IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 11, November 2017

REAS - Robust and Efficient Authentication Scheme for Secure Healthcare System in Body Area Network

K. Manjula Devi[1] **K. Brindha MCA, M.Phil.,**[2]

Student, Sri Jayendra Saraswathy Maha Vidyalaya College of Arts and Science, Coimbatore[1]

Assistant Professor, Dept of Computer Science, Sri Jayendra Saraswathy Maha Vidyalaya College of Arts and Science, Coimbatore[2]

Abstract: The Wireless Body Area Network (WBAN) technology is one of the core technologies of developments in healthcare system, where a patient can be monitored using a collection of tiny-powered and lightweight wireless sensor nodes. However, development of this new technology in healthcare applications without considering security makes patient privacy vulnerable. In this article, at first we highlight the major security requirements in BAN based healthcare system. Subsequently, we propose Robust and Efficient Authentication Scheme (REAS) based healthcare system using WBAN - HealthCare, which can efficiently accomplish those requirements. And then we used Lightweight Authentication Protocol for secure data sharing in WBAN. Using secure key management Scheme. WBANs not only bring us conveniences but also bring along the challenge of keeping data's confidentiality and preserving patients' privacy. In the past few years, several authentication schemes for WBANs were proposed to enhance security by protecting patients' identities and by encrypting medical data. However, many of these schemes are not secure enough. First, we review the most recent REAS scheme for WBANs and point out that it is not secure for medical applications by proposing an impersonation attack. After that, we propose a new REAS system for WBANs and prove that it is provably secure. Our detailed analysis results demonstrate that our proposed REAS scheme not only overcomes the security weaknesses in previous schemes but also has the same computation costs at a client side.

Keywords: Wireless Body Area Network, Robust and Efficient Authentication Scheme, Security

I. INTRODUCTION

The different types of networks available today are Wired and Wireless networks. Wired are differentiated from wireless as being wired from point to point. Each of these types of networking has their advantages and disadvantages according to security. Wired networking has different hardware requirements and the range and benefits are different. Wireless networking takes into consideration the range, mobility and the several types of hardware components needed to establish a wireless network. There are different types of configurations of networks and the security measures that need to be taken to ensure a secure network. Organizations rely heavily on the ability to share information throughout the organization in an efficient and productive manner. Computer networks have allowed for this technology and are now a part of almost every business.

An organization has two options when it comes to setting up a network. They can use a completely wired network, which uses networking cable to connect computers, or they can use a wireless network, which uses radio frequencies to connect computer. Wireless networks have allowed organizations to become more therefore organizations are now using a combination of both wired and wireless networks. These networks are generally connected with the help of wires and cables. Generally the cables being used in this type of networks are CAT5 or CAT6 cables. The connection is usually established with the help of physical devices like Switches and Hubs in between to increase the strength of the connection. These networks are usually more efficient, less expensive and much faster than wireless networks.

Once the connection is set there is a very little chance of getting disconnected. Wired networks provide users with plenty of security and the ability to move lots of data very quickly. Wired networks are typically faster than wireless networks, and they can be very affordable. A wired is a common type of wired configuration. Most wired networks use cables to transfer data between connected. In a small wired network, a single may be used to connect all the computers. Larger networks often involve multiple routers or that connect to each other.

In previous, we used a wearable sensor node with solar energy harvesting and Bluetooth Low Energy (BLE) transmission to implement an autonomous WBAN. The solar energy harvester is controlled by an output based Maximum Power Point Tracking (MPPT) technique to extract the maximum power from a flexible solar panel.

DOI 10.17148/IJARCCE.2017.61124

Multiple sensor nodes can be deployed on different positions of the body to measure the subject's body temperature distribution, heartbeat, and detect falls. A web-based smartphone application is also developed for displaying the sensor data and fall notification. To extend the lifetime of the wearable sensor node, a flexible solar energy harvester with an output-based maximum power point tracking technique is used to power the sensor node.

II. RELATED WORKS

BSN-Care: A Secure IoT-based Modern Healthcare System Using Body Sensor Network [1] Advances in information and communication technologies have led to the emergence of Internet of Things (IoT). In the modern health care environment.

Body Sensor Networks: In the Era of Big Data and Beyond [2] Body sensor networks (BSN) have emerged as an active field of research to connect and operate sensors within, on or at close proximity to the human body. BSN have unique roles in health applications, particularly to support real-time decision making and therapeutic treatments.

