. This eventually enables CR-Networks nodes to determine optimum path nodes and channels for an efficient communication in CR-Networks. The CR technology allows Secondary Users (SUs) to seek and utilize “spectrum holes” in a time and location-varying radio environment without causing harmful interference to Primary Users (PUs). This opportunistic use of the spectrum leads to new challenges to the varying available spectrum. Using a Trust-Worthy algorithm, it improves the trustworthiness of the Spectrum sensing in CR-Networks.

## II. TWEAKEY FRAMEWORK

We bring together key schedule design and tweak input handling for block ciphers in a common framework that we call TWEAKEY (9).However, handling the key and the tweak material in the same way would be attractive in terms of performance, implementation, but more important is , it will simplify the security analysis, which is currently the main difficulty of the designers while constructing an ad-hoc tweakable block cipher. TWEAKEY construction framework allows to add a tweak of any length to a key-alternating block cipher and/or to extend the key space of the block cipher to any size(10). TWEAKEY framework offers more flexibility with regards to tweak and/or key sizes. TWEAKEY

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

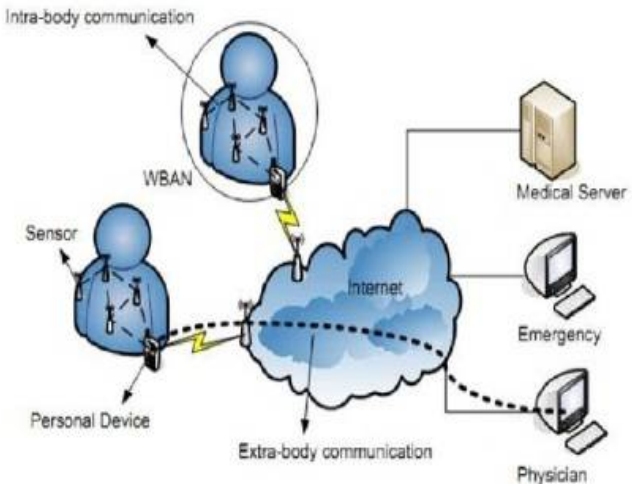
*(An ISO 3297: 2007 Certified Organization)*

**Vol. 5, Issue 3, March 2016**

leads to secure ciphers. For a tweakable block cipher the distinction between the tweak input and the key input is clear: the former is public and can be fully controlled by the attacker, while the later is secret. Tweak input must be handled more carefully than the key input, since the attacker is given more power. Tweak input should not use more computations than the key input.

## III. CHARACTERISTICS OF WBAN

Basically, WBAN is a communication network between the humans and Ad-hoc Network. A typical sensor node in WBAN should ensure the accurate sensing of the signal from the body and carry out low-level processing of the sensed signal ,wirelessly transmit the processed signal to a local processing unit(11) . However, because of the typical properties of a WBAN, current protocols designed for these networks are not always well suited to support a WBAN.




## IV. CHALLENGES IN WBAN

Body Sensor Network (BSN) is a suitable combination of wearable tiny devices attached to patient's body or implanted in patient's body. Their purpose is to monitor patient's physiological data (or BSN data) values. Sensors continuously monitor and collect patient's data and send it to a remote server through a network. This server can be called Database Server (DBS). DBS collect and stores the received patient's medical data which can be later used for any medical emergency by the Healthcare provider. This patient's data may be used to educate medical students, to provide data for medical research and analysis. Since the patient's physiological data are highly sensitive and fragile, BAN is very susceptible to attacks(12). Hence, it must be given a lot of care that patient identity will not be exposed or altered by unauthorized users. Hence, privacy of patient's data over the network becomes the most important aspect. So communication between BAN and DBS has to be secure(13). A strong security mechanism should be applied to maintain patient's privacy and confidentiality. Some paper proposes information security of physiological data which flow through network which is highly susceptible to attack and unauthorized access(14,15). The existing papers focus on patient's data transmission along with key causing it heavy weighted. The existing system transmits the encrypted patient's sensed data with key using HMAC authentication, Elliptic curve cryptography, etc. to all the nodes to reach the hospital administrator. This makes the packets transmitted heavy weighted. Also this gives the unauthorized user an opportunity to alter the data and make it unavailable to the hospital administrator for monitoring.

