Volume 4, Issue 11, November 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

# Study on Security Methods, threats in Wireless Body Area Networks

**Shubhangi Sonone, Prof. VishalShrivastava**
Arya college of Engg and Information Jaipur
Rajashthan Technical University, Kota
Rajashthan, India

***Abstract:* As there is more research is going on Wireless Body Area Networks (WBANs) on their QoS and Energy Improvement as every sensor node in WBANs is having some constraints like energy consumption. However another major constraint is security, as this network collecting the important information. Therefore there must have efficient security method in WBAN. In addition to this, in real like applications such as smart home, community monitoring, it is required to transmit and store the data in sensor nodes memories. There are many security schemes already presented by different authors; however because of resource constrained sensor nodes, these methods not efficient for WBANs. The real challenge of such networks is the efficient secure network protocol as well as data access control mechanism. Therefore in this paper we are taking the review of all existing security mechanisms presented for WBANs. Different techniques of authentication, different techniques of data leakage as well as different techniques of access control are presented during this paper. This paper is review paper and base for our future roadmap.***

***Keywords:* WBAN, Data Leakage, Authentication, Access Control Policies, security threats.**

## I. INTRODUCTION

The WBANs is collected of different number of tiny sensor nodes. These sensor nodes are resource constrained. The resource constraint of sensor nodes in WBAN is limited battery power, transmission range, storage memory etc. Therefore all routing protocols used in WBAN should be efficient by considering these constraints of WBAN. There are many routing protocols are designed with aim of improving the energy efficiency of WBAN which means longer life of WBAN. Apart from this resource constraints, the another challenge of WBAN is security method. As WBAN is sharing important information, one needs to have security method which secures the communication and avoid the security threats. This security mechanism is efficiently presenting through the routing protocols. It means that routing protocol should provide the security while achieving the efficiency of energy consumption.

In this paper we are presenting the review of different concepts those are related to routing security in WBAN. During this paper first we are presenting the security issues and challenges in WBAN in section II. The remainder of this paper is organized as follows. Section 2 WBAN &amp; security issues discussed in section 3, we briefly review the authentication mechanisms. "Then the current authentication technologies are available in section 4. Section 5 showing papers.

## II. WBAN SECURITY CHALLENGES

**2.1 Threats/Data Leakage in WBAN:** Following listed are all possible security attacks that happens on WBAN.

- **Spoofed/Replayed/Altered Routing Information:** This type of attacks can create incorrect message routing loop is generated, increasing latency detail from end or minimize source routes, etc.
- **Selective Forwarding:** this consists of the risk that they are not propagated any further ensuring that some messages to forward some malicious nodes may refuse when the malicious node behaves like a black hole and all refuse the message received is the worst case.
- **Sinkhole Attacks:** attacks a patched node through a specific area to all traffic.
- **Sybil Attacks:** That other node for multiple identities presents a single node a Sybil attack.
- **Wormholes:** message this attack can get an opponent and a tunnel through various parts of the reply.
- **HELLO Flood Attacks*:*** in this attack nodes can be convinced by the adversary to believe that the adversary is its nearer neighbor. This can be possible by sending false information with large enough transmission power.
- **Acknowledgement Spoofing*:*** this attack has the goal of convincing the sender that a weak link is strong enough or that a dead node is still alive. That is how the adversary can remove information sending it to these weak links or to these dead nodes. This is possible due to the fact that the adversary can overhear packets addressed to other nodes and can have a general view of all the network knowing which links are weak or which nodes are dead.

### 2.2. Requirements Security in WBANs

- **Authentication.** It is ensuring that sensor nodes, cluster heads and base stations are authenticated before granting a limited resource or revealing information. Authentication ensures a receiver that data, mobile code and control data like a route updates, location information and key management messages originates from the correct source.

- **Authorization**. It ensures that only authorized nodes are involved in a specific activity.
- **Integrity and freshness.** It is ensuring that a message or an entity under consideration is not altered in transit and recent.
- **Availability.** It is ensuring that service offered by whole WBAN, by single section of it or a single sensor node is available whenever required.
- **Non-repudiation.** It prevents malicious nodes to hide their activities.
- **Confidentiality.** It provides privacy for wireless communication channels so that eavesdropping is prevented. Application data, mobile codes, control messages such as route updates, location information and key management traffic should be kept secret.

**2.3. Challenges in WBAN:** WBAN showing far more challenges than wired networks towards design of efficient security solution.

