*International Journal For Technological Research In Engineering*
*Volume 4, Issue 9, May-2017* *ISSN (Online): 2347 - 4718*

# AUTHENTICATION PROCESS IN BODY AREA NETWORK AND SECURITY OPTIMIZATION THROUGH KEY MANAGEMENT USING GENETIC ALGORITHM IN BODY AREA NETWORK

Pradeep Kumar[1], Anand Sharma[2]
[1,2]Mody University of Science and Technology, Lakshmangarh, Sikar-332311, Rajasthan, India

***Abstract: Body Area Networks (BANs) are key technique for human's life now days. BANS are emerging field in computer science as well as in electronics engineering. Many researches are going on BANs with respect to their applications, implementations and adoptability. As BANs are directly related to wireless sensor networks, there are some constraints like energy consumption, security and interoperability. In BANs the network nodes are collecting the important information; therefore they must have some security methods for the security of data in BAN. If we talk about applications of BANs, there we require transmission and storing of the data in sensor nodes memories. Then we will be using some access methods to retrieve the data for further process. Here the authentication comes under the picture. Authentication is essential for the data to be accessed. In this paper we will be discussing the authentication process for BANs.***

***Keywords: Body Area Networks, BANs Security, Authentication in BANs, Wireless Communication, Sensor Network, Genetic Algorithm***

## I. INTRODUCTION

We describe a Body Area Network (BAN) as a wireless sensor network of heterogeneous/homogeneous computing devices that are wearable. The BANs are a combination of various tiny sensors nodes connected to each other by some communication techniques. This is basically dependent on the feasibility of implantation of tiny biosensors inside the human body that won't create ant problem for the body and that don't impair normal activities. The sensors in the human body will collect the various physiological changes and record the same [1,2,3].There are many application for BANs like medical, entertainment, military, and sports. BANs can be customized and implemented as per the requirement of particular application. It requires an advanced information and communication technology system for controlling the BANs for a wide range of applications. BANs contain three types of devices: sensors, actuators, and a sink.

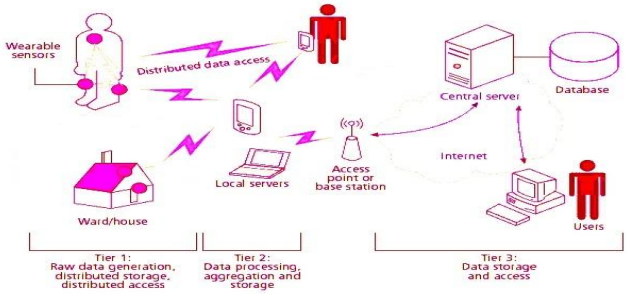


Figure 1. Basic 3 -Tier structure of BANs

In Figure 1, various sensors are implanted atvarious locations on the body that support different network topologies, and forward the sensed data to a device like server (e.g., a Smartphone or a laptop). Unlike wireless sensor networks, BANs have some notable differences with respect to battery availability, wear ability (e.g., size and power), and transmission topology. In addition, the requirement of reliability may be rigorous than in a wireless sensor network. There are three types of communication in BANs

- Unsecured communication: In this type of communication no security mechanism will be there for communication. This is the lowest level of security in which the data is transmitted in unsecure manner.
- Authentication only: This is something better then unsecure communication. In this the data transmitted in secured authentication but is not encrypted. Only the authentication is there but privacy and confidentiality are not supported by this mode.
- Authentication as well as Encryption: It is the best mode of communication. In this we are following authentication and encryption both. That gives us integrity, confidentiality, replay defense and privacy protection.

## II. ISSUES AND REQUIREMENTS FOR SECURITY IN BANS

There are various issues which requires to be considered in the area of BANs, like frequency band selection, energy-efficient hardware, real time connectivity, protocol design, , antenna design, QoS and reliability, MAC protocol design, , over heterogeneous networks, regulatory compliance, and security and privacy. We are going to present only security related issues in this section.

*2.1 Data Confidentiality*

For the prevention of data from leakage it is necessary to keep data confidential at the locations, node itself as well as local server. Confidentiality can be threatened by hardware compromise or the transmission medium threat. The attacker can owe the node or the local server or the path in which the data is traversing. In order to prevent data confidentiality one must have some cryptographic mechanism.