High-Efficient Energy Harvester with Flexible Solar Panel for a Wearable Sensor Device[3] This paper proposes an optimal energy harvester (OEH) that uses a flexible photovoltaic (FPV) module to prolong battery life for a wearable body sensor node under indoor and outdoor conditions.

Autonomous Wearable System for Vital Signs Measurement With Energy-Harvesting Module [4] the growing demand for wearable devices is imposed by the ability to monitor in real-time critical situations in the different areas of daily life. In many cases, power is the limiting factor for such devices.

A Wearable Energy Harvester Unit using Piezoelectric-Electromagnetic Hybrid Technique [5] Wearable sensor electronics require a sustainable electrical power supply to operate. Energy harvesting techniques can be used to convert available nonelectrical energy sources into electrical energy. This paper presents WE-Harvest system, which is a new wearable energy harvesting system that combines piezoelectric and electromagnetic energy harvesters in one unit to generate a combined electrical energy source.

Autonomous Wearable Sensor Nodes with Flexible Energy Harvesting [6] Distributed wearable wireless sensors are widely employed in wireless body sensor network for various physiological monitoring purposes like health or performance related monitoring applications.

Feasibility of Energy Harvesting Techniques for Wearable Medical Devices [7] Wearable devices is arguably one of the most rapidly growing technologies in the computing and health care industry. These systems provide improved means of monitoring health status of humans in real-time.

In order to cope with continuous sensing and transmission of biological and health status data, it is desirable to move towards energy autonomous systems that can charge batteries using passive, ambient energy.

Smartphone-mediated Body Sensor Network [8] an ever-growing range of wireless sensors for medical monitoring has shown that there is significant interest in monitoring patients in their everyday surroundings.

A Multimedia Healthcare Data Sharing Approach Through Cloud-based Body Area Network [9] Wireless Body Area Network (WBAN), as a dramatic platform for pervasive computing and communication, has been widely applied in healthcare domains. Since the patient-related data in the form of text, image, voice, etc. is significant in the process of healthcare services

supply massive computing A wearable Bluetooth LE sensor for patient monitoring during MRI scans [10] this paper presents a working prototype of a wearable patient monitoring device capable of recording the heart rate, blood oxygen saturation, surface temperature and humidity during an magnetic resonance imaging (MRI) experiment

III. PROPOSED METHODOLOGY

In this article, at first we address the several security requirements in WBAN based modern healthcare system. Then, we propose a secure Robust and Efficient Authentication Scheme (REAS) based healthcare system using WBAN - HealthCare, which can efficiently accomplish those requirements. And then we used Lightweight Authentication Protocol for secure data sharing in WBAN. Using secure key management Scheme. These sensors collect the physiological parameters and forward them to a coordinator called Local Processing Unit (LPU), which can be a portable device such as PDA, smart-phone etc. The body sensor network technology is one of the most imperative technologies used in IoT-based modern healthcare system. It is basically a collection of low-power and lightweight wireless sensor nodes that are used to monitor the human body functions and surrounding environment. Since BSN nodes are used to collect sensitive (life-critical) information and may operate in hostile environments, accordingly, they require strict security mechanisms.

METHODOLOGIES

To achieve mutual authentication property, to achieve anonymity property, to achieve secure localization property, to defeat forgery attacks, to reduce computation overhead. Improved Data delivery ratio compared to previous process, Reduce Delay and Network Traffic, Achieve better life time ratio. When the server receives data of a person from LPU, then it feeds the data into its database and analyzes those data.

DOI 10.17148/IJARCCE.2017.61124

3.1 Data Collection Process

Generally, proposed framework consists of in-body and on-body sensor networks. An in-body sensor network allows communication between invasive/implanted devices and base station. On the other hand, an on-body sensor network allows communication between non-invasive/wearable devices and a coordinator.These sensors collect the physiological parameters and forward them to a coordinator called Local Processing Unit (LPU), which can be a portable device such as PDA, smart-phone etc. The LPU works as a router between the nodes and the central server called server, using the wireless communication mediums such as mobile networks 3G/CDMA/GPRS. Besides, when the LPU detects any abnormalities then it provides immediate alert to the person that wearing the bio-sensors.

