Security in Body Area Network: An Application Perspective

Pradeep Kumar
Research Scholar
CET, MUST, Lakshmangarh
email- pmsuccess81@gmail.com

Anand Sharma
Asst.Prof. CSE
CET, MUST, Lakshmangarh
email- anand_glee@yahoo.co.in

Abstract- Recently, with the rapid development in wearablesmall sensors and wireless communication,body area networks (BANs)have emerged as a key technique that willrevolutionize the way of living.BANs are a type of wireless sensor networks, where agroup of sensors placed on the human body measure specific physiological parameters of aperson and relay it to the monitoring system. There are several applications of BANs for the betterment of human life. Applications of BANs include continuous health monitoring and non medical application. The use of BAN can introduce location independence monitoring systems. BAN application can also be extended to sport training area where athletes or players can be monitored to find their deficiencies or to improve their skills.So far, although there are already severalprototype implementations of BANs, studieson data security and privacy issues are few, andexisting solutions are far from mature. Among the various research issues required to be addressed to implement this technology effectively, security issue is one of the key issues. In this paper we will discuss the security issues as per the applications of BANs.

Keywords: *Body Area Networks; BANs Security; Wireless Communication; Sensor Network*

*****

I. INTRODUCTION

A BAN is a special purpose sensor network fabricated to perform autonomous connection of various sensors and equipments, located inside and outside of human body. A number of intelligent physiological sensors can be integrated into a wearable wireless body area network. This area relies on the feasibility of implanting very small biosensors inside the human body that are comfortable and that don't impair normal activities. The implanted sensors in the human body will collect various physiological changes[1,2,3]. A growing application of wireless sensor network is in body area networks (BAN). Each BAN device is attached to a human body and monitors the state of that body. The emerging BANs have great potential to revolutionize the future of ubiquitous technologies.

The BAN is increasingly looking forward for advanced Information & Communication Technology (ICT) systems to efficiently administer the system for a wide range of applications. A BAN is consisting of number of tiny sensor nodes and a connecting node which connects the external database server or it can connect the sensor node to a range of telecommunication networks. The telecommunication network can be a telephone network, a mobile network or a dedicated local area network. BAN is classified into Off-body, On-body, and In-body communication. Off-body communication is the communication from the base station to the transceiver on a human side. On-body communication is the communication within on-body networks. In-body communication is the communication between invasive or implantable devices and external monitoring equipment.

II. APPLICATIONS of BANs

The major applications are healthcare, control and automation, home and office, environmental monitoring, logistics and transportation, security and surveillance, tourism and leisure, education and training and entertainment. The BAN applications are broadly divided into following categories. Medical applications include collecting various information of a patient and forward it to a monitoring center for further analysis. BAN can also be used to help disable people. Forexample, retina prosthesis chips can be implanted in the human eye to see at an adequate level. Presently BANs are widely used for entertainment purpose, which includes 3D video and Games. Further the BANs are used for sports, in which sensors in BAN can collect coordinates movements of different parts of the body and subsequently make the movement of a character in the game, e.g., moving soccer player or capturing the intensity of a ball in table tennis.Last but not the least miscellaneous applications those include forgotten things monitoring, data file transfer and social networking applications. For better functionality authors discussed about the target system that has a scalable platform that requires minimum human interaction during setup and monitoring [4, 5].

III. SECURITY THREATS in BANs

The security of BANs arethree indispensable components for the systemsecurity of the BAN. By data security, wemean data is securely stored, data can only beaccessed by authorized people and transferred securely.Security issues

are major concern raised by most authors. These include works by authors such as [6, 7].
The implementation of BANs for various applications must satisfy the stringent security requirements. These requirements are based on different applications ranging from medical (blood sugar monitoring) to non-medical (Forgotten things monitoring) applications. In case of medical applications, the security threats may lead a patient to a dangerous condition, and sometimes to a death[8, 9].

A. Threats from device compromise

The sensornodes in a BAN are subjected to compromise,as they are usually easy to capture and not tamper-proof. If a whole piece of data is directlyencrypted and stored in a node along with itsencryption key, the compromise of this node willlead to the disclosure of data.

B. Data access control

Access controlneeds to be enforced for patient-related data inBANs so that private information will not beobtained by unauthorized parties. In the applicationscenario we described one's medical datamay be viewed by doctors, support staff, pharmacies, and other agencies to enhance their services.However, if an insurance company seesone's disease report, it might discriminateagainst one's by offering health insurance at ahigh premium.
Therefore, a fine-grained accesspolicy must be defined to specify and enforcedifferent access privileges for different users.Fine-grained refers to the small granularity ofthe data access policy, which distinguishes amongeach part of the patient-related data and eachuser role. For example, "doctors are only allowedto view the medical data of those patients theyare treating, but not that of other patients," or"personal identifiable information such as patient profile shall not be disclosed to insurancecompanies."