*2.2 Data Integrity*

In BANs the data is important, and its modification would lead to disastrous consequences. Thus there must have some security mechanism for data integrity. In particular, not only we would be able to detect modification of data at end users,

  

but also check and detect that during storage periods, in order to identify that particular modification in advance and accordingly alert the user.

*2.3 Data Freshness*

As per the application of BANs we require updated and latest data for controlling and maintaining. It means that we are using the fresh data and none can replay old messages. Data freshness is of two types: strong freshness, which guarantees data frames ordering as well as delay and weak freshness, which guarantees partial data frames ordering but does not guarantee delay.

*2.4 Availability*

Availability is basically meant for efficient availability of data. The attacker may approach the availability of BAN by disabling or capturing a particular node, which may lead to loss of information. We can protect our system by shifting the operation of a attacked node to a different node in the network.

*2.5 Accountability*

It is required for data access in BAN, especially when a user abuses his/her access privileges, such as giving the key toamalicioususer. To defend against it many techniques are developed. The pirate device is used to decrypt a value that is encrypted under its ID, which will not succeed.

Apart from the security issues, we are presenting the security threats and security requirements for BANs in the Table 1.

Table 1. Security threats and security requirements for BANs

| Security Threats | Security Requirements |
|---|---|
| Data disclosure | Confidentiality and privacy |
| Node capture and compromised node | Resilience to node compromise |
| Data modification | Integrity and authenticity |
| Data Collision/ Exhaustion | Error correcting code |
| Routing attacks | Secure routing |
| Intrusion | Intrusion detection |
| Black holes/De-synchronization | Secure Management |
| Unauthenticated access | Key establishment and trust setup |

## III. NODE DEPLOYMENT IN BANs

Authentication validates the identity of the particular source node. Let us consider a security threat in which, the adversary not only modifying the data packets but also integrates fabricated packets to change a packet stream. The mangers that are controlling the communication must be capable of verifying the original source of data. Message Authentication Code is used for authentication that is mostly computed from the shared secret key. Here in this section we are going to present some issues related to authentication in BANs as per the node deployment.

*3.1 Static Node Deployment*

In static node deployment nodes are static and never move. As nodes are easy to find in this deployment, such nodes are vulnerable to attacks. Authentication protocol should respond to these issues.

*3.2 Dynamic Node Deployment*

In this type of node deployment the nodes are moving and not stable at any particular location. In this there are some issues like message integrity, node capture & compromise, re-authentication of a moving node, and un-traceability of node's movement.

## IV. AUTHENTICATION IN BANs

Authentication is an important security service to prevent false data injection. There are three types of authentication.

*4.1 One-way authentication*

Only a single message will be sent from the sender to the receiver node in this type of authentication. This is going to install the sender's identity and then the message is intended for receiver. The message is not altered during transit is the necessary point.

*4.2 Two-way / mutual authentication*

It is two-sided process in which we will send communications link to each other and both members will be certified. BANs two-way authentication assures that each other's identity can refer to two counterparts.

*4.3 Three-way authentication*

In this authentication process a third party messenger sends a message and both the parties will accept it. It is used when the clocks of the nodes are unable to synchronize.

## V. AUTHENTICATION PROCESSES

Previous related work has shown an approach for securing the communication using biometrics extraction from the data provided by the wireless sensors [4]. A combination of biometrics devices can be used to seed a random number generator. Further this can be used derive keys. It sidesteps the problems as well as provides a kind of proof (the derived key) and thus it becomes a promising solution. Another approach i.e. data-based approach cites that it is impossible to know a priori which the user will be carrying. In this, we make a hypothesis that each sensor will be coupled with an accelerometer. We choose an Accelerometer as per the size, amount and energy unlike some sensors, they can be placed anywhere on the body. Moreover, prior research has shown that we require efficient accelerometers for activity recognition [5], recognizing on-body positions of wearable sensors [6], for authentication[7]. Previous research has proven a technique in which we can detect accurately when two devices are placed at the same position on the body while a user is walking [8]. In [9], Ying et al, described scalable and efficient protocol to establish and update the key for authentication among any pair of sensors in dynamic BAN. The solution is appropriate for static and dynamic environments. The solution has and high probability of sharing a key and the communication cost is very less in it.