3.2 Data Analysis

Where we can see that if the BP rate is less than or equal to 120 then the server does not perform any action. Now, when the BP rate becomes greater than 130, then it informs family members of the person. If the BP rate becomes greater than 145 and there is no one attending the call in family, then the server will contact the local physician. Furthermore, if the BP rate of the person cross 160 and still there is no response from the family member or the local physician then the BSN-Care server will inform an emergency unit of a healthcare center and securely provides the location of the person.Here, the response parameters “FR” (Family Response), “PR” (Physician Response).For example, when the family response parameter “FR: F”, then the server repeatedly call his family members. Once, the family members of the concern person pick-up the call, then the value of the family response parameter (FR) will become true i.e. “FR: T”. Now, if “FR: F” and BP > 130 then the BSN-Care server will call the local physician.

3.3 Routing Scheme

Normally the source can find the route when the data is waiting in buffer without route by using the route request and route reply. In this scheme, we are also going to use same method with different style, such as creating the fake route request. The source will generate fake request with destination address as cooperating neighbor. Source already knows the information, for Frequency no reply. Based on the error message the source node will find another route to destination with secure route discovery model. In this module, we have used the timer to keep the time expire and intimates to generate the periodic packet.

3.4 Enforcement of Security

In our system, when a LPU wants to send the periodical updates to server, then the server needs to confirm the identity of LPU using a lightweight anonymous authentication protocol. In this section we describe our anonymous authentication protocol in details. Our proposed authentication protocol consists of two phases:

In Phase 1, the server issues security credentials to a LPU through secure channel, this phase is called registration phase. The next phase of the proposed authentication protocol is the anonymous authentication phase, where before data transmission from the LPU to server, both the LPU and the server will authenticate each other. This phase achieves goals of mutual authentication among the LPU, and the server by preserving anonymity, and secure localization. This phase consists of the following steps: Finally, the

Phase I: Registration Phase

LPU forms a request message MA1 and then sends it to the server. Here, LAIl is the location area identifier of the base station, which represents the physical connection between the LPU and the base station of a mobile network and it will be used to provide secure localization. Upon receiving the request message from the LPU, the server at first checks the track sequence number is valid or not and simultaneously also computes and checks whether the parameters valid or invalid.

Phase II: Authentication Protocol

This phase achieves goals of mutual authentication among the LPU, and the server by preserving anonymity, and secure localization. Finally, the LPU forms a request message M A1 and then sends it to the BSN-Care server. Here, LAIl is the location area identifier of the base station, which represents the physical connection between the LPU and the base station of a mobile network and it will be used to provide secure localization.

Phase III: Password Renewal Phase

In this scheme, a mobile user can freely change his/her password on the smart card, without any help of the HA. When a mobile user MS wants to renew a password, the MS needs to insert his identity IDM, old password PSWM, and the new password PSW∗ M to the smart card. Thereafter, the smart card will retrieve device.

IV. EXPERIMENTAL RESULT AND DISCUSSION

This research work used ns-2 as the network simulator and conducted numerous simulations to evaluate the REAS performance. All sensor nodes are randomly scattered with a uniform distribution. The location of the sink is randomly determined. This research work evaluates the following main performance metrics:

Throughput ratio is the ratio of the number of report messages the sink receives to the total number of report messages the source node sends.

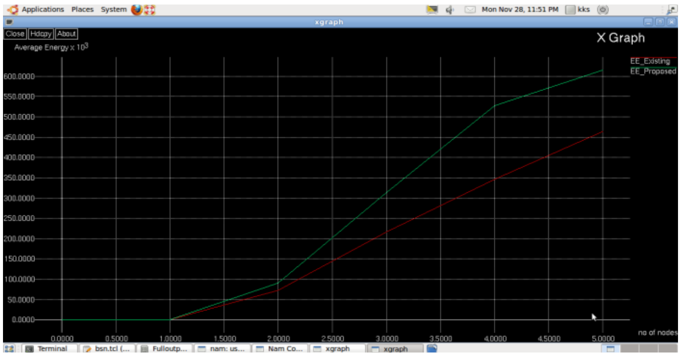
Energy efficiency ratio measures the mean value of the energy of all alive sensor nodes when simulation terminates.

DOI 10.17148/IJARCCE.2017.61124

End-to-end Delay means the time delay experienced by the source node while transmitting a report message to the sink.