## V. PROPOSED SYSTEM

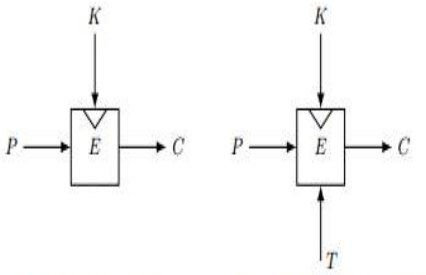
In this paper, we focus on two objectives. First we need to transmit patient's sensed sensitive data with more security preserving privacy. Second, we introduce the concept of data freshness. By considering these two objectives, the entire transmission is made light weighted.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 5, Issue 3, March 2016**




(a) Regular Block Cipher. (b) Tweakable Block Cipher.

**Figure 2:** Types of ciphers

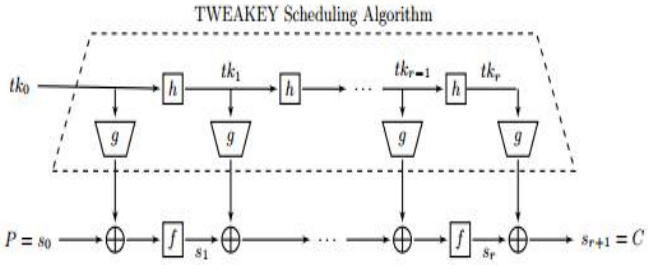



**Figure 3:** The TWEAKEY framework.

The security is provided by encrypting the key using TWEAK encryption.It is an addition of third key called TWEAKEY along with key and data for encryption.

The TWEAKEY construction framework that allows to add a tweak of any length to a key and/or to extend the key space of the block cipher to any size. In some sense, one can view the TWEAKEY framework as a simple generalization of key-alternating ciphers, offering more flexibility with regards to tweak and/or key sizes. The concept of tweakable block ciphers goes back to the Hasty Pudding cipher [14], and has later been formalized by Liskov, Rivest and Wagner in [15], where they suggest to move the randomization of symmetric primitives brought by the high-level operations of the modes directly at the block-cipher level. The signature of standard block ciphers can be described as E : {0, 1} k×{0, 1} n → {0, 1} n where an n-bit plaintext P is transformed into an n-bit ciphertext C = E(K, M) using a k-bit key K. On top on these inputs, tweakable block ciphers introduce an additional t-bit parameter T called tweak ( Figure 2). The signature for a tweakable block cipher therefore becomes

P : {0, 1} k × {0, 1} t × {0, 1} n → {0, 1} n ,

Cphertext C = E(K, T, P)

where the tweak T does not need to be secret and thus can be placed in the public domain. Similarly to a regular block cipher where E(K, ·) is a permutation for all K * {0, 1} k , a tweakable block cipher preserves this behavior as E(K, T, ·) is a permutation for all (K, T) * {0, 1} k × {0, 1} t .

Usually, the security notion expected from a tweakable block cipher is indistinguishable from a tweakable random permutation (a family of independent random permutations parameterized by T). It is important to note that the security model considers that the attacker has full control over both the message and the tweak inputs.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 5, Issue 3, March 2016**

The TWEAKEY construction is a framework to build a n-bit tweakable block cipher with t-bit tweak and k-bit key. It consists of two states: the n-bit internal state s and the (t + k) bit tweakey state tk, si and tki are the round values. The state s0 is initialized with the plaintext P (or ciphertext C for decryption), and tk0 is initialized with the tweak and key material. Then, the cipher is composed of r successive rounds each composed of three steps: (i) a subtweakey extraction function g from the tweakey state (ii) incorporation of this subtweakey to the internal state (for ease of description, we consider that the subtweakey incorporation is done with a simple XOR, but this can be trivially extended to other operations.