In [10], Wong et al, has given a dynamic user authentication scheme for BAN. It imposes less computational load that allows the authenticated users to ask the data from any of the sensor nodes. This scheme is secure against forgery attacks and replay. In [11], Tan et al presented an identity based cryptography approach in BANs for security purpose. In this

  

authors surveyed the various security requirements in a BAN, and proposed the use of the identity based encryption (IBE) scheme, called IBE-Lite. In [12], Tseng et al, presented a mechanism for authentication that is vulnerable to forgery attacks. The proposed mechanism possesses the reduction in the risk of password leakage. In [13], T.Yao et al, proposed a protocol for authentication to broadcast messages using secure acknowledgements and one way key chain. But it have some drawback that because of unknowing key chain the whole broadcasting would be disrupted and there is no sync of time. In [14], Kim et al, have given an algorithm for dropping and detecting fabricated reports using message authentication nodes from representative nodes. But this scheme results in communication overload because of number of MACs. In [15], Ning et al, proposed an authentication scheme which is slightly weak to filter bogus/false messages using one way key chain. But this mechanism needs periodic broadcasting and synchronization between the access points and sensor nodes when it is used with signature based authentication. In [16] Wang et al, authors are using additive increase multiplicative decrease for dynamic window scheme to regulate the size of window. The proposed mechanism permits switching among the authenticating first mode or forward- first. In [17], Huang et al, using ECC for self-organizing algorithm which has 2 phases. That includes Implicit Certificate Generation Process and Hybrid key Establishment Process. Proposed mechanism has some issues where each sensor node need to have direct contact with the Certificate Authority which would be a bottleneck. Halperin et al. [18] using a low-frequency audio channel for Out-of-Band (OOB) Authentication. OOB techniques are using auxiliary channels, like visual, audio, and tactile, which are not included in the established data communication channel. Denning et al. [19] proposed visual OOB authentication. Authors proposed the use of visible tattoos or ultraviolet to record sensor nodes keys. This schemes permits authentication in the emergency, but it may suffer from usability concerns. It will not allow the key revocation. Li et al. [20] proposed a method that requires LED blinking patterns for authentication. In this the user is to visually inspect the LED blinking pattern simultaneous. The usability of this method is not clear yet. It is suitable for emergency scenarios, so its applicability to sensor nodes as wearable devices is limited.

Security optimization through key management using genetic algorithm in body area network:

Genetic algorithm is a randomized search and optimization technique guided by the principle of natural selection systems. Three basic operators used in Genetic [21] algorithms contain: selection, crossover and mutation. The GA goes through the following cycle: Evaluate, select, mate, and mutate until some stopping criteria are reached. Reproduction and crossover together give genetic algorithms most of their searching power.

*A. Selection*

It is quantitative criterion based on fitness value to choose the chromosomes from population which are going to reproduce.

*B. Crossover*

In crossover operation two chromosomes are taken and a new is generated by taking some attributes of first chromosome and the rest from second chromosome.[21]

For example, the strings 11001111 to 01101110 could be crossed over after the third locus in each to produce the two offspring 11001110 to 01101111.

Mutation

Mutation is used to maintain genetic diversity from one generation of population to the next. It is similar to biological mutation. GAs involves string-based modifications to the elements of a candidate solution. These include bit-reversal in bit-string GAs. This operator randomly flips some of the bits in a chromosome. For example, the string 01000100 might be mutated in its second position to yield 00000100.

## VI. PROPOSED METHODOLOGY

In the proposed method GA will be used in key generation process. The crossover and mutation operation is used along with Pseudo random number generators to make the key very complex. For encryption we have proposed AES. Symmetric key algorithm is proposed due to its computation speed and less overhead in key management. The process of generating the key from the Genetic Population has the following steps:

STEP 1: A pseudo random binary sequence is generated on the basis of blood pressure reading of person with the help of sensor of body area network.

STEP 2: The generated string or population is divided in to two halves.

STEP 3: On the selected string crossover operation is performed to achieve good randomness among the key.