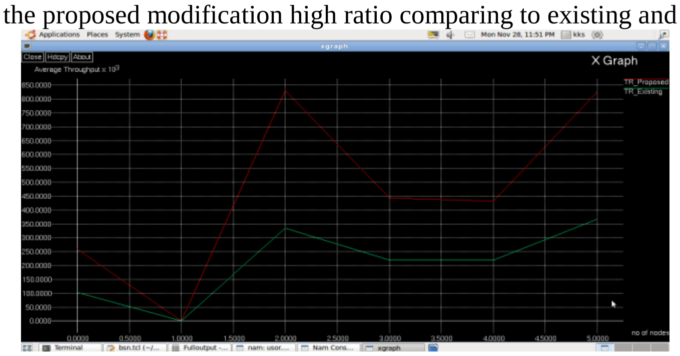
Energy efficiency ratio

Energy efficiency ratio compare the proposed modification life time ratio increased comparing to existing and proposed methods.



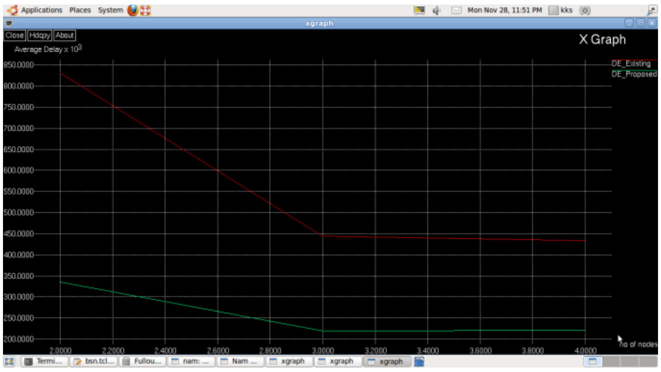
Throughput Ratio

Throughput Ratio, compare the proposed modification high ratio comparing to existing and proposed frameworks



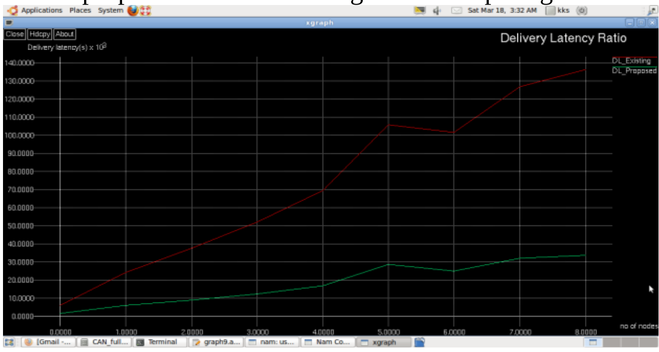
.End-to-End Delay

End-to-End Delay compare the proposed modification low delay ratio comparing to existing frameworks.



Delivery Latency Ratio

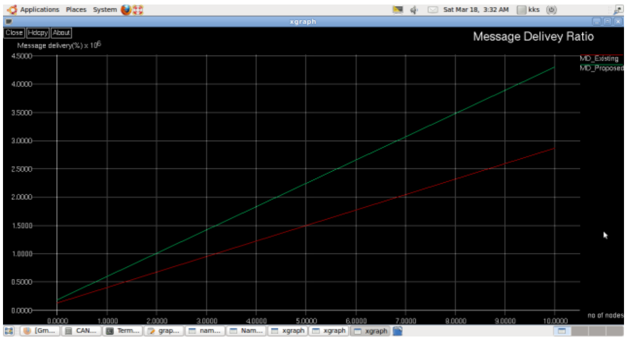
Delivery Latency Ratio compare the proposed modification high ratio comparing to existing frameworks



DOI 10.17148/IJARCCE.2017.61124

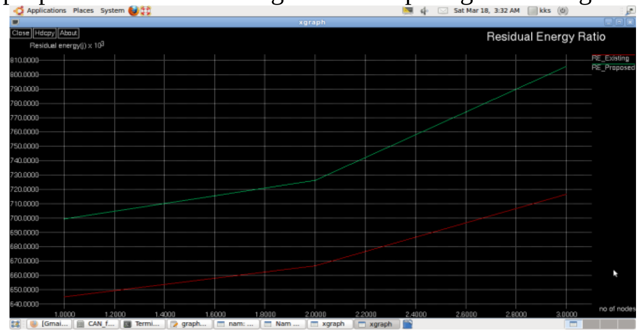
.Message Delivery Ratio

Message Delivery Ratio compare the proposed modification high ratio comparing to existing frameworks.