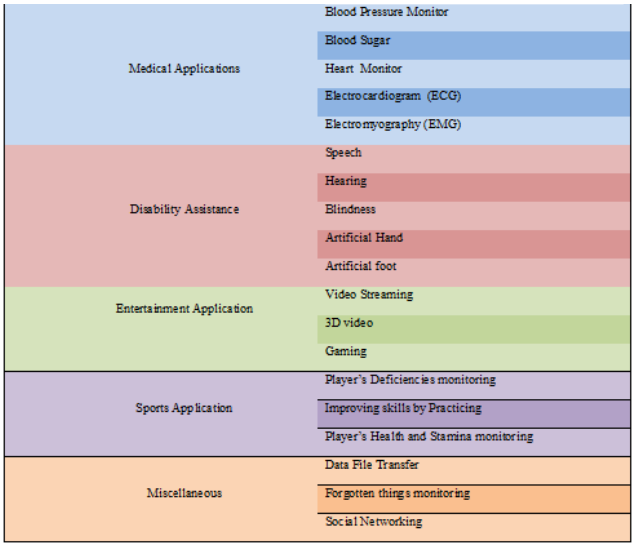

Figure1. BANs Applications

C. Threats from network dynamics

The BAN ishighly dynamic in nature. Due to accidental failureor malicious activities, nodes may join orleave the network frequently. Nodes may die outdue to lack of power. Attackers may easily placefaked sensors in order to masquerade authenticones, and could take away legitimate nodesdeliberately.

IV. SECURITY REQUIREMENTS in BANs

Here in this section we are categorizing the various security requirement from confidentiality to availability of data.

A. Confidentiality

Like WSNs, confidentiality is considered an important issue in BANs. In order to prevent data from leaking during storage periods, thedata needs to always be kept confidential at anode or central server. Data needs to be kept secure from disclosure. Data confidentiality shouldbe resilient to device compromise attacks. Even if the node or server is compromised the attacker should not be able to gain any information.

B. Dynamic integrity assurance

Only keeping the data confidential does not protect it from external modifications. In BANs thedata is vital, and modified datawould misleadto consequences. Anadversary can always alter the data by adding some fragments or by manipulating the data within a packet.Thus,data integrity will be dynamically protected allthe time. By data Integrity we are ensuring that unauthorized changes to the data cannot be made during storage or transmission.
Any malicious changes should bedetected before use and the appropriate persons alerted. Lack of data integrity mechanism is sometimes verydangerous especially in case of life-critical events (when emergency data is altered). Data loss can also occurdue to bad communication environment.In particular, we shall be able to notonly detect modification of data at end users,but also check and detect that during storageperiods, in order to discover potential maliciousmodification in advance and alert the user.

C. Data Freshness

Ensuring confidentiality and integrity is not always enough unless supported by data freshness. The adversary may capture data in a transit and replay them later to confuse the monitoring system. Data freshness ensures that the data is fresh, i.e., the data frames are in order and are not reused. There are two types of data freshness: 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. Weak freshness is required by applications such as Blood Pressure (BP)monitoring, while strong freshness is required during synchronization.

D. Accountability and nonrepudiation:

The origin of a piece of patient-related data cannot be denied by the source that generated it. The sender of a message should not be able to falsely deny later that he/she sent the message, and this fact should beverifiable independently by a thirdpartywithout knowing too much about the content of the disputed message(s).

E. Scalability

As the number of users becomes larger the system should scale without undue latency. Since there are numerous users of data, the distributed access control mechanism should be scalable with the number of users This requires that thecomputational and storage overheads should be controlled. It should not be resource intensive to implement access policies and management overheadshould also be kept under check.

F. Availability

Data availability means that correct data is available to the genuine users. The adversary may target the availability of BAN by capturing or disabling a particular node. Failure to receive correct data may become life threatening. It is also necessary toauthenticate any exchange of data with other machines or humans. One of the best ways is to switch the operation of a node that has been attacked to another node in the network.

V. CHALLENGES OF SECURITY FOR APPLCATIONS

Recently, many security solutions [10, 11] have been designed for BANs, but they cannot be directly employed to ensure the data security. To satisfy the said requirements in BAN, weface several important challenging issues for the applications to be implemented, mostof which arise from efficiency and practicalityaspects. These issues constrain the solutionspace, and need to be considered carefully whendesigning mechanisms for securityin BANs. [10,11]

A. Security v/s Efficiency

Highefficiency is strongly demanded for data security in BANs for the applications. As wearable sensors are extremely tiny and haveinsufficient power supplies, they are inferior in computation and storage capacity.Thus, the cryptographic primitives for security used by thesensor nodes should be as lightweight as possible. Here by lightweight we mean fast computation and lowstorage overhead. Otherwise, the power andstorage space of the nodes could be drainedquickly. In addition, a DoS attack could easily overwhelm the whole BAN if the authenticationprotocol is not fast enough.

B. Security v/s Safety

If we talk about medical application, whetherthe data can be accessed whenever needed couldbe a matter of patients' safety. In this case if we are too strict or tooinflexible in data access control then it may prevent themedical information being accessed in time by legitimate medical staff.The second scenario, in case of emergencywhere the patient may be unconsciousand unable to respond the safety of data is very much essential.

