Volume 5, Issue 1, January 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Survey on Security Issuses in WBAN

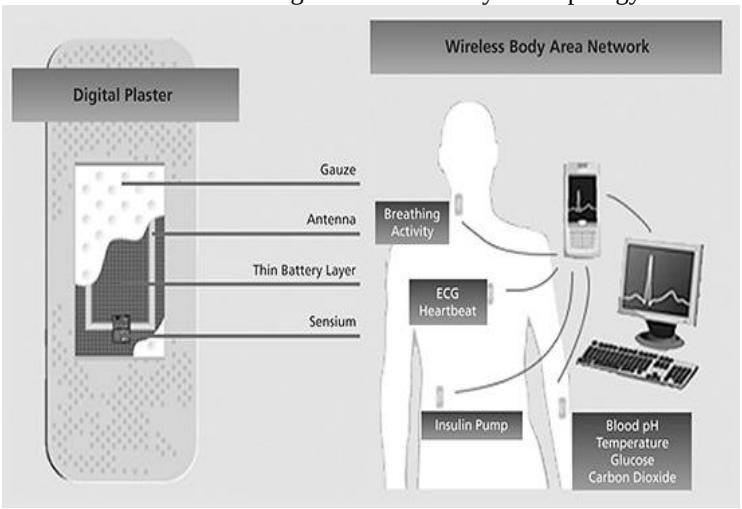
P Usha, N Priya
Assistant Professor, Department of computer science, Dr N.G.P Arts and Science College, Coimbatore, India
M Phil Research scholar, Department of computer science, Dr N.G.P Arts and Science College, Coimbatore, India

Abstract: Wireless Body Area Sensor Network is most challenging and emerging technology for the research due to their vital scope in the field coupled with their low processing power and associated low energy. Today wireless sensor networks are used in various applications like Military and Healthcare etc. Wireless sensor networks are deployed in an open or hostile environment .In this paper we are going to see about different type of attack, mechanisms to prevent the attacks and simulations

Keyword: Wireless Body Area Network (WBAN), Attacks, Security, Security Mechanism, Simulator.

I. INTRODUCTION

Sensor networks have several distinguish features. Wireless sensor network have much number of nodes than a typical ad hoc network. Body Area Network is one of the networks among the different type of networks. It is always desire better coverage and connectivity. Sensor network hardware should be Power-efficient, small, low cost device and flexible. Flexibility sensor network should be able to changes in node density and topology.



Data collection is always related to network connectivity and coverage. Wireless Body network (WBN) of spatially distributed autonomous sensor monitor physical or environment conditions like temperature, sound, pressure etc.They pass their data through the network to a main location. Wireless Body network applications are increasing day by day in our physical world. The wireless sensor networks mostly operate in public and uncontrolled area; hence the security is a major challenge in sensor application.

II. SECURITY REQUIREMENTS IN WBN

1. Confidentiality

During communication, there is a possibility of overhearing and eavesdropping. Encrypting the data with a secret key and sharing the secret key through a secure channel is one of the ways to acquire confidentiality.

2. Self organization

Wireless sensors network are spatial kind of Ad-hoc networks in which every sensor node should be self healing and self organizing. The dynamic nature of WAN makes it sometimes impossible to deploy any preinstalled shared key mechanism among the nodes and the base station.

3. Authentication

This ensures that the communication from one node to another node is genuine, that is, a malicious node cannot masquerade as a trusted network node.

4. Integrity

Integrity is necessary when the data that is transmitted over an insecure channel. Data integrity is attained through data authentication protocols, which ensure that the received data is not changed by the adversary.

5. Secure Location

In WBN each sensor node is required to locate itself in the network accurately and automatically to identify the location of the fault.

6. Freshness

The Data freshness technique is essential to assure data confidentiality and integrity. The adversary may confound the BAN by taking data during transmission and retransmit them later. it checks the arrangement of data frames. Strong freshness and weak freshness are the two types of freshness.

Different Categorized Attack

1. Tampering

Tampering attack is an attack which attacks the physical node in which it contains Cryptographic Keys or other data. The node may also be altered or replaced to create a compromised node which the attacker controls.

2. Jamming

Jamming is a type of attack which interferes the radio frequencies. An attacker sends some radio waves at a same frequency that it is used by wireless sensor network.[image]

3. Collisions

A collision results when two nodes trying to send data on same frequency. When packets collide, a change will likely occur in the data portion, causing a checksum mismatch at the receiving end. Then the packet will discarded as invalid. An adversary may strategically cause collisions in specific packets such as ACK control messages. A possible result of such collision is the costly exponential back-off.