Residual Energy

Residual Energy compare the proposed modification high ratio comparing to existing frameworks



.

V. CONCLUSION

In conclusion, successfully replicated previous veracity findings and reported data consistent with the deception probability model of deception detection. Message judges were found to be truth-biased and consequently truthful messages were correctly identified as such more often than lies. Truth accuracy was significant above 50% and lie accuracy was significant below 50%. Message veracity base-rate had a substantial, positive, and linear effect on accuracy, observed accuracy levels were within sampling error of predicted values, and accuracy was predicted to within 95% in all nodes. These results suggest that accuracy at detecting deception depends on base-rate. In the future, we intend to consider other identity-related information, such as biometrics, behavior characteristics, and social context. A good example of behavior characteristics is MO, which is often used to identify a criminal in crime investigation.

REFERENCES

[1] C. Lin, P. Wang, H. Song, Y. Zhou, Q. Liu, G. Wu, “A differential privacy protection scheme for sensitive big data in body sensor networks,” 2016, ISSN 0003-4347.

[2] A. Siva Sangari, J. Martin Leo Manickam, “Secure Communication over BSN Using Modified Feather Light Weight Block (MFLB) Cipher Encryption,” Journal of Software, vol. 10, pp. 961, 2015, ISSN 1796217X.

[3] T. Hayajneh, B. Mohd, M. Imran, G. Almashaqbeh, A. Vasilakos. “Secure Authentication for Remote Patient Monitoring with Wireless Medical Sensor Networks,” 2016.

[4] Y. Zhou, B. Yang, W. Zhang, “Provably secure and efficient leakage-resilient certificateless signcryption scheme without bilinear pairing,” vol. 204, no. 5, 2016

.[5] P. Kumar,and H. Lee, “Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey.” Sensors (Basel, Switzerland) 12.1 (2012): pp. 55–91.

[6] D. Malan, T. F. Jones, M. Welsh,S. Moulton, "CodeBlue: An AdHoc Sensor Network Infrastructure for Emergency Medical Care,“ Proceedings of the MobiSys 2004 Workshop on Applications of Mobile Embedded Systems (WAMES 2004); Boston, June 2004.

[7] K. Lorincz, D. J. Malan, T. R. F. Fulford-Jones, A. Nawoj, A. Clavel, V. Shayder, G. Mainland, M. Welsh, "Sensor Networks for Emergency Response: Challenges and Opportunities", Pervas. Comput. vol.3, pp.16–23, 2004.

[8] A. Wood, G. Virone, T. Doan, Q. Cao, L. Selavo, Y. Wu, L. Fang, Z. He , S. Lin, J. Stankovic, "ALARM-NET: Wireless Sensor Networks for Assisted-Living and Residential Monitoring," Department of Computer Science, University of Virginia; Charlottesville, VA, USA: 2006. Technical Report CS-2006-01;

[9] S. Pai, M. Meingast, T. Roosta, S. Bermudez, S. Wicker, D. K. Mulligan , S. Sastry, "Confidentiality in Sensor Networks: Transactional Information," IEEE Security and Privacy Magazine. 2008

[10] J.W.P. Ng, B.P.L Lo, O. Wells, M. Sloman, N. Peters, A. Darzi, C. Toumazou, G. Yang, "Ubiquitous Monitoring Environment for Wearable and Implantable Sensors (UbiMon)," Proceedings of 6th International Conference on Ubiquitous Computing (UbiComp’04); Nottingham, UK. 7–14 September 2004.

BIOGRAPHIES

Manjula Devi K received her M.C.A., degree from Madurai Kamaraj university in 2014. At present she is doing M.Phil in Sri Jayendra saraswathy maha vidyalaya college of arts and science and her area of interest is advanced networking.

K.Brindha M.C.A., M.Phil., working as assistant professor with nine years of experience in the department of computer science, Sri Jayendra saraswathy maha vidyalaya college of arts and science, Coimbatore-5. Her area of interest is advanced networking.

DOI 10.17148/IJARCCE.2017.61124