STEP 4: After crossover operation the bits of the string are swapped again to permute the bit values.

STEP 5: The same process is iterated two times.

Here the crossover and mutation is done two times to create more complexity and randomness in the key. This key will be then used for encryption process. Here AES will be used for encryption as it is one of the most efficient symmetric key algorithms and its whole security lies in the key used.

## VII. CONCLUSION

The BAN is an emerging technology that will alter people's every day experiences revolutionarily. Privacy and data security in BANs is a significant area, and still there are number of challenges which need to be overcome. In this paper we have surveyed the papers of various authors with respects to authentication in BANs. Through authentication we can ensure that the wireless sensors in a BAN are transmitting data from and to an authenticated user. The research in this field is still in its beginning as of now, but it will draw interest of researches in upcoming years. Hopefully this article will motivate researchers to do research in this domain and develop novel and practical designs of authenticated BANs and Security optimization through key management using genetic algorithm in body area network.

  

REFERENCES

[1] Campbell AT, Eisenman SB, Lane ND, Miluzzo E, Peterson RA, Lu H, Zheng X, Musolesi M, Fodor K, Ahn G. The rise of people-centric sensing. IEEE Internet Comput. 2008; 12(4): 12–21. doi: 10.1109/MIC.2008.90.

[2] Dohler A. Wireless sensor networks: The biggest cross-community design exercise to-date. Recent Patents Comput. Sci. 2008;1:9–25. doi: 10.2174/1874479610801010009.

[3] Latré, Benoît, Bart Braem, Ingrid Moerman, Chris Blondia, and Piet Demeester. "A survey on wireless body area networks," Wireless Networks, vol. 17, 2010, pp. 1-18, doi: 10.1007/s11276-010-0252-4

[4] Sriram Cherukuri, Krishna K. Venkatasubramanian, and Sandeep K. S. Gupta. BioSec: A Biometric Based Approach for Securing Communication in Wireless Networks of Biosensors Implanted in the Human Body. In WiSPr, pages 432–439, 2003.

[5] Ling Bao and Stephen S. Intille. Activity Recognitionfrom User-Annotated Acceleration Data. In Pervasive,pages 1–17, 2004.

[6] Kai Kunze, Paul Lukowicz, Holger Junker, and GerhardTr¨oster. Where am I: Recognizing On-body Positions of Wearable Sensors. In LOCA, pages 264–275, 2005.

[7] Rene Mayrhofer and Hans Gellersen. Shake Well Before Use: Authentication Based on Accelerometer Data. In Pervasive, pages 144–161, 2007.

[8] Jonathan Lester, Blake Hannaford, and Gaetano Borriello."Are You with Me?"–Using Accelerometers to Determine If Two Devices Are Carried by the Same Person. In Pervasive, pages 33–50, 2004.

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

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

[11] Robshaw, M. J. B, "Stream Ciphers", In RSA Laboratories Technical Report TR-701, version 2.0. 1995

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

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

[14] 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.

[15] P.Ning, ALiu, W.Du," Mitigating DOS attacks against broadcast authentication in WBAN", ACM transactions on body areas, vol 4,no 1, jan 2008.

[16] 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

[17] 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.

[18] Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. H. Maisel, "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," in Proc. 29th Annual IEEE Symposium on Security and Privacy (SP 2008), May 2008, pp. 129–142.

[19] T. Denning, A. Borning, B. Friedman, B. T. Gill, T. Kohno, and W. H. Maisel, "Patients, pacemakers, and implantable defibrillators: Human values and security for wireless implantable medical devices," in Proc. SIGCHI Conference on Human Factors in Computing Systems (CHI '10), 2010, pp. 917–926.

[20] M. Li, S. Yu, J. D. Guttman, W. Lou, and K. Ren, "Secure ad hoc trust initialization and key management in wireless body area networks," ACM Trans. Sen. Netw. (TOSN), vol. 9, no. 2, pp. 18:1–18:35, Apr. 2013.

[21] Aarti Soni, Suyash Agrawal," Using Genetic Algorithm for Symmetric key Generation in Image Encryption", ISSN: 2278 – 1323, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 1, Issue 10, December 2012

  