4. Spoofed

An attacker may spoof, alter, or replay routing information in order to disrupt traffic in the network. These disruptions include the creation of routing loops, attracting or repelling network traffic from select nodes, extending and shortening source routes, generating fake error messages, partitioning the network, and increasing end-to-end latency.

5. Sybil attack

In this, attacker gets illegally multiple identities on one node. Because of this, the attacker mostly affects the routing mechanism.sybil attacks are generally prevented by validation techniques.

6. Hello floods attack

This is one of the simplest attacks in WSN in which attacker broadcasts HELLO packets with high transmission power to sender or receiver. By this attack congestion occurs in the network. This is a specific type of DOS.Blocking techniques are used to prevent HELLO Flood attacks.

7. Flooding

An attacker may repeatedly make new connection requests until the resources required by each connection are exhausted or reach a maximum limit. In either case further legitimate requests will be ignored.

III. SECURITY MECHANISMS

1. Shared keys

Key exchange like Diffie- Hellman, does not provide authentication, and is thus vulnerable to Man-in-the-middle attacks. These methods generally mathematically bind the agreed key to other agreed-upon data, such public/private key pairs shared secret key, password.

2. Encryption

Encryption is to provide confidentiality, authentication, integrity protection.Digital signatures Checksum/Hash algorithm are used to provide authentication, integrity protection and repudiation.

3. Secure data aggregation

Two main security challenges in secure data aggregation are confidentiality and integrity of data. While traditionally encryption is used to provide end to end confidentiality in wireless sensor network. The aggregators in secure data aggregation scenario need to decrypt the encrypted data to perform aggregation.

4. SPINS [Security protocols for sensor networks]

SPIN offers many security properties like semantric security, Data authentication, Replay protection, Data freshness, and Low communication overhead. It is optimized for resource constrained and wireless communication. SPIN which a three-part approach is providing an authentication routing protocol as well as a two-party data authentication, data confidentiality and freshness.

5. Tinysec

Efficiency-minimum communication, computation and memory overhead.TinySec supports two special security options: authenticated encryption [Tinysec-AE] and authentication only [TinySec-Auth].Tinysec-AE [authenticated encryption]-encrypt the payload and compute the MAC over the packet header and encrypted data.Tinysec-Auth [Authentication only]-Authenticated the entire packet with a MAC, but the data is not encrypted.

6. Defending Against Attacks on Routing Protocol

To prevent attacks like sinkhole, wormhole and Sybil attacks, Tanachaiwiwat, et al. presents a novel technique named TRANS [Trust Routing for Location Aware sensor Network].This TRANS routing protocol is designed for use in data centric network.

7. Defending Against DOS Attacks

One strategy in defending against the classic jamming attacks to identify the jammed part of the sensor network and effectively route around the unavailable portion. To overcome the transport layer flooding denial of service attack server.

IV. SIMULATOR

WSNs Simulation is important for WSNs development. WSNs Simulator is a time running real experiment which is always time consuming. There are two key aspects in WSNs Simulation. [1] The Correctness of the Simulation Model, [2] The suitability of a particular tool to implement the Model.

1. NS-2 [Network Simulator Version 2]

NS-2 is supported by Defense Advanced Research Project Agency and National Science foundation.NS-2 is built in Object Oriented extension of Tool Command Language and C++. Network Simulator Version 2 can support a considerable range of protocols in all layers. It is an Open Source Model that saves the cost of simulation, and online documents and also it allow the user to modify easily and to improve the codes.

2. EmStar

Emstar is an emulator specifically designed for WSN and it is built in C. EmStar is a trace – driven emulator running in real-time. Modular programming mode in EmStar allows the users to run each module separately without sacrificing the reusability of the software. EmStar has a robustness feature that it can mitigate faults among the sensors, and evaluate much easier. There is a flexible environment in EmStar in which the users can freely change between deployment and simulation. EmStar can only run in real time simulation; moreover this emulator can only apply in iPAQ – class sensor nodes and MICA@ motes.

3. J- Sim

J-Sim is a discrete event network simulation and it is built in Java. This simulator provides GUI library, which facilities users to model or compile the mathematical modeling language ,that is a "text-based language " written to J-Sim models-Sim provides open source models and online documents .J-Sim is commonly used in physiology and biomedicine area ,but it also can be used in WSN Simulation. Models in J-Sim have good reusability and interchangeability, which facilities easily simulation-Sim contains large number of protocols; this simulator can also support data diffusion, routings and localization simulation in WSNs.