- **Resource Constraints on Sensor Nodes**: Storage, processing, communication and battery life limitations on a sensor node prevent use of costly key management solutions. Energy is the biggest concern because sensor nodes operate on battery and it may not be possible to visit large number of nodes to replace their batteries. The biggest energy consuming operation for a sensor node is the communication. Thus, security solutions with large communication overhead are not feasible.
- **Wireless Nature of Communication:** Communication media is the air where everybody has access to. An adversary can perform variety of active and passive attacks on traffic due to broadcast nature of the communication.
- **Unknown and Dynamic Network Topology:** There is no fixed infrastructure in a distributed WBAN. Although there are resource rich members such as base stations in a hierarchical WBAN, still large amount of sensor nodes are randomly scattered over a target area.
- **Very Large and Dense WBAN:** Most of the proposed sensor applications require hundreds to thousands of nodes densely deployed on a target application area.

## III. REVIEW OF AUTHENTICATION PROCESS IN WBAN

Authentication is ensuring that sensor nodes, cluster heads and base stations are authenticated before granting a limited resource or revealing information. Location information and key management messages originate from the correct source.

**3.1 Procedure of Authentication:** Following are different kinds of authentication procedures.

- **One-way authentication:** Only a single message sent from the sender to the receiver node, message me: will be able to install the sender's identity and that the message was generated by the sender, II: the message is intended for receiver and iii: the message is not modified during transit.
- **Two-way / mutual authentication:** Mutual authentication, also called two-sided certification, a process in which a communications link to each other both institutions certified. Body areas in environments, mutual authentication is not only among General nodes and base station refers to the authentication, it also assures that each other's identity can refer to two counterparts.
- **Three-way authentication:** is an authentication process when the clocks of the nodes cannot be synchronized. A third message from the sender to the receiver is sent.
- **Implicit authentication:** Built-in authentication did not perform as an independent process. Instead, it is a byproduct of other processes, such as setting up the authentication key pattern in wireless body areas operating can reduce complexity and reduce power consumption.

**3.2 Authentication Issues**

- **Issues based on Static Node Deployment:** In this type of deployment nodes are stable and never move. As nodes are easy to find understanding, play such nodes are vulnerable to such attacks. Authentication protocol should respond to these issues.
- **Issues based on Dynamic Node Deployment:** some of the issues in this category are re-authentication of a moving node, un-traceability a node’s movement should be untraceable, message integrity, perfectly, node capture & compromise.

## IV. REVIEW OF AUTHENTICATION TECHNIQUES

In [3], K Han et al, proposed an efficient model for authenticated key agreement in dynamic WBAN and that this protocol enables reduced authentication process for mobile node and can be used in various application of WBAN.

In [4] Vaidya et al, proposed a user authentication scheme in WBAN, which is a variation of strong password based solution proposed.

In [5], Ying et al, proposed an efficient and scalable protocol to establish and update the authentication key between any pair of sensor nodes in dynamic WBAN. The proposed solution is suitable for both static and dynamic environments. The solution has less communication cost and high probability of sharing a key.

In [6] Chuchaisri: Proposed a 2 PKC-based broadcast schemes called the key pool scheme and key chain scheme using bloom filter to aid the node to decide/solve the dilemma when to forward the data first or authenticate first.

In [11], Wong et al, proposed a dynamic user authentication scheme for WBAN. It allows the genuine users to query the sensor data from any of the sensor nodes by imposing very less computational load. This scheme claimed that it is secure against replay and forgery attacks in which it fails.

In [12], Tseng et al, this paper shows that is vulnerable to replay and forgery attacks and proposed an authentication mechanism that retains the advantages of. The scheme possesses the advantage of resistance to the replay attacks and forgery attacks, with reduction in the risk of password leakage.

In [13], Abhram and ramanatha, proposed an authentication and initial shared key establishment model of hierarchical clustered networks.

In [14], Perrig et al, proposed a suite of security protocols called Security Protocols for WBANs (SPINS) optimized for WBANs. SPINS includes two protocols: secure network encryption protocol (SNEP) and μTESLA. SNEP provides unicast authentication, confidentiality, and replay protection through authentication with MAC and encryption. μTESLA offers a solution for broadcast authentication.

In [15], Zhu et al, in this proposed each node generates a one-way key chain and sends the commitment of it to their neighbors. If a node wants to send a message to its neighbors, it attaches the next authorization key from its key chain to the message. The receiving node can verify the validation of the key based on the commitment it has already received. This scheme does not provide a solution for attacks from inside where the adversary knows nodes cluster key.

In [16], Fanatacci et al: proposed a distributed node authentication model that does not require a central authority to authenticate. This model has increased communication and computational overhead as every node shares partial information of others and all nodes involve in the authentication procedure as an authenticator.