If we talk about other application, aweak access control scheme opens back doors tomalicious attackers. It is hard to ensure strongdata security while allowing flexibleaccess.

In Some applications where there is networkcoverage, stronger user authentication isrequired, it is achieved by contacting an authority; when noinfrastructure exists such as during disasterresponse, weaker or no authentication is adopted.Their approach can be regarded as the firststep towards addressing the conflict betweensecurity and safety.

C. Security v/s usability

TheSensor devices should be easy to use and foolproof,since their operators might be non-expertpatients in case of medical application. The setup and control process of thedata security mechanisms are node related and they involve few and intuitive human interactions.For other applications, to bootstrap initial securecommunication between all the nodes in aBAN for secure data communication, devicepairing techniques are adopted, which is obviously not easyto use. If we ignore the manual steps for usability increment then it will sacrifice security.

D. Device interoperability

Various application installations may use sensor nodes from different manufacturers,among which it is difficult to shareany secure data. It is essential toestablish data security mechanisms that requirethe least common settings and efforts, and workwith a wide range of devices. BAN systems would have to ensure seamless data transfer across standards such as Bluetooth, ZigBee, etc. Ensure efficient migration across networks and offer uninterrupted connectivity.

VI. CONCLUSION

A growing application of wireless sensor network is inbody area networks (BAN). Each BAN device is attachedto a human body and monitors the state of that body.The BAN is an emerging and promising technologythat will change human's experiencesrevolutionarily. Body area networks (BANs) and theirsupporting information infrastructures offer unprecedentedopportunities to deploy the various application without constrainingthe activities of a wearer.Security in BANsis an important area, and there still remaina number of considerable challenges to overcome.The research in this area is still in itsinfancy now, but we believe it will draw an enormousamount of interest in coming years. Wehope this article inspired novel and practicalapplications in which the security is essential.As the population of the world grows, it will become increasinglynecessary to use technology to monitor, diagnose,and treat populations. If we expectBANs to become a solution to monitoring the world'saging population, then it is imperative that we are mindfulof their security. Furthermore, we must also remind ourselvesthat secure solutions should be usable, because the target populationfor these kind of systems is often the elderly.

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] Chen, M., Gonzalez, S., Vasilakos, A., Cao, H., & Leung, V. C. M. "Body Area Networks: A survey," Mobile Networks and Applications, vol. 16, 2011, pp. 171-193, doi: 10.1007/s11036-010- 0260-8.

[5] Oliver, N., and Flores-Mangas, F., HealthGear: a real-time wearable system for monitoring and analyzing physiological signals. International Workshop on Wearable and Implantable Body Sensor Networks, 2006. BSN 2006, pp. 4 pp.-, 3–5 April 2006.

[6] Wolf, L., and Saadaoui, S, Architecture concept of a wireless body area sensor network for health monitoring of elderly people. Consumer Communications and Networking Conference, 2007. CCNC 2007. 4th IEEE , pp.722–726, Jan. 2007

[7] Ming Li et.al "Data security and privacy in wireless body area networks" wireless communication, IEEE(Volume:17, Issue:1), pp 51-58, Feb 2010,doi: 10.1109/MWC.2010.5416350

[8] Kouvatsos D., Min G., and Qureshi B., Performance issues in a secure health monitoring wireless sensor network. In Proceedings of 4th Int. Conference on Performance Modelling and Evaluation of Heterogeneous Networks (HET-NETs'2006), British Computer Society (BCS), IEE, Ilkley, UK, September 11–13, 2006, pp. WP01(1-6).

[9] Dr. Shinyoung Lim et.al "Security Issues on Wireless Body Area Network for Remote Healthcare Monitoring" 2010 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, pages 327-332, IEEE Computer Society Washington, DC, USA

[10] C. Cornelius and D. Kotz, "On Usable Authentication for Wireless Body Area Networks", Proceedings of the 1st USENIX Workshop on Health Security and Privacy, (2010) August 10, Washington DC, USA.

[11] A. F. A. Rahman and R. Ahmad, "Hybrid Method to Measure Vulnerability in Wireless Body Area Network", Proceedings of the 6th International Conference on Sensor Asiasense, August 2013, Malacca, Malaysia.

[12] Daojing He ; Sammy Chan ; Yan Zhang ; Haomiao Yang "Lightweight and Confidential Data Discovery and Dissemination for Wireless Body Area Networks" IEEE Journal of Biomedical and Health Informatics, Volume: 18, Issue: 2, 2014

[13] James Kang, SasanAdibi "A Review of Security Protocols in mHealth Wireless Body Area Networks (WBAN)" Communications in Computer and Information Science, Volume 523, pp 61-83, Springer, 2015

[14] GeethapriyaThamilarasu "iDetect: an intelligent intrusion detection system for wireless body area networks" International Journal of Security and Networks , Volume 11, Issue 1-2, pp. 82–93, Inderscience Publishers, 2016