4. TOSSIM

TOSSIM is a bit –level discrete event network emulator and built in python, high-level programming Language emphasizing code readability, and C++.TOSSIM also provides open sources and online documents, it save the cost.

Also TOSSIM has a GULI, Tiny viz, which is very convenience for the user to interact with electronic devices because it provides images, instead of the text commands.TOSSIM is a very simple but powerful emulator for WSN.each node can be evaluated under perfect transmission condition.

5. Avrora

Avrora is built in Java. It is and also similar to ATEMU, Avrora is also an simulator which has AVR-based micro controller MICA2 sensor nodes. Avrora also supports energy consumption simulation. This simulator also provides open sources and online documents. The code in Avrora runs to as instruction by instruction, which provides faster speed and better scalability. Avrora can support thousands of nodes simulation, and can save much more execution time with approximate accuracy.

6. OMNeT++

OMNeT++ is built In C++. This Simulator support module programming model. Users can run OMNeT++ simulator on Linux operating system, Unix- like system and windows. OMNeT++ is a popular non-specific network simulator, which can be used in both wire and wireless area. OMNeT++ Provides a powerful GUI. This strong GUI makes the tracing and debugging process much easier than using other simulators. This simulator can support MAC protocols as well as some localized protocols in WSN.

7. ATEMU

ATEMU is built in c, AVR is a single chip commonly used in the MICA platform.ATEMU provides GUI,xatdb; people can use this GUI to run codes on sensor node, debug codes and monitor program executions.ATEMU can simulate multiple sensor nodes at the same time and each sensor node can run in different program. ATEMU has a large library for a wide range of hard devices.

V. CONCLUSION

Wireless sensor Networks often operate in a resource constrained environment. Ensuring security in a hostile operational environment of WBAN is a hurricane task. The idea of this paper is to provide comprehensive information on type of attacks WBAN is exposed to and possible methods of countering such attacks effectively .The motto here is to help my research work on security challenges in Wireless Body Area Sensor Network. Then we have seen many type of simulation I choose the simulator which provides faster speed and better scalability simulator in my research work

REFERENCES

[1] Dr.Shinyoung Lim.; Dr.Tac Hwan Oh.; Dr.YoungB.Choi.; security Issue on Wireless Body Area Network for Remote Healthcare Monitoring,2010 IEEE International Conference on Sensor Network,Ubiquitous,and

Trustworthy Computing,2010 IEEE International Conference on Sensor Network,Ubiquitous,and Trustworthy Computing.

[2] A.Banerjee.; K. Venkatasubramanian.; S.K.S.Gupta; Challenges of implementing Cyber-physical security solution in body area networks, presented at the 4th Int.conf.Body Area Netw.; Los Angeles, CA, Apr.2009.

[3] Fei hu; Sunil Kumar.; Yang Xiao; towards a secure RFID/Sensor based Tele cardiology system, 2007 IEEE.

[4] Pooja, M.and D.y.Singh, 2013.security Issues and Sybil Attack in wireless Sensor Network. International Journal of P2p Network Trends and Technology, 3(1):7-13.

[5] Kalita.h.k.and A.kar, 2009.Wireless sensor network security analysis. International Journal of Next-Generation Network (IJNGN), 1(1):1-10.

[6] Giruka, V.C., et al., 2008.Security in wireless sensor networks. Wireless communications and mobile computing, 8(1): 1-24.

[7] Frank Stajano.Security for Ubiquitous Compuing.John Wiley and Sons, February 2002.

[8] Chris Karlof and David Wagner, Secure routing in wireless sensor network: Attacks and countermeasures. Elsevier's Ad Hoc Networks Journal, Special Issues on Sensor Network Application and Protocols, 1(2-3):293-315, May 2003.

[9] Zaw Tun and Aung Htein maw,(2008),"Worm hole Attacks Detection in wireless Sensor network", proceedings of world Academy of Science, Engineering and Technology Volume 36,December 2008,ISSN 2070-3740.

[10] A.D.wood and J.A.Stankovic,(2002) Denial of Service in Sensor Network," Computer, vol.35.no.10,2002,pp, 54-62.

BIOGRAPHY

Mrs. P. Usha, working as a Assistant professor, Department of Computer Science, Dr N.G.P Arts and Science College, Coimbatore, India

Miss.N.priya Pursuing M Phil Resource Scholar, Department of Computer Science, Dr N.G.P Arts and Science College, Coimbatore, India