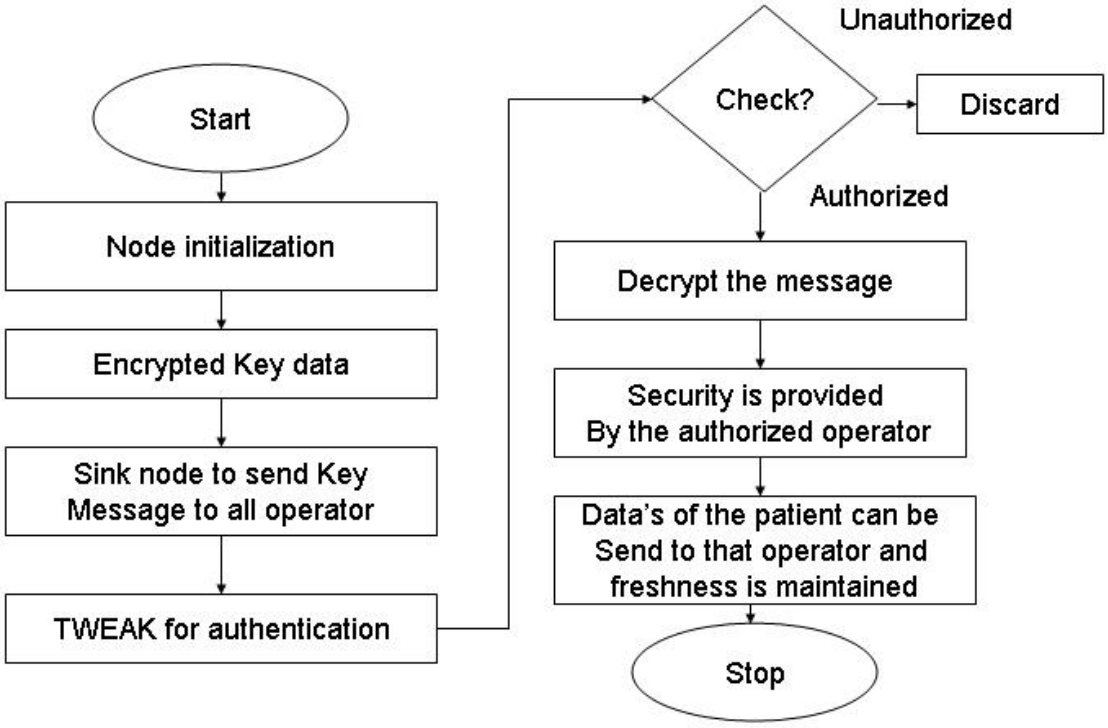



Figure 4:Flow chart

(iii)an internal state permutation f, a tweakey state update function h.

This can be summarized as: si+1 = f(si * g(tki)) followed by tki+1 = h(tki). At the end, the last sub tweakey is incorporated to the last internal state . sr * g(tkr) represents the ciphertext C . The subtweakeys are usually of size n bits, but they might be smaller. The framework is depicted in Figure 3. Increasing the amount of tweak or key material obviously renders the task of the designer much more complex in terms of security analysis. To overcome these situations, we denote TK-p , a class of tweakable block ciphers. For example, a simple single-key cipher would fit in TK-1, while an n-bit key, n-bit tweak block cipher (or for a double-key cipher with no tweak input) would fit in TK-2. By extension, a public permutation would fit in TK-0. The tweakey material can be any of length with respect to the key and/or tweak. It is up to the designer to ensure picking a proper TWEAKEY instance. The functions f, g and h must be chosen along with the number of rounds r such that no known attack can apply on the resulting primitives. More precisely, this must be true for any choice of the tweak/key size tradeoff inside the tweakey input. A natural way to achieve this while keeping the same f, g and h would be, to set the number of rounds as the maximal number of required rounds over all the possible tweak/key size tradeoffs.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 5, Issue 3, March 2016**

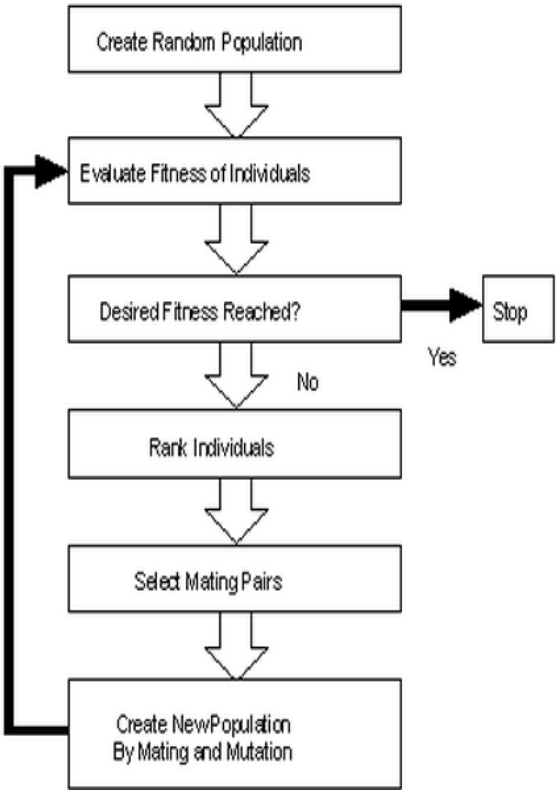



Figure 5: Tweak block diagram

Moreover, the key schedule is often used to break inherent symmetries from the internal state update function and to break round similarities (for example in the case of AES), hence this has to be taken in account as well.

## VI.CONCLUSION

The physical parameters that are sensed by the sensor nodes in or on the human body are transmitted to the sink along with key. The patient's data is encrypted by using TWEAKEY method. The encrypted key is broadcasted to the nodes nearby, to reach the destination or hospital administrator. The hospital administrator decrypts the key and sends acknowledgement to the sink to get access to the data. Later the data is sent to authorized person. Thus the proposed Tweaky framework suits well for the resource constrained devices.