In [17], Huang et al, proposed a self organizing algorithm using ECC which has 2 phases 1: Implicit Certificate Generation Process and Hybrid key Establishment Process. Supports dynamic node re-authentication but the author did not state it. Proposed scheme has major problem where each sensor node must have direct contact with the CA which would be a bottleneck.

In [18], Mahagoub: proposed an efficient model that deployed a Partial key escrow table for sinks. Using this table the sink can self generate a shared key for the attached nodes? To support node mobility all the sinks have to maintain this table, which is an overhead.

In [19] Wang et al, proposed the dynamic window scheme using additive increase multiplicative decrease to regulate the window size. The scheme allows switching between the forward- first or authenticating first mode.

In [20], Dong et al, overcomes the shortcoming of which is not effective against the malicious node attack, by establishing a group key with the nodes neighbors and filtering out misbehaving nodes. But this method despite improvements still allows the broadcast of forged messages.

In [21], Ning et al, proposed a weak authentication scheme to filter bogus/false messages using one way key chain. But this approach requires synchronization and periodic broadcasting between the access points and sensor nodes when it is used with signature based authentication.

In [22], Wang et al, PK by using multiple short lived at the time of signature verification public keys in order to reduce the proposed small but requires that all sensor nodes stored in these keys when these keys lifetime expires then sink node periodically broadcasts and public keys redistributes.

In [23], Ren et al, proposed a scheme of multi-user authentication using bloom filter to store multiple user IDs and Public keys. The disadvantage is that the Bloom filter can be forged and cannot prevent the DOS attack.

In [24], T.H.Lee, proposed a password based authentication protocol similar to [11].these algorithms and reduce computational load and have reliable time synchronization but they are weak against user-password security attacks and not mentioned about which MAC algorithm to use.

In [25], T.Yao et al, proposed an authentication protocol for broadcasting messages using one way key chain and secure acknowledgements. But the drawback is there is no sync of time and whole broadcasting would be disrupted with single malicious node because of unknowing key chain.

In [26], Kim et al, proposed the algorithm for detecting and dropping fabricated reports from representative nodes using message authentication nodes. However, this scheme brings to communication overload due to number of MACs which are computed by representative nodes.

In [27], Y.K.Lee et al, The proposed scheme uses pre-shared secret key which is obtained from ECDH key exchange algorithm and is based on modified SHA-1 hash function which helps to compute MAC for given messages. The algorithm provides both integrity and authenticity of the message with only one hash value.

In [28], Ravi et al: proposed a PKC certificate based scheme for user authentication, certificate being generated by the Sink. This scheme is vulnerable to DOS attack.

In [29] Omar et al: proposed a key distribution scheme for dynamic conferences. In this scheme a trusted server distributes private pieces of information to a set of users. Each member of any group of users of a given size can compute a secure group key.

## V. REVIEW OF ACCESS CONTROL METHODS

Most of access control methods presented so far for WBANs concentrates on the authentication step of the access control while ignoring the authorization step. The main algorithm considered for this kind of access control (authentication only) is a cryptographic challenge-response protocol, in which a user and network are mutually authenticated to each other.

Nodes in WBAN &amp; defense against capture the most important yet difficult problems, and node capture attacks provides a solution to propose a structure which is a writers. WBAN &amp; to access control of a certain number (n) is achieved by cooperation of sensor nodes members. Access control the action; Neighboring nodes (n) to authenticate and authorize users who request to participate in the WBAN &amp; Although the proposed solution node is sufficient to deal with attacks from capture, these overhead sensor nodes, which supplies power to deplete rapidly would create communications nodes.

In [7], the energy efficient access control scheme is presented for WBANs based on Elliptic Curve Cryptography (ECC). Authors propose an energy efficient way to use ECC (which is a Public Key Cryptography (PKC) scheme). The proposed scheme has better performance compared to the other PKC based access control schemes and fair performance compared to Secret Key Cryptography (SKC) based ones. On the other hand, the proposed scheme requires the Key Distribution Center to be available all the time, which may not be the case in some situations and may cause users to be rejected by the access controlling nodes of the WBAN.

In [8], three different methods are presented for WBANs. Proposed schemes have the following advantages compared to existing access control schemes: low expenses in calculation and communication, resistance to node capture, query replay and DoS attacks. On the other hand, the proposed schemes are based on SKC algorithms, which is not scalable compared to PKC algorithms. Besides, in the proposed schemes realizing the privilege control of users is not provided.

In [9], the author introduced dynamic user authentication method for WBANs. In the proposed scheme authorized users can access any of the sensor nodes in WBANs using mobile devices, such as PDAs, PCs, etc. The proposed scheme allows legitimate users to query sensor data at any of the sensor nodes in an ad hoc manner. It imposes very little computational load and requires only simple operations.