## REFERENCES

[1] Abbas Ali Rezaee, Amir Hossein and Mohajerzadeh , "HOCA: Healthcare Aware Optimized Congestion Avoidance and control protocol for wireless sensor networks", ELSEVIER Journal on Network and Computer Applications,2013..

[2] Shahnaz S., Ullahemail S., Kwakemail K.S., A Study of IEEE 802.15.4 Security Framework for Wireless Body Area Networks, *Sensors*, 2011,11(2), 1383-1395; doi:10.3390/s110201383.

[3] Daojing He, Hun Chen, Sammy Chan, Jiajun Bu, and Athanasios V.Vasilakos, "A Distributed Trust Evaluation Model and Its Application Scenarios for Medical Sensor Networks", IEEE transactions on information theory in biomedicine, Vol.16, No.6.,2012.

[4] Devendra Gurjar, Md. Iftekhar Alam, Prof B Tiwari, Prof G N Pandey, "Wireless Sensor Network: an emerging entrant in Healthcare", IOSR Journal of Computer Engineering, ISSN: 2278-0661 Vol. 4, Issue 4, pp. 43-48,2012.

[5] Enan A. Khalil, Bara'a A.Attea, "Energy-aware evolutionary routing protocol for dynamic clustering of wireless sensor networks" ELSEVIER Journal on Swarm and Evolutionary Computation, pp. 195-203,2011.

[6] Francesco chiti, Member, IEEE, Romano Fantacci, Fellow, IEEE, Francesco Archetti, Enza Messina, and Daniele Toscani, "An Integrated Communications Framework for Context Aware Continuous Monitoring with Body Sensor Networks" , IEEE journal on selected areas in communication, vol. 27,No. 4,2009.

[7] Hande Alemdar, Cem Erosy, "Wireless sensor networks for healthcare: A survey", ELSEVIER Journal on Computer Networks, Vol.54, pp. 2688-2710,2010.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 5, Issue 3, March 2016**

[8] Hang Su, Student Member, IEEE, and Xi Zhang, r, IEEE, "Battery-Dynamics Driven TDMA MAC Protocols for Wireless Body-Area Monitoring Networks in Healthcare Applications", IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, Vol. 27, No. 4.

[9] Hooi Been Lim, Dirk Baumann, and Er-Ping Li, Fellow, "A Human Body Model for Efficient Numerical Characterization of UWB Signal Propagation in Wireless Body Area Networks", IEEE TRANSACTIONS ON BIOMEDICAL ENGINEERING, Vol.58, No. 3,2011.

[10] Jamshid Abouei, David Brown, Konstantinos N. and Subbarayan Pasupathy, Life Fellow, IEEE,2011 "Energy Efficiency and Reliability in Wireless ,Biomedical Implant Systems" IEEE transactions on information technology in biomedicine, Vol. 15, No. 3,2009.

[11] Matiar M. R., Howlader, Thomas E. Doyle, "Low temperature nanointegration for emerging biomedical applications", ELSEVIER Journal on Microelectronics Reliability, Vol.52, and pp. 361-374,2011.

[12] Msafumi Fujii, Ryo Fujii, Reo Yotsuki, Tuya Wuren,Toshio Takai, and Iwata Sakkagami, Member, IEEE, "Exploration of Whole Human Body and UWB Radiation Interaction by Efficient and Accurate Two-Debye-Pole Tissue Models", IEEE TRANSACTIONS ON ANTENNAS AND PROPAGATION, Vol. 58, No. 2,2010.

[13] Moshaddique Al Ameen and Kyung-sup K wak, Social Issues in Wireless Sensor Networks with Healthcare Perspective", The International Arab Journal of Information Technology, Vol. 8, No. 1,2011.

[14] Phond Phunchongharn, Dusit Niyato, Member, IEEE, Ekram Hossain, Senior Member, IEEE, and Sergio Camorlinga, "An EMI-Aware Prioritized Wireless Access Scheme for e-Health Applications in Hospital Environments" , IEEE TRANSACTIONS ON INFORMATION TECHNOLOGY IN BIOMEDICINE, Vol. 14, No. 5,2010..

[15] Robert W. Day a, 1, Matthew D. Dean b, Robert Garfinkel a, Steven Thompson c, "Improving patient flow in a hospital through dnamic allocation of cardiac diagnostic testing time slots", ELSEVIER Journal on Decision Support Systems, Vol. 49, pp. 463–473,2010.