In [10], Wong et al. Plan that not only fixes the vulnerabilities, but also enhances the security of the proposed revision of the plan for the current proposed scheme against replay and forgery attacks is flexible and it can reduce the risk of password leak from sensor nodes. It users don’t have the ability to change their password. This compared to previous plans for better efficiency. On the other hand, the proposed plan users and does not provide mutual authentication between sensors nodes. Moreover, it is a centralized gateway node registration and password change. Centralized approach could be trouble for body areas; that’s why most of the currently employed networks employ base stations.

In [11], authors propose a distributed user access control under a realistic adversary model in which sensors can be compromised and may collude. Authors propose a practical and scalable certificate-based local authentication based on ECC. PKC eliminates the complicated key management and pre-distribution required by SKC schemes. The proposed scheme is resilient to user collusion attacks. On the other hand, the feasibility of the proposed scheme is questionable. They state that it takes 3.1 seconds to generate a public key and 10.8 seconds to conduct local authentication. These rates are not acceptable in real life, in which a user must be authenticated with system in minimum than a second (actually in milliseconds).

In [1], in authors implement access control based on ECC on TelosB mote test bed. Security of ECC relies on critically of the Elliptic Curve Discrete Logarithm Problem. Authors provide an application for access control which shows that PKC is feasible to secure WBANs. On the other hand, the proposed access control scheme is vulnerable to impersonation attacks. Besides, the performance of the proposed scheme is poor and it is 80 times more expensive than SKC based access control schemes. The proposed scheme achieves user authentication in 10.1 seconds, which is not acceptable in practical real life applications.

In [2], the author presented ECC based access control algorithm in WBAN. The malicious nodes from the very beginning, on the basis of the proposal for an access control protocol for WBANs. Moreover, key also new nodes with your neighbors to help in setting up the shared key. The proposed Protocol and flexible WBANs well against known attacks better computation and communication protocols based on the RSA algorithm compared to performance. On the other hand, sensors in the network are the subject of a heated debate of PKC and it will be for a while. Unless it proves SKC major equipment are will be used for resource obstacle in body areas.

In [3], new access control scheme is presented based on ECC. The proposed scheme is useful in a sense that it provides a solution to the problem of new node admissions to the WBAN which require establishment of keys with the neighboring nodes. On the other hand, the proposed scheme is insecure against replay attacks. Besides it lacks hash chain renewability, causing the WBAN to be non-usable after the usage of the last key in the hash key chain.

## VI. CONCLUSION AND FUTURE WORK

The literature review is presented in this paper over the WBAN, security issues, and challenges. In addition to this we have discussed the authentication process, its different procedures, and different methods presented for providing the efficient authentication techniques for WBAN. The goal of this survey paper is to present the possible future directions in security of WBAN. Finally the different methods are discussed for access control schemes for WBAN. This paper is our future roadmap in security of WBAN. For this future work, new efficient routing protocol should be presented to provide efficient security as well as efficient routing performance under different routing conditions. This proposed work should be based on recent research done.

## REFERENCES

[1] H. Wang, B. Sheng, and Q. Li,”Elliptic curve cryptography-based access control in body areas,” International Journal of Security and Networks, vol. 1, no. 3, pp. 127-137, 2006.

[2] H. Wang, B. Sheng, C. Tan, and Q. Li, ”Comparing symmetric-key and public-key based security schemes in

body areas: A case study of user access control.” The 28th International Conference on distributed Computing Systems, ICDCS’08, 2008, pp. 11-18.

[3] H.F. Huang, ”A novel access control protocol for secure body areas”, Journal of Computer Standards and Interfaces, Elsevier, 2009.

[3] Kyusuk Han Taeshik Shon(2012),” Sensor Authentication in Dynamic Wireless Body area Environments” International Journal of RFID Security and Cryptography (IJRFIDSC), Volume 1, Issues 1/2

[4] Binod Vaidya,Jorge Sa Silva, Joel J P C Rodrigues,”Robust Dynamic User Authentication Scheme For Wireless Body area”, Q2SWinet’09,2009,ACM 978-1-60558-619-9/09/10.

[5] Ying Qiu, Jianying Zhou, Joonsang Back, Javier Lopez,“Authentication and Key Establishment in Dynamic WBAN”, Sensors 2010,3718-3731,DOI:10.3390/s100403718.

[6] Panoat chuchaisri, Richard Newman,”Fast Response PKCBased Broadcast Authentication in Wireless Body areas”, COLLABORATECOM 2010. DOI 10.4108/icst.collaboratecom.2010.55.

[7] X.H. Le, S. Lee, I. Butun, M. Khalid, and R. Sankar, ”An energy efficient access control for body areas based on elliptic curve cryptography,” Journal of Communications and Networks, 2009.

[8] Y. Shen, J. Ma, and Q. Pei, ”An access control scheme in wireless body areas,” in Network and Parallel Computing Workshops, 2007. NPC Workshops. IFIP International Conference on, 2007, pp. 362-367.

[9] K. Wong, Y. Zheng, J. Cao, and S. Wang, ”A dynamic user authentication scheme for wireless body areas.” IEEE International Conference on Body areas, Ubiquitous, and Trustworthy Computing, 2006.

[10] H. Tseng, R. Jan, and W. Yang, ”An improved dynamic user authentication scheme for wireless body areas.” IEEE Global Communications Conference, 2007.

[11] H. Wang and Q. Li, ”Distributed user access control in body areas,” Distributed Computing in Sensor Systems, pp. 305-320.

[12] K H M Wong , Y Zheng, J Cao and S Wang, ”A Dynamic user authentication scheme for WBAN”, in the proceedings of IEEE International Conference on Body areas, Ubiquitious Computing, and Trustworthy Computing(SUTC ’06) vol 1, Jun 2006, pp 244-251

[13] Huei-ru Tseng, Rong-Hong Jan, Wuu Yang,”An Improved Dynamic User Authentication Scheme for WBAN” NSC 94-2219-E-009-005.

[14] Jibi Abraham and K S Ramanatha ,“An Efficient Protocol for Authentication and Initial Shared key Establishment in clustered WBAN”, Proceeding of third International conference on Wireless and optical Communication networks 2006.

[15] Adrian Perrig, Robert Szewczyk,J D Tygar, Victor Wen, David E Culler,”SPINS: Security Protocols For Body areas”, Wireless Networks 8:521-534, September 2002.

[16] Sencun Zhu, Sanjeev Setia and Sushil Jajodia,”LEAP: efficient security mechanisms in large scale distributed networks”, in proceeding of 10th ACM CSS’03.

[17] Kyusuk Han, TaeShiak Shon , Kwangjo Kim,”Efficient Mobile Sensor Authentication in Smarth Home”, IEEE transaction on Consumer electronics,56(2):591-596,2010.

[18] Qiang Huang and Johnas Cukier and Hisashi Kobayashi and Bede Liu and JInyun Zhang,”Fast authenticated key establishment protocols for Self organizing Body areas ”, WBANA ’03.

[19] J Ibriq and I Mahgoub,”A Hierarchial Key Establishment Scheme for WBAN”, Proceedings of 21st AINA’07.

[20] R Wang, W DU and P Ning,”Containing DOS attacks in broadcast authentication in body areas”in MobiHoc ’07.proceedings in the 8th ACM international symposium on mobile and adhoc networking and computing,NY,USA.

[21] Q.Dong, D Liu and P Ning,”Pre-authentication filters: providing DOS resistance for signature based authentication in body areas”,in WiSec 2008, proceedings in the 8th ACM international symposium on mobile and adhoc networking and computing, NY, USA.

[22] P.Ning,A Liu,W.Du,”Mitigating DOS attacks against broadcast authentication in WBAN”, ACM transactions on body areas,vol 4,no 1, jan 2008.

[23] W D Ronghua Wang and X.Liu,”ShortPK:a short term public key scheme for broadcast authentication in WBAN”,ACM trans,Body area,VOL 6,1,p.29,Decemeber 2009.

[24] K.Ren,S Yu,W.Lou and Y Zang,”Multi-User Broadcast Authentication in WBAN”, IEEE Transaction on Vehicular Technology,Vol.PP.No.99,p.1.2009.

[25] Tsern-Huei lee,”Simple Dynamic User Authentication Protocols for WBAN”, Second International conference on sensor technologies and Applications(SENSORCOMM’08),pages 657-660,France 2008.

[26] Taketsugu Yao,Shigeru Fukunaga and Toshihisa Nakai,”Reliable Broadcast authentication in WBAN”,LNCS,vol 4097,pages 271-280,2006.

[27] Byung Hee Kim and Tae Ho Cho,”Efficient Selection Method of Message authentication codes for filtering scheme in WBAN ”, In the proceedings of the 2nd International conference on Ubiquitous information management and communication, Pages 511-514,2008.

[28] Abror Abduvaliev, Sungyoung Lee Young-Koo Lee,”Simple Hash Based Message Authentication Scheme for WBAN”, work supported by IT & RnD program of MKE/KEIT